AVG Antivírus 7.0 Windows változat

Használati utasítás

1.0 változat

A dokumentációt a **FOOLY Stúdió** az AVG Anti-vírus hivatalos magyarországi forgalmazója készítette.

http://www.avg.hu/

A dokumentumot készítette:

FOOLY Stúdió © 2004
az AVG Anti-virus hivatalos magyarországi forgalmazója

A dokumentum, csak elektronikus formában került kiadásra.

Értékesítés: sales@avg.hu
Terméktámogatás: support@avg.hu

Honlap: http://www.avg.hu/

Telefon: +36 20 9825-380
Fax: +36 20 9895-241

Adószám: 61457786-2-24

A dokumentumban előforduló védjegyek:

- Microsoft és Windows… szavak a Microsoft Corporation bejegyzett védjegyei
- AVG és Grisoft szavak a Grisoft s.r.o. bejegyzett védjegyei

Tartalomjegyzék

Bevezetés

Köszönjük, hogy az Ön által választott termék használatba vétele előtt elolvassa ezt a leírást! Ennek dokumentációnak a célja, hogy általános ismertetőt adjon az AVG Anti-vírus funkcióiról és megismertesse Önt a termékben felhasznált technológiákkal, víruskeresési módszerekkel. A következő fejezetben megtudhatja, hogy hogyan kell telepíteni ezt a terméket, valamint megismerteti Önt a program alapvető kezelésével és magával kezelő felülettel. Ügyfeleink nagy megelégedésére a legfontosabb és leggyakrabban használt funkciókat (alapvető ellenőrzési és frissítési funkciók) összegyűjtöttük és egy alapszintű (Basic) kezelőfelületbe integráltuk, ahonnan mélyebb számítástechnikai- szakmai ismeretek nélkül is kiaknázhatók a termék képességei.

Természetesen amennyiben Ön ennél mélyrehatóbb ismeretekre kíván szert tenni, akkor az alapszintű ismertetést követő fejezetekben ezekre a kérdéseire is választ fog találni.

Szeretnénk felhívni a figyelmét arra, hogy tökéletes védelem, akár csak tökéletes vírus nem létezik. Egy számítógépes rendszerben alkalmazott védelem szintje mindig egy kompromisszumon alapul. A biztonsági szintet lehet fokozni, ezzel a kockázat csökkenthető, de nem küszöbölhető ki teljes mértékben.

Jelen dokumentáció elkészítése során mindent elkövettünk, hogy abban a lehető legpontosabb információkat tegyük közzé. Az itt javasolt beállítások és a használati ötletek az átlagos felhasználás igényeit vették alapul, és nem jelentenek garanciát arra, hogy ezek a beállítások minden környezetben optimálisak és minden felhasználó igényeit maradéktalanul kielégítik. Egy adott környezetre a legjobb beállítások mindig annak számítógépes rendszernek a mélyreható ismeretében készíthetők el, amelyben az AVG Anti-vírus programot alkalmazni fogják.

Mi az Anti-vírus programok feladata?

Megelőzés – Optimális esetben az Anti-vírus programok megakadályozzák, hogy a számítógépes vírusok bejussanak az Ön számítógépre. A mai vírusok jellemzően háromféle módon terjednek: elektronikus levelekben, hálózatokon megosztott lemezterületeken, valamint weboldalakról a gyanútlan felhasználók által letölthető formában. A számítógép-hálózatok és hálózati alkalmazások elterjedésével a korábban jellemző, hajlékony és CD-ROM lemezeken keresztüli fertőzés mára szinte teljesen megszűnt, de előfordulásával mindenképpen számolni kell és nem hagyhatjuk ki ezeknek az adathordozóknak az ellenőrzését sem. Ma egy felhasználói számítógépen az egyik legfontosabb tehát **a levelező program védelme**, és legalább ugyanilyen fontos, hogy minden állomány a megnyitáskor, lemezre mentéskor és futtatáskor ellenőrizzünk. Ez utóbbi funkciót az állandóan éberen őrködő **Resident Shield** állandó védelmi rendszer látja el.

Ellenőrzés amikor kéri. Komoly veszélyforrást jelentenek azok a vírusok, amelyek az AVG Anti-vírus telepítése előtt kerülhettek az Ön számítógépére. Emiatt az AVG Anti-vírus lehetővé teszi, hogy Ön tetszőleges időpontokban ellenőrizhesse számítógépe vírusmentességét. Ezt a feladatot akár **automatizálhatja is.** Használhatja az **előre elkészített** vagy az **Ön által beállított, testre szabott** keresési szabályokat,

amelyeket akár **kézzel**, akár pedig automatikusan, **meghatározott időpontokban** indíthat el.

A vírusok eltávolítása. Ez a megállapítás nem mindig helytálló. A vírusok egy része olyan, amelyektől a fertőzött fájl nem tisztítható (**heal**) meg. Ilyenek azok a vírusok, amelyek nem csak társulnak egy fájlhoz (mint például a makró jelentős része, ezektől a fájlok megtisztíthatók), hanem lecserélik az adatállomány tartalmát saját magukra, így az állomány eredeti tartalma már nem állítható helyre. Ebben az esetben az érintett állományokat törölni kell, vagy választhatjuk azok karanténba (**virus vault**) mozgatását. A törölt vagy karanténba helyezett állományok nem képesek újabb fertőzést okozni.
Vannak továbbá olyan vírusok is, amelyek olyan rendszerterületeket támadnak meg, amelyek akadályozzák a víruskereső program működését. Ezekhez vírusokhoz rendszeresen eltávolító programokat adunk közre. Az ilyen vírusoknál szüksége lehet a fertőzött rendszer telepítő lemezeire is, hogy a vírus által felülírt program állományok eredeti állapota helyreállítható legyen.

Nem győzzük hangsúlyozni, hogy a hatékony védelem érdekében **mindig tartsa AVG Anti-vírus programját naprakészen (update)** [http://www.avg.hu/] és természetesen rendszeressen telepítse számítógépe **operációs rendszerének javító csomagjait** [http://windowsupdate.microsoft.com/].

Észlelési módszerek és védelmi szintek

- **Keresés (Scanning)** vírusokra jellemző adatsor keresése az állományokban vírusminták segítségével.
- **Részletes keresés (Heuristic analysis).** Nagy hatékonyságú és erőforrás igényesebb eljárás. A keresés úgy zajlik, hogy az AVG Anti-vírus egy „virtulális számítógépet” létrehozva megfigyeli, hogy tesztelt fájl a futtatáskor milyen műveleteket hajt végre, illetve, hogy ezek a műveletek veszélyesek lehetnek-e a számítógép működésére. Ez a megoldás lehetőséget nyújt arra is, hogy eddig ismeretlen vagy módosított vírusok ellen is megvédhesse számítógépét. Természetesen ez az ellenőrzés sem nyújt tökéletes védelmet, hiszen bármikor megjelenhetnek új viselkedési módot mutató, alattomosabb számítógépes vírusok.
- **Általános észlelés (Generic detetction).** Szintén a vírusokra jellemző műveletek után kutat. Megfigyeli, hogy behatolásra jellemző módszert alkalmaz-e az ellenőrzés alatt álló állomány. Vírusok, vírus csoportok/családok (haszonló viselkedésű) jelenléte azonosítható.
- **Sértetlenség vizsgálat (Integrity check).** Követi az állományok változásait. Használatával az ellenőrzés folyamata felgyorsítható, hiszen az ép (a legutóbbi ellenőrzés óta **tartalmilag** nem módosult) állományokat nem ellenőrzi.

Ez itt csak az alkalmazható eljárások felsorolása volt és egyenként nem feltétlenül nyújtják a megfelelő eredményt. A kívánt hatékonyság eléréshez az AVG a különböző módszereket kombináltan alkalmazza, illetve lehetőséget nyújt az Ön számára, hogy az alkalmazandó keresési eljárásokat (akár többet is) kiválaszthassa.

Az olyan víruskereső program, amely csak egy bizonyos terület figyelésére képes, az gyakran nem képes a támadók ellen megfelelő védelmet nyújtani. Az AVG Anti-vírus többszintű védelmet nyújt az elektronikus levelezés ellenőrzésén keresztül a számítógépen tárolt adat és programállományok ellenőrzéséig.

- **AVG Elektronikus levelezés ellenőrző (AVG E-Mail Scanner).** Ellenőrzi a fogadott és küldött elektronikus leveleket. Néhány elterjedtebb levelező programhoz (ahol erre lehetőség van) speciális kiegészítő modul is készült, de az AVG **bármilyen** SMTP és POP3 képességű levelező programmal képes együttműködni, ezzel egyedülálló illeszthetőséget biztosítva. Az ilyen módon felállított védelmi rendszer a felhasználó igényétől (beállításaitól) függően kiterjedhet a fogadott és küldött elektronikus levelekre egyaránt. Az elektronikus levelekben talált vírusok automatikusan karanténba kerülnek. Azt, hogy a levelek valóban átestek-e vírusellenőrzésen ellenőrizheti, ha bekapcsolja az elektronikus levelek hitelesítése (**certify incoming/outgoing e-mail**) funkciót az AVG-ben.
- **AVG Állandó védelem (Resident Shield).** Ellenőrzi a fájlokat másoláskor, megnyitáskor és mentéskor. Amikor az **Állandó védelem** érzékeli, hogy egy fájlhoz hozzá szeretnének férni, és azonnal ellenőrzi, hogy az adott fájl tartalmaz-e vírust. Amennyiben igen, úgy a folyamatban lévő műveletet megszakítja, és nem engedi a vírust aktiválódni. Az Állandó védelem a számítógép indulásakor töltődik be, és hatékonyan védi a számítógép rendszerterületeit is.
- **Ellenőrzések (Test).** Amikor azt igényli. Ön használhat előre beállított ellenőrzéseket, vagy létrehozhatja saját beállításait is, amelyek esetleg jobban megfelelnek az Ön számítógépes környezetéhez. Itt minden lényeges jellemzőt, keresési módszert, az ellenőrizendő meghajtókat, könyvtárakat, stb. szabadon választhat meg. Az ellenőrzéseket futtatja kívánsága szerinte kézzel indítva vagy előre meghatározott időpontokban automatikusan (a számítógép bekapcsolt állapota mellett).

Telepítés és az első indítás

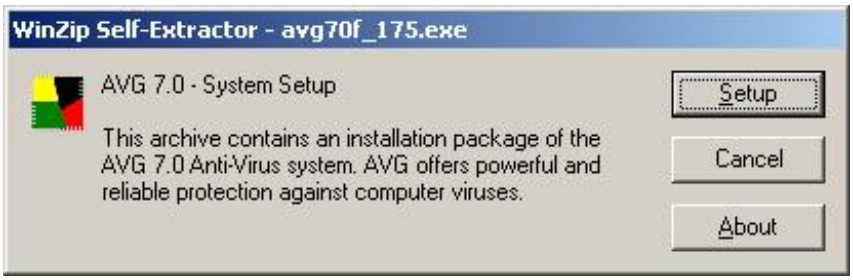
Előkészítés
A telepítés megkezdése előtt győződjön meg róla, hogy az összes, a telepítéshez szükséges információ (telepítő készlet és a regisztrációs / licenc kulcs) a birtokában van-e. Javasoljuk, hogy amennyiben a regisztrációs kulcsa elektronikus formában (fájlban vagy elektronikus levélben) a rendelkezésére áll, úgy a telepítés során a regisztrációs kulcs megadásánál használja a „Másolás” „Beillesztés” funkciókat. Győződjön meg arról, hogy egyéb vírusellenőrző program fut-e a számítógépen. Ha igen, akkor azt az AVG Anti-vírus telepítése előtt el kell távolítani.
Megkönnyíti a telepítést, ha ismeri, hogy milyen levelező programot használ. Néhány levelező alkalmazáshoz az AVG kiegészítő modult (plugin) telepít. Ilyenek programok például az Outlook98/2000 (nem Outlook Express!, ezt később ismertetjük), az Exchange ügyfélprogram, az Eudora, a The Bat!. A használt levelezőprogram ismeretével időt takaríthat meg a telepítés során.

Más levelező programok, amelyek POP3 és SMTP alapon működnek az AVG EMS modulját használják, amely az AVG Anti-vírus általánosan használt megoldása. Amennyiben Ön Outlook Express levelező programot használ, úgy beállításait elkészítheti AVG EMS Varázsló (AVG EMS Wizard for Outlook Express) segítségével. Ugyanezt a varázslót használhatja néhány más levelező program beállításához is. A részletekért kérjük, hogy olvassa el a „Személyes E-mail ellenőrző" fejezetet!

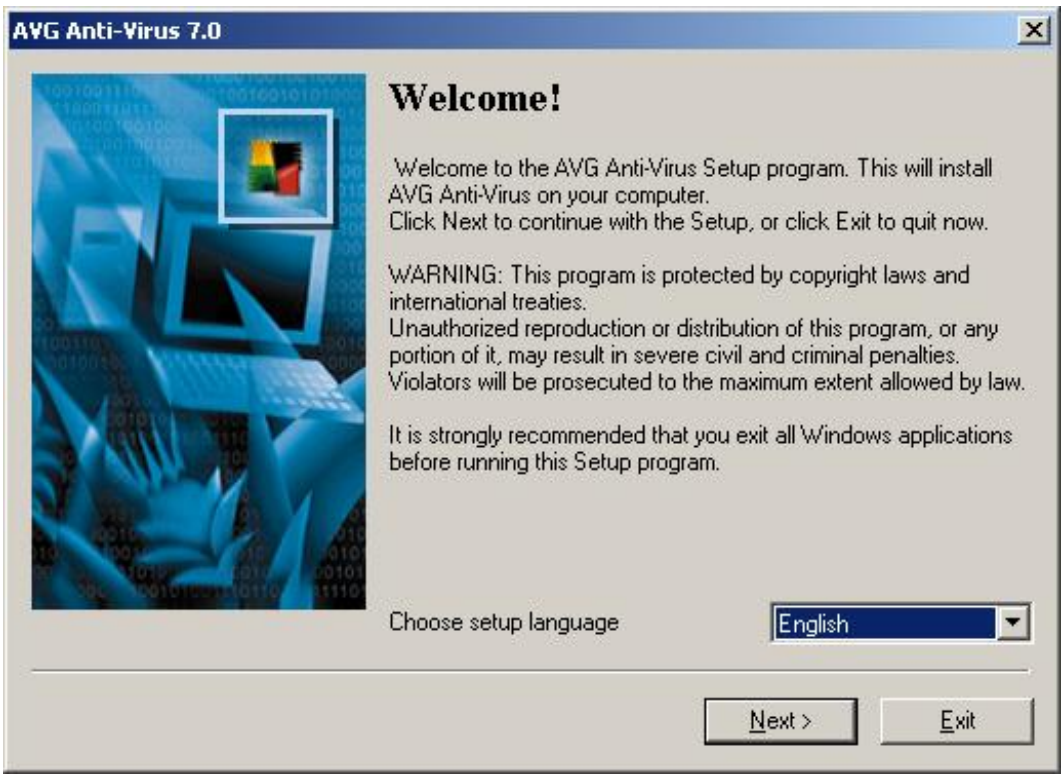
Windows95 felhasználók esetében a telepítéshez szüksége lehet a Microsoft DCOM komponensre. Amennyiben ezt korábban nem telepítette, úgy kérjük, hogy töltse le a Microsoft honlapjáról:
http://www.microsoft.com/com/dcom/dcom95/download.asp

Az AVG Anti-vírus telepítése

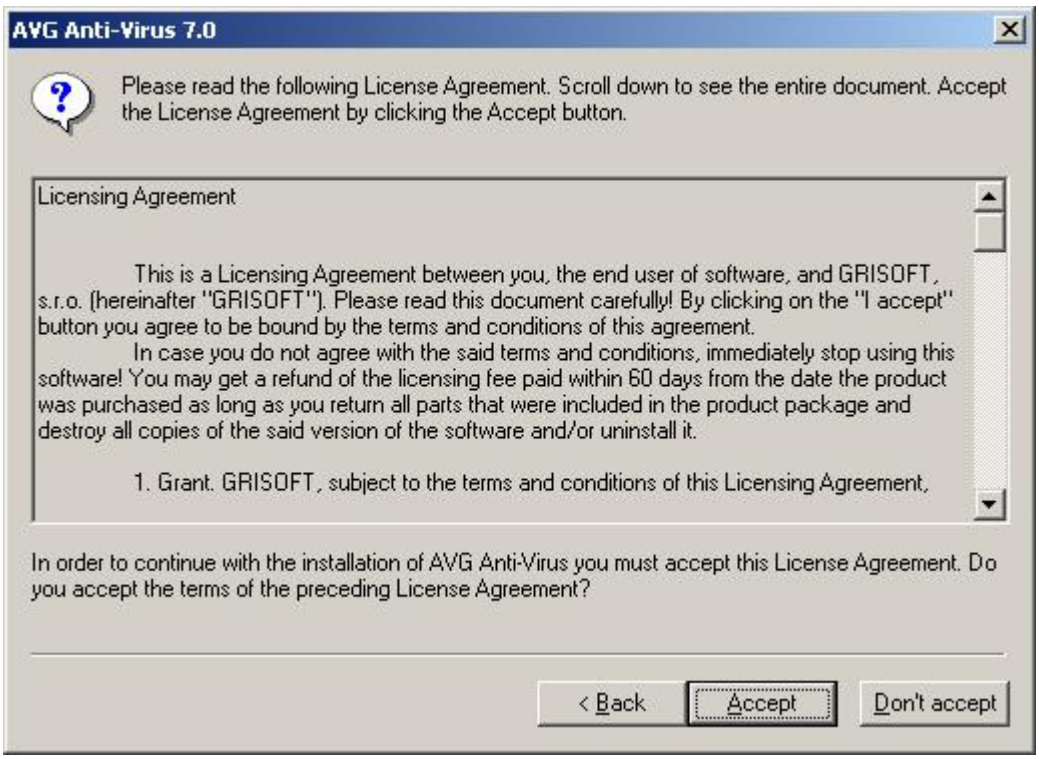
Az AVG Anti-vírus telepítését egy varázsló vezeti végig. Ennek lépései a következők:



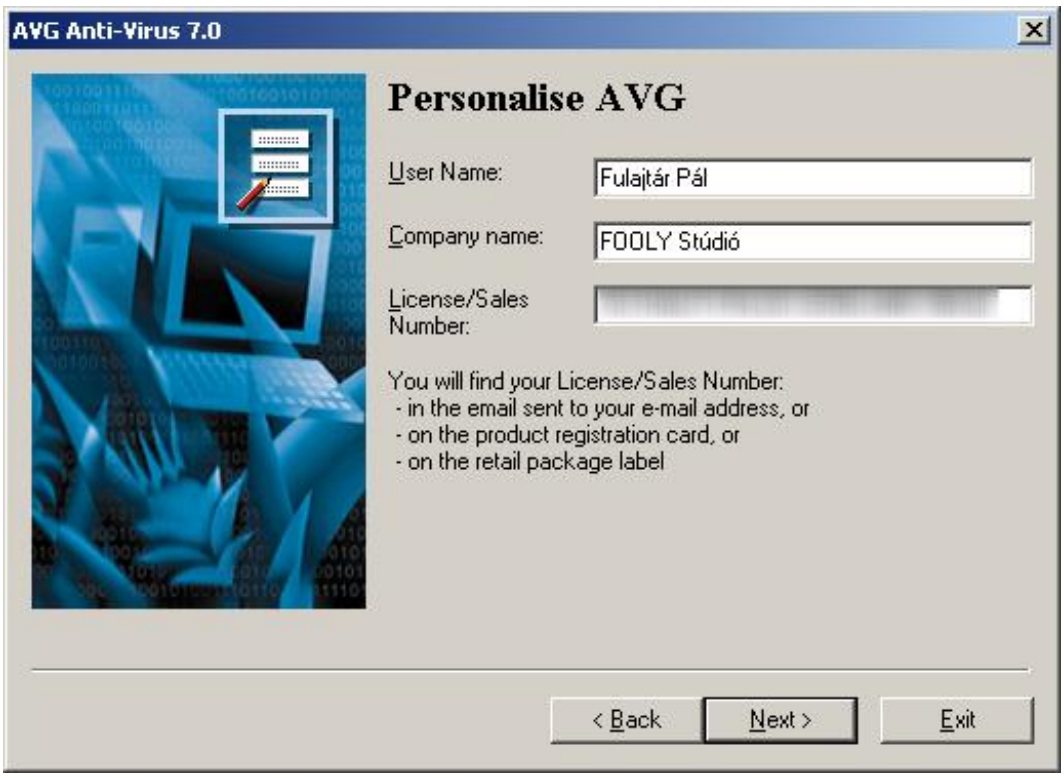
A telepítő program elindítása során a **Setup** gombra kattintva indíthatja el a telepítést.



Válassza ki telepítés nyelvét. (Jelenleg az Angol, Német, Francia és Cseh nyelvek közül választhat). A nyelv kiválasztása után kattintson a **Next** gombra.



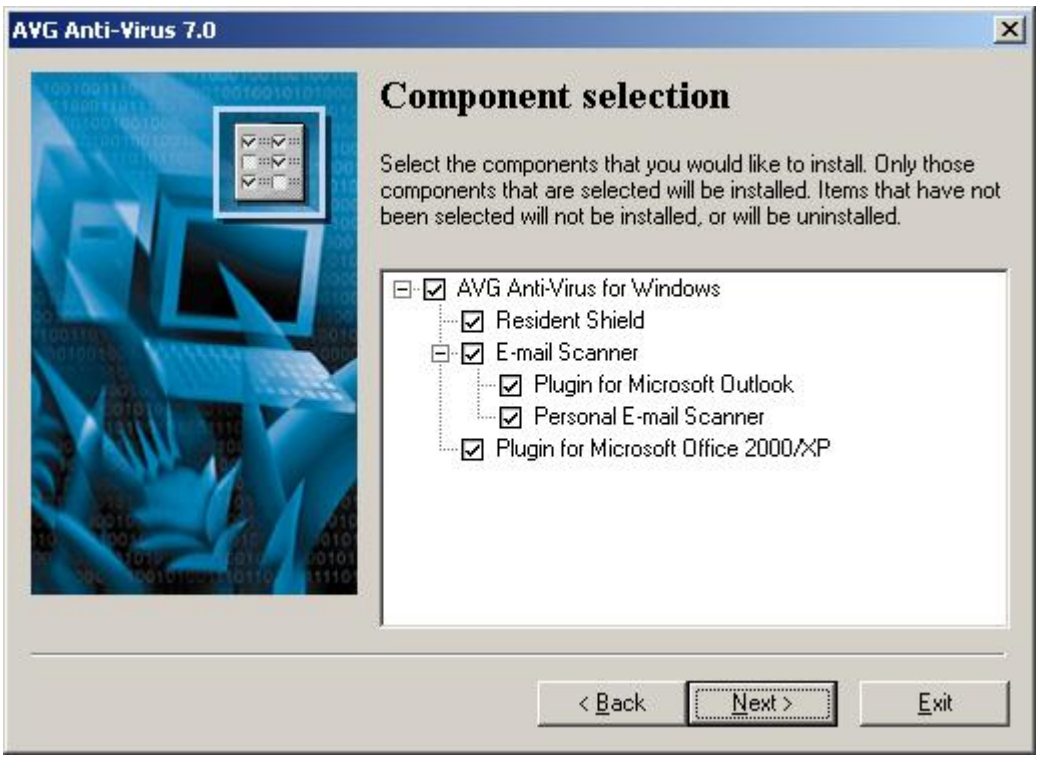
A következő ablakban elolvashatja a szoftver felhasználási (lincenc) feltételeit. Amennyiben Egyetért az abban foglaltakkal, úgy kérjük, hogy válassza az **Accept** gombot, ellenkező esetben pedig a **Don't accept**-et. A licenc feltételeket Magyar nyelven is elolvashatja honlapunkon (**http://www.avg.hu/**). A licencfeltételek elfogadásának hiányában a program nem telepíthető.



Ebben az ablakban meg kell adni saját, illetve cége nevét (ha a termék tulajdonosa cége/munkahelye). Ugyancsak itt kell megadnia terméke regisztrációs kulcsát is a **License/Sales Number** mezőben. Amennyiben a regisztrációs kulcsot

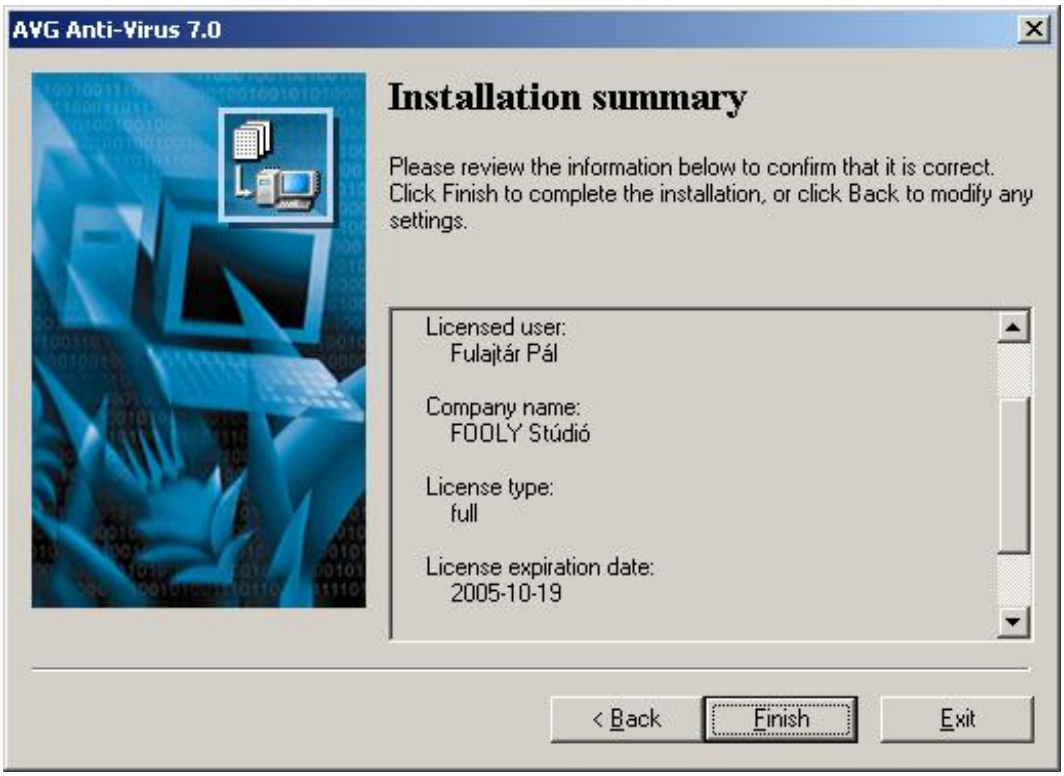
elektronikus formában, például elektronikus levélben kapta, úgy javasoljuk a Másolás és Beillesztés (Copy - Paste) funkciók használatát. Kérjük, hogy ügyeljen a kis és nagybetűk helyes begépelésére!

Itt megadhatja, hogy lemezén hová kívánja az AVG Anti-vírust telepíteni. Amennyiben az alapbeállítás nem megfelelő az Ön számára, úgy a **Browse** gomb segítségével másik helyet telepítési helyet választhat.



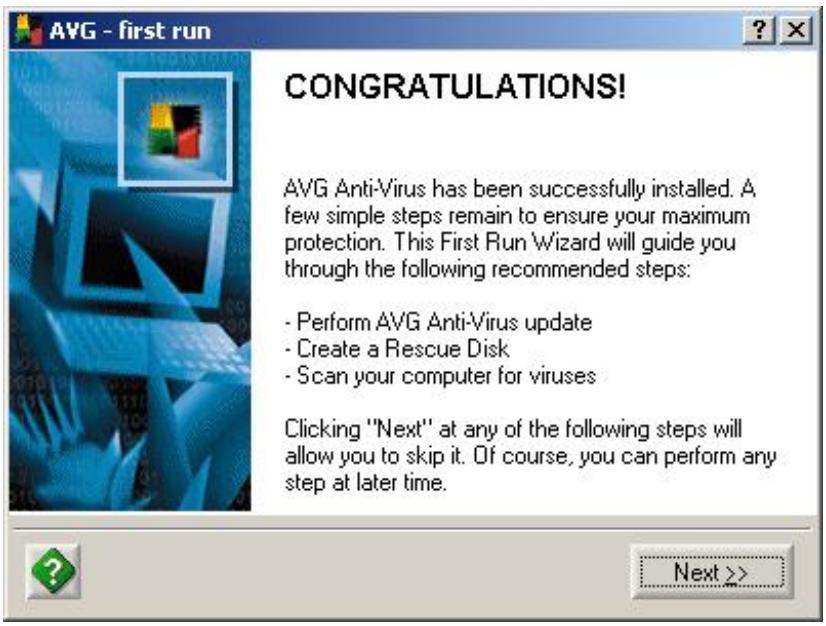
Itt kiválaszthatja a telepítendő komponenseket.

- Resident Shield: Állandó: védelem
- E-mail Scanner: Elektronikus: levelek ellenőrzése
  - Plugin for Microsoft Outlook: Microsoft Outlook (Nem Outlook Express!) kiegészítés
  - Presonal E-Mail scanner: Egyéni/Személyes levél ellenőrző
- Plugin for Microsoft Office 2000/XP: Kiegészítés Microsoft Office 2000 és XP irodai programcsomagokhoz.



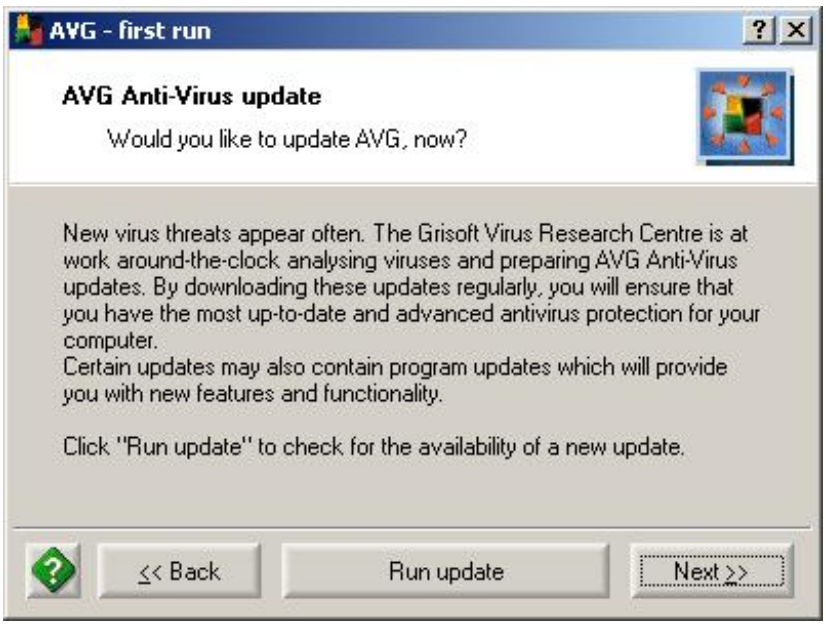
A beállítások után itt ismét áttekintheti, hogy minden adatot helyesen adott-e meg. Amennyiben nem, akkor a **Back** gombbal visszaléphet és módosíthatja a megfelelő adatokat. A **Finish** gombra kattintva telepítés elkezdődik.

A telepítés befejezése után Önnek a következő ablakot kell látnia:

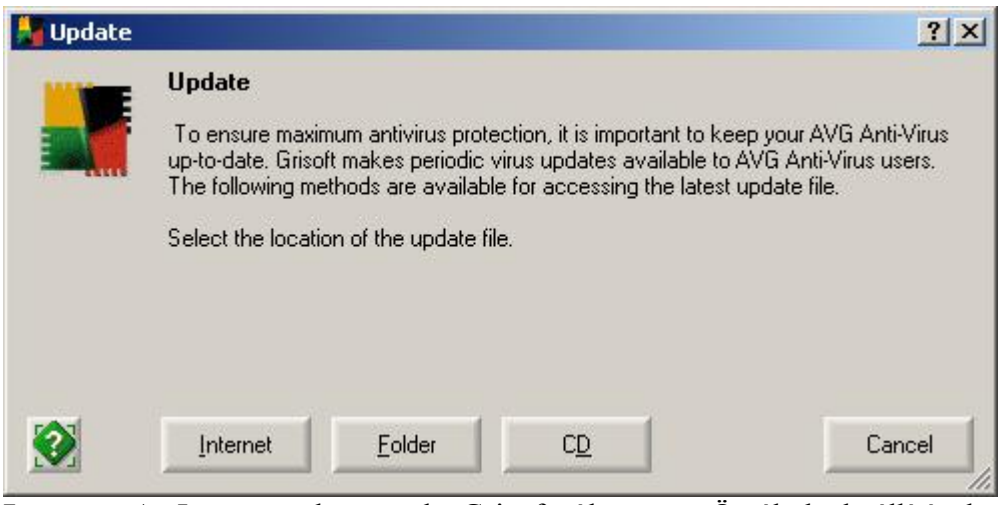


A **Next** gombra kattintva a telepítő végigvezeti Önt néhány alapvető lépésen, amelyek segítségével használatba veheti az AVG Anti-vírust. Ezek a lépések ki is hagyhatók, amennyiben Ön a beállításokat saját maga szeretné elvégezni.

Első lépésként javasoljuk, hogy ellenőrizze, illetve töltse le az AVG Anti-vírus legújabb frissítéseit:



A **Run update (Frissítés indítása)** gombra kattintva az AVG Anti-vírus az alábbi frissítési lehetőségeket kínálja fel:



Internet: Az Interneten keresztül a Grisoft-tól vagy az Ön által a beállításoknál meghatározott helyről töltheti le a frissítéseket.
Folder: Könyvtárból (lehet hálózati megosztás is) végzi el a frissítést
CD: AVG Anti-vírus frissítő CD-ROM-ot használ (nem javasolt)

Figyelem! Amennyiben az Ön tűzfalon vagy proxy szerveren keresztül kapcsolódik az Internetnetre, úgy az Internetről történő frissítés egyéb beállításokat igényelhet. Ebben az esetben a frissítést csak később a beállítások elvégzése után tudja végrehajtani.
*Ebben az esetben most válassza a **Cancel (Mégsem)** gombot és ugorja át **(Next)** a frissítést. A frissítéshez esetlegesen szükséges tűzfal / proxy beállításokhoz, kérjük, hogy tekintse át a dokumentáció **Frissítés Kezelő (Update Manager)** részét.*

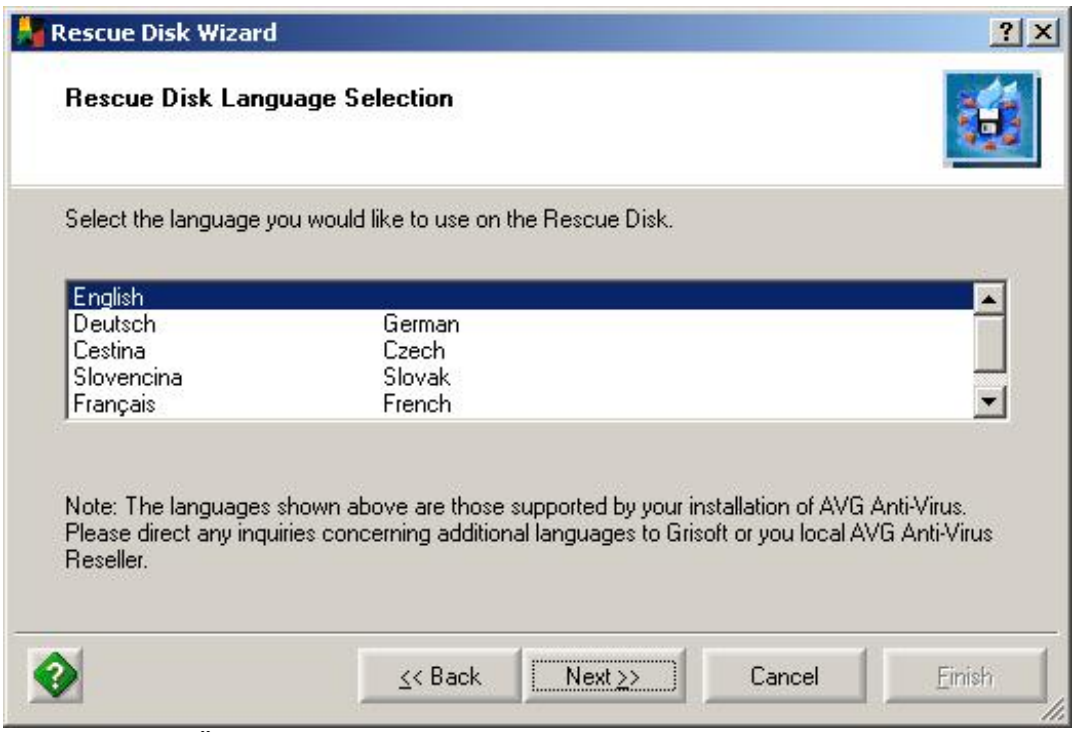
A következő lépés a helyreállító lemez elkészítése:

Bizonyos vírusok a számítógép rendszerterületeit és beállításait támadják meg. Egy ilyen támadás esetleges következményeinek elhárításánál hasznos segítség egy helyreállító lemez, amely tartalmazza az AVG Anti-vírus néhány ellenőrző rutinját, valamint az operációs rendszere fontosabb beállításait.

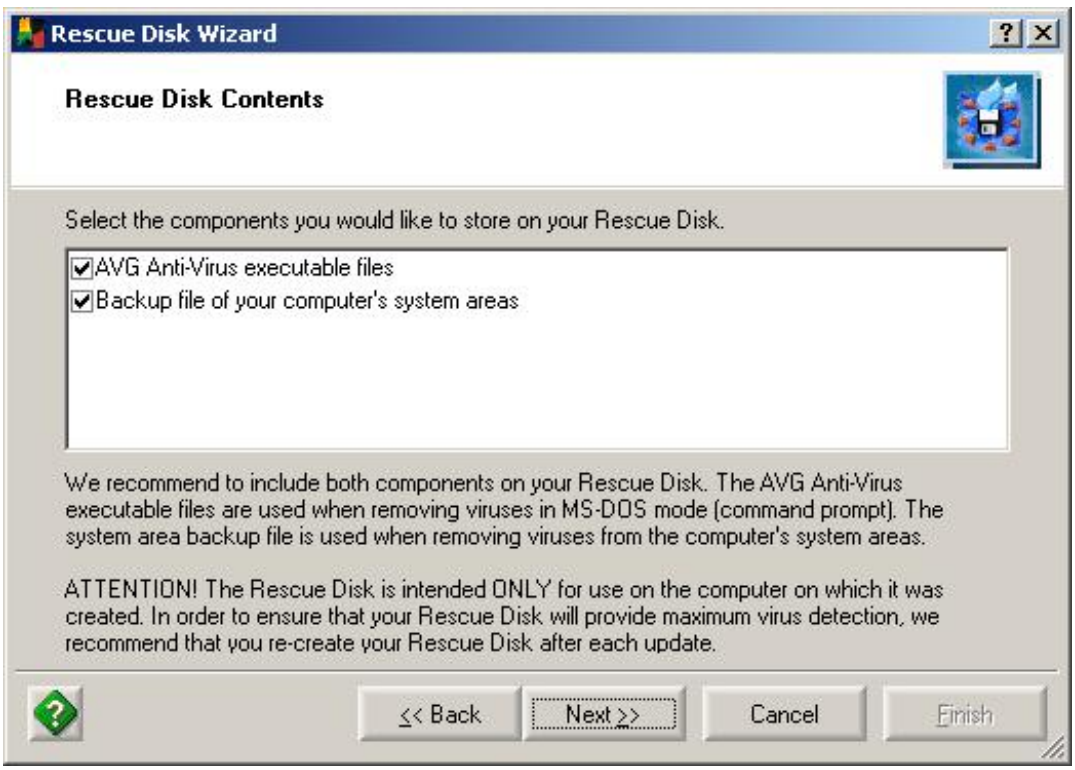
Figyelem! Célszerű helyreállító lemezt készíteni, amennyiben új programot telepített vagy egy korábban telepítettet távolított el számítógépéről, illetve ha frissítette AVG Anti-vírus programját.

A lemez elkészítéséhez kattintson a **Create Backup Disk** gombra. Ha nem kíván helyreállító lemezt készíteni, akkor válassza a **Next** (következő) opciót

Ez az ablak rövid tájékoztatást ad a helyreállító lemez használatához. A helyreállító lemez MS-DOS (parancssori) módban használható. A fertőzött rendszerterületek és a normál üzemmódban megosztás vagy egyéb ok folytán zárolt állományok vírusmentesítéséhez.
A következő lépéshez nyomja meg a **Next** gombot!



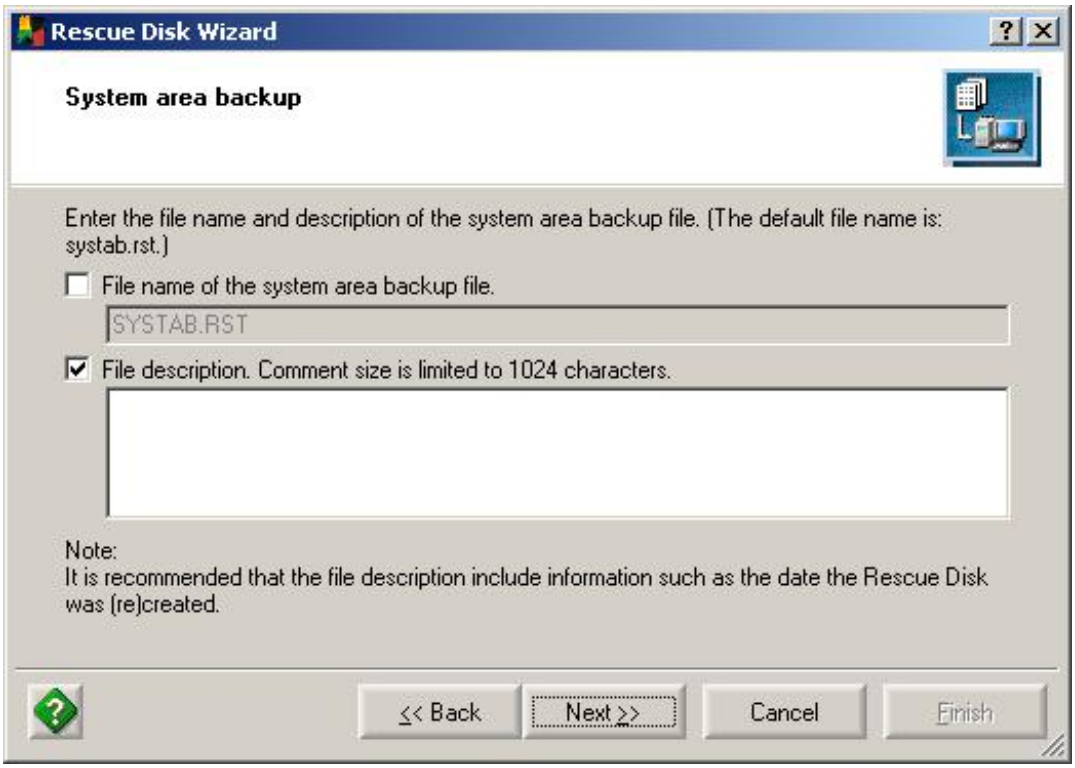
Válassza ki az Ön számára legmegfelelőbb nyelvet (pillanatnyilag az Angol, Német, Cseh, Szlovák, Francia és Portugál nyelvek támogatottak.) majd lépjen tovább a **Next** gombbal.



Válassza ki, hogy mit tartalmazzon a helyreállító lemez:

- **AVG Anti-Virus executable files** – Az AVG Anti-vírus futtatásához szükséges állományok
- **Backup file of your computer's system areas** – Az Ön számítógépe rendszerterületeinek biztonsági mentése

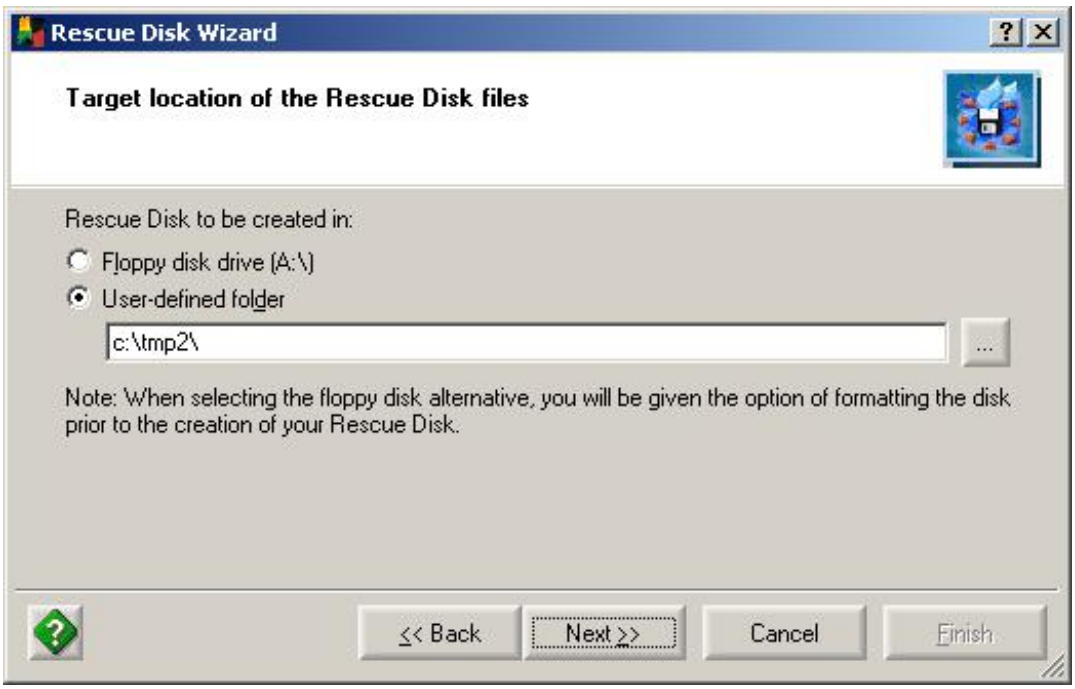
A legnagyobb biztonság elérése érdekében javasoljuk, hogy mindkét opciót válassza ki.
Az igényelt beállítások kiválasztása után nyomja meg a **Next** gombot!



Szükség esetén a rendszerterület mentését tartalmazó állományt átnevezheti és megjegyzést szúrhat be. A választható mezők:

- **File name of the system area backup file** – jelölje be a négyzetet ha meg szeretné változtatni a fájlnevet és az alatta levő mezőbe írja be, hogy mi legyen az.
- **File description** – Jelölje be a négyzetet ha megjegyzést kíván fűzni a mentéshez, majd legfeljebb 1024 karakter (betű, szám, írásjel) hosszban adja meg megjegyzését.

Ha elkészült, akkor nyomja meg a **Next** gombot.

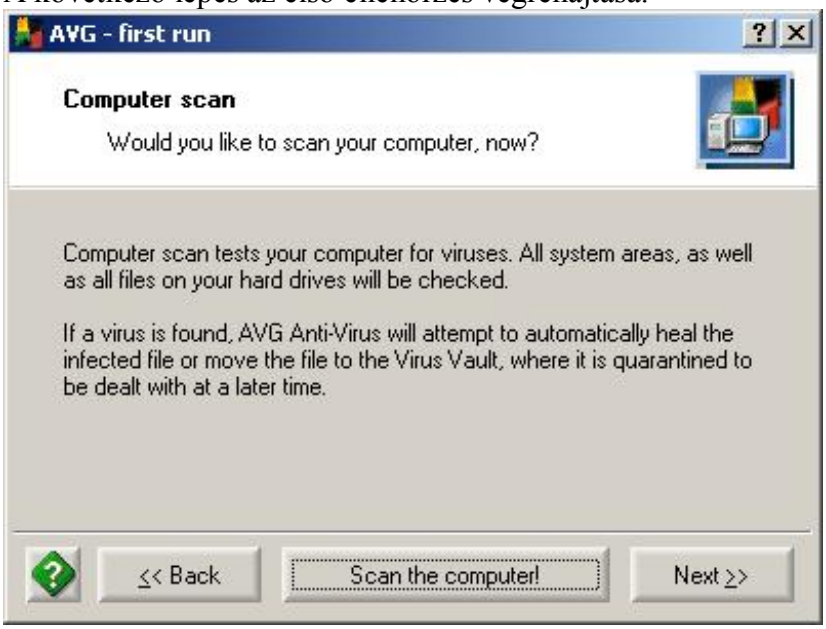


Válassza ki, hogy hová kívánja a mentést elkészíteni. Hajlékony lemezhez válassza a **Floppy disk drive (A:\)** opciót. Elfordulhat, hogy rendszere olyan sok telepített programot és beállítást tartalmaz, hogy az nem fér el egy hajlékony lemezen. Ebben az esetben beállításokat egy tetszőleges könyvtárba mentheti a **User defined folder** opció segítségével. Ezután a könyvtár tartalmát más nagyobb kapacitású lemezre (pld CD-R) mentheti, amely akár rendszerindításra is alkalmas lehet. Ehhez kérjük, hogy tanulmányozza a periféria (pld. CD író) kezelő programja használati utasítását.
A választás után, kérjük, hogy nyomja meg a **Next** gombot.

Ellenőrizze ismét a helyreállító lemez beállításait. Ha egyet ért kattintson a **Create (lemez készítés)** gombra, ha módosítani szeretne a beállításokon, akkor válassza a **Back (vissza)** opciót. A folyamat megszakításához válassza a **Cancel (Mégsem gombot)**

Ha helyreállító lemeze elkészült, akkor ezt az ablakot kell látnia. Bezárásához nyomja meg a **Finish (kész)** gombot.

A következő lépés az első ellenőrzés végrehajtása.

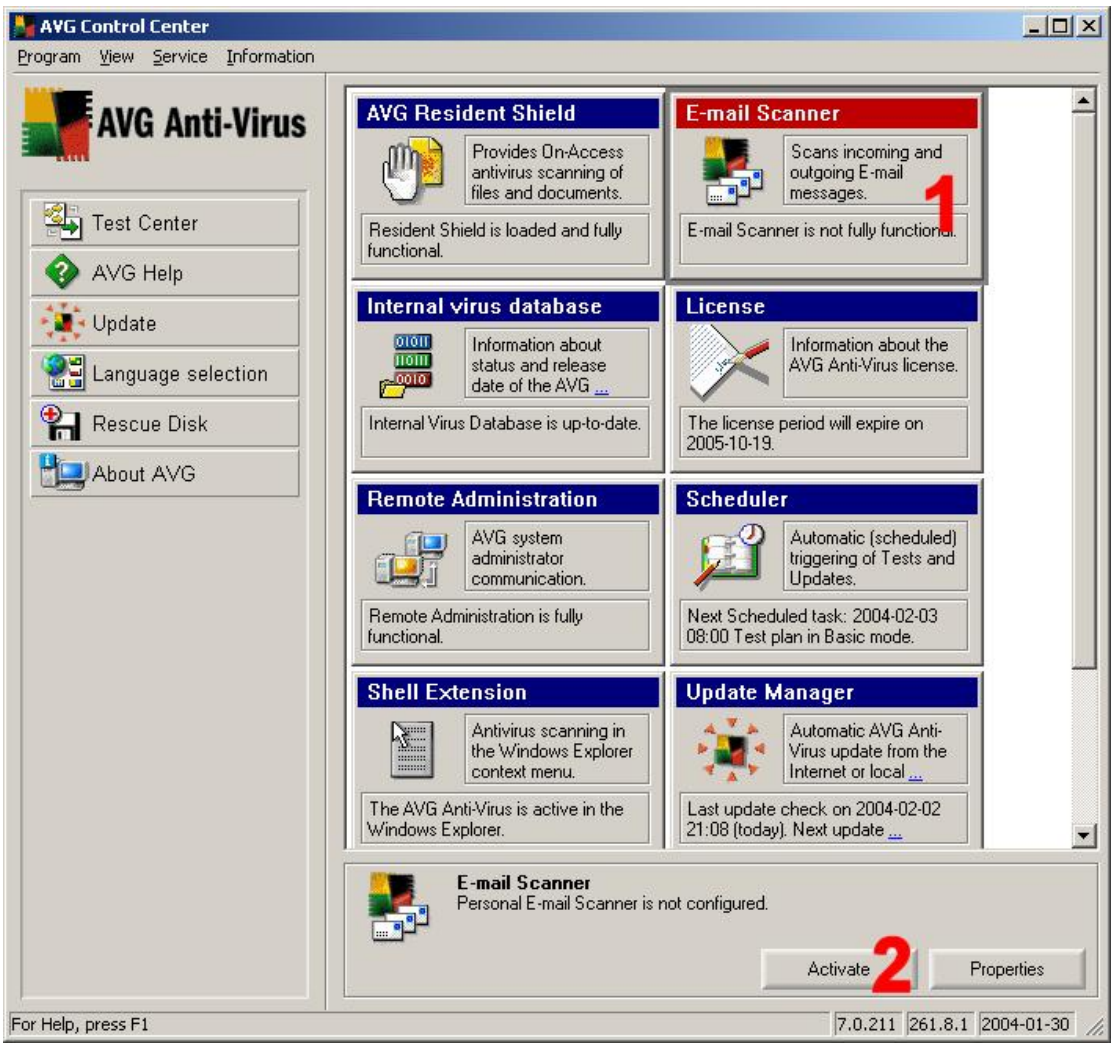


A **Scan the computer (a számítógép ellenőrzése)** gombot választva az AVG Anti-vírus végrehajtja számítógépe teljes körű ellenőrzését. Ha ezt nem kívánja azonnal végrehajtani, például azért mert a frissítést, illetve annak beállításait még nem végezte el, úgy válassza a **Next** gombot.

Az ellenőrzés végrehajtása után az AVG Anti-vírus készen áll a használatra. A **Continue (folytatás)** gombra kattintva elindul az AVG Anti-vírus alapszintű (Basic) kezelő felülete valamint a tálcán megjelenik az AVG Control Center (AVG Vezérlő Központ ikonja).

Amint az ábrán látható az ikon lehet fekete-fehér vagy színes. A fekete-fehér ikon azt jelzi, hogy nem minden funkció működik tökéletesen, illetve valamilyen veszélyre hívja fel a felhasználó figyelmét.

Ezek az esetek többségében nem jelentenek igazi hibát, hanem csak a frissítésre vagy hibás beállításra hívja fel a figyelmet. Az ikonra duplán kattintva megjelenik az **AVG Control Center** (vezérlő központ) és itt megtudhatja a probléma okát, azzal, hogy az érintett modul fejléce kékről pirosra vált.



Jelen esetben csak arra figyelmeztet a rendszer, hogy az **E-mail Scanner (levél ellenőrzés)** funkciót még nem állította be.

Az AVG Anti-vírus beállítása

Ahhoz, hogy az AVG Anti-vírus a lehető legmagasabb szintű védelmet nyújtsa olyan módon kell beállítania, hogy az a lehető legjobban illeszkedjék az Ön számítógépes környezetéhez.

A tálca AVG Anti-vírus  ikonjára kattintva megjelenik a **Control Center (Vezérlő Központ)** képernyője. A program legtöbb funkciója és beállítása ebből az ablakból elérhető.

Figyelem: A tálcán lévő AVG Anti-vírus ikon csak azt jelzi, hogy Vezérlő Központ be van töltve és működik. Ez független a Resident Shield (állandó védelem) működésétől, amely akkor is fut, tekintet nélkül arra, hogy a tálcán a vezérlő központ ikonja esetleg nem látható, mert azt valamilyen oknál fogva leállították.

Az elektronikus levelek ellenőrzésének beállítása

Az AVG levelező proxy kiszolgáló az Ön levelező kiszolgálója és a levelező programja között áll. Levelező programja minden a levelező kiszolgálónak szánt kérést Az AVG proxy kiszolgálónak küld el, amit az ellenőrzés után továbbít a tényleges levelező kiszolgálóhoz. A levelező kiszolgálóról érkező levelek először az AVG proxy kiszolgálóhoz érkeznek és amennyiben az veszélytelennek ítéli a küldemény tartalmát, csak abban az esetben továbbítja az Ön levelező programja felé, ellenkező esetben a küldeményből a vírusokat, férgeket eltávolítja.

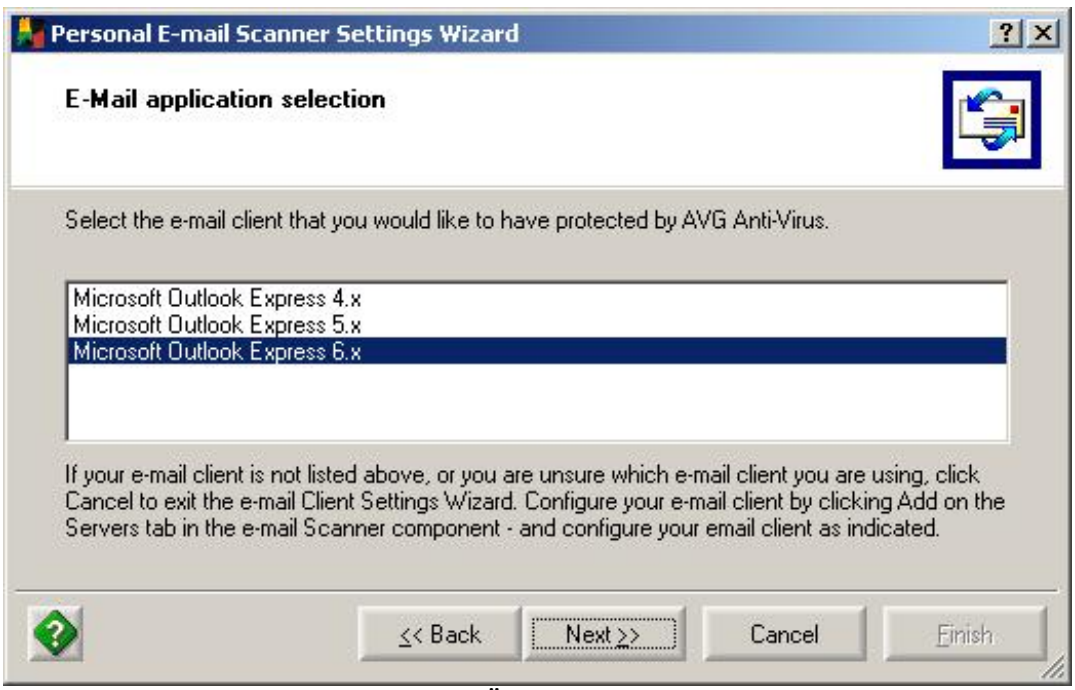
A beállításhoz kattintson egyszer a **E-mail Scanner** cellára, majd

- Ha automatikus beállítást szeretne, akkor az **Activate (Aktiválás)**
  Az aktiválás csak akkor indítja el a beállítás varázslót, ha még nincsenek személyes e-mail ellenőrző beállításai, ellenkező esetben csak a letiltott ellenőrző funkció újra engedélyezésére szolgál!
- Ha kézi beállítást választ, akkor pedig a **Properties (beállítások)**

gombok valamelyikére.

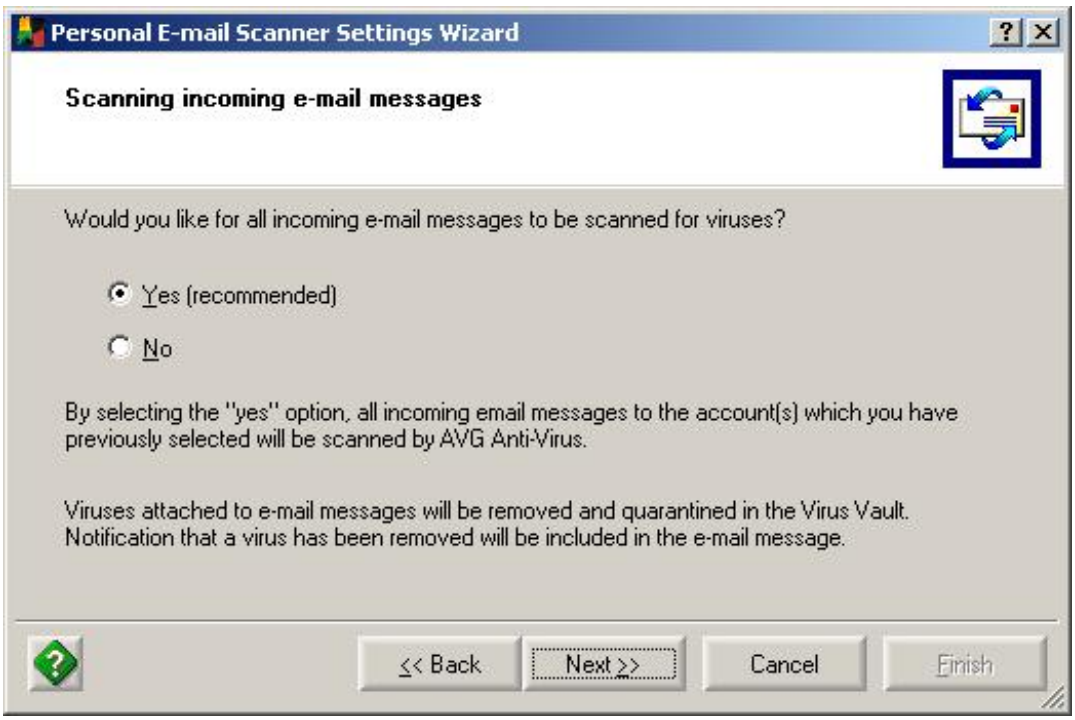
Automatikus beállítás

A következő ablakban elindul a levelezés védelmét beállító varázsló. Javasoljuk, hogy válassza az **Expert settings (Szakértői beállítás)** opciót, majd kattintson a **Next (következő)** gombra. *A beállítás a **Cancel (Mégsem)** gombra kattintva bármikor megszakítható.*



A megjelenő ablakban válassza ki az Ön által használt levelező programot. Az ablakban nem minden levelező program jelenik meg, ugyanis vannak olyanok, amelyet az AVG automatikusan, kiegészítő modullal (plugin) támogat. Ilyen például az MS Outlook (Nem Outlook Express!), de olyanok is vannak, amelyekhez a varázsló nem alkalmazható (mint például Netscape Mail). Az ilyen programok (egyéb POP3 és SMTP alapú levelező programok) beállításához a kézi beállítást kell választani.

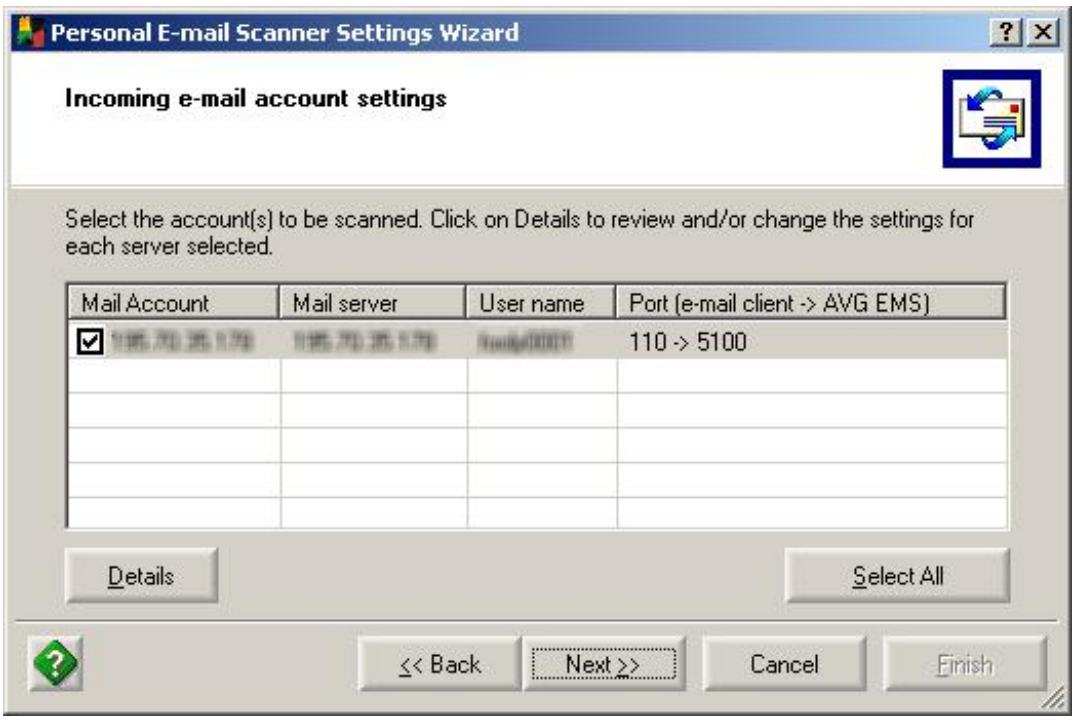
A levelező program kiválasztása után nyomja meg a **Next** gombot!



Ebben az ablakban eldöntheti, hogy minden érkező levelét szeretné-e ellenőrizni?

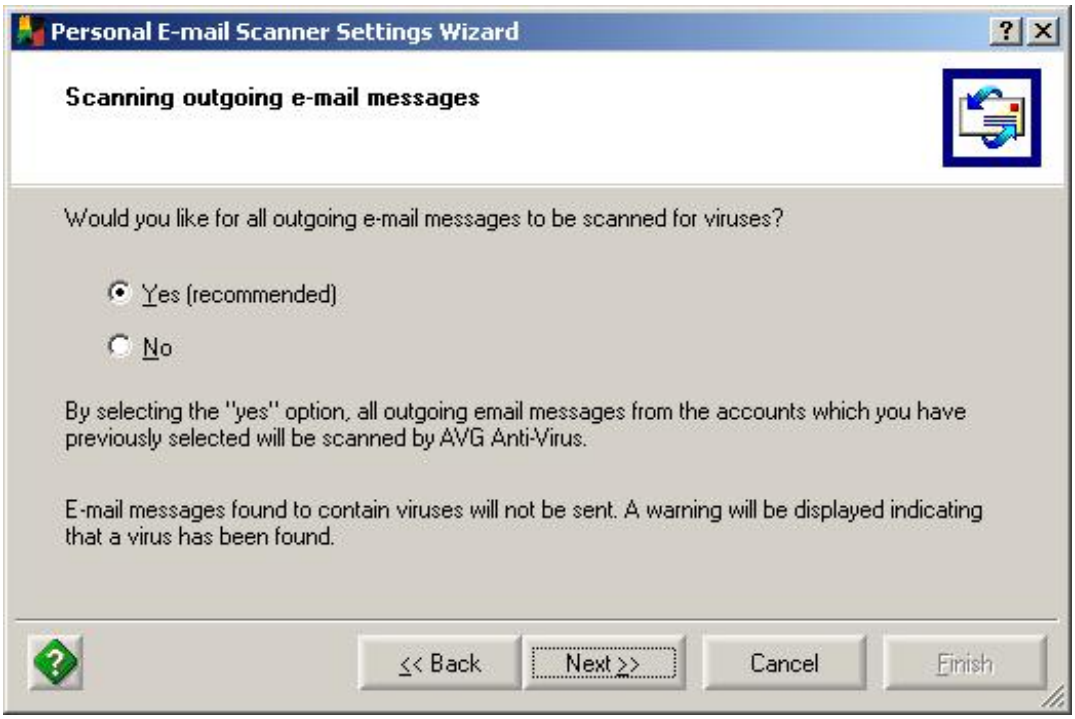
- **Yes** – igen (ajánlott)
- **No** – nem

Választása után nyomja meg a **Next** gombot!



Az AVG Anti-vírus kiolvassa levelező programjának **POP3** beállításait és automatikusan illeszti magát hozzájuk. A víruskereső program egyidejűleg több

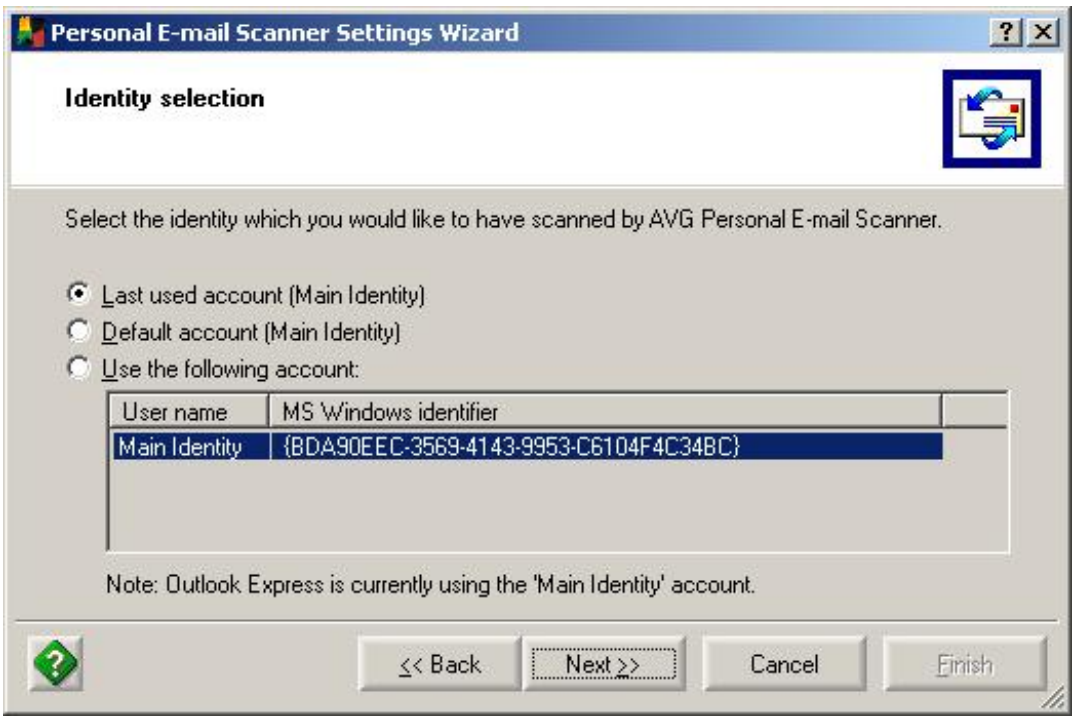
POP3 postafiók kezelésére is alkalmas, természetesen ezt a levelező programnak is támogatnia kell.
A megjelenő listában jelölje be azon postafiókjait, amelyeket szeretné bevonni a vírusellenőrzés alá. A **Select all (mindet kiválaszt gomb)** segítségével az összes felsorolt címet kiválaszthatja. A **Details** gombbal a beállítások részleteit kézzel módosíthatja. Erről a bővebben a kézi beállításnál írunk.
Ha elvégezte a postafiókok kiválasztását és a szükséges beállításokat, kérjük, hogy válassza a **Next** gombot!



Ebben az ablakban eldöntheti, hogy minden kimenő (küldött) levelét szeretné-e ellenőrizni?

- **Yes** – igen (ajánlott)
- **No** – nem

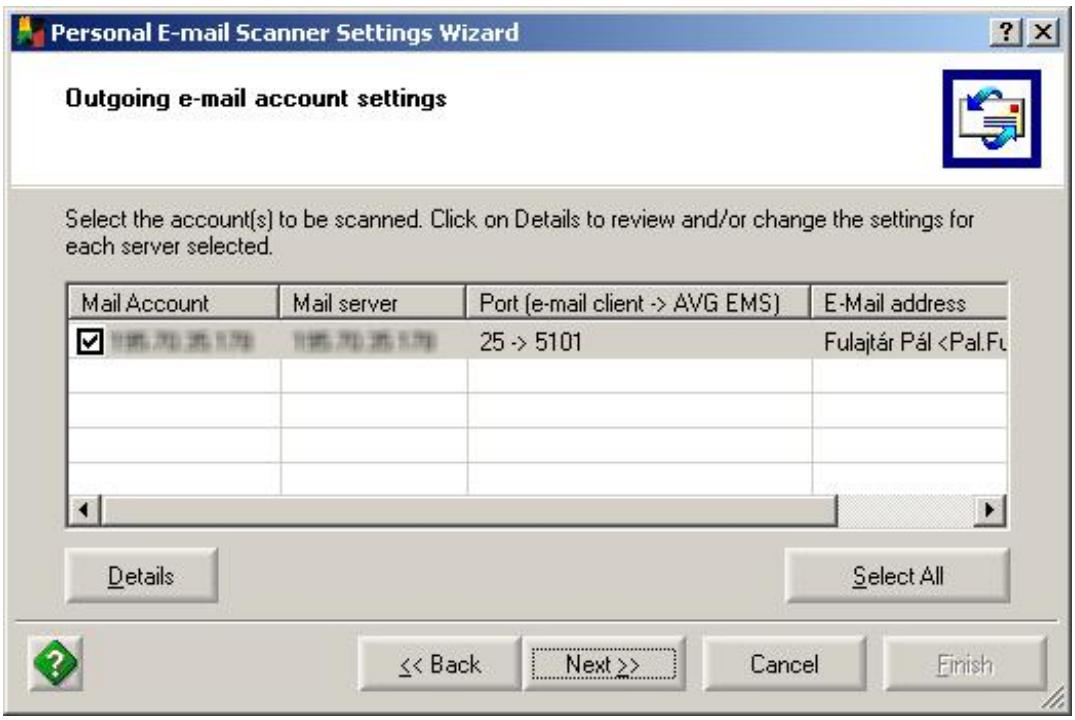
Választása után nyomja meg a **Next** gombot!



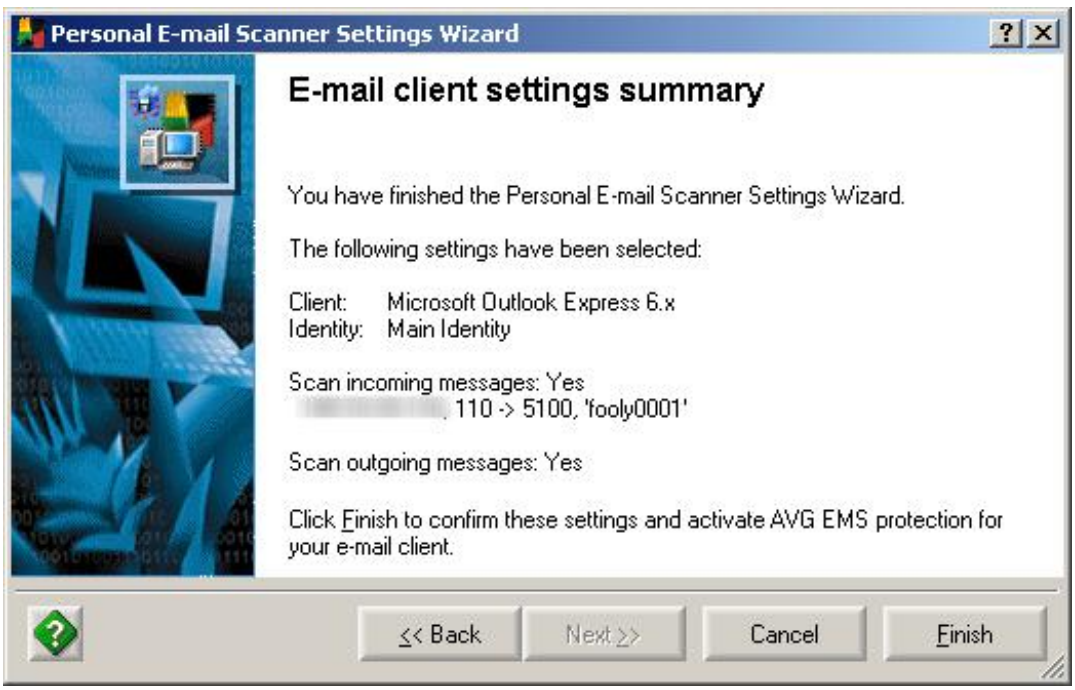
Ebben az ablakban kell megadni, hogy mely személyiségéhez (Identity) tartozó SMTP szervert szeretné használni a levélküldéshez:

- **Last used account** – azt, amit legutoljára használt
- **Default account** – Alapértelmezett személyiség
- **Use following account** – maga szeretné kiválasztani az alatta lévő listából

A harmadik opció használata több felkészültsége igényel, mivel a Microsoft egy sokjegyű betű-szám kombinációval azonosítja az személyiségeket. Önnek ez alapján a kód alapján kell kiválasztani a megfelelőt.
Az esetek többségében az első vagy a második opció használata megfelelő.
Amennyiben személyiségét hibásan adná meg, úgy a beállítások később bármikor módosíthatóak!
Választása után nyomja meg a **Next** gombot!



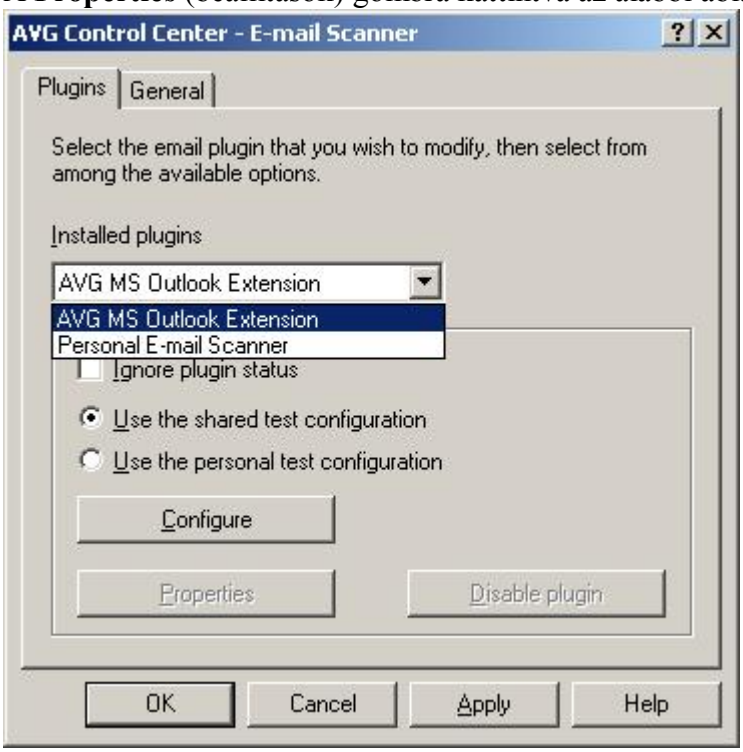
Itt a levél fogadáshoz hasonlóan kiválasztja, hogy mely postafiókjai esetében legyenek ellenőrizve a küldött levelek. A megjelenő listában jelölje be azon postafiókjait, amelyeket szeretné bevonni a vírusellenőrzés alá. A **Select all (mindet kiválaszt gomb)** segítségével az összes felsorolt címet kiválaszthatja. A **Details** gombbal a beállítások részleteit kézzel módosíthatja. Erről a bővebben a kézi beállításnál írunk.
Ha elvégezte a postafiókok kiválasztását és a szükséges beállításokat, kérjük, hogy válassza a **Next** gombot!



A beállítások jóváhagyása előtt még egyszer áttekintheti a beállításokat. Ha módosítani kíván rajtuk, akkor válassza a **Back (vissza)** gombot! Ha elfogadja a beállításokat, akkor válassza a **Finish (befejezés)** gombot.

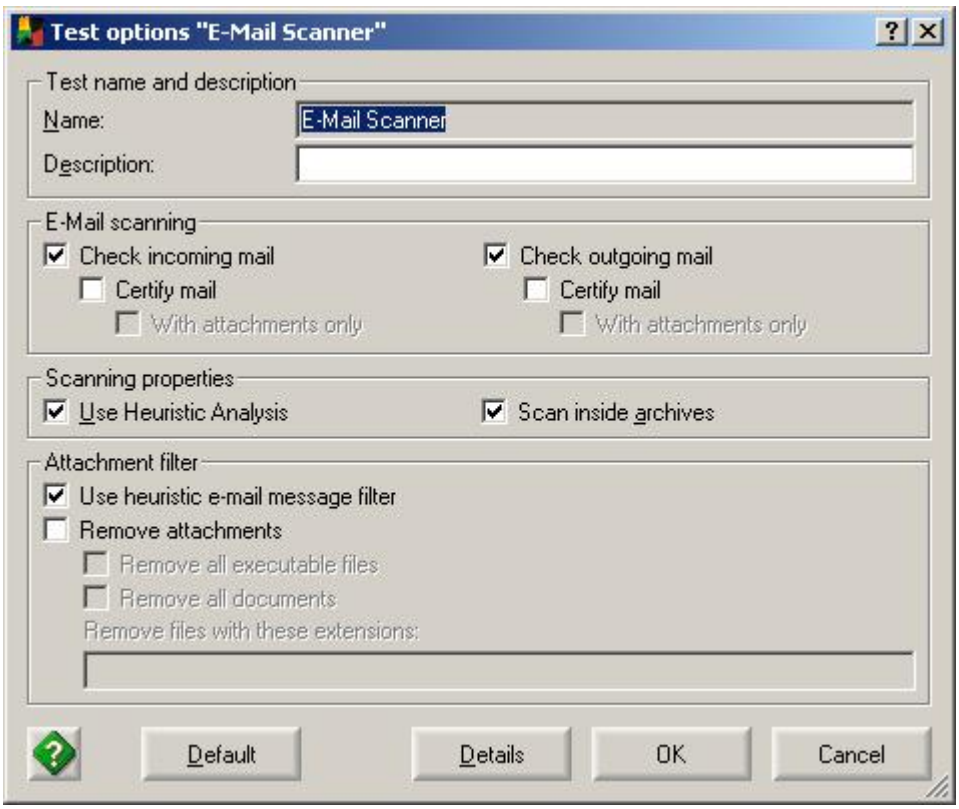
Az elektronikus levél szűrés viselkedésének beállításai

A **Properties** (beállítások) gombra kattintva az alábbi ablak jelenik meg:



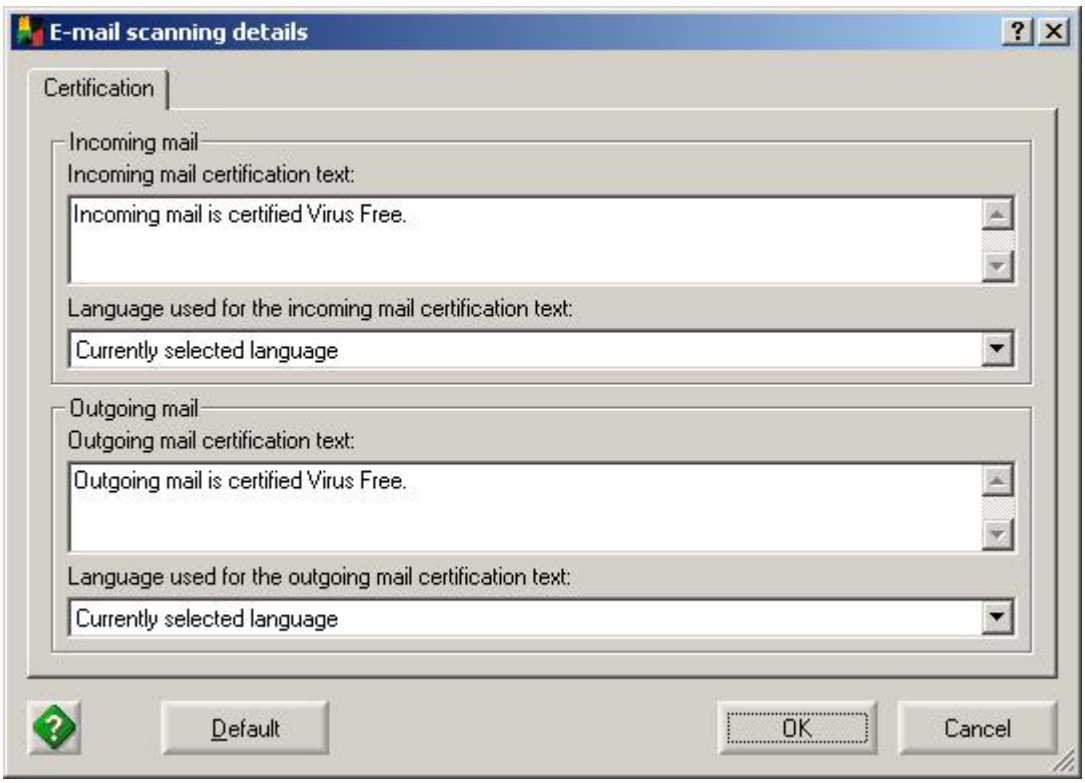
Az **Installed plugins** (telepített modulok) listájában láthatóak, hogy milyen modulok érhetőek el pillanatnyilag. A nem használt modulok esetében célszerű a modult kiválasztva az **Ignore plugin status (modul állapot figyelmen kívül hagyása)** jelölő négyzetet megjelölni és az **Apply (jóváhagy)** gombra kattintva a modul hiba és egyéb üzeneteit letiltani. Ezzel megelőzheti, hogy egy helytelenül beállított, de nem használt modul megtévesztő hibaüzeneteket adjon.

Az **Use the shared test configuration (közös beállítások használata)** segítségével az elektronikus levelek tesztelése az levelező programok illesztő moduljaira általában érvényes beállításokkal fog történni, míg a **Use the personal test configuration (személyes beállítások használata)** opciót választva lehetőség nyílik a beállítások modulonkénti egyedi beállítására.
A beállítások a **Configure (beállítás)** gomb segítségével végezhetők el.
A **Properties (tulajdonságok)** gomb a modulok paramétereinek (szerver címek, stb.) beállítására szolgál. Ez a funkció nincs minden modul esetében értelmezve.
A Disable plugin (modul letiltása). Bizonyos modulok, mint például a **Personal E-mail scanner** (személyes levél ellenőrző) működése átmenetileg letiltható. Ebben az esetben a modul vírusellenőrzést nem végez. Ez a funkció sem értelmezhető minden modul esetében.



A modul kiválasztása, majd a **Configure** gomb megnyomására a fenti ablak jelenik meg. Az ablak beállítáasi a következők:

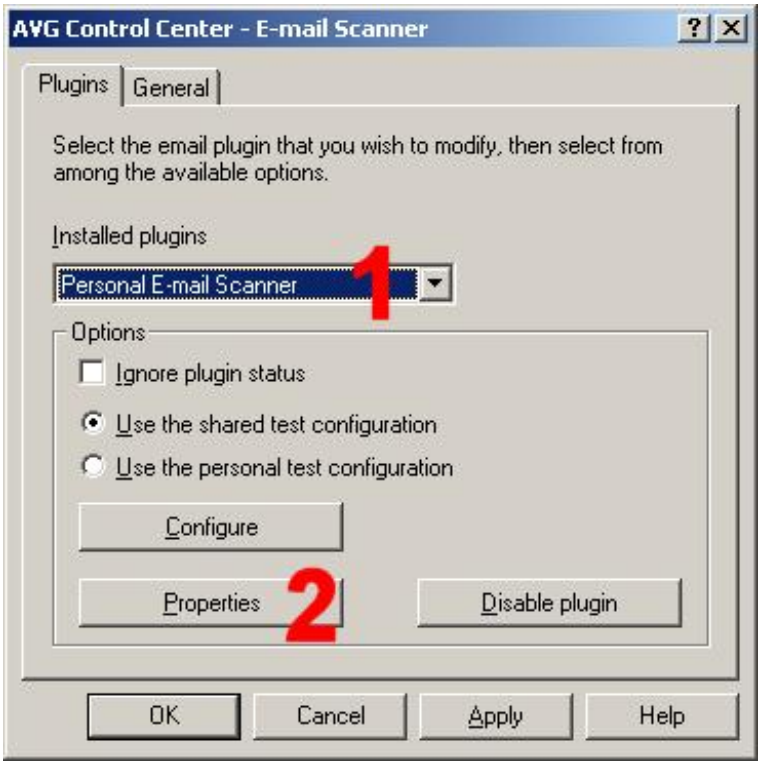
- **Name**: Az ellenőrzési beállítás neve
- **Description**: Az ellenőrzési beállítás leírása (tetszőleges szöveg)
- **Check incoming mail**: fogadott levelek ellenőrzése
- **Check outgoing mail**: a küldött levelek ellenőrzése
- **Certify mail**: a levelekhez egy az ellenőrzés megtörténtét és eredményét tartalmazó hitelesítő szöveget fűz.
- **With attachments only**: csak akkor fűz hitelesítő szöveget a levélhez ha az mellékletet (potenciális vírushordozót) tartalmazott.
- **Use Heuristic Analysis**: Használja a heurisztikus, szimulált környezetű ellenőrzést. Ez a módszer nagyobb biztonságot ad, de lassítja az ellenőrzést.
- **Scan inside archives**: Ellenőrizze a tömörített fájlokat is.
- **Use heuristic e-mail message filter**: Használja a szimulációs levél szűrőt.
- **Remove attachments**: Távolítsa el a mellékleteket (tekintet nélkül arra, hogy tartalmaz-e vírust)
- **Remove all executable files**: távolítsa el a futtatható fájlokat (csak azokat!)
- **Remove all documents**: távolítsa el a dokumentumokat (MS Word, stb.)
- **Remove files with these extensions**: A megadott kiterjesztésű fájlokat távolítsa el.
- **Defaults**: Gyári beállítások visszaállítása
- **Details**: Ha kiválasztotta hitelesítő szöveg használatát, akkor a hitelesítő szöveg paramétereit itt állíthatja be.



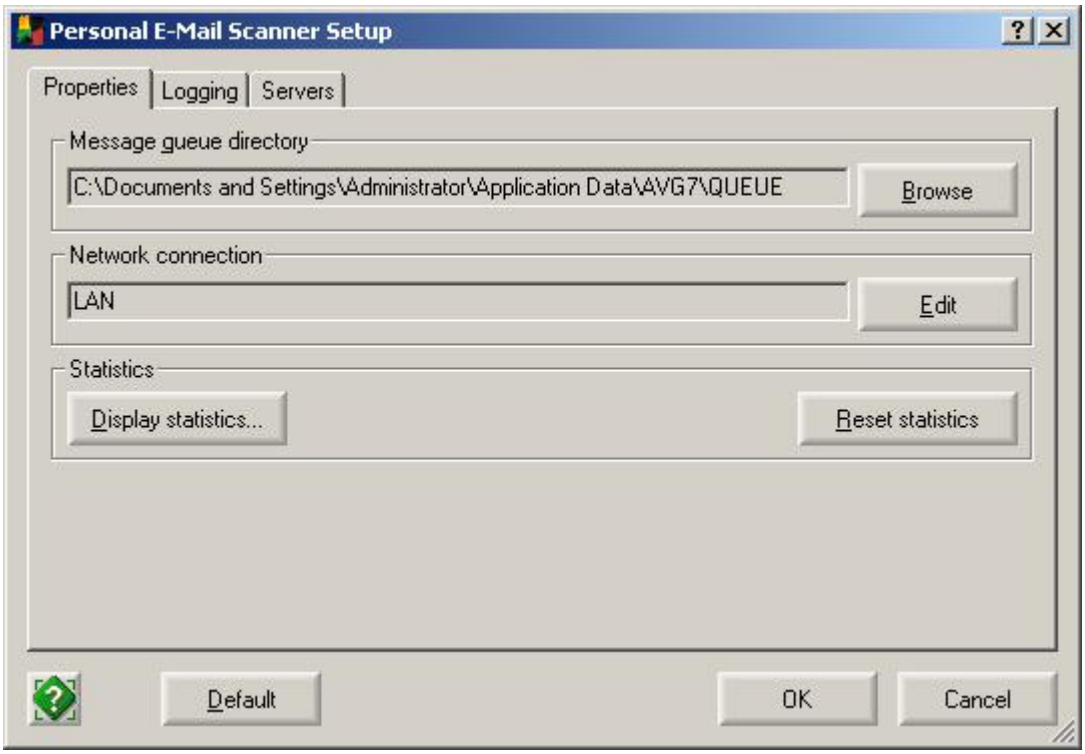
Incoming mail certification text: A bejövő levelekhez csatolandó hitelesítő szöveg
Language used for the incoming mail certification text: Ezen a nyelven jelenjen meg a hitelesítő szöveg és vírusellenőrző verziója a fogadott levelek esetében.
Outgoing mail certification text: A küldött levelekhez csatolandó hitelesítő szöveg
Language used for the outgoing mail certification text: Ezen a nyelven jelenjen meg a hitelesítő szöveg és vírusellenőrző verziója a küldöt levelek esetén.
Default: A gyári beállítások visszaállítása

A módosított beállításokat az **OK (Rendben)** gomb segítségével fogadhatja el és a **Cancel (Mégsem)** gomb segítségével vetheti el.

A személes levél ellenőrző funkció kézi beállítása



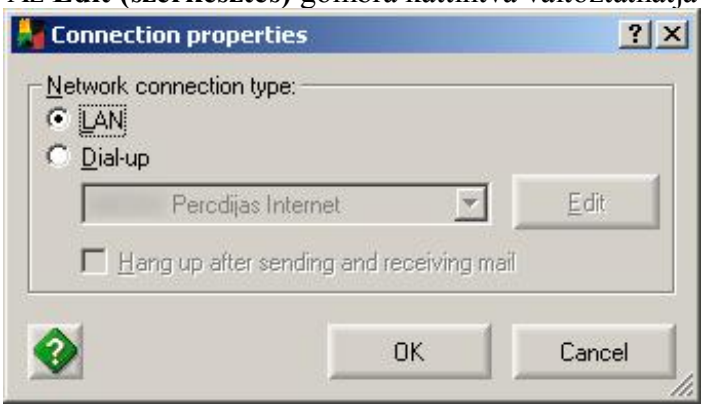
Válassza ki a **Personal E-mail Scanner (személyes levél ellenőrző)** modult, majd kattintson a **Properties (tulajdonságok)** gombra.



Az ablak **Properties** (tulajdonságok) fülén az alábbi paraméterek beállítására van lehetőség:

- **Message queue directory (várakozási sor helye)**: A feldolgozásra (vírusellenőrzésre) váró levelek átmeneti gyűjtőhelye. A feldolgozás befejeződéséig a levelek ebben a könyvtárban fognak várakozni. Az

alapbeállításon rendszerint nem szükséges változtatnia. Erre általában csak akkor szokott sor kerülni, ha az alapértelmezett lemezegységen nem áll rendelkezésre elegendő hely. Új könyvtárat a **Browse (böngészés)** gombra kattintva állíthat be.

- **Network connection (hálózati kapcsolat):** Itt megadhatja, hogy a levelek fogadásához, illetve küldéséhez melyik hálózati, tárcsázó kapcsolatát használja. Az **Edit (szerkesztés)** gombra kattintva változtathatja meg a beállítást. 

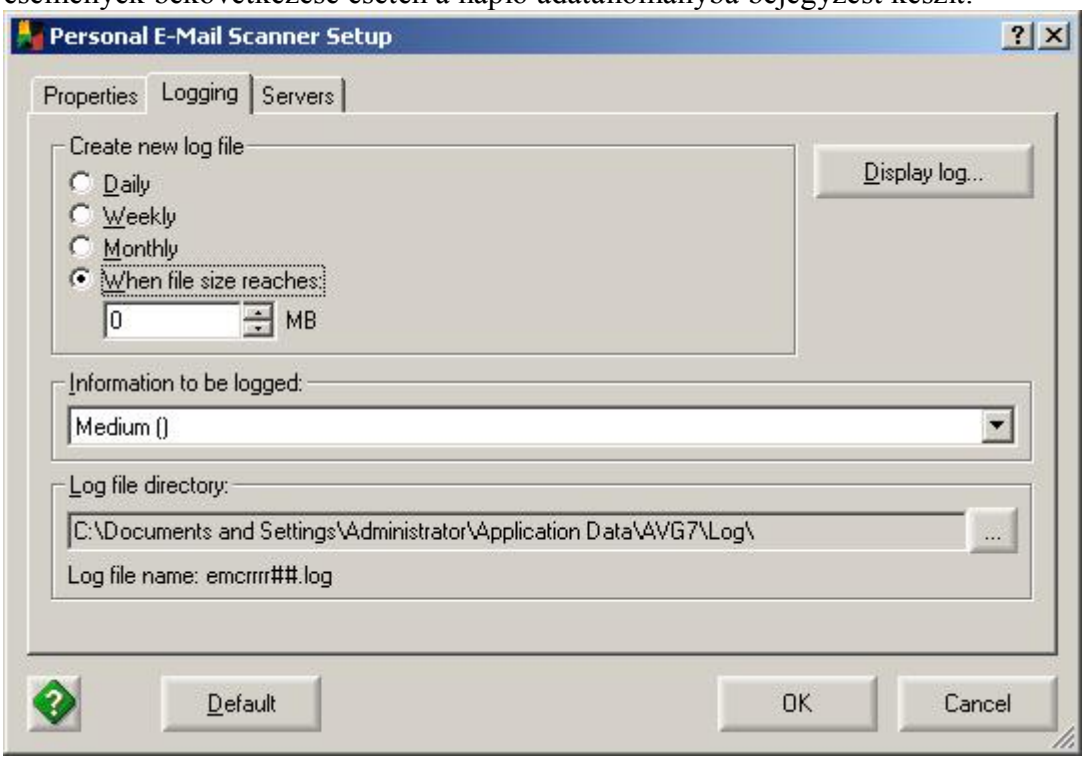
    - A megjelenő ablakban választhat a **LAN (helyi hálózat)** vagy valamelyik tárcsázó beállítás között. Tárcsázó beállítást választása esetén, ha az Edit (szerkesztés) gombra kattint, akkor módosíthatja a kiválasztott tárcsázó profil beállításait (ugyanazt a funkciót érheti el, mint a Windows operációs rendszerek vezérlő pultjának tárcsázó beállításainál). Tárcsázós kapcsolat beállítása esetén lehetőség van továbbá a **Hang up after sending and receiving mail (a kapcsolat bontása a levelek küldése és fogadása után)**. Ezt kiválasztva levél küldés- fogadás után a telefonos kapcsolatot lebontja a rendszer, ezzel telefonköltséget takaríthat meg. Nem célszerű az opció használata olyankor, ha az Internetre kapcsolódáskor nem csak levezni szeretne, hanem például böngészni is, mivel ilyenkor a kapcsolat bontása az egyéb tevékenységeket is megszakítja. Amennyiben nem szeretné, ha a levél küldés- fogadás automatikus indítaná a tárcsázást és inkább, saját maga szeretné felügyelni az Internetre kapcsolódást és a kapcsolat bontását, akkor javasoljuk, hogy használja a **LAN** opciót. A LAN opció mindig az aktuálisan felépített Internet kapcsolatot használja, tekintet nélkül arra, hogy az tárcsázós-e vagy sem. Választását az **OK (Rendben)** gombra kattintva hagyhatja jóvá.
- A **Display statistics (statisztikai adatok megjelenítése)** gombra kattintva a levél küldések és fogadások során végzett vírusellenőrzések eredményeit láthatja.

A megjelenő információk tartalma a következő:

- **On-Line E-Mail servers:** beállított levelező szerverek száma
- **Message received:** fogadott levelek száma
- **Message sent:** küldött levelek száma
- **Messages in outbound queue:** elküldésre váró levelek száma
- **Viruses found:** Talált vírusok száma
- **Last detected virus:** Az utoljára elfogott vírus
- **Reset statistics:** A számlálók nullázása
- **Close:** Az ablak bezárása

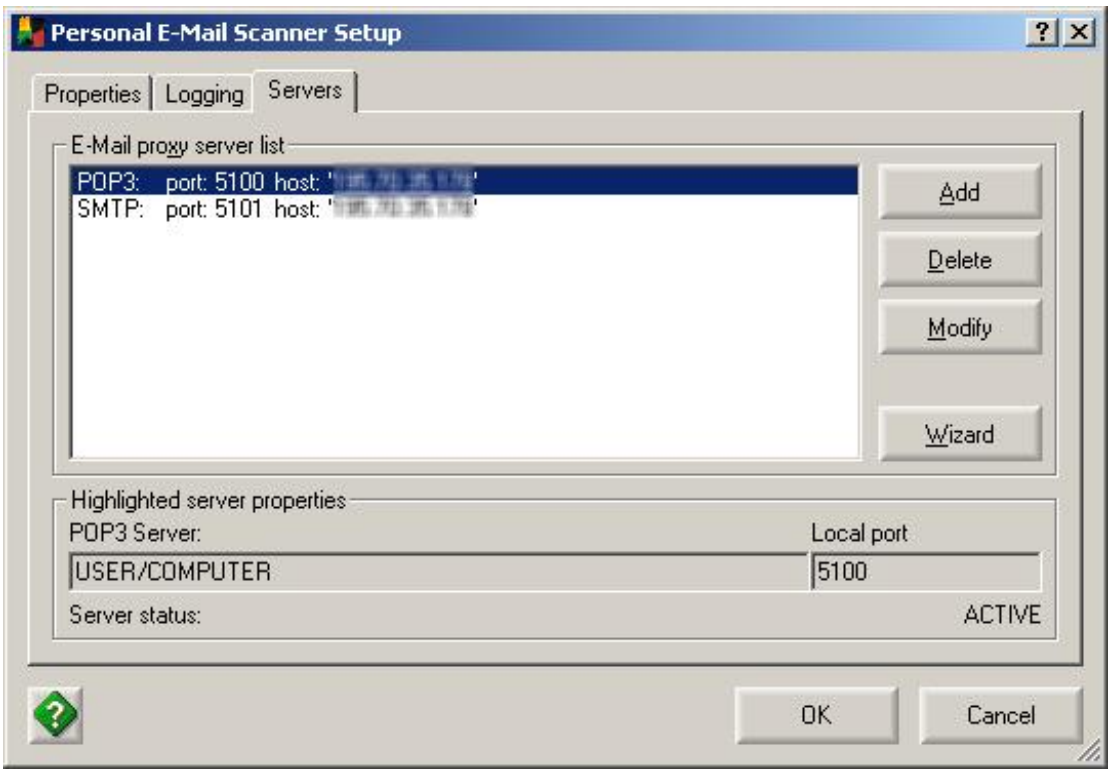
- A **Reset statistics** nyomógomb itt is a számlálók nullázására szolgál. A számlálók nullázása
- A **Default (alapértelmezés)** gombra kattintva visszaállíthatja a gyári beállításokat
- A beállításokat az **OK (Rendben)** gomb segítségével hagyhatja jóvá a beállítások változtatásait
- A **Cancel (Mégsem)** gomb megnyomásával elvetheti a beállításokat. *Figyelem! A számlálók nullázását a Cancel gomb megnyomása nem vonja vissza!*

A levél ellenőrző funkció működése követhető a **Logging (naplózás)** fülnél található beállítások elvégzésével. Ennek segítségével az AVG Anti-vírus meghatározott események bekövetkezése esetén a napló adatállományba bejegyzést készít.



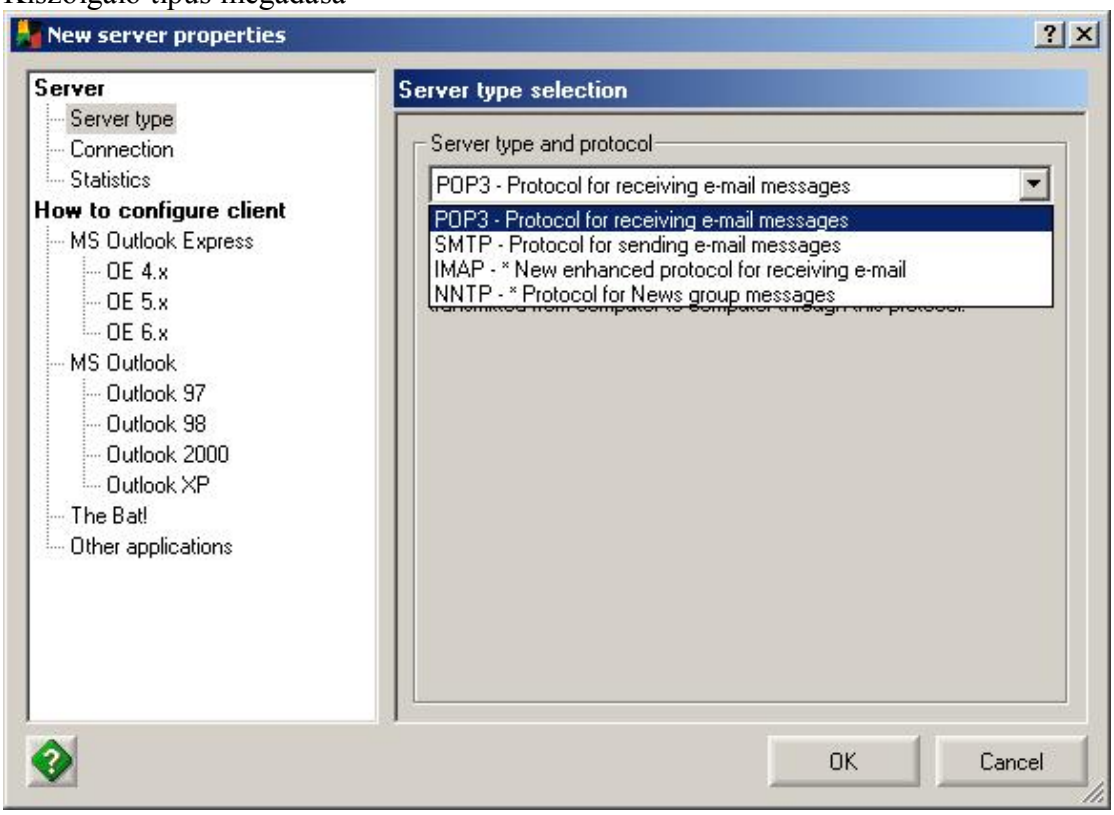
Az ablak beállítási lehetőségei:

- **Create new log file (új napló készítése).** A napló információnak rendezése és rendszerezése, könnyű kezelése érdekében az AVG Anti-vírus bizonyos feltételek teljesülése esetén új naplót nyit. A lezárt naplófájlt a rendszer NEM törli, mivel az fontos információkat tartalmazhat. Erről Önnek kell gondoskodnia, szem előtt tartva a szabad lemezterületet. Választási lehetőségek:
  - **Daily**: Naponta
  - **Weekly**: Hetente
  - **Monthly**: Havonta
  - **When file size reaches**: Ha napló mérete meghaladja a megadott méretet (megabájtban) Az opció kiválasztása és 0 érték megadása azt jelenti, hogy soha nem nyitunk új naplót.
- **Information to be logged:** A rögzítendő információ részletessége
  - **Minimum:** csak a legfontosabb információkat naplózzuk
  - **Medium:** átlagos mennyiségű információ (a napi használatnál elegendő)
  - **Maximum:** sok, részletes információ naplózása. Bekapcsolása rendellenes működés esetén, hibakereséskor célszerű. *Bekapcsolása esetén a nagy információ mennyiség miatt tekintettel kell lenni a rendelkezésre álló szabad lemezterületre!*
- **Log file directory**: A naplóállományok gyűjtőhelye (könyvtára). Ebbe a könyvárba kerülnek a naplófájlok.



A **Servers (kiszolgálók)** fülre kattintva megjelenik a levelezés kézi beállítására szolgáló ablak, amelyről **az automatikus beállítás** részben is szót ejtettünk.
Az ablakon látható mezők és beállításai lehetőségek:

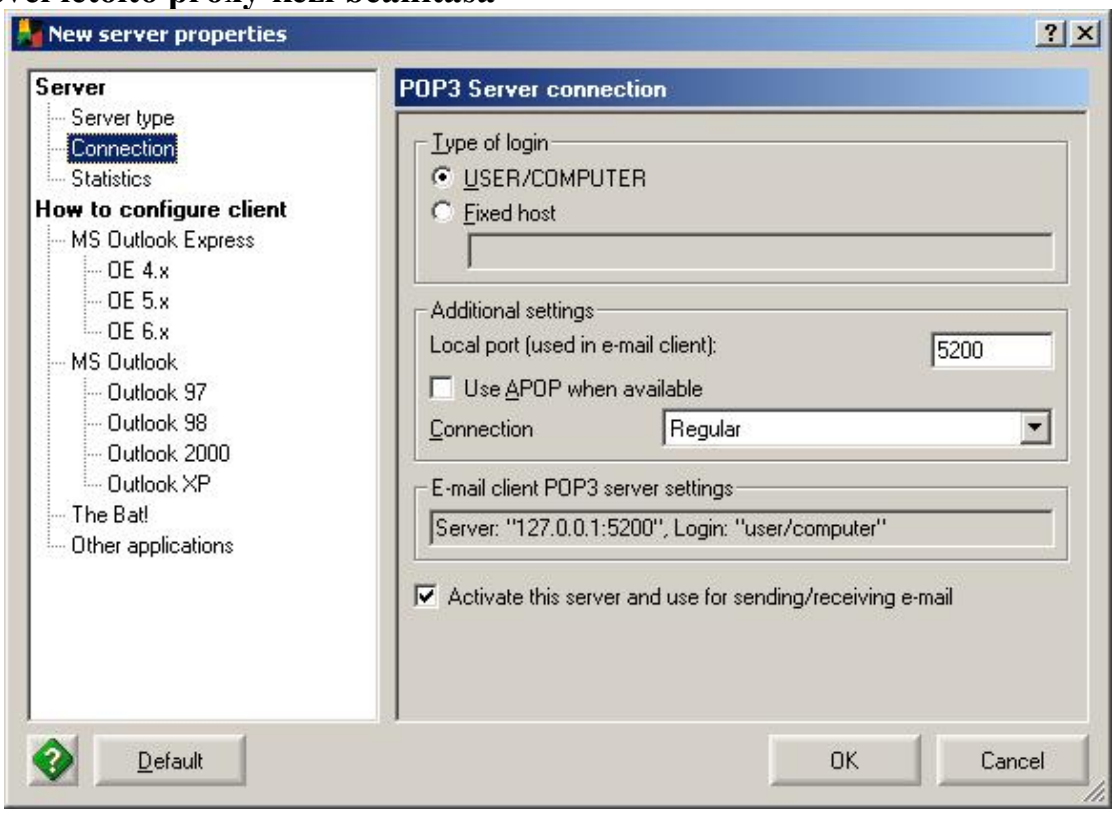
- E-Mail proxy server list – levelező proxy kiszolgálók listája. Itt vannak felsorolva a postafiókokból a levelek letöltésére és küldésére szolgáló, már beállított kiszolgálók.
- Add – Új kiszolgáló hozzáadása
  - Kiszolgáló típus megadása



A megjelenő ablakban beállíthatja kiszolgáló **(Server)** paramétereit. Ezek a következők:

- **Server type** – kiszolgáló típus:
  - **POP3** – levelek letöltésére használatos protokoll
  - **SMTP** – levelek küldésére használatos protokoll
  - **IMAP** (még fejlesztés alatt)
  - **NNTP** (még fejlesztés alatt)

POP3 Levél letöltő proxy kézi beállítása



A **Connection** elemet kiválasztva megadhatja a:

- **Type of login** – A bejelentkezés típusa. Az AVG Anti-vírus kétféle bejelentkezési módot támogat
  - **USER/COMPUTER** – Felhasználó/Számítógép: Ezt a módszert akkor célszerű használni, ha több különböző kiszolgálón is van postafiókja, és mindegyiknek a védelmét szeretné megoldani. Tegyük fel, hogy az Ön kiszolgálójának neve: **mail.cegnev.hu** postafiókjának azonosítója pedig: **kovacs**. Tetszőleges POP3 képességű levelező programjában ezentúl, a felhasználói név helyére, ahová eddig csak a **kovacs** szót írta, ezután a **kovacs/mail.cegnev.hu** kombinációt kell megadnia. Ebből az AVG antivírus levelező proxyja tudni fogja, hogy melyik kiszolgálón és milyen postafiókot kell elérnie. A jelszó megadása a korábbival megegyező.
  - **Fixed host**: Ha csak egyetlen postafiók leveleit szeretné letölteni, akkor legegyszerűbb ezt az opciót kiválasztania és a mezőbe beírni az Ön levelező

kiszolgálójának nevét vagy IP címét. Az előbbi példából kiindulva a **mail.kovacs.hu**-t.

§ **Local port (used in email client) –** A levelező programban a kiszolgálóhoz megadandó kapu száma. Itt azt adhatja meg, hogy a számítógépén futó AVG proxy kiszolgáló melyik kapun fogadja levelező programja kéréseit. Ezt a kapu számot kell majd levelező programjában is beállítania. Itt 0-65535 közötti értékeket adhat meg, amelyekből a számítógép és más programok már bizonyos címeket (jellemzően 1024 alattiakat) lefoglalnak. Az AVG Anti-vírus alapértelmezésben a nagy valószínűséggel szabad 5100-tól kezdődő tartományt használja. Amennyiben az Ön által kiválasztott kapu már foglalt lenne, úgy válasszon másikat és próbálkozzon újra!
Szakembereknek: a foglalt kapuk listája lekérdezhető parancssori ablakot (command prompt) indítva a **netstat –a** parancs kiadásával. Ahol a TCP-vel kezdődő soroknál a helyi címek (local address) oszlopban a kettőspont után következő számok a lefoglalt kapuk sorszámát jeletik.

§ **Use APOP when available –** használjon APOP azonosítást, ha a kiszolgáló támogatja. Speciális, biztonságosabb azonosítási módszer. Alkalmazhatóságáról kérdezze meg rendszergazdáját vagy Internet szolgáltatóját.

§ **Connection** – a proxy szervernek a kiszolgálóhoz való kapcsolódásának módja választható meg itt.

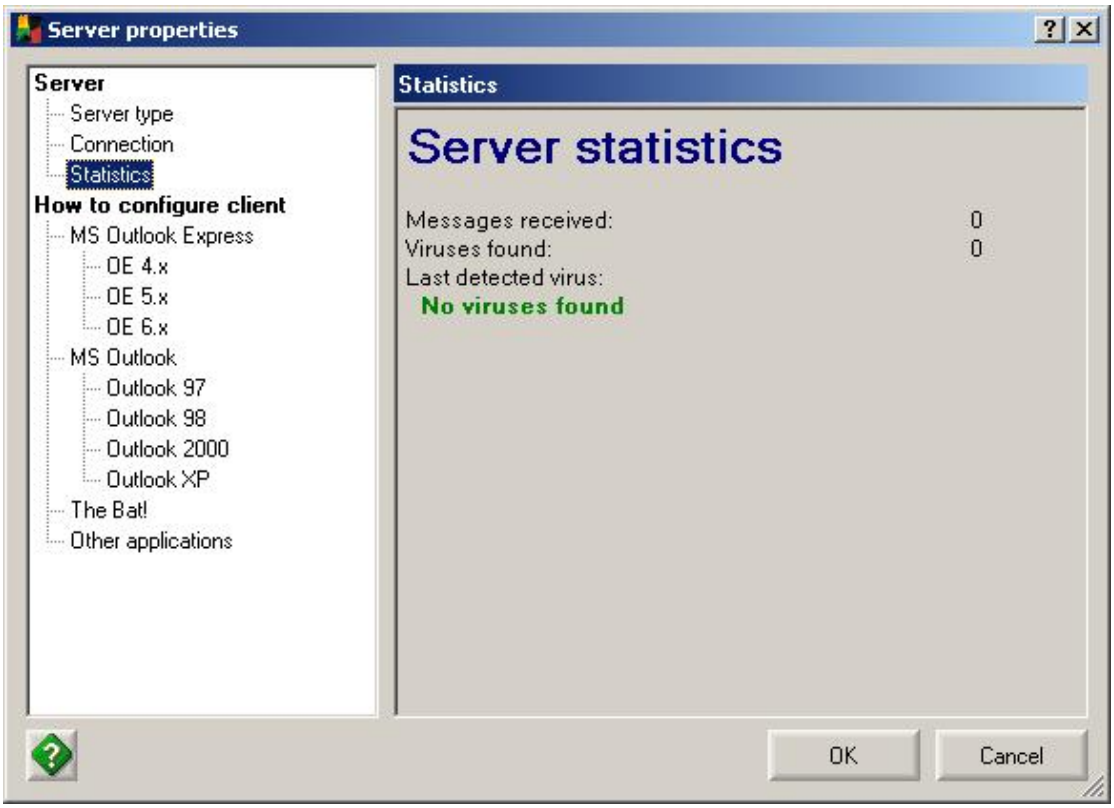
- **Regular** – szokásos (nem titkosított)
- **Secure to dedicated port (TLS)** – Titkosított kapcsolat, külön erre a célra fenntartott (ez a kapu mindig csak titkosított kapcsolatokat fogad) kapura. A módszer lehetővé teszi, hogy számítógépe és a kiszolgáló között titkosított kapcsolat jöjjön létre. Az Ön adatai, beleértve leveleit, azonosítóját és jelszavát, egy igen erősen titkosított csatornán fognak közlekedni a kiszolgáló és a számítógépe között. A kódolás megfejtése olyan nagy számítási kapacitást igényel, hogy a hozzá szükséges technikai háttér legfeljebb a titkosszolgálatok számára érhető el.
- **Secure to regular port (STARTTLS)** – Titkosított kapcsolat, a szokásos kapura. A titkosítatlan kérések is ide érkeznek, de a levelező kiszolgáló támogatja a titkosított kéréseket és a kapcsolat felépítése után kiválasztható az üzemmód. Biztonsága az előzőével megegyező.

§ **E-mail client POP3 server settings** – A pop3 levelező program beállítása. Ebben sorban összefoglalva olvashatja, hogy levelező programját hogyan kell beállítani, hogy az AVG Proxy kiszolgálón keresztül érhesse el postafiókját.
Server (kiszolgáló): 127.0.0.1 *(a saját számítógépnek szabvány szerint mindig ez az IP címe, függetlenül attól, hogy más IP címeken is elérhető (Ethernet, tárcsázó, stb.). A 127.0.0.1-es cím más számítógépről nem érhető el, illetve ott is saját magát*

a számítógépet jelenti) Port (kapu): 5200. Azok a levelező programok, amelyek nem rendelkeznek külön mezővel a kapu megadásához, ott rendszerint a kapu számát is kiszolgáló sorba kell beírni a címtől**:** jellel elválasztva. Pld: 127.0.0.1:5200 .
A sorban ezt követi a felhasználói (postafiók) név, ahogyan a levelező programnak meg kell adni. Korábbi példánkból kiindulva ez most a **kovacs/mail.cegnev.hu** –t jelenti.

§ **Activate this server and use for sending/receiving e-mail –** A négyzetet bejelölve aktiválhatja jelölést törölve, pedig felfüggesztheti az adott proxy működését.

- **Statistics - kimutatások**

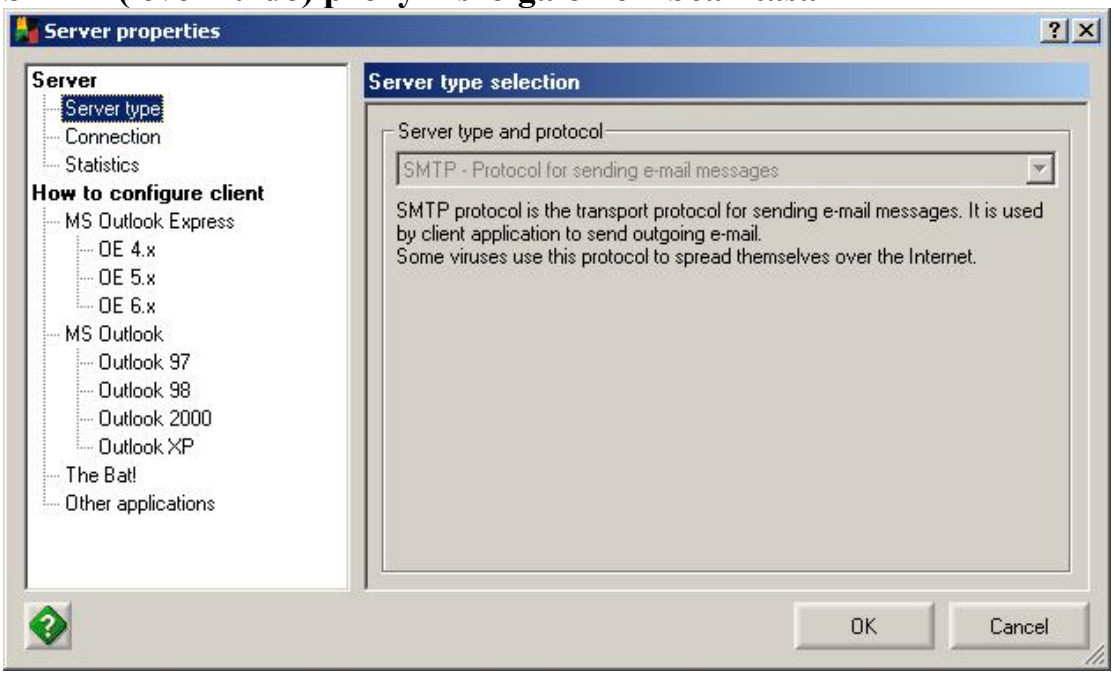


A levél proxy kiszolgáló statisztikai adatai.

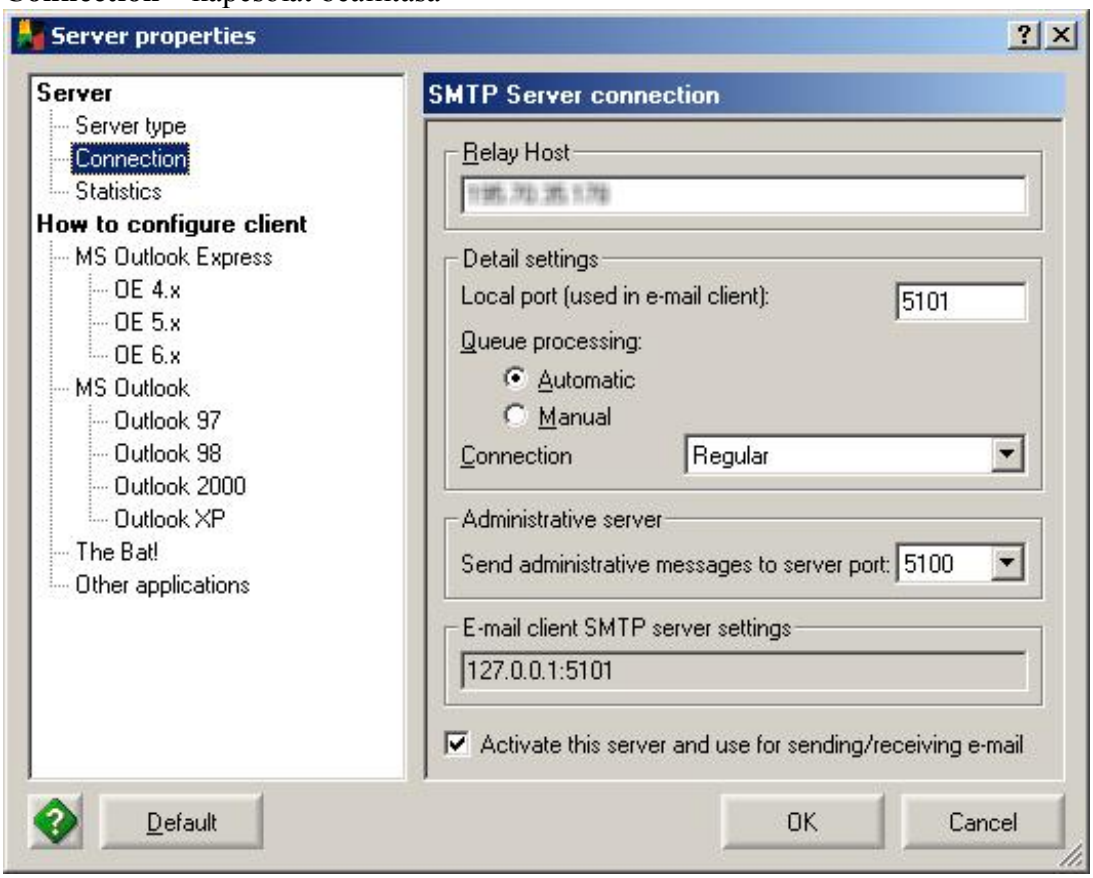
§ **Messages received** –fogadott levelek száma
§ **Viruses found** – elfogott vírusok száma
§ **Last detected virus** – a legutoljára elfogott vírus
A **No viruses found** üzenet azt jelzi, hogy eddig nem volt fertőzött levél.

- **How to configure client** – levelező programok beállítása. Ez a rész röviden ismét összefoglalja az általunk az imént részletesen tárgyalt beállításokat.

SMTP (levél küldő) proxy kiszolgáló kézi beállítása



- **Server type** – itt az SMTP – Protocol for sending e-mail messages (levél küldéshez szükséges protokoll) lehetőséget kell kiválasztani.
- **Connection** – kapcsolat beállítása



§ **Relay host** – Továbbító állomás. Itt kell megadni, hogy a küldött leveleket hová, melyik SMTP kiszolgálóra kell továbbítani. A mezőbe a levelező kiszolgáló nevét vagy IP

címét kell megadni. Azt az értéket kell ide beírni, amelyet a levelező programja SMTP kiszolgáló mezőjébe írt be.

§ **Local port (used in email client) –** A levelező programban a levélküldő (SMTP) kiszolgálóhoz megadandó kapu száma. Itt azt adhatja meg, hogy a számítógépén futó AVG proxy kiszolgáló melyik kapun fogadja levelező programja kéréseit. Ezt a kapu számot kell majd levelező programjában is beállítania. Itt 0-65535 közötti értékeket adhat meg, amelyekből a számítógép és más programok már bizonyos címeket (jellemzően 1024 alattiakat) lefoglalnak. Az AVG Anti-vírus alapértelmezésben a nagy valószínűséggel szabad 5100-tól kezdődő tartományt használja. Amennyiben az Ön által kiválasztott kapu már foglalt lenne, úgy válasszon másikat és próbálkozzon újra!
Szakembereknek: a foglalt kapuk listája lekérdezhető parancssori ablakot (command prompt) indítva a **netstat –a** parancs kiadásával. Ahol a TCP-vel kezdődő soroknál a helyi címek (local address) oszlopban a kettőspont után következő számok a lefoglalt kapuk sorszámát jelentik.

§ **Queue processing** – várakozó levelek feldolgozása
- **Automatikus** – automatikus, levélküldés után a proxy kiszolgáló automatikusan ellenőrzi és átadja a leveleket a továbbító állomás felé
- **Manual** – kézi feldolgozás. A proxy kiszolgáló a feldolgozást elindító parancsig csak gyűjti az elküldött leveleket.

§ **Connection** – a proxy szervernek a kiszolgálóhoz való kapcsolódásának módja választható meg itt.
- **Regular** – szokásos (nem titkosított)
- **Secure to dedicated port (TLS)** – Titkosított kapcsolat, külön erre a célra fenntartott (ez a kapu mindig csak titkosított kapcsolatokat fogad) kapura. A módszer lehetővé teszi, hogy számítógépe és a kiszolgáló között titkosított kapcsolat jöjjön létre. Az Ön adatai, beleértve leveleit, azonosítóját és jelszavát, egy igen erősen titkosított csatornán fognak közlekedni a kiszolgáló és a számítógépe között. A kódolás megfejtése olyan nagy számítási kapacitást igényel, hogy a hozzá szükséges technikai háttér legfeljebb a titkosszolgálatok számára érhető el.

§ **Secure to regular port (STARTTLS)** – Titkosított kapcsolat, a szokásos kapura. A titkosítatlan kérések is ide érkeznek, de a levelező kiszolgáló támogatja, a titkosított kéréseket és a kapcsolat felépítése után kiválasztható az üzemmód. Biztonsága az előzőével megegyező.

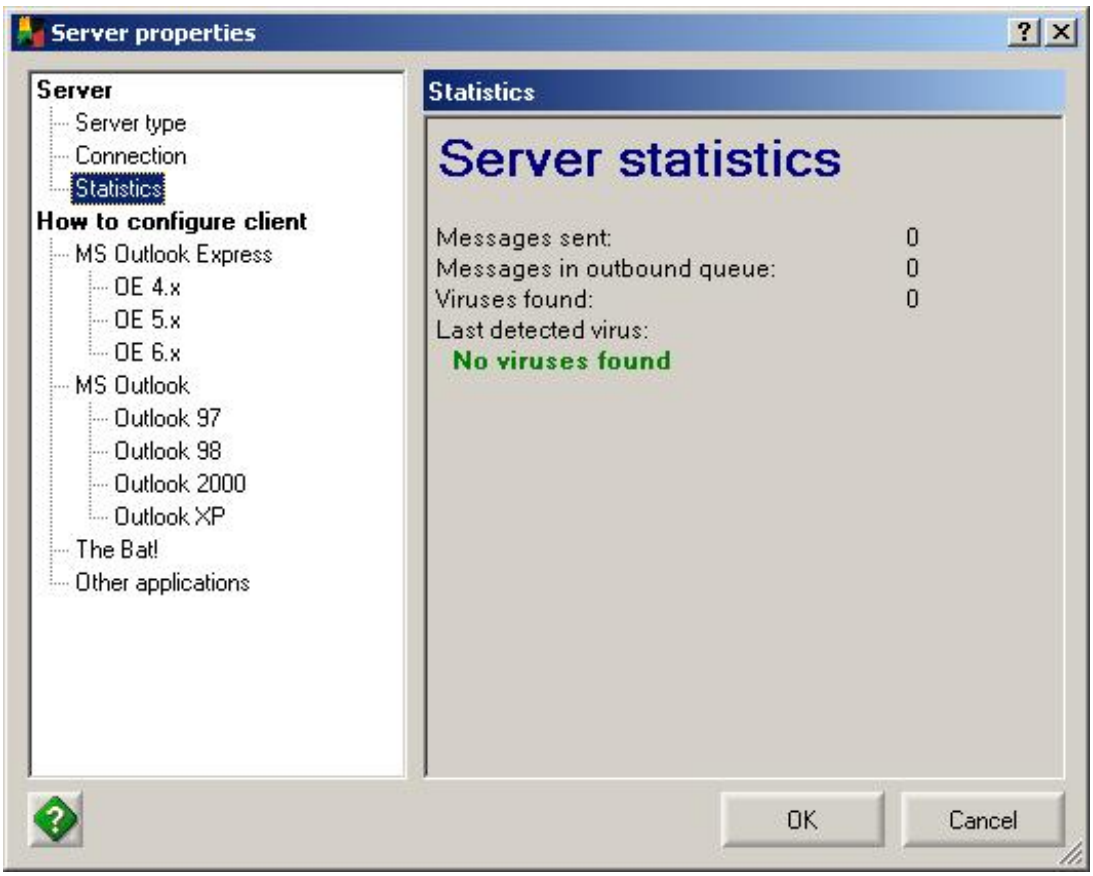
§ **Send administrative messages to server port** – A rendszerüzeneteket küldje a .....kapura. Ha az AVG Anti-vírus vírust talált vagy egyéb információt kíván küldeni Önnek, akkor ezt a kaput használja. Itt a POP3 (a korábban leírt bejövő levél ellenőrző) proxy kapuját célszerű megadnia, így az AVG

Anti-vírus üzenetei az Ön postafiókjába érkezett levélként fognak megjelenni.

§ **E-mail client SMTP server settings** – Az SMTP levelező program beállítása. Ebben sorban összefoglalva olvashatja, hogy levelező programját hogyan kell beállítani, hogy az AVG Proxy kiszolgálón keresztül küldhesse el leveleit.
Server (kiszolgáló): 127.0.0.1 *(a saját számítógépnek szabvány szerint mindig ez az IP címe, függetlenül attól, hogy más IP címeken is elérhető (Ethernet, tárcsázó, stb.). A 127.0.0.1-es cím más számítógépről nem érhető el, illetve ott is saját magát a számítógépet jelenti)* Port (kapu): 5101. Azok a levelező programok, amelyek nem rendelkeznek külön mezővel a kapu megadásához, ott rendszerint a kapu számát is az SMTP kiszolgáló sorba kell beírni a címtől**:** jellel elválasztva. Pld: 127.0.0.1:5101 .
A sorban ezt követi a felhasználói (postafiók) név, ahogyan a levelező programnak meg kell adni. Korábbi példánkból kiindulva ez most a **kovacs/mail.cegnev.hu** –t jelenti.

§ **Activate this server and use for sending/receiving e-mail** – A négyzetet bejelölve engedélyezheti a jelölést törölve, pedig felfüggesztheti az adott proxy működését.

- **Statistics** – kimutatások. Az elküldött levél ellenőr munkájának adatait/kimutatásait tartalmazza



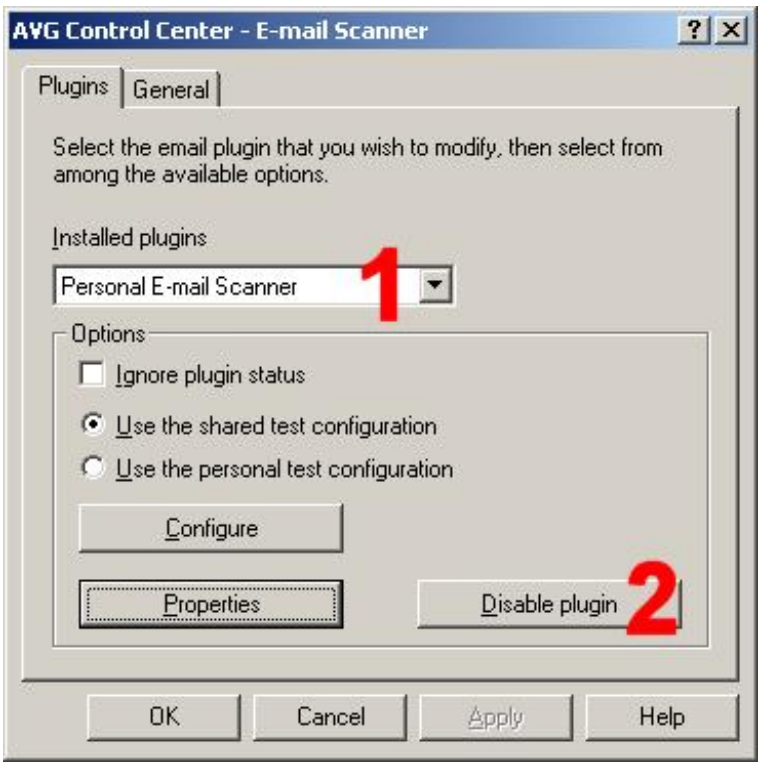
§ **Message sent** – a elküldött levelek száma
§ **Messages in outbound queue** – elküldésre váró levelek száma
§ **Virus found** – elfogott vírusok száma

§ **Last detected virus** – Az utoljára elfogott vírus neve
A **No viruses found** üzenet azt jelzi, hogy eddig nem volt fertőzött levél

- **How to configure client** – levelező programok beállítása. Ez a rész röviden ismét összefoglalja az általunk az imént részletesen tárgyalt beállításokat.

- **Delete** – Kiszolgáló törlése
- **Modify** – Kiszolgáló módosítása
- **Wizard** – Varázsló indítása (ld. automatikus beállítás)
- **Highlighted server properties** – az **E-Mail proxy server list** mezőben kiválasztott beállítás részletei.
- **OK** – a változtatások jóváhagyás
- **Cancel** – a változtatások elvetése

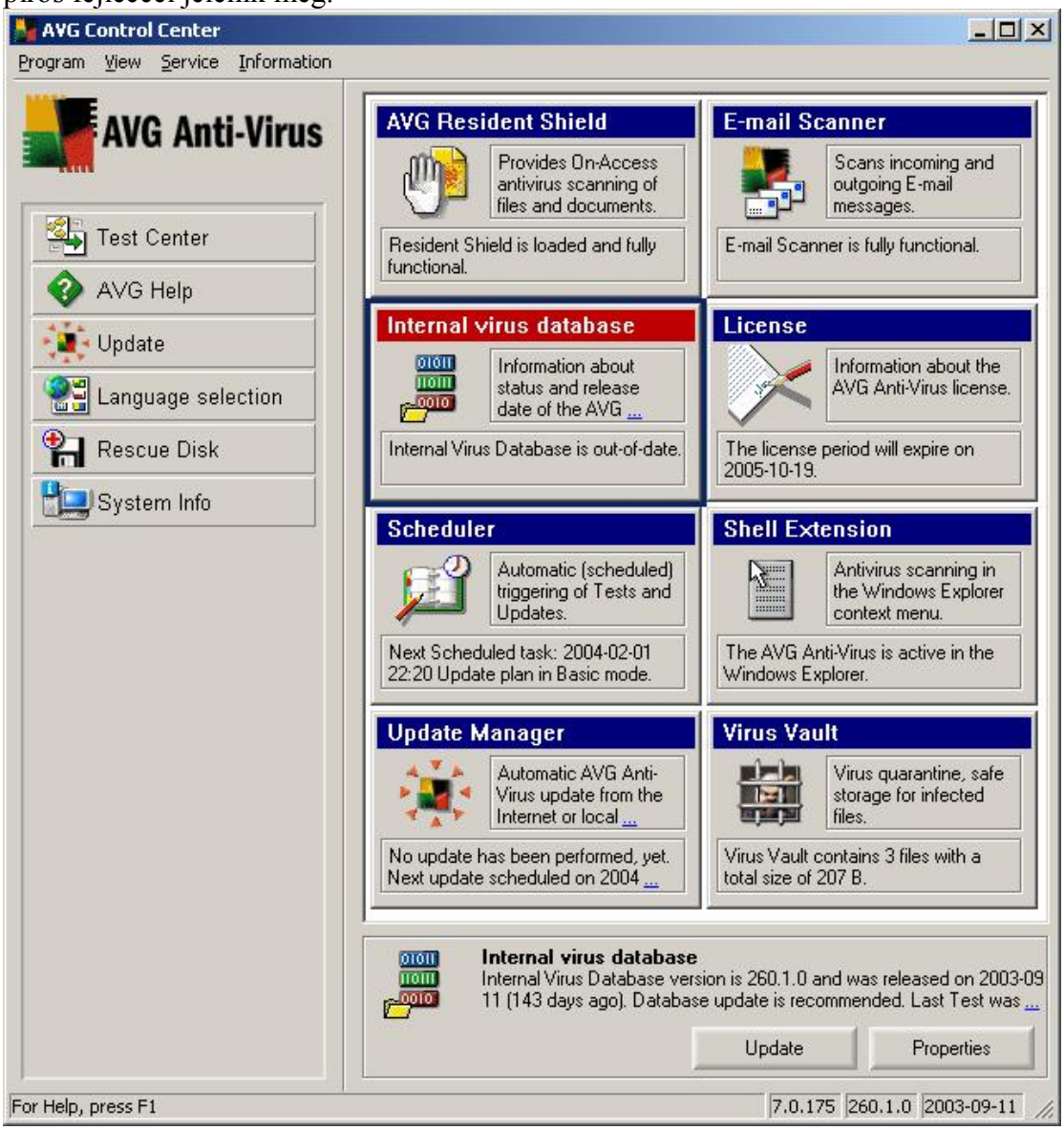
Levél ellenőrző modul letiltása



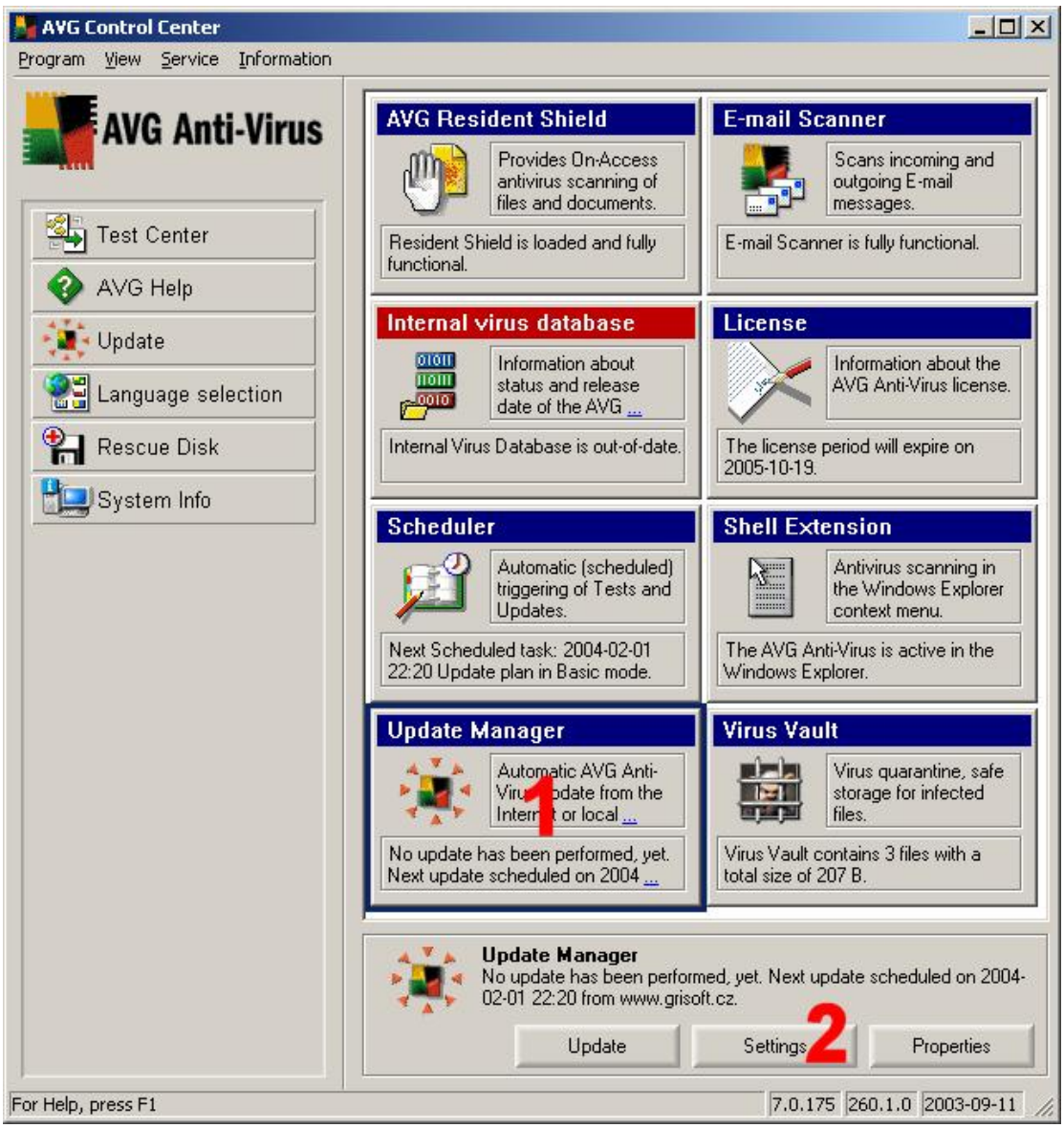
Amennyiben egyáltalán nem szeretné a **Personal E-mail Scanner-t (személyes levél ellenőrző)** használni, úgy a modul működése a modul kiválasztása [1], majd a **Disable plugin (modul letiltása)** [2] gombra kattintva a modul működése letiltható.
Figyelem! Ha korábban használta a funkciót és most letiltja, akkor az Ön által használt levelező program beállításait vissza kell állítania az AVG telepítése előtti állapotra!

A vírus adatbázis frissítése.

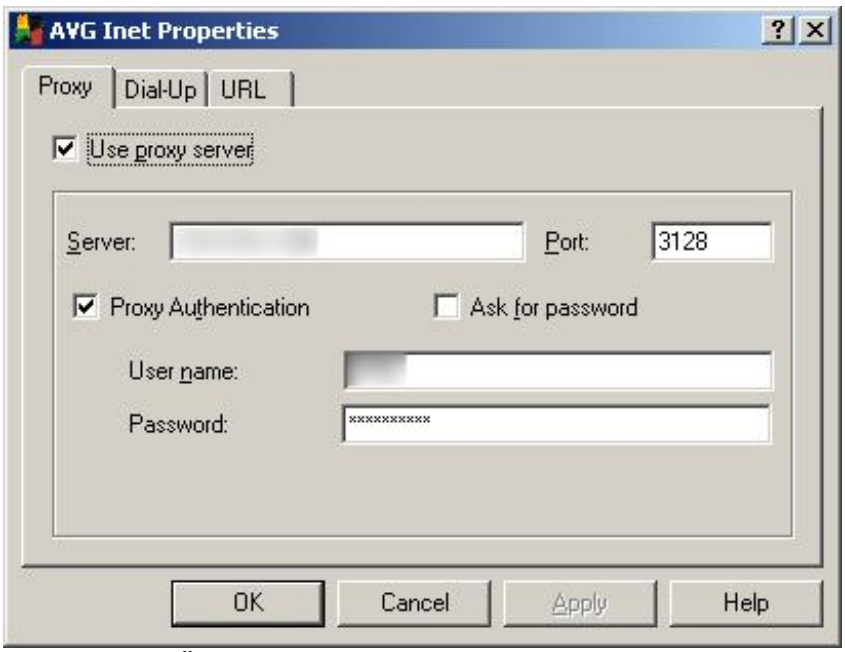
Ahhoz, hogy az AVG Anti-vírus a lehető legnagyobb biztonságot nyújtsa, időnként szükség van a vírus adatbázis frissítésére. Ha ezt hosszabb időn keresztül elmulasztja, akkor az AVG figyelmezteti Önt erre. A tálcán lévő AVG Anti-vírus ikon feketére vált, az Vezérlő központ **Internal virus database (belső vírus adatbázis)** cellája piros fejléccel jelenik meg.



A víruskereső programok hatékonyságának alapvető eleme, hogy mindig naprakészen tartsuk vírus és program adatbázisainkat. Ezért a telepítés után az első lépésként mindig ellenőrizze, hogy áll-e rendelkezésre újabb frissítés. Amennyiben Ön a legfrissebb verziót most töltötte le honlapunkról, úgy valószínűleg nem lesz ilyen, de amennyiben a telepítést CD-ROM-ról végezte, amely a programnak és a vírus adatbázisnak egy korábbi változatát tartalmazza, úgy ez a lépés nagyon fontos.



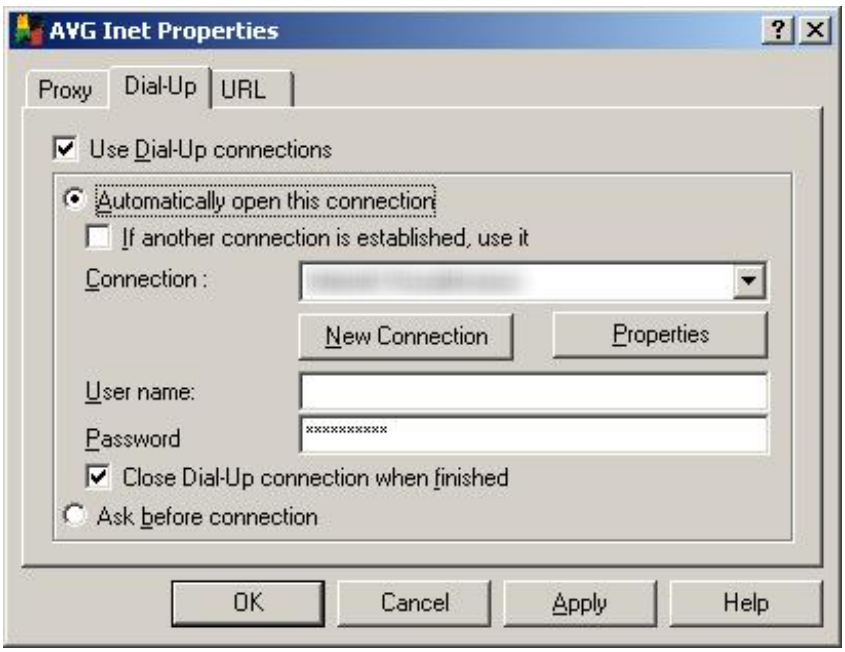
Először végezze el a frissítés hálózati beállításait az **Update Manager** cellára, majd az ablak alján található **Settings** gombra kattintva.



Amennyiben Ön nem használ proxy (web, http) szervert és/vagy tűzfalat, akkor az összes mezőt és jelölő négyzetet hagyja üresen. Amennyiben használ ilyet, úgy kérjük adja meg az alábbi adatokat az alábbi módon. A mezőkbe írandó adatokról rendszergazdájától vagy Internet Szolgáltatójától tájékozódhat.

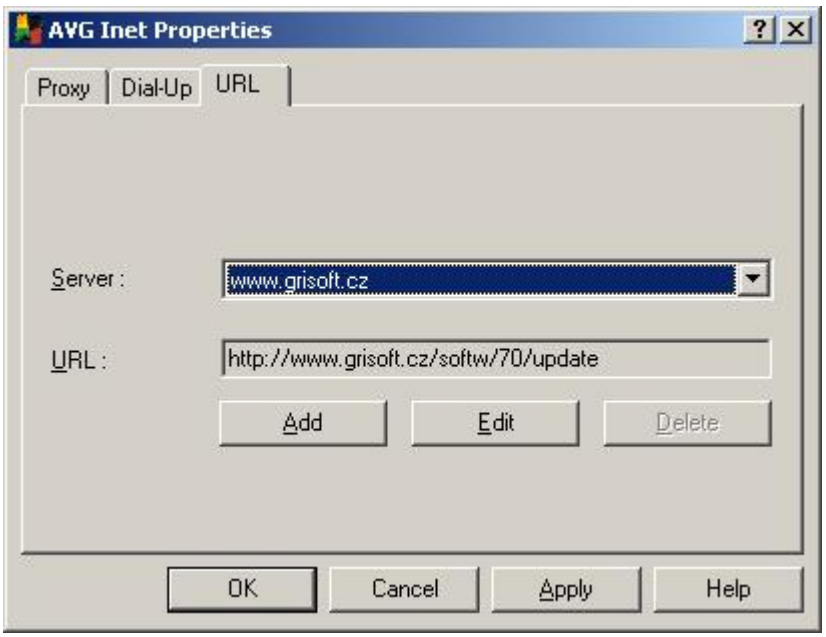
- **Use proxy server:** Jelölje be a négyzetet, ha használ proxy szervert.
- **Server:** A proxy szerver Neve vagy IP címe
- **Port:** A proxy szerver kapujának száma
- **Proxy Authentication:** jelölje meg a négyzetet, ha a proxy szerver azonosítást (felhasználói név és jelszó) kér.
- **User name:** Az Ön felhasználói neve a proxy szerverhez
- **Password:** Az ön jelszava a proxy szerverhez. Figyelem! Az itt megadott adatokat az AVG lementi!
- **Ask for password:** A mezőt akkor jelölje be, ha nem szeretné a proxy szerverre szóló jelszavát lementeni, hanem azt kívánja, hogy minden frissítés előtt az AVG kérdezzen rá.

Figyelem! A proxy szerver helytelen beállítása esetén a Proxy szerveren tárolt adatok nem/lassan évülnek el. Ez azt okozhatja, hogy a frissítéseket késve vagy nem tudja letölteni. Ha proxy szerveren keresztül használ frissítés igényes alkalmazásokat, mint például az AVG Anti-vírust, kérjük, hogy **minden esetben tájékoztassa a rendszergazdát,** hogy az AVG Anti-vírus frissítéseinek letöltéséhez megfelelő proxy szabályokat alkalmazzon. A frissítéseket szolgáltató szervereink a proxy szerverek részére minden esetben továbbítják az elévülésre vonatkozó információkat, ezt azonban főleg régebbi kiadású proxy szerverek nem mindig kezelik automatikusan, illetve ez ki is tiltható rajtuk.



Az ablak **Dial-Up** fülében állíthatja be az Internet kapcsolat adatait, amennyiben Önnek hagyományos modemes vagy ISDN Internet kapcsolata van a gépén. Ha Ön nem kíván Internet kapcsolatot felépíteni csak az AVG Anti-vírus frissítése kedvéért, akkor ezt az ablakot nem kell használnia. Ebben az esetben az a frissítést elvégezheti akkor is ha egyébként is (pld web böngészés miatt) Internet kapcsolatot épít fel. Ilyenkor nem kell használnia ezeket a funkciókat. (**Javasolt megoldás!**)
Amennyiben mégis szeretne tárcsázásos kapcsolatot felépíteni, úgy az ablak paramétereit az alábbi módon állíthatja be:

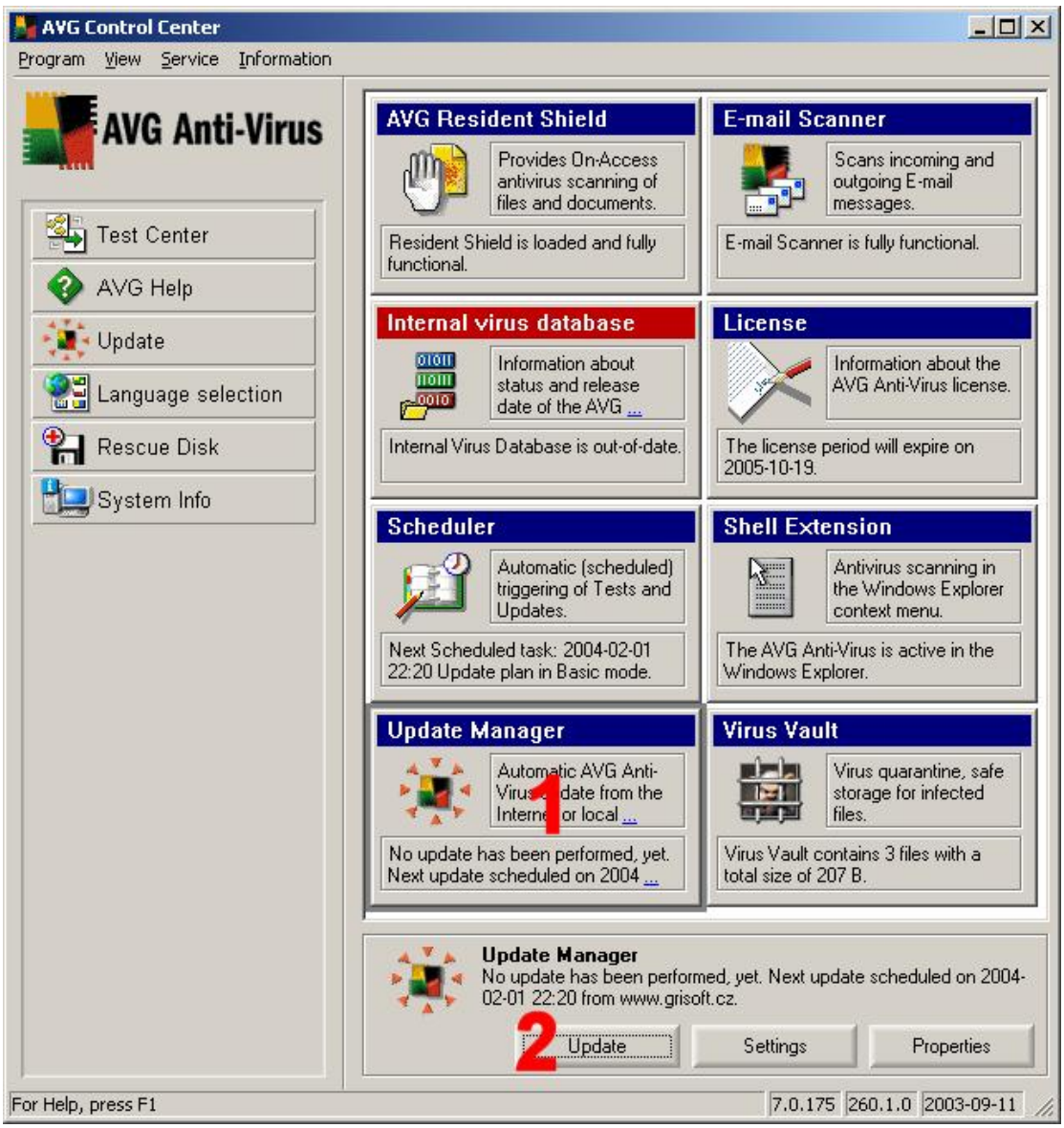
- **Use Dial-Up connections**: tárcsázásos kapcsolatok engedélyezése
- **Automatically open this connection**: Automatikus tárcsázás szükség esetén
- **Connection**: A tárcsázási profil kiválasztása a tárcsázó beállításoknál létrehozottak közül
- **New Connection**: Új tárcsázási profil létrehozása
- **Properties**: A tárcsázási beállítás módosítása
- **Username**: A tárcsázásnál használandó felhasználói név
- **Password**: A tárcsázásnál használandó jelszó
- **Close Dial-Up connection when finished**: Jelölje be a négyzetet, ha szeretné, hogy frissítés után megszakítsa a telefonos kapcsolatot. Ennek az opciónak a használata azt okozhatja, hogy ha az egyéb pld. Böngésző funkciót is elindított miközben a frissítéseket töltötte le, úgy az a funkció is megszakad a frissítés befejeződése után. Amennyiben Ön automatikus tárcsázást engedélyez, de ezt a jelölőnégyzetet nem választja ki, úgy a vonalbontás elmaradása komoly telefonszámlát okozhat.
- **Ask before connection**: Itt nem használ automatikus tárcsázást. A frissítés megkezdése előtt az AVG Anti-vírus megkérdezi Önt, hogy akarja-e a telefonos kapcsolaton keresztüli frissítést és mely beállításokkal.



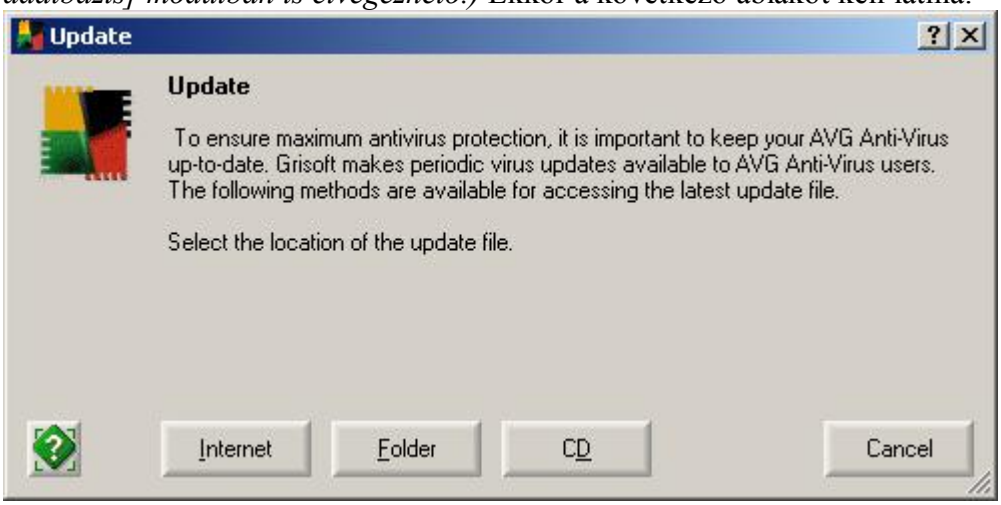
Az URL fülre kattintva megadhatja, hogy a frissítések listáját honnan töltse le a program. Az (földrajzi területenként esetleg eltérő) alapbeállítás megfelelő. Akkor lehet szükség ettől elérő szerver beállítására, ha Ön például vállalati környezetben saját frissítő szervert (Egy szokásos webszerveren) telepít és így nem kell minden gépüknek külön letöltenie a frissítést. Ezzel csökkentik saját Internet kapcsolatuk továbbá a Grisoft szervereinek a terheltségét.
Megjegyzés: *Vállalati környezetben javasoljuk az AVG Anti-vírus Hálózati változatát. Annak funkcionalitása mind a beállítások, mind pedig csoportos a frissítés terén többet kínál ennél a megoldásnál!*

Amennyiben végzett a beállításokkal, kérjük, hogy az ablakot zárja be az **OK** gombbal.

Ha minden adatot helyesen adott meg, akkor próbálkozzon meg a frissítéssel. Példánkban feltételezzük a fennálló (állandó vagy már tárcsázott) Internet kapcsolatot. A frissítés szintén elvégezhető kézi indítással vagy pedig automatikus módon. Most következő példánkban a kézi frissítést mutatjuk be.



Végezze el a frissítést először az **Update Manager** cellára, majd az ablak alján található **Update** gombra kattintva *(Ez az Internal virus database [belső vírus adatbázis] modulban is elvégezhető.)* Ekkor a következő ablakot kell látnia:

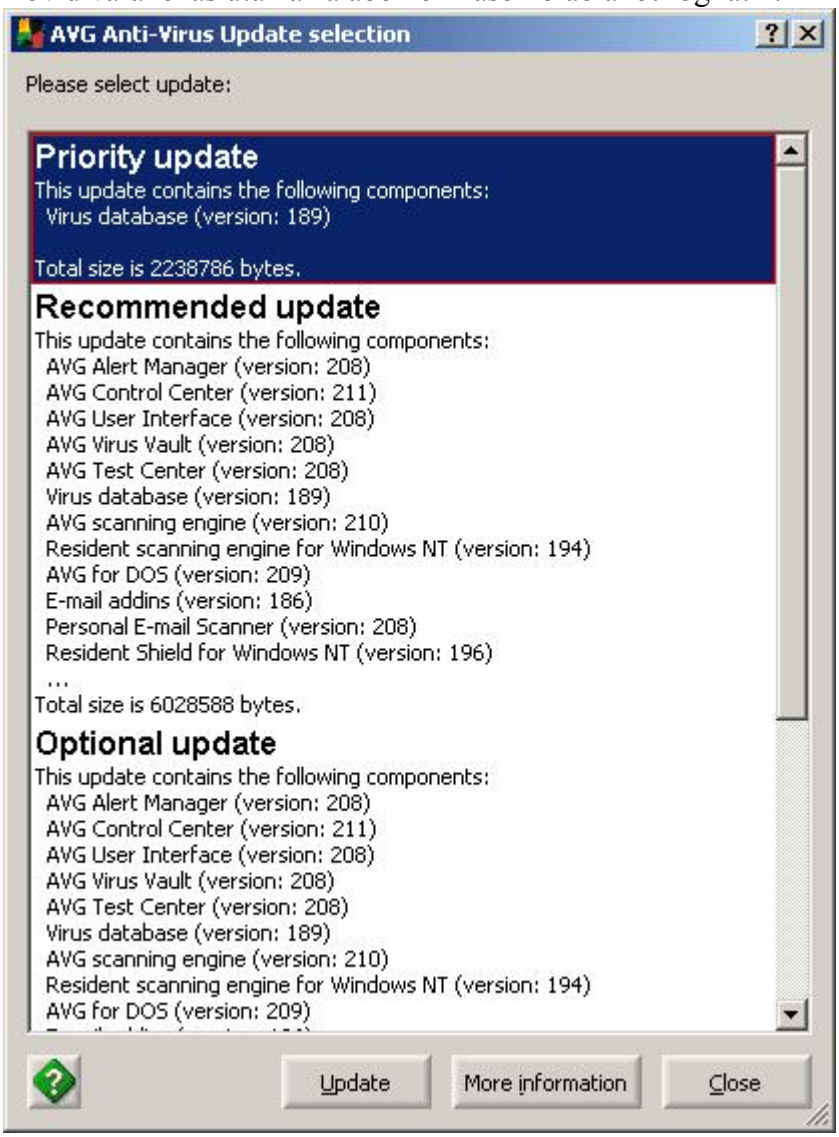


A frissítésre háromféle lehetőség áll a rendelkezésére:

Internet: Az Interneten keresztül a Grisoft-tól vagy az Ön által a beállításoknál meghatározott helyről töltheti le a frissítéseket.
Folder: Könyvtárból (lehet hálózati megosztás is) végzi el a frissítést
CD: AVG Anti-vírus frissítő CD-ROM-ot használ (nem javasolt)

Jelen esetben az **Internet** gombot válassza ki.

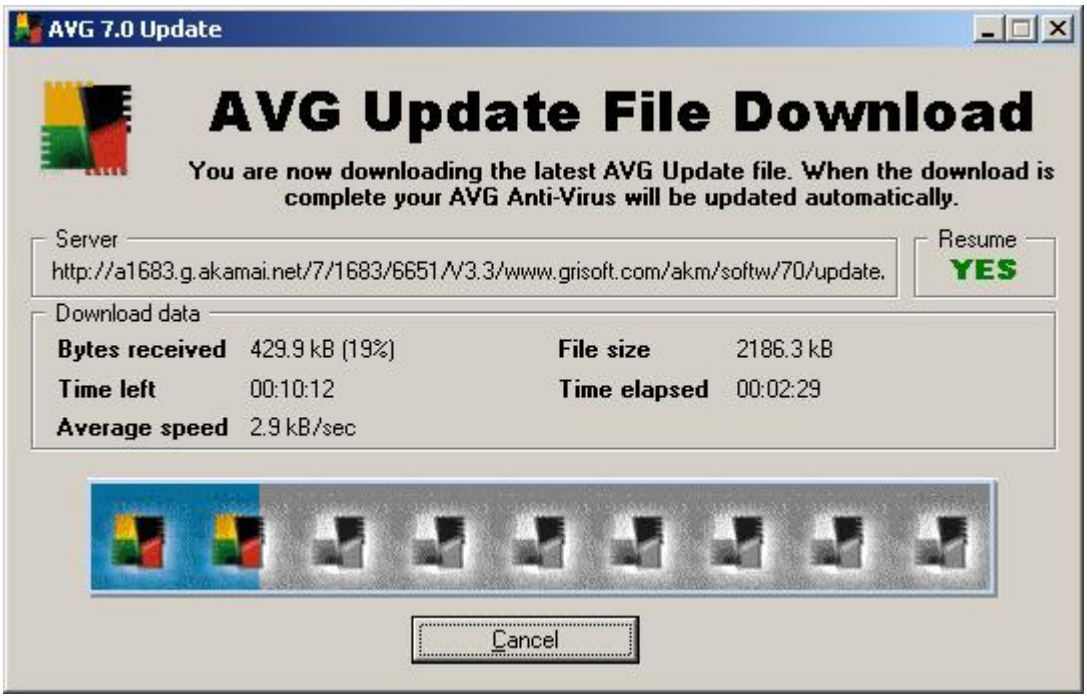
Rövid várakozás után az alábbihoz hasonló ablakot fog látni.



A frissítések lehetnek **Kötelezőek (Priority)**, **Ajánlottak (Recommended)** és **Választhatóak (Optional).** A **kötelező** frissítéseket mindenképpen célszerű letölteni! Olyan programmódosításokat és adatbázis frissítéseket tartalmaz, amelyek szükségesek az AVG Anti-vírus hatékony és biztonságos működéséhez. Az **ajánlott** frissítések tartalma olyan változtatásokat tartalmaz, amelyek átmenetileg ugyan elhagyhatók, de a Grisoft semmiképpen sem javasolja azok mellőzését, ugyanis e nélkül nem kap teljes körű védelmet. A frissítés elmaradása a megelőző funkciók hatékonyságának csorbulását okozhatja. Az **opcionális** frissítések csak, biztonsági szempontból kevésbé/nem jelentős változtatásokat tartalmaznak tartalmuk jellemzően kényelmi, kezelő felületi funkciókat tartalmaz, így letöltésük **átmenetileg** elhagyható.
Figyelem: *A frissítések mérete a fent láthatónál lényegesen kevesebb. Jellemzően néhány 10 kByte. A példában látható nagyméretű frissítések oka a szemléltetés ezért a*

telepítést egy régi alapverzióval mutatjuk be, amely elavultsága miatt sok frissítést igényel és mindhárom (Kötelező, Ajánlott és Választható) frissítés típus megjelenik.
A frissítés kiválasztása után válassza az **Update** gombot. Ekkor a kiválasztott frissítés letöltése, majd telepítése megkezdődik.

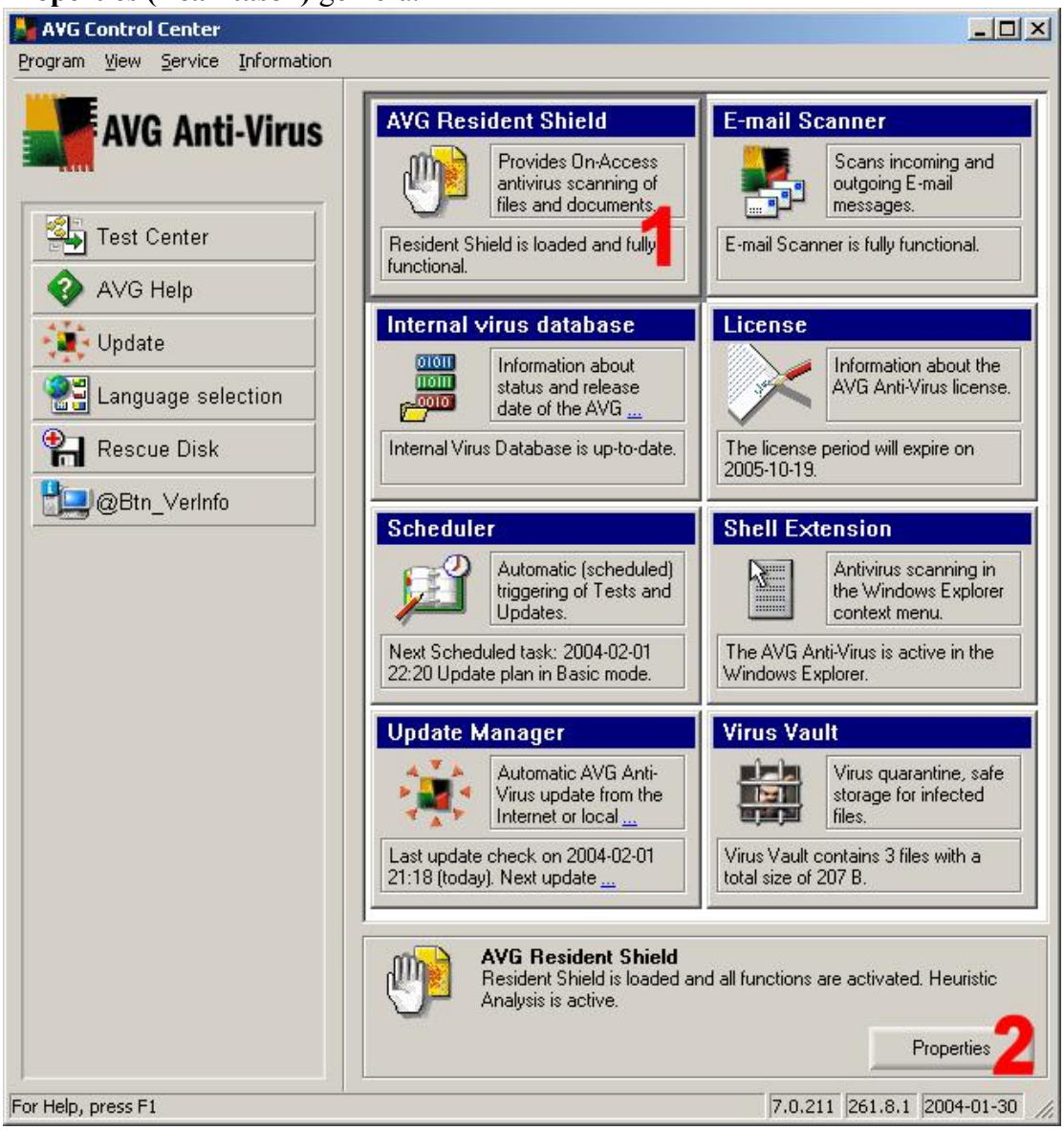
A letöltés alatt az alábbi ablakot kell látnia:



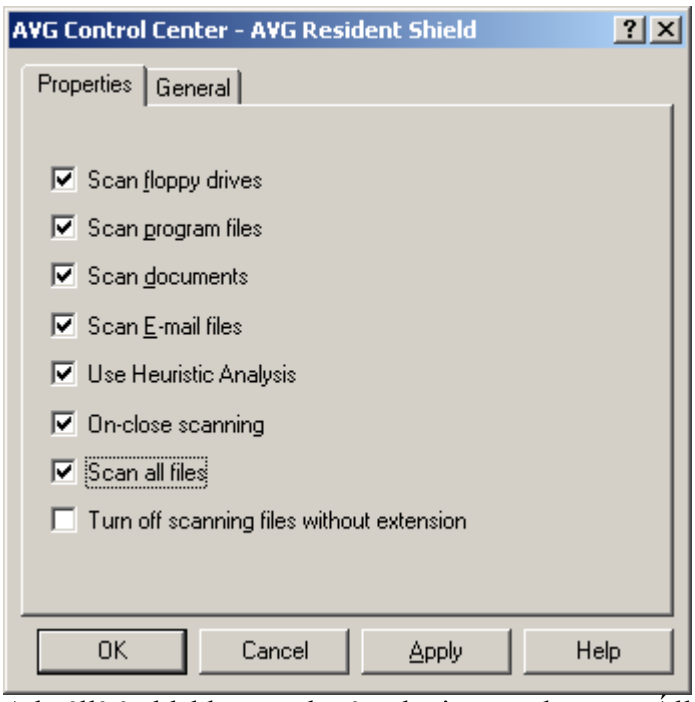
A kék sáv előrehaladása jelzi a letöltés állapotát. A letöltést bármikor megszakíthatja a **Cancel** gomb segítségével. A Resume: **YES** mező azt jelzi, hogy a letöltés megszakadása esetén nem kell a frissítést elölről kezdenie, hanem az a megszakítás/megszakadás helyétől folytatható. Ez alól kivétel, ha a letöltés megszakítása és az újbóli elindítása között eltelt időben új frissítés jelent meg. Az új frissítés lehet olyan, amely részben letöltöttnél bővebb funkcionalitást biztosít és a korábbi frissítés letöltése feleslegessé válik. Ebben az esetben a frissítés folytatódhat az újabb frissítés elkezdésével is. *Megszakított, majd újra kezdett frissítés után célszerű egy ismételt frissítést elindítani, hogy meggyőződhessen arról, hogy minden szükséges frissítést letöltött.*

Az állandó védelem (Resident Shield) beállítása

A vezérlő központban válassza ki a **Resident Shield** cellát, majd kattintson a **Properties (Beállítások)** gombra.



Ez után a következő ablakot kell látnia:

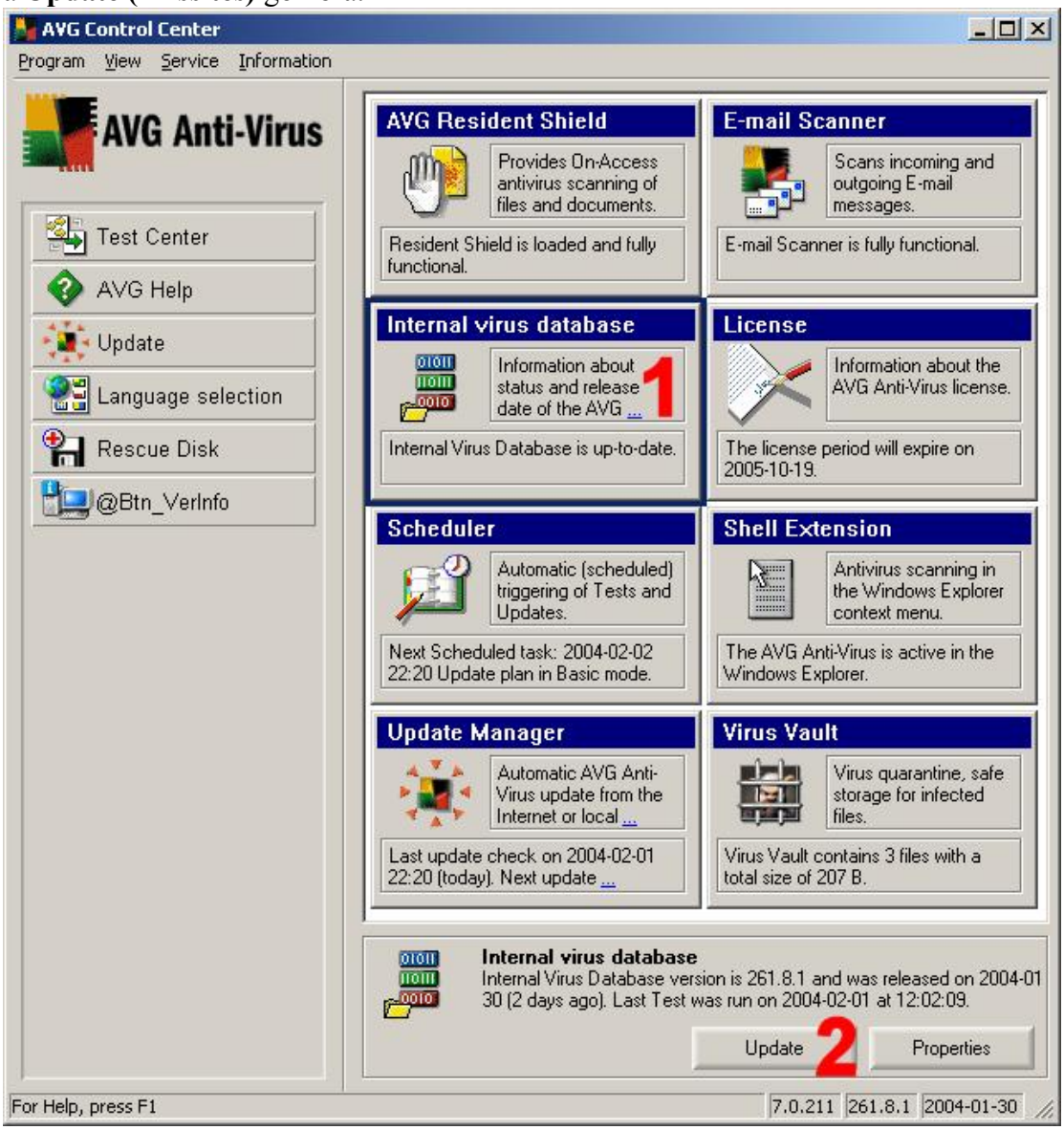


A beállító ablakban azt határozhatja meg, hogy az Állandó Védelem milyen esetekben végezzen vizsgálatot. A fenti példában egy meglehetősen szigorú beállítás látható.
A választható opciók:

- **Scan floppy drives** – A hajlkony lemezes meghajtók ellenőrzése (általában A: és/vagy B:)
- **Scan program files** – A futtatható állományok (programok) ellenőrzése
- **Scan documents** – Dokumentumok, táblázatok, adatállományok ellenőrzése
- **Scan E-mail files** – Elektronikus leveleket tartalmazó állományok ellenőrzése
- **Use Heuristic Analaysis** – Részletes keresés (működés szimuláció) használata
- **On-close scanning** – A fájlokat nem csak megnyitáskor, hanem lezáráskor is ellenőrzi. Arra az esetre, ha használat közben a memóriában fertőződött volna.
- **Scan all files** – minden fájlt ellenőrizzen, ne csak azokat, amelyekben potencálisan vírushordozók lehetnek.
- **Turn off scanning files without extension** – Ne ellenőrizze azokat a fájlokat, amelyeknek nincs kiterjesztése.

Vírus adatbázis (Internal Vírus Database) frissítése

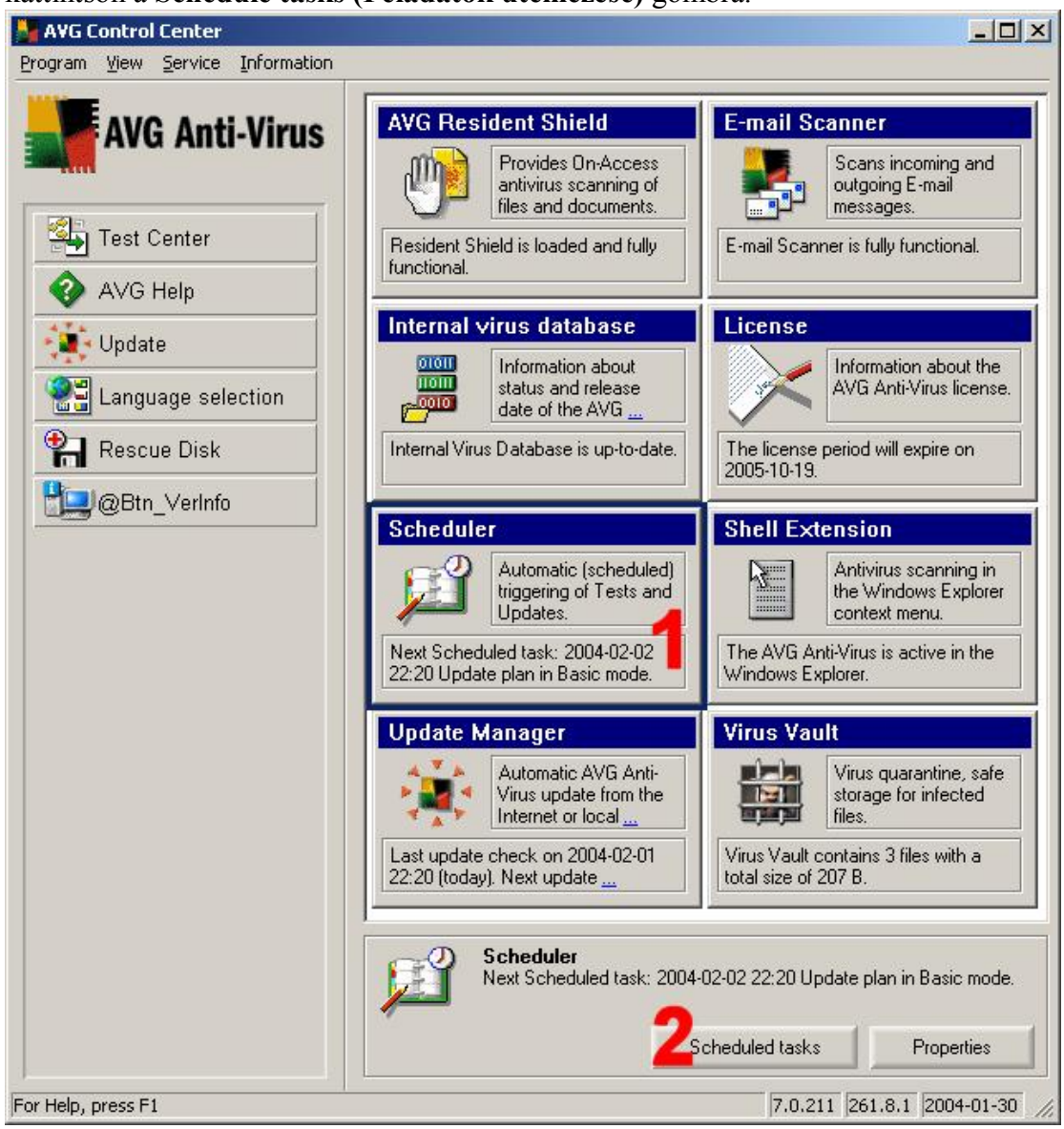
A vezérlő központban válassza ki az **Internal Virus Database** cellát, majd kattintson a **Update (Frissítés)** gombra.



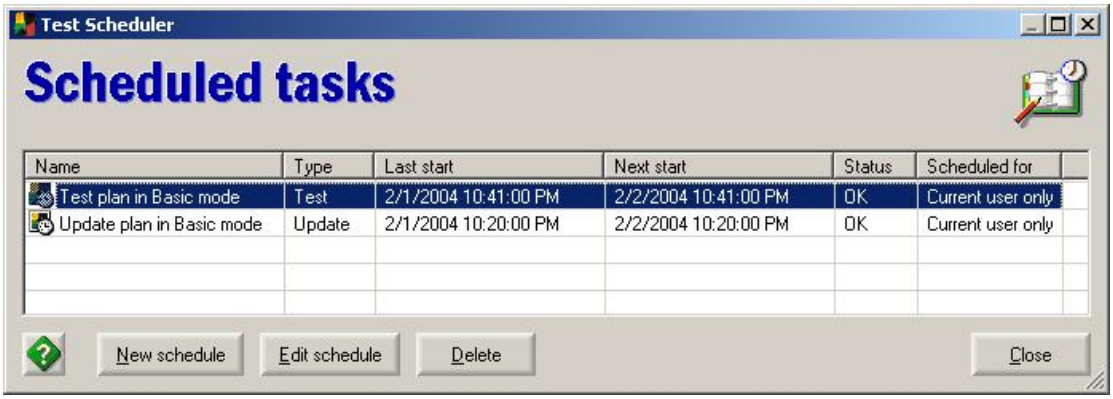
A frissítés menete megegyezik az Update Manager (Frissítés kezelő) Update (Frissítés) funkciójának leírásával. A részletekért kérjük, hogy olvassa el a Frissítés kezelőről szóló részt!

Feladat ütemező (Scheduler)

Ennek a funkciónak a segítségével bizonyos feladatokat, mint a frissítés vagy tesztek futtatása meghatározott időpontban ütemezetten elvégezhet. Természetesen a feladat a meghatározott időpontban csak akkor hajtódik végre, ha akkor a számítógép be van kapcsolva. Amennyiben az időpontot valami miatt elmulasztja (például kikapcsolt számítógép) úgy ha másképpen nem rendelkezik, akkor az elmulasztott ütemezett feladat az első adandó alkalommal végre fog hajtódni.
A beállítások elvégzéséhez a vezérlő központban válassza ki a **Scheduler** cellát, majd kattintson a **Schedule tasks (Feladatok ütemezése)** gombra.



Ezt követően a következő ablakot kell látnia:

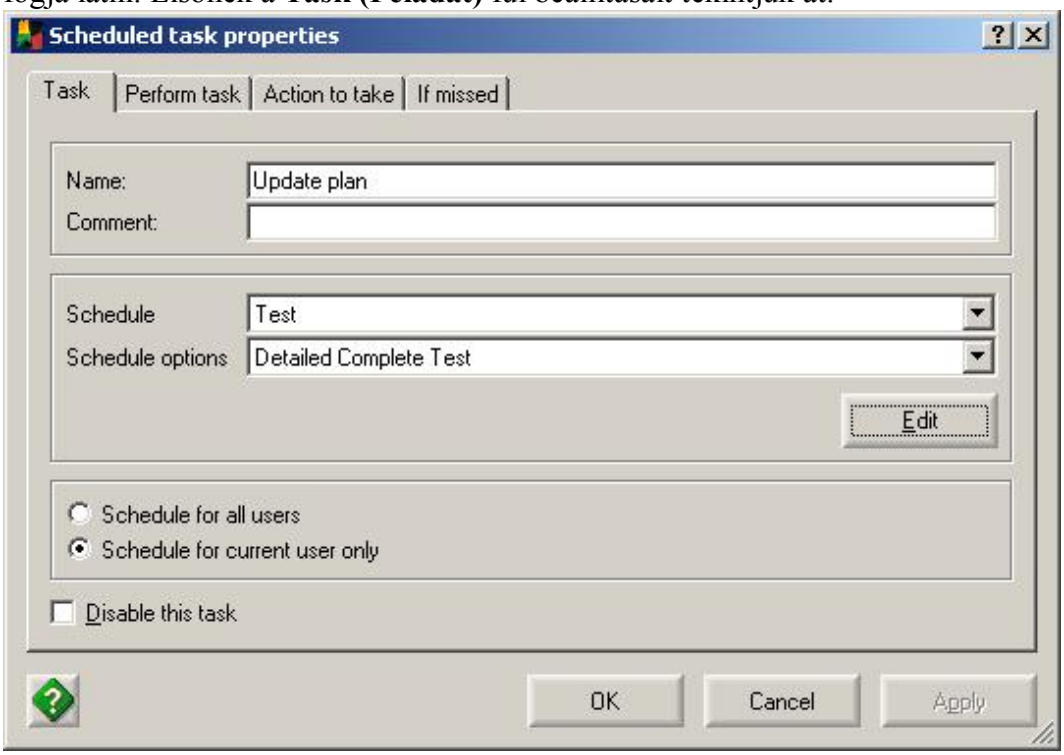


Látható, hogy alapértelmezésben két ütemezett feladat látható. Az első egy tesztelés a második pedig egy frissítés.

A mezők és nyomógombok értelmezése:

- **Name**: Az ütemezett feladat felhasználó által megadott neve
- **Type**: Az ütemezett feladat típusa. Értéke Test (Ellenőrzés) vagy Update (Frissítés) lehet.
- **Last start**: Az időpont, amikor a feladat utoljára futott.
- **Next start**: Az időpont, amikor a feladatot legközelebb futtatni kell.
- **Status**: A feladat állapota végrehajtásának sikeressége (OK: Sikeres)
- **Scheduled for**: Mely felhasználóknál fog végrehajtódni (Current user only: csak az ütemezett feladatot létrehozó felhasználónál hajtódik végre)
- **New schedule**: új ütemezett feladat létrehozása
- **Edit schedule**: a kiválasztott feladat módosítása
- **Delete**: a kiválasztott feladat törlése
- **Close**: az ablak bezárása

A **New schedule** (új ütemezett feladat létrehozása) pontot választva az alábbi ablakot fogja látni. Elsőnek a **Task (Feladat)** fül beállításait tekintjük át.



Mezők és gombok magyarázata:

- **Name**: a feladat elnevezése (tetszőleges szöveg lehet)
- **Comment**: Magyarázó szöveg
- **Schedule**: A feladat típusa. Lehet **Test** (Ellenőrzés) vagy **Update** (Frissítés típusú).
- **Schedule options**: Az előző (Schedule) mezőben meghatár feladat típuson belüli feladat. Ellenőrzések esetében az előre beállított ellenőrzés mintákból választhat (ld. Test manager (Ellenőrzés kezelő)). Ha szükséges, akkor a kiválasztott ellenőrzés beállításait az **Edit** gomb segítségével módosíthatja is. *Figyelem! Az ellenőrzés itteni módosítása visszahat az Ellenőrzés kezelőben megadott beállításokra is!*
- **Schedule for all users:** A számítógép minden felhasználójára érvényes lesz a beállítás (rendszergazdai jogok szükségesek a használatához)
- **Schedule for current user only:** Csak az aktuális felhasználó (saját) által használható beállítás létrehozása.
- **Disable task**: A feladat letiltása (amíg a jelölőnégyzet ki van választva addig a feladat végrehajtása fel van függesztve)

A következő a **Perform task** (feladat végrehajtás) fül.

Itt a feladat végrehajtásának időbeni paramétereit állíthatja be. Az ablakban beállítható tulajdonságok:

- **Periodicity** - a futtatás gyakorisága

- **Only once** - csak egyszer

A **Run on** mezőben megadható, hogy melyik napon legyen végrehajtva a feladat. A **Start time** pedig megadott napon az órát és a percet határozza meg, amikor a feladatot futtatni szeretné.

- **Interval** – időközönként

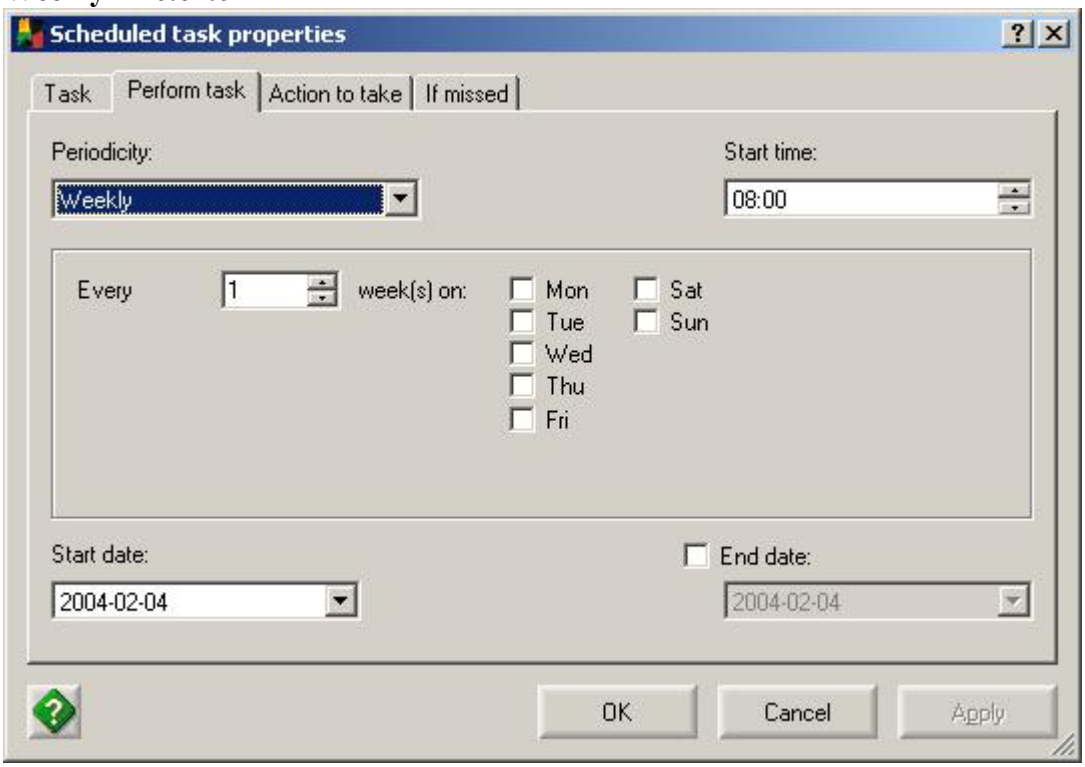
A **Repeat every** mezőben megadhatja, hogy hány óránként (**hour**), vagy hány percenként (**min**) szeretné futtatni a feladatot. Megadható továbbá az is, hogy melyik napon kezdje végrehajtani a feladatot

(**Start date**), illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- **Daily** – naponta

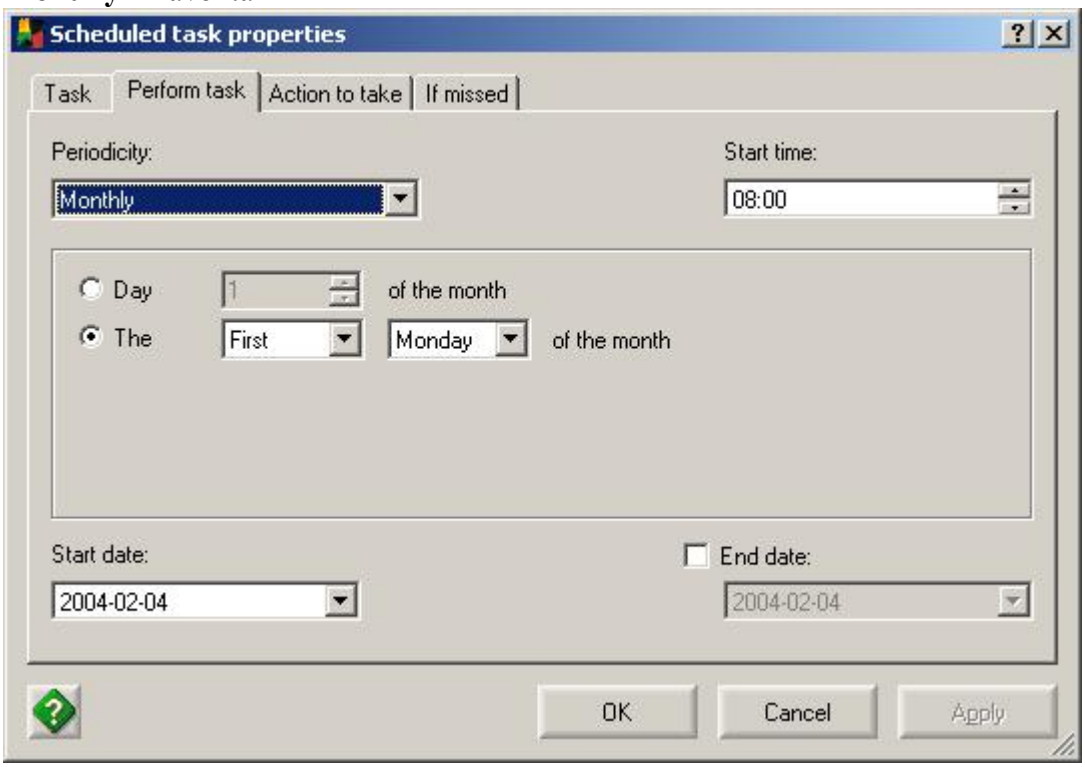
Az **Every** mezőben megadhatja, hogy hány naponta szeretné futtatni a feladatot. A **Start time** mezőben azt állíthatja be, hogy ezeken a napokon mikor (óra:perc) kezdje el a feladatot. Megadható továbbá a dátum is, hogy melyik napon legyen feladat (**Start date**) végrehajtásának első napja, illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- **Weekly** – hetente



Az **Every** mezőben megadhatja, hogy hány hetente történjen a végrehajtás, illetve a megfelelő négyzetek bejelölésével ezt szűkítheti is a hét bizonyos napjaira. (**Mon**: Hétfő, **Tue**: Kedd, **Wed**: Szerda, **Thu**: Csütörtök, **Fri**: Péntek, **Sat**: Szombat, **Sun**: Vasárnap). A **Start time** mezőben azt állíthatja be, hogy ezeken a napokon mikor (óra:perc) kezdje el a feladatot. Megadható továbbá a dátum is, hogy melyik napon legyen feladat (**Start date**) végrehajtásának első napja, illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- **Monthly** – havonta



A **Day** opciót kiválasztva megadhatja, hogy minden hónap hányadik napján induljon el a feladat. A **The** opcióval pedig logikai indirekt módon a hónap heteivel és azok napjaival írhatja le az időzítés módját. Az első legördülő menüből kiválaszthatja, hogy a hónap hányadik hetén szeretné a feladatot futtatni:

- **First** – első
- **Second** – második
- **Third** – harmadik
- **Fourth** – negyedik
- **Last** – utolsó

A második legördülő menüben meghatározhatja, hogy az imént megadott hét melyik napján szeretné futtatni a feladatot:

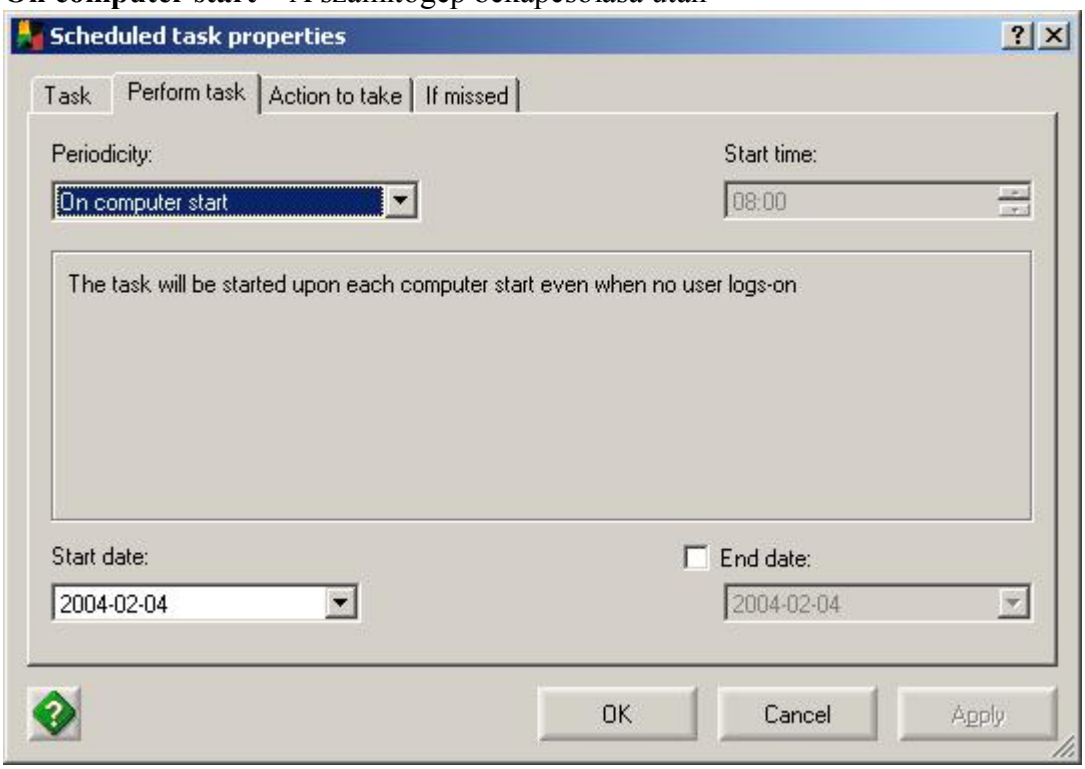
- **Moday** – Hétfő
- **Tuseday** – Kedd
- **Wednesday** – Szerda
- **Thursday –** Csütörtök
- **Friday –** Péntek
- **Saturday –** Szombat
- **Sunday –** Vasárnap

A már megszokott további paraméterek itt is élnek: A **Start time** mezőben azt állíthatja be, hogy ezeken a napokon mikor (óra:perc) kezdje el a feladatot. Megadható továbbá az dátum is, hogy melyik napon legyen feladat (**Start date**) végrehajtásának első napja, illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- **At logon** – a számítógépbe bejelentkezéskor

Csupán két további paraméter megadására van lehetőség: A dátum, hogy melyik napon legyen feladat (**Start date**) végrehajtásának első napja, illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- **On computer start** – A számítógép bekapcsolása után



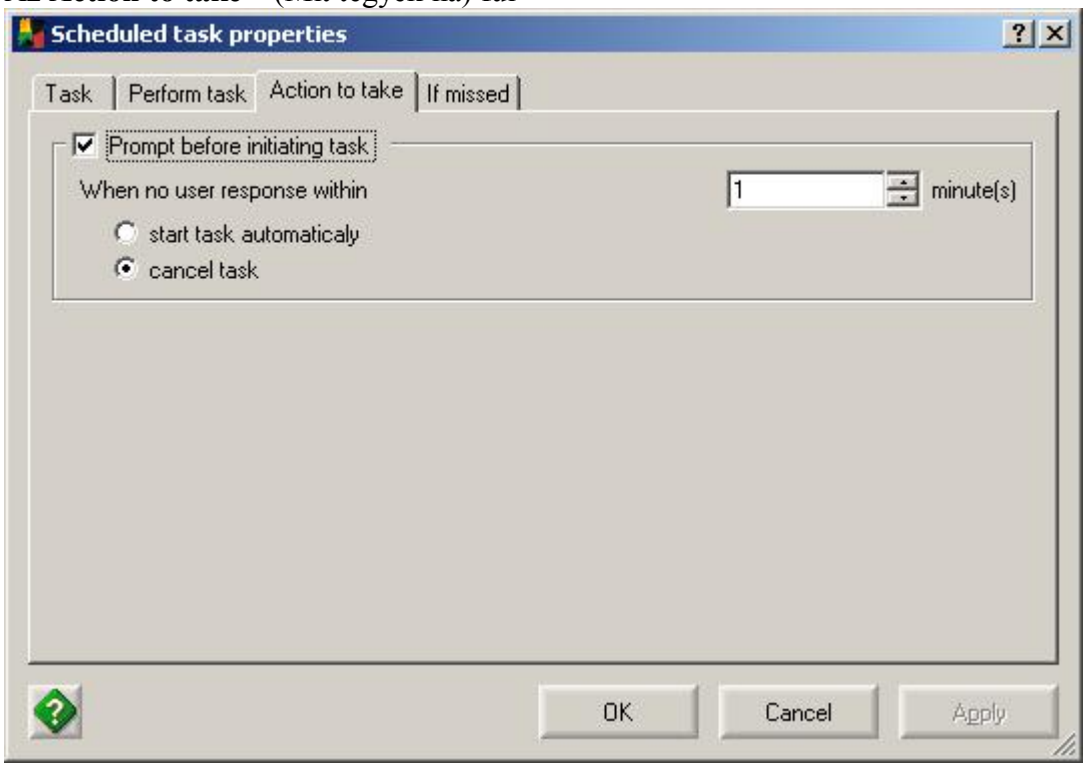
A számítógép bekapcsolása után akkor is elindul a feladat, ha nem jelentkezett be senki. Ez az opció csak rendszergazdai jogosultságokkal

használható. Itt is élnek továbbá a szokásos paraméterek: A dátum, hogy melyik napon legyen feladat (**Start date**) végrehajtásának első napja, illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- **When Internet connection established** – Amikor van Internet kapcsolat

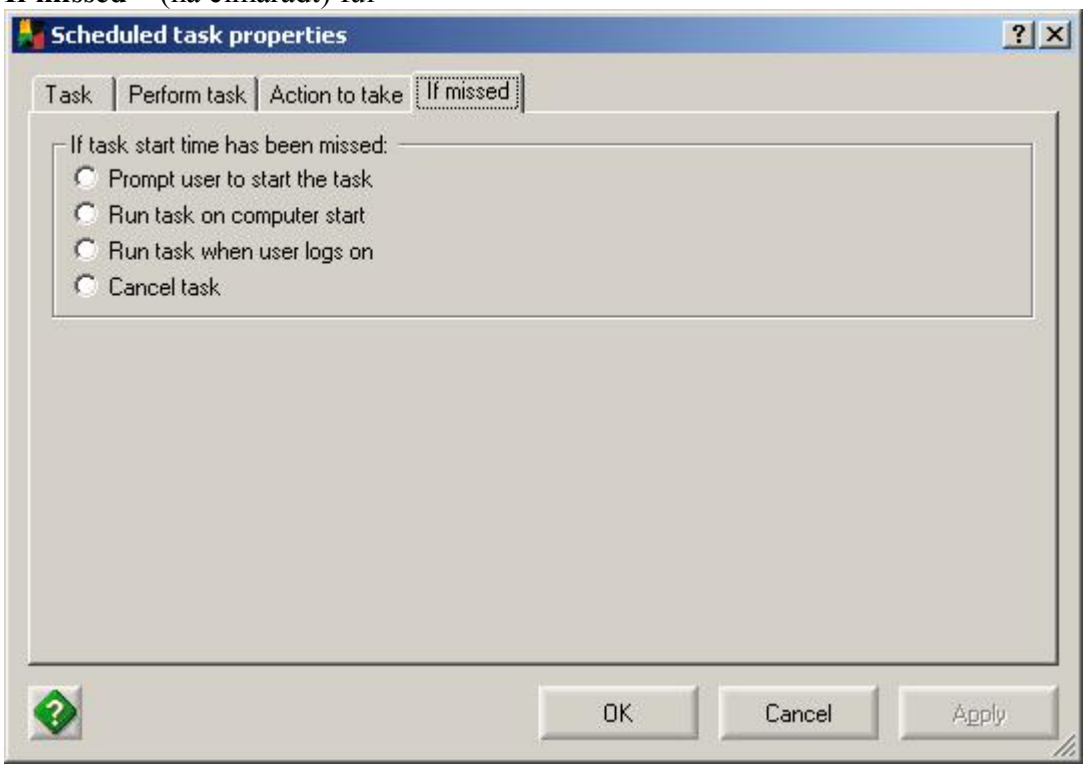
A **Wait at least before trying again** – várjon legaláb parméterben megadhatja, hogy ha nem lenne élő Internet kapcsolat, akkor az újra próbálkozás előtt hány órát (**hour**) vagy percet (**min**) várjon, mielőtt a folyamatot újra megpróbálná elindítani. További paraméterek: A dátum, hogy melyik napon legyen feladat (**Start date**) végrehajtásának első napja, illetve szükség esetén az **End date** négyzetet bejelölve azt is megadhatja, hogy melyik napon hajtsa végre utoljára a feladatot.

- Az **Action to take** – (Mit tegyek ha) fül



A **Prompt before init task** négyzetet bejelölve az ütemezett feladatok indítása előtt mindig fog kapni egy figyelmeztető kérdést, hogy hozzájárul-e a feladat futtatásához. A **When no user resposnse within** (ha nincs válasz) sorban megadhatja, hogy számítógépe hány percet várjon az Ön válaszára (például, ha Ön nem ül a számítógépe előtt), mielőtt a kiválasztott akciót (**start task automatically** – a feladat elindítása, **cancel task** – a feladat kihagyása) megtenné.

- **If missed** – (ha elmaradt) fül

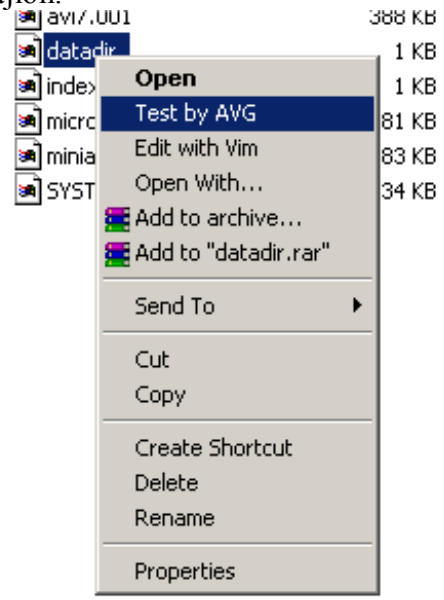


Előfordulhat, hogy amikor a feladatot ütemezés szerint végre kellen hajtani, ennek a feltételei nem állnak fenn. Például azért mert a számítógép ki van kapcsolva és így programokat sem képes végrehajtani. Itt megadhatja, hogy mi történjen azokkal a feladatokkal, amelyek végrehajtását az ütemező elmulasztotta:

- **Prompt user to start the task** – kérdezzen rá a felhasználótól, hogy elindíthatja-e a feladatot
- **Run task on computer start** - Indítsa el a feladatot a számítógép legközelebbi bekapcsolásakor (csak rendszergazdai jogokkal hatásos!)
- **Run tasok when users logs on** – Indítsa el a feladatot, amikor a felhasználó bejelentkezik.
- **Cancel task** – Ne próbálja újra az elmaradt feladatok végrehajtását.

Az AVG Shell Extension (fájlkezelő kiterjesztés)

Az AVG Antivírus fájlkezelő kiterjesztése lehetővé teszi, hogy ahhoz, hogy egy fájlt, vagy könyvtárat ellenőrizzen, ne kelljen elindítani az AVG Antivírust és új teszt profilt létrehoznia. Az ellenőrzés paramétereit előre meghatározhatja és azt két egérkattintással bármikor felhasználhatja. A fájlt egyszerűen válassza ki a Windows Explorerben (Windows Intéző), majd az egér jobb gombjával kattintson egyet a fájlon.

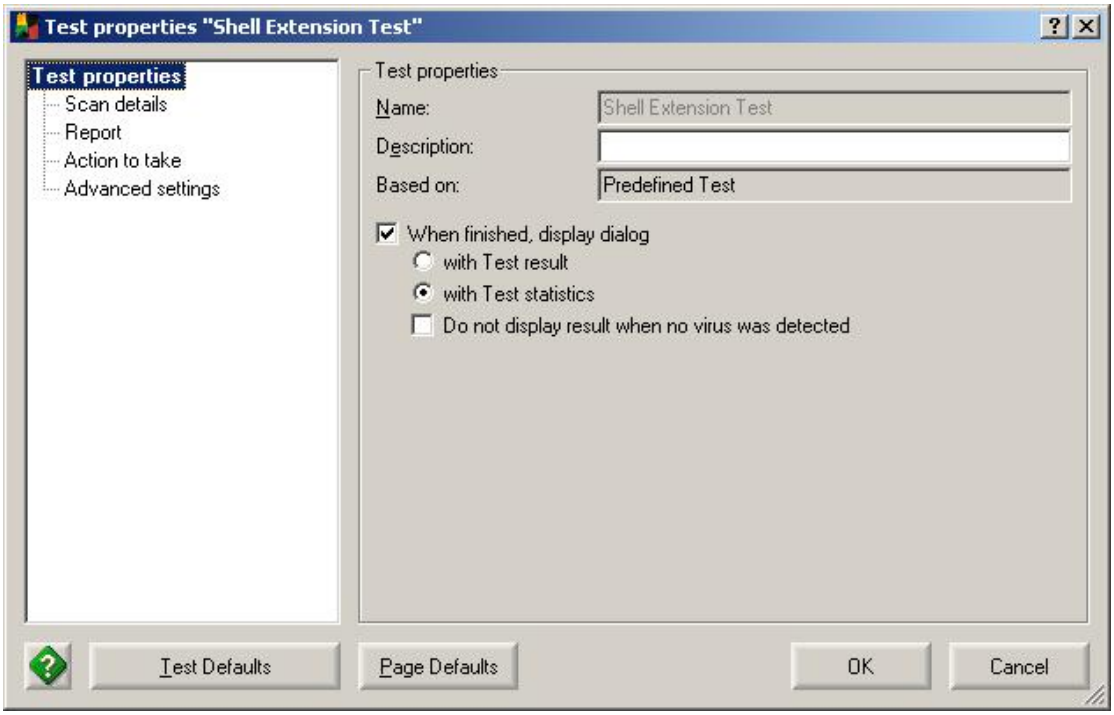


Az itt megjelenő menüben válassza a **Test by AVG** menüpontot és a kiválasztott objektum ellenőrzése, máris elkezdődik.

Az AVG Shell Extension beállításához következőket kell tennie:

Kattintson a Shell Extension cellán [1] majd a Settings (beállítások) [2] gombon.

Ekkor az alábbi beállító ablakot kell látnia:

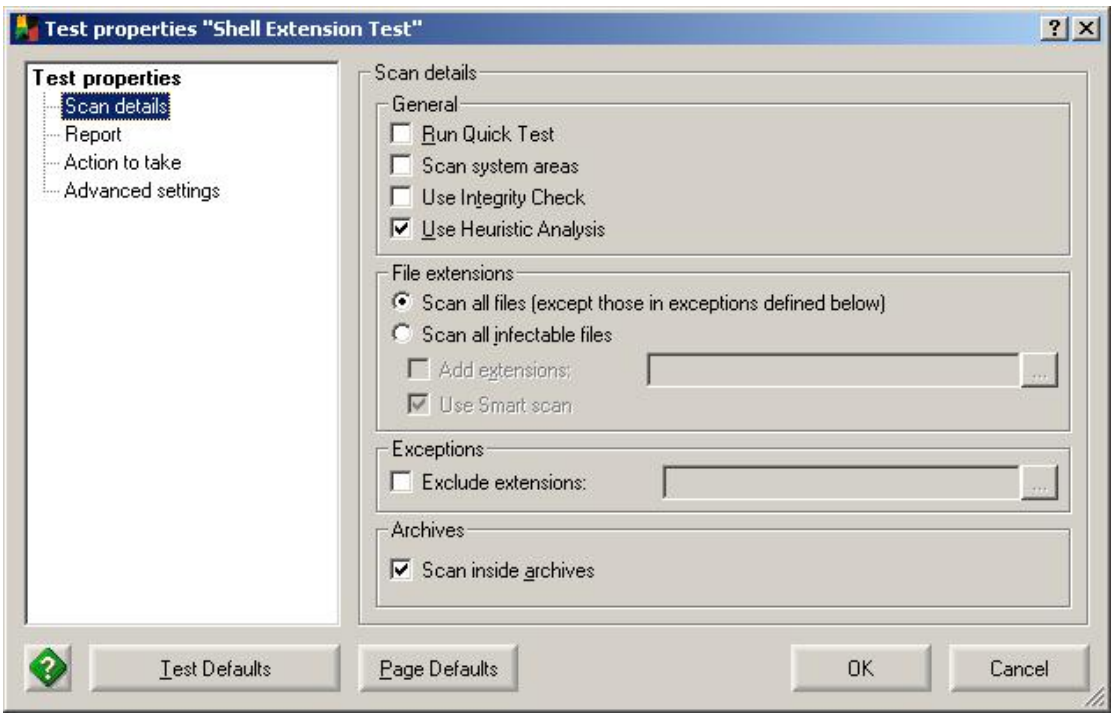


*A gyári alapbeállításokhoz bármikor visszatérhet a **Test defaults** (a teljes **Shell Extension** modulra érvényes) vagy a **Page Defaults** (az éppen látható beállításokra érvényes) gombok valamelyikének lenyomásával. Így bátran kísérletezhet és gyűjthet tapasztalatokat.*

A **Test properties** pontot kiválasztva az ellenőrzés néhány formális paraméterét állíthatja be.

- **Description:** rövid emlékeztető, magyarázó szöveg (tetszőleges)
- **When finished**, display dialog – A négyzetet bejelölve az ellemőrzések után tájékoztató ablak jelenik meg.
    - **With Test result** – az ellenőrzés eredményével (volt vírus vagy sem)
    - **With Test statistics** – Kimutatás a talált ellenőrzött fájlokról (számuk, fertőzöttségük)
    - **Do not display result when no virus was detected** – csak akkor mutasson tájékoztató ablakot, ha vírust talált

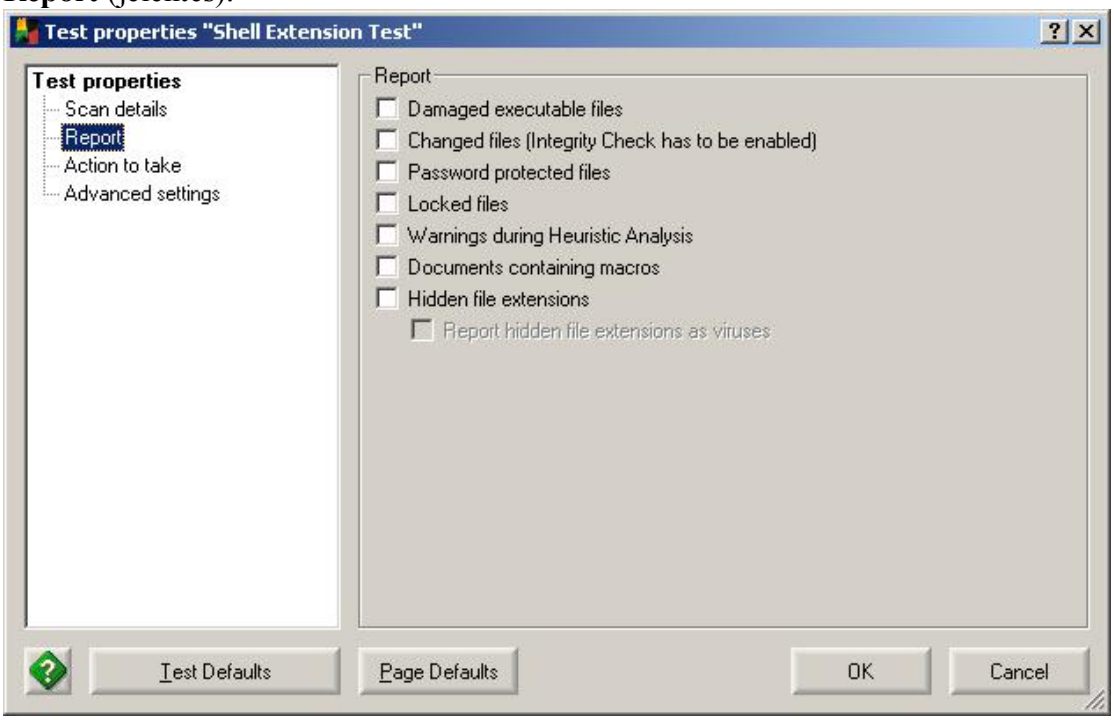
A **Scan details** (az ellenőrzés részletei) pontot választva aprólékosan beállíthatja, hogy milyen teszteket futasson ebben az esetben.



- **Run Quick test** – a program indulásakor egy igen gyors áttekintő ellenőrzést futtat a számítógépen.
- **Scan system areas** –az operációs rendszerhez tartozó területek ellenőrzése
- **Use integrity check** – Először ellenőrzi, hogy a tesztelendő fájl módosult-e a legutóbbi ellenőrzés óta (nem dátum alapján) és csak akkor végez vírusellenőrzést, ha igen. Az opció használatával jelentős sebsségnövekedés érhető el.
- **Use Heuristic Analysis** – programszimulációs ellenőrzés. Nagyon hatékony, bizonyos esetekben a vírusok mutánsait is képes felismerni, anélkül, hogy azok különálló vírusként ismertek lennének.
- **Scan all files** – Minden fájlt ellenőriz, tekintet nélkül arra, hogy az adott fájl műszakilag tartalmazhat-e fertőzésre képes állapotban vírust.
- **Scan All infectable files** – Csak azokat a fájlokat ellenőrzi, amelyek műszakilag tartalmazhatnak fertőzésre képes állapotban vírust.
    - **Add extensions** – az AVG által ilyennek minősítetteken kívül Ön megjelölhet további fájl típusokat kiterjesztésük segítségével, amelyek ellenőrzését kéri.
    - **Use smart scan** – Intelligens keresés. Az AVG képes felismerni a fájlokat, hogy azok fertőzhetőek-e, akkor is, ha a kiterjesztésük nem utal erre. A négyzet bejelölésével engedélyezheti a kiterjesztés nélküli fájlazonosítás funkciót.
- **Exclude extensions –** kiterjesztések kihagyása. Az Ön által meghatározott kiterjesztésű fájlokat az AVG nem fogja ellenőrizni. Akkor lehet rá szüksége, ha Ön vírus kutatással foglalkozik és bizonyos állományokat ki szeretne hagyni az ellenőrzés alól, illetve ha olyan alkalmazásokat használ, amelyek kiterjesztése megegyezik valamelyik más fertőzhető állománytípus kiterjesztésével, de az Ön által használ fájlok nem fertőzhetőek. Ezeknek a fájloknak a kihagyása gyorsabb ellenőrzést eredményez. *Elővigyázattal használja az opciót!*

- **Scan inside archives –** A tömörített fájlok tartalmát is ellenőrizze.
  Figyelem! A jelszóval védett, tömörített fájlok tartalma nem ellenőrizhető!

Report (jelentés).

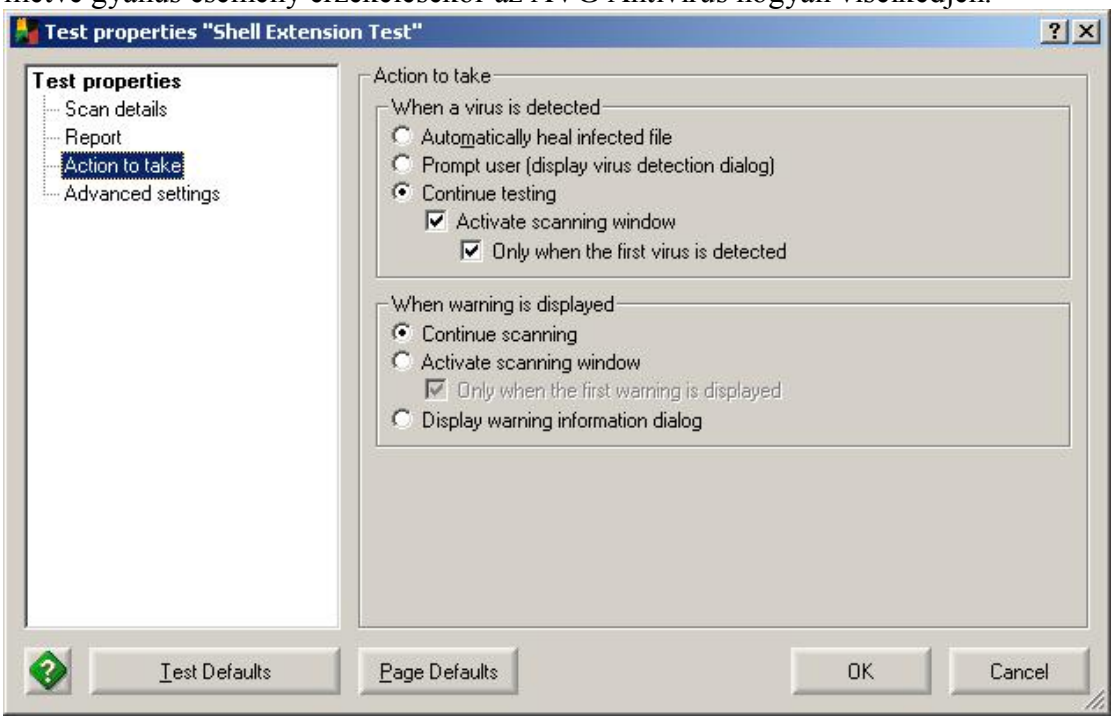


A megjelenő ablakban beállíthatja, hogy az ellenőrzés eredményéről milyen részletességű kimutat kér. Ezzel olyan problémás állományok felderítésére is lehetőség van, amelyek esetlegesen ismeretlen vírussal fertőzöttek, vagy valamilyen oknál fogva tartalmuk megváltozott. Ez az esetek többségében általában nem fertőzést jelent. Ezeknek a kimutatásoknak az értelmezése a szokásosnál magasabb szintű informatikai ismeretket igényel.
Több lehetőség egyidejű kiválasztására is mód van:

- **Damaged executable files** – Sérült futtatható állományok. Ez program fájlok sérülésére utal. Valamilyen oknál fogva a programfájl csonkolódott, tartalma megváltozott. Ha Ön programozó, előfordulhat, hogy a közelmúltban módosított programjai is megjelennek a listán.
- **Changed files (Integrity Check has to be enabled)** – Módosult fájlok. Minden olyan állomány megjelenik a riportban, amely az előző ellenőrzés óta megváltozott. Ennek oka rendszerint a napi szokásos munkavégzés. Az opció használatának előfeltétele, hogy az **Integrity Check (változás ellenőrzés)** opció az ellenőrzéseknél be legyen kapcsolva.
- **Password protected files** – Megjeleníti azokat az állományokat. Amelyek jelszóval védettek és emiatt az ellenőrzésük nem lehetséges.
- **Locked files** – Kisajátított állományok. Bizonyos állományokhoz a hozzáférést más programok, vagy az operációs rendszer saját részre lefoglalja. Ezeket az AVG Antivírus megpróbálja tesztelés miatt használatba venni. Amennyiben ez több különféle módon való próbálkozás ellenére sem sikerül, úgy a fájl megjelenik a kimutatásban.
- **Warnings during Heuristic Analysis** – Figyelmeztetések a szimulációs keresés közben. Ezek nem jelentenek feltétlenül fertőzést, de a gyanús események a kimutatásban megjelennek.

- **Documents containing macros** – Makrókat tartalmazó dokumentumok. A makrók rendszerint a felhasználók által készített az ismétlődő feladatokat segítő rövid programok. Ezek a programok rosszindulatú tevékenységeket is végezhetnek, az ilyen programkódok a makró vírusok. Ez az opció megjelenít minden olyan állományt, amely makrókat tartalmaz, akkor is ha abban egyébként vírust nem érzékelt. Ez abban lehet az Ön segítségére, ha valamelyik állománya eddig nem tartalmazott makrókat és egyszer csak megjelenik a listán, noha Ön nem változtatta meg. Ez rosszindulatú kódrészletre utaló nyom lehet.
- **Hidden file extensions** – Rejtett kiterjesztések. A vírusok igyekeznek elkerülni a lelepleződést. Erre programozójuk sokféle trükköt vet be. Gyakran kettős, rejtett kiterjesztéssel vannak ellátva amiatt, hogy másnak ismerjék fel Őket, mint amik valójában. A többszörös, rejtett kiterjesztés nem feltétlenül jelent veszélyt. A programozók, rendszergazdák sok esetben használják a fájlok tartalmának, tömörítési módjának szakemberek által értelmezhető leírására.
    - **Report hidden file extensions as viruses**– A rejtett kiterjesztéseket mindig vírusként érzékelje. Ezt az opciót csak akkor érdemes bekapcsolni, ha biztos benne, hogy az előző pontban említett lehetőségek nem állnak fenn. A fájlok nem jelölési céllal rejtett kiterjesztésűek.

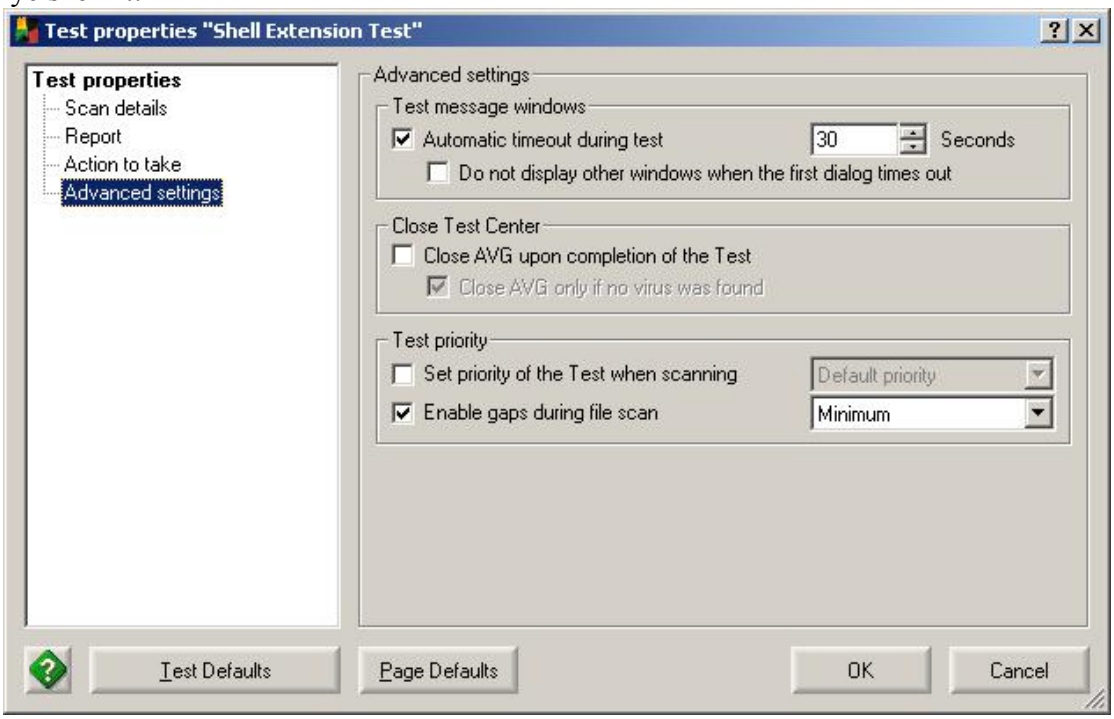
Action to take (mit tegyek, ha...) menüpontban meghatározhatja, hogy vírus, illetve gyanús esemény érzékelésekor az AVG Antivírus hogyan viselkedjen.



- **When a virus is detected** – Ha vírust talált
    - **Automatically heal infected files** – Automatikusan próbálja vírusmentesíteni a fájlt (ha lehetséges), az eredeti tartalom helyreállítása mellett
    - **Prompt user (display virus detection dialog)** – Kérdezze meg a felhasználót. Általában négy lehetőséget kínál fel ilyenkor: Heal –

vírus mentesít, Delete: töröl, Move to virus vault: karanténba helyez, Continue: nem tesz semmit
    - **Continue testing** – ne tegyen semmit, csak jelezze
        - **Activate scanning window** – jelenítse meg az ellenőrzés képernyőjét ha nem lenne látható
            - **Only when first virus detected** – csak az első vírus esetében tegye ezt
- **When warning is displayed –** A figyelmeztető ablak jelenik meg
    - **Continue scanning –** folytassa az ellenőrzést
    - **Activate scanning window** – jelenítse meg az ellenőrzés képernyőjét ha nem lenne látható
        - **Only when first warning displayed** – csak az első figyelmeztetés esetében tegye ezt
    - **Display warning dialog –** Külön ablakban hívja fel a figyelmet az üzenetre

Advanced settings - Haladó beállítások
Itt megadhatja, hogy milyen egyéb automatizmusokat kíván alkalmazni. Ezzel javíthatja számítógépe teljesítményét, gyorsíthatja az ellenőrzéseket, mindezeket igénye szerint.



- **Test message windows** – Ellenőrzés közbeni üzenetek
    - **Automatic timeout during test** – Az ellenőrzés közben üzenetek automatikusan tűnjenek el a megadott idő (másodperc) múlva, ha nem történik felhasználói beavatkozás
        - **Do not display other windows when the first dialog times out** – Ha az első üzenetre nem érkezett felhasználói válasz, akkor a több ne jelenjen meg.
- **Close test center –** Az ellenőrző központ ablakát zárja be
    - **Close AVG upon completion of the Test –** ha az ellenőrzés befejeződött

        - **Close AVG only if no virus was found –** Csak akkor zárja be, ha nem talált vírust.
- **Test priority** – Az ellenőrzés fontossága. Ezekkel a beállításokkal befolyásolhatja, hogy számítógépe mennyire kezelje elsőbbséggel a vírusuellenőrzést. Az alacsonyabb fontosság nem jelent alacsonyabb biztonságot, csupán annyit, hogy az ellenőrzés lassabban zajlik. Így ha Ön közben dolgozik számítógépén, úgy az Ön feladataival a gép többet foglalkozik, az ellenőrzés pedig lassabb lesz. Ez természetesen fordítva is igaz, vagyis az Ön munkájával szemben is előtérbe helyezheti a vírusellenőrzés fontosságát.
    - **Set priority of the Test when scanning** – az ellenőrzés fontossága
        - **Low priority** – csekély fontosság
        - **Lower priority** – alacsony fontosság
        - **Default priority** – normál fontosság (gyári beállítás)
        - **High priority** – nagy fontosság
    - **Enable gaps during files can –** A kiválasztott fájlok ellenőrzése közötti szünet. Két fájl ellenőrzése között az AVG szünetet tart.Ennek mértékét Ön a számítógépe teljesítményének és a keresés gyorsaságának függvényében Ön állíthatja be. Az ellenőrzések közötti szünet áll az Ön rendelkezésére a beavatkozáshoz, illetve az AVG ilyenkor veszi figyelembe az Ön módosító parancsait.
      Választható lehetőségek, novekvő sorrendben:
        - **None –** nem várakozik
        - **Minimum –** minimális időt vár
        - **Default –** alapértelmezés
        - **5 milliseconds –** 5 ezredmásodperc
        - **10 milliseconds –** 10 ezredmásodperc
        - **50 milliseconds –** 50 ezredmásodperc

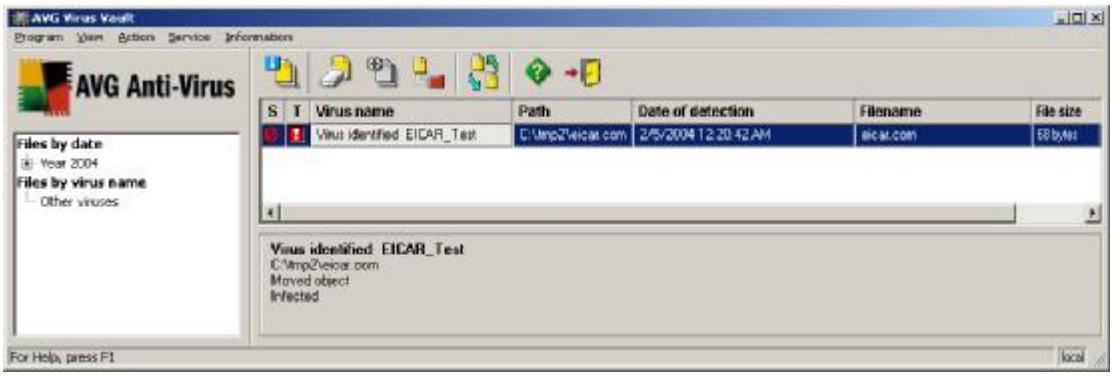
Amennyiben szeretné a Shell extension (fájlkezelő kiterjesztést ki is kapcsolhatja) Ettől az állandó védelem (Resident shield) nem veszít hatékonyságából, viszont elveszíti a gyors és könnyen indítható ellenőrzés lehetőségét, ezért kikapcsolását nem javasoljuk.

A kikapcsoláshoz először a **Shell Extenison** cellán majd a **Deactivate** gombon kell kattintania. Amennyiben a kiterjesztés nem aktív, úgy a **Deactivate** gomb helyett az **Activate** látható, a visszakapcsolás annak segítségével történhet.

Virus vault – Karantén.

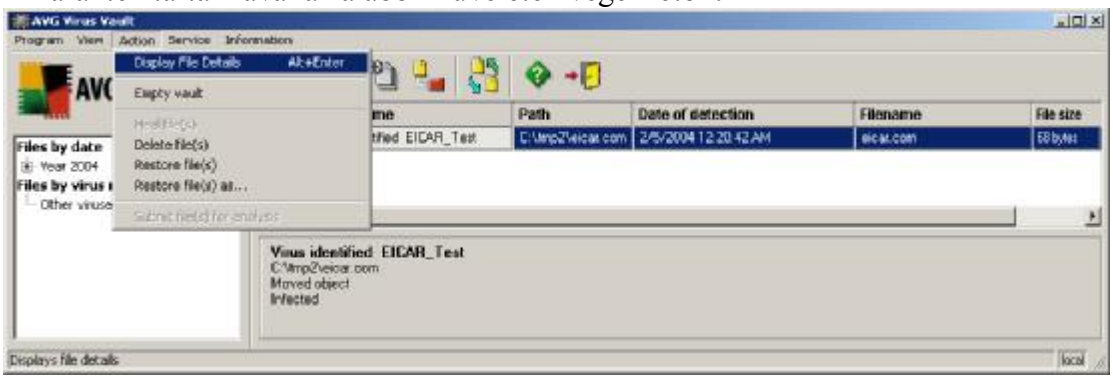
Előfordulhat, hogy az AVG Anti-vírus olyan vírussal fertőzött állományt talál, amelyet nem tud kiirtani úgy, hogy a fájl hasznos tartalmát is megőrizze. Ebben az esetben az állományt karanténba helyezheti. Hogy ha a vírus irtása megoldottá válik, újra elővehesse. Nagyon sok felhasználó gyűjtőszenvedélyének hódolva helyezi karanténba a fájlokat. Önnek lehetősége van számítógépes vírusokat gyűjteni, de kérjük, hogy ezt ne ártó szándékkal tegye! A karanténban lévő vírusok nem képesek kárt okozni, azok az AVG folyamatos felügyelete alatt vannak.

A **Virus vault** cellára majd az **Open** gombra kattintva megtekintheti a karantén tartalmát.



Látható, hogy a karanténunkban egyetlen vírus található. Listában megtalálhatja a vírus nevét (**Virus name**), az eredeti helyet, útvonalat, ahol a vírust az AVG azonosította (**Path**), az elfogás idejét (**Date of detection**), a fertőzött állomány nevét (**Filename**) és a fertőzött fájl méretét (**File size**).

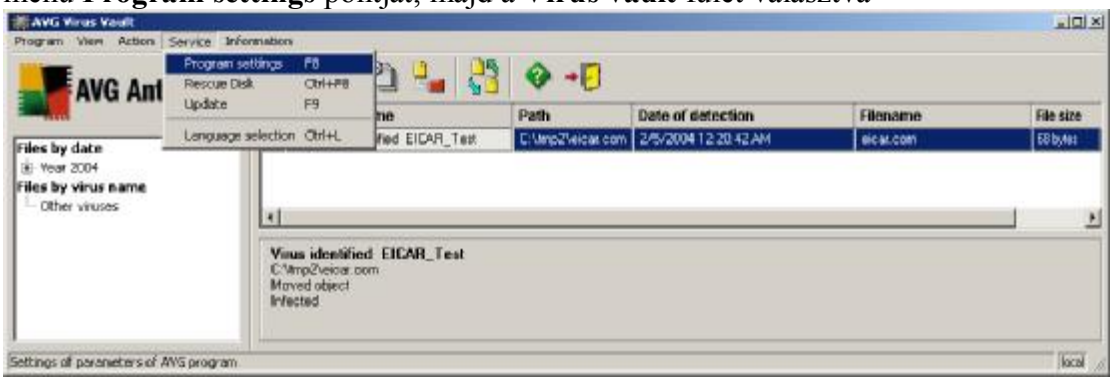
A karantén tartalmával az alábbi műveletek végezhetők:



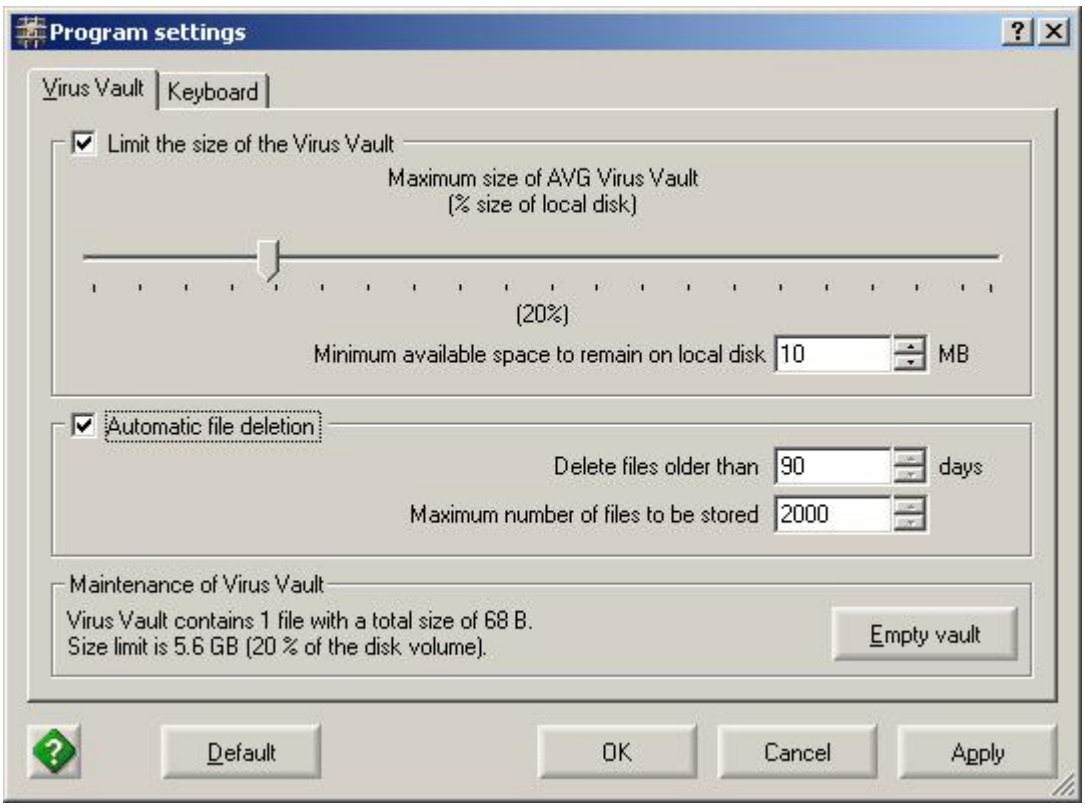
A Karantén Action menüjébe az alábbi funkciók állnak rendelkezésére:

- **Display file details** – A kiválasztott állomány még részletesebb adatainak megtekintése
- **Empty vault** – A karantén teljes tartalmának törlése
- **Heal file(s)** – A kiválasztott fájl(ok)ból a vírus eltávolítása (ha lehetséges)
- **Restore file(s)** – A kiválasztott fájl(ok) visszamásolása az eredeti helyükre
- **Restore file(s) as** – A kiválasztat fájl(ok) visszamásolása, más néven
- **Submit files for analysis** – a fájl elküldése a Grisoft-nak további elemzésre

Itt van lehetőség továbbá a Karantén tulajdonságainak beállítására is. A **Service** menü **Program settings** pontját, majd a **Virus vault** fület választva



meghatározhatja, hogy:



- **Limit the size of the vírus vault** – legfeljebb a lemezterület hány százalékát foglalhatja el a karantén
  - **Minimum available space to remain on local disk** – legalább hány megabájt szabad terület maradjon szabadon
- **Automatic file deletion** – automatikusan törlje a karanténből a
  - **Delete files olther than** – a megadott napnál idősebb fájlokat
  - **Maximum number of files stored to be** – a legrégebbi fájlokat, ha karantén tartalma meghaladja a 2000 db fájlt
- **Empty vault –** A gombra kattintva törölheti a karantén teljes tartalmát.

Ez utóbbi feladat egyszerűbben is elvégezhető a vezérlő központ (Control Center) segítségével:

A karantén kiürítéséhez kattintson a **Virus vault** cellára, majd az **Empty vault** gombra.

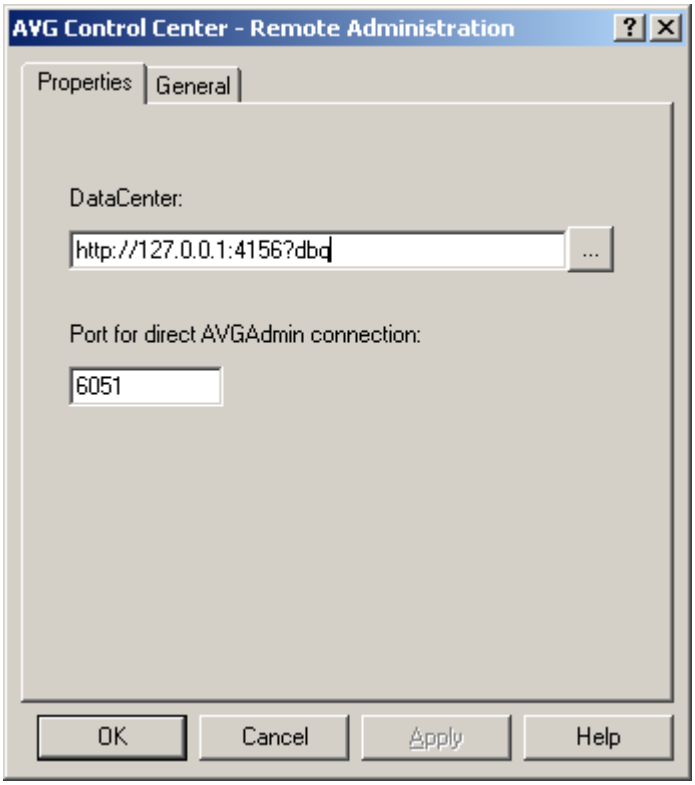
Remote extension – Távvezérlő modul.

Ez a lehetőség csak a Hálózati változatban valamint a fájl és levelező szerver verziókban érhető el!.

Ez a modul lehetővé teszi, hogy ha Ön egy sok számítógépből álló hálózatot üzemeltet, úgy az összes számítógép beállítását központilag elvégezhesse. A hálózati adminisztráció arra is lehetőséget nyújt, hogy a telepítést is központilag végezze el. A távvezérlés beállításához először az **ingyenes** AVGAdmin nevű programot kell telepítenie egy központ szervergépen vagy a rendszergazdai munkaállomáson. A távvezérlés funkció segítségével az AVG minden paramétere beállítható és az esetleges események jelentései is erre a központi gépre érkeznek. Ugyancsak lehetőség van arra, hogy a központi gép automatikusan elvégezze az összes számítógépen az AVG Anti-vírus rendszeres frissítését. Erről és a részletekről a hálózati adminisztrációról szóló leírásban olvashat. Most csak az AVG Anti-vírusnak a távvezérlésbe való bekapcsolását mutatjuk be, amennyiben azt a telepítésnél elmulasztotta volna.

A beállításhoz kattintson a **Remote Administration** cellára majd a **Properties** (beállítások gombra).

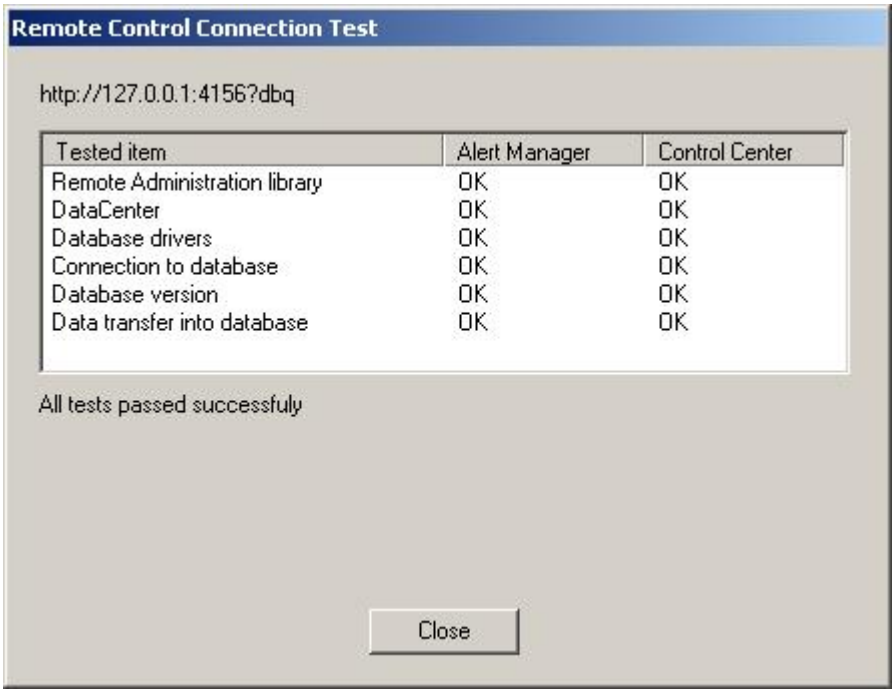
Ennek hatására a következő ablakot kell látnia:



A DataCenter mezőbe kell megadni az központi adminisztrációs gép IP címét az elérés módját. Valamint a kapuszámot (Port for direct AVGAdmin connection).
A példában látható beállítások az AVGAdmin alapszintű telepítése esetében megfelelőek. Önnek csupán az ábrán látható **127.0.0.1** címet kell kicserélnie az AVGAdmin csomag AVG TCPServer programjának helyet adó számítógép címére. A beállítások elfogadásához kattintson az **OK** gombra.

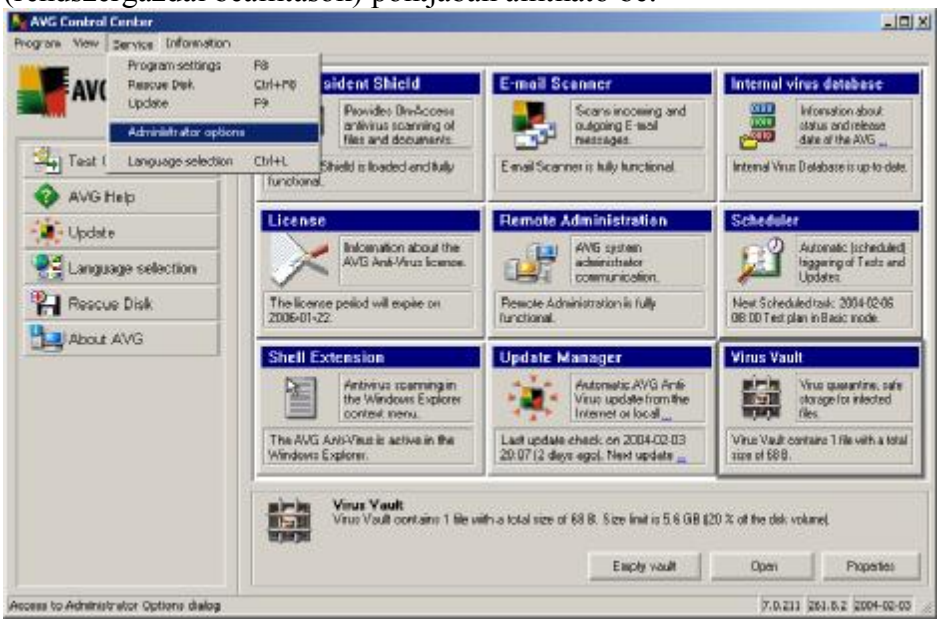
Ha a beállításokat elvégezte, akkor lehetősége van annak tesztelésére, hogy az AVG TCP Server valóban elérhető-e?

Ehhez először a **Remote Administration** cellára majd a **Test** gombra kell kattintania. Ha minden rendben van, akkor az alábbi eredményt kell látnia:

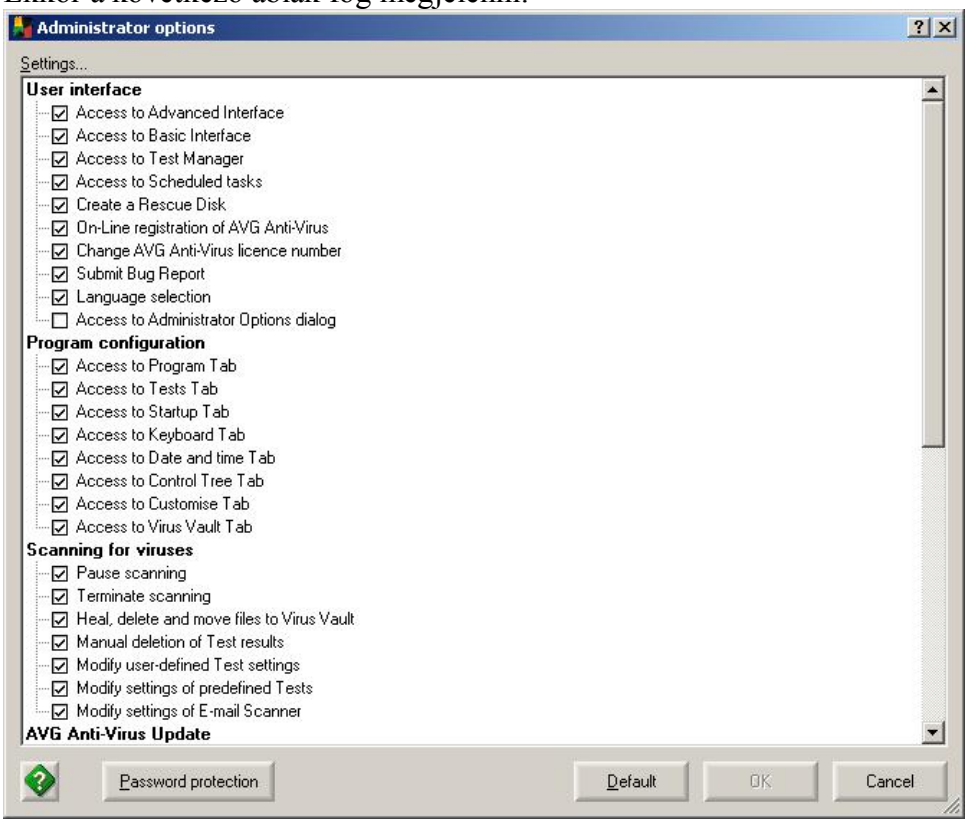


Jogosultságok beállítása

Az egyik legfontosabb funkció, hogy a rendszergazda (Nem csak a hálózati változatban) megadhatja, hogy a felhasználók milyen tevékenységeket végezhetnek, milyen változtatásokat tehetnek az AVG beállításaiban. Például megadhatja, hogy felhasználó ne állíthassa le kényelmi okok miatt az ellenőrzéseket, veszélyeztetve ezzel a teljes rendszer biztonságát.
A funkció a vezérlő központ **Service** menüjének **Administrator options** (rendszergazdai beállítások) pontjában állítható be:



Ekkor a következő ablak fog megjelenni:



Beállításai:

- **User interface** – kezelő felület
  - **Access to advance interface** – Haladó felület kiválasztható
  - **Access to basic interface** – Kezdő felület kiválasztható
  - **Access to Test manager** – Ellenőrzés beállításai módosíthatók
  - **Access to Schedule tasks** – Ütemező beállításai módosíthatók
  - **Create a Rescue Disk** – Helyreállító lemez készíthető
  - **On-Line registration of AVG Anti-vírus** – Regisztrálhatja a terméket a Grisoftnál
  - **Change AVG Anti-Virus lincence number** – Kicserélheti a regisztrációs kódot
  - **Submit Bug Report** – az AVG esetleges hibájáról jelentést küldhet a Grisoftnak
  - **Language Selection** – Nyelvet válthat
  - **Access to administrator options dialog** – Módosíthatja ezeket a beállításokat
  -
- **Program configuration** – Program beállítások (**Service** menü/**Program settings** pontja)
  - **Access to Program tab** – Program fül kiválasztható
  - **Access to Tests tab** – Ellenőrzések fül kiválasztható
  - **Access to Startup tab** – indítási beállítások kiválaszthatók
  - **Access to Keyboard tab** – billentyűzet beállítások módosíthatók
  - **Access to Date and time tab** – Dátum és időformátum változtatható
  - **Access to control Tree tab** – Ellenőrzés és ütemező megtekintésének beállítása
  - **Access to Customize tab –** A menürendszer testre szabásának engedélyezése
  - **Access to Virus vault tab** – A Karantén beállításának módosítása
- **Scanning for viruses** – Vírusellenőrzés
  - **Pause scanning** – a keresés szüneteltethető
  - **Terminate scanning** – a keresés megszakítható
  - **Heal, delete and move files to Virus vault** – a felhasználó választhat, hogy vírusmentesíteni, törölni, vagy karanténba helyezni szeretné a fertőzött fájlt
  - **Manual deletion of test result** – az ellenőrzés jelentése a felhasználó által törölhető
  - **Modify user-defined Test settings** – az egyéni ellenőrzési beállítások módosíthatóak
  - **Modify settings of predefined Tests** – a gyári ellenőrzési beállítások módosíthatók
  - **Modify settings of E-mail scanner** – a levelezés ellenőrzésének beállításai módosíthatók
- **AVG Anti-Virus Update** – Az AVG Antivírus frissítése
  - **Initiate manual update from the Internet** – A frissítéseket a felhasználó készileg letöltheti
  - **Postpone restart of computer after update** – A frissítés után esetlegesen a számítógép újraindítása lehet szükséges. Ezt a felhasználó elhalaszthatja-e?

- **AVG Control Center –** AVG Vezérlő központ
  - **Access to AVG Control center –** A vezérlő központot a felhasználó megnyithatja
  - **Modify settings of Scheduler component** – módosíthatja az ütemező beállításait
  - **Modify settings of Resident shield component** – módosíthatja az állandó védelem beállításait
  - **Modify settings of Virus vault component** – módosíthatja a karantén beállításait
  - **Modify settings of Update manager component** – módosíthatja a frissítés kezelő beállításait
  - **Modify settings of Internal virus database component** – módosíthatja a belső vírus adatbázis beállításait
  - **Modify settings of Virus Encyclopedia component** – módosíthatja a vírus ismertető beállításait
  - **Modify settings of Shell extension component** – módosíthatja a fájlkezelő (intéző) kiterjesztés beállításait
  - **Modify settings of Remote administration component** – módosíthatja a távvezérlő beállításait
  - **Modify settings of Alert manager component** – módosíthatja a riasztás kezelő beállításait
  - **Modify settings of License component** – módosíthatja a felhasználási engedély beállításait
  - **Modify settings of E-mail scanner component** – módosíthatja az e-mail ellenőrző beállításait
  - **Perform shutdown of AVG Control Center** – leállíthatja a vezérlő központot
- **AVG Virus vault** – AVG Karantén
  - **Access to virus vault** – A karantén hozzáférhető
  - **Restore files from Virus vault** – Kivehet állományokat a karanténból
  - **Delete files in Virus vault** – Törölhet fájlokat a karanténban
  - **Heal files in Virus vault** – Vírusmentesíthet fájlokat a karanténban

A képernyő alján látható a **Password protection** (jelszavas védelem) gomb. Ide kattintva jelszót adhat meg, amely ismerete nélkül a beállítások nem módosíthatók. A módosítás engedélyezéséhez is a **Password protection** gombot kell használni. E nélkül az **OK** (jóváhagyás) gomb nem használható (mint előbbi képünkön is).

Ezzel áttekintettük az AVG Control Center (AVG Vezérlő központ) összes funkcióját. A következőkben az kezelő felülettel és az ellenőrzések beállításaival fogunk foglalkozni.

Az AVG 7.0 for Windows változatának kezelő felülete

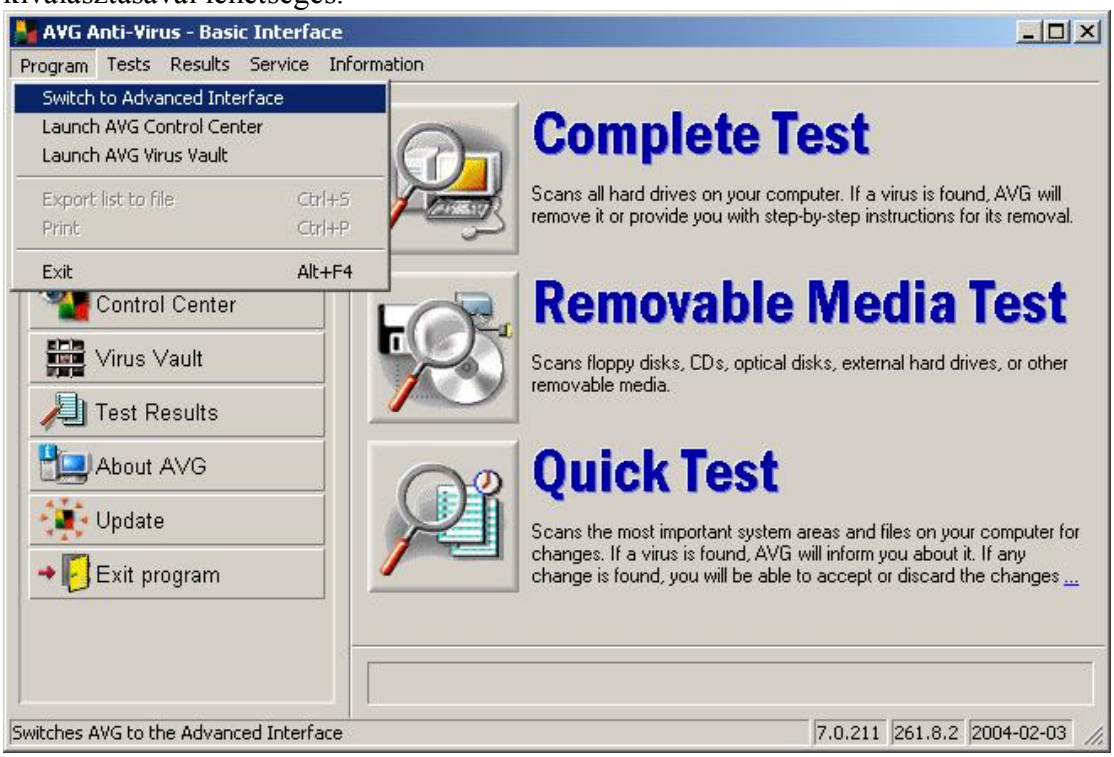
Indítsa el az AVG 7.0 programot a Start menüből vagy az Asztalról az 

ikonra kattintva.

Az AVG 7.0 kétféle kezelőfelülettel rendelkezik, amelyek között **menet közben is válthat**.

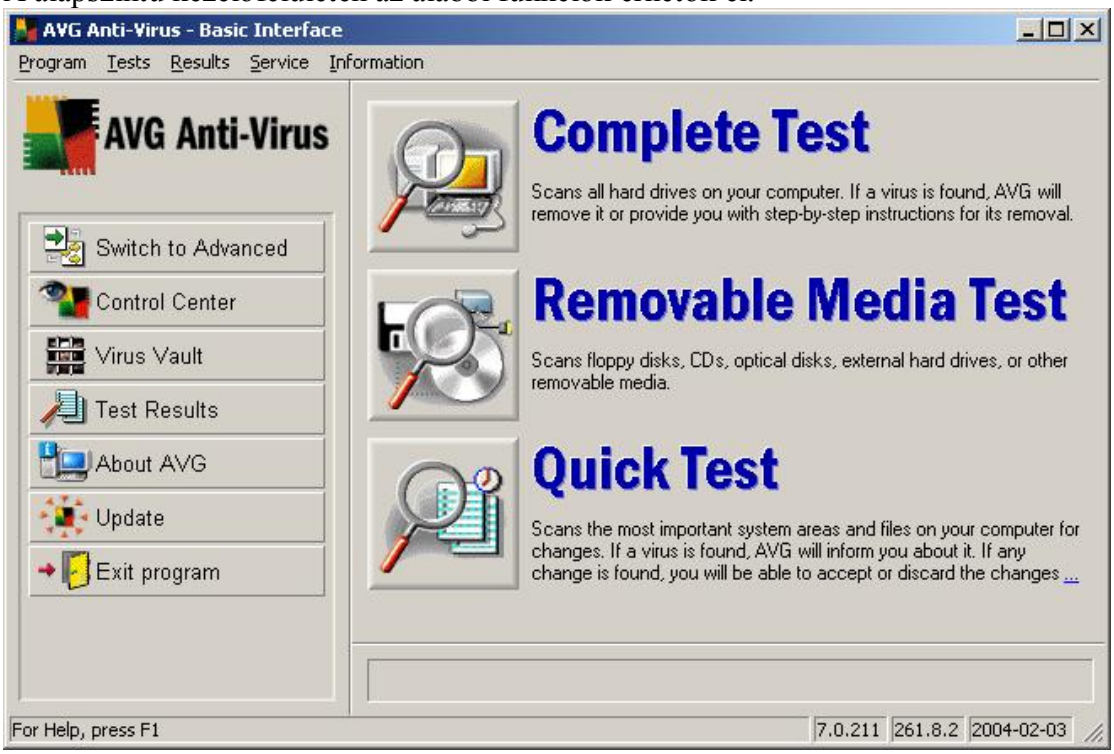
- **Basic** – Alapszintű, a napi munkában és nem gyakorlott felhasználók részére ajánlott
- **Advanced** – Haladó, a gyakorlott felhasználók részére illetve a részletes beállításokhoz.

A program mindig abban az üzemmódban indul el, ahogyan utoljára használták.
A váltás a **Program** menü **Set to Advanced (Basic) Interface** pontjának kiválasztásával lehetséges.



Az alapszintű kezelőfelület

A alapszintű kezelőfelületen az alábbi funkciók érhetők el:



A legfontosabbak a **nagy nyomógombok**. Ezek lehetővé teszik, hogy a leggyakoribb ellenőrzési funkciókat egyetlen gombnyomással érhessék el.
Ezek:

- **Complete test** – Teljes ellenőrzés. A számítógép minden lemezegységét átnézi vírus után kutatva
- **Removable media test** – hordozható lemezek ellenőrzése. Hasznos segítség, ha frissen érkezett hajlékony lemezt vagy CD-t kell ellenőrizni.
- **Quick test** – Az operációs rendszer, rendszer területeit ellenőrzi. Hasznos funkció, ha számítógépétől szokatlan, meglepő viselkedést tapasztal.

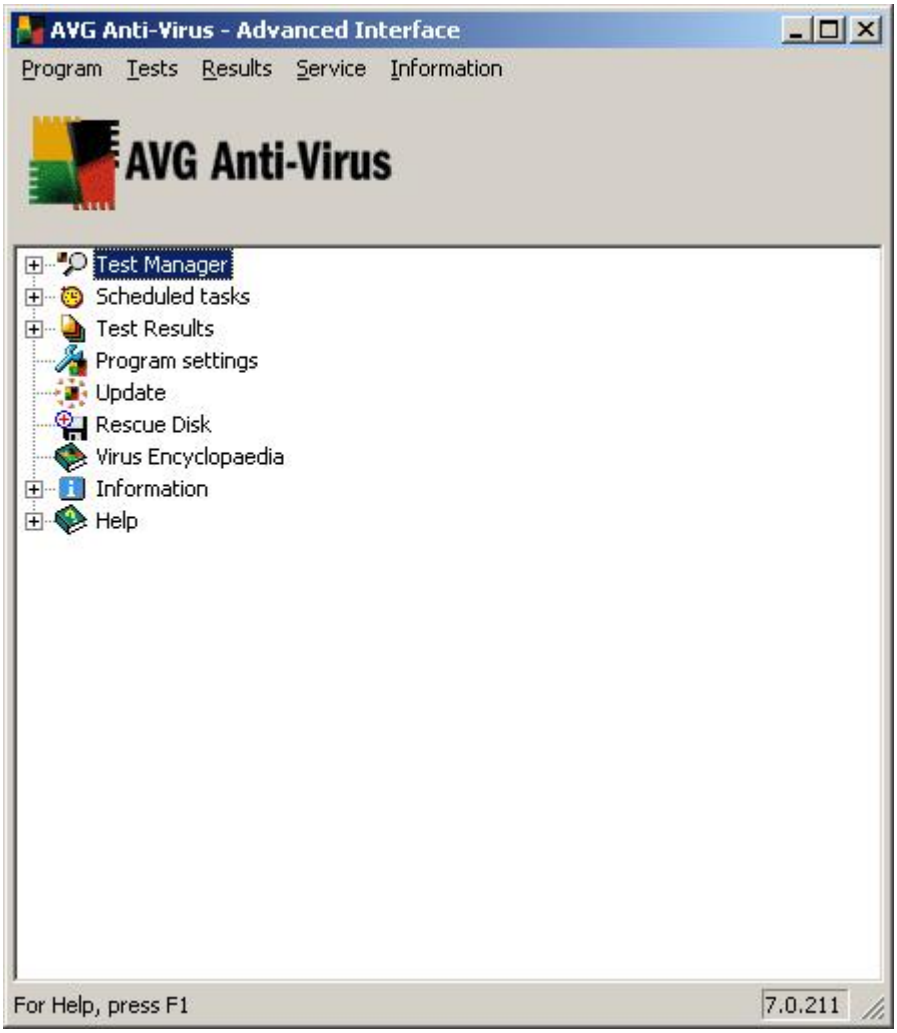
További lehetőségek:

- **Switch to advanced** – váltás a haladó (kiterjesztett) kezelőfelületre. Bizonyos beállítási lehetőségek csak azon érhetők el!
- **Control Center** – A már megismert vezérlő központ indítása
- **Virus vault** – A Karantén megtekintése
- **Test results** – Az ellenőrzések eredményeinek megtekintése
- **About AVG** – A program névjegye
- **Update** – Frissítés
- **Exit program** – Kilépés

Ahhoz, hogy minden funkciót elérhessünk a továbbiakban a haladó (kiterjesztett) kezelőfelülettel fogunk foglalkozni.

A haladó kezelő felület

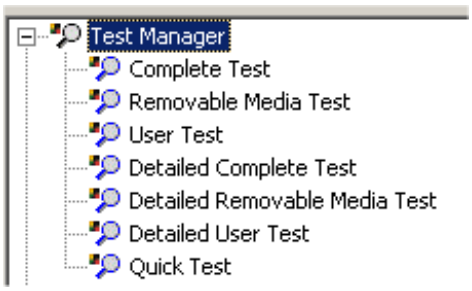
A napi munkához a tapasztalt, informatikai képzettséggel rendelkezők számára is megfelelő a Basic (alapszintű) felület. Ha azonban saját teszteket és egyéb finom beállításokat szeretnénk létrehozni, akkor az egyetlen lehetőség a Haladó (Advanced) felület használata:



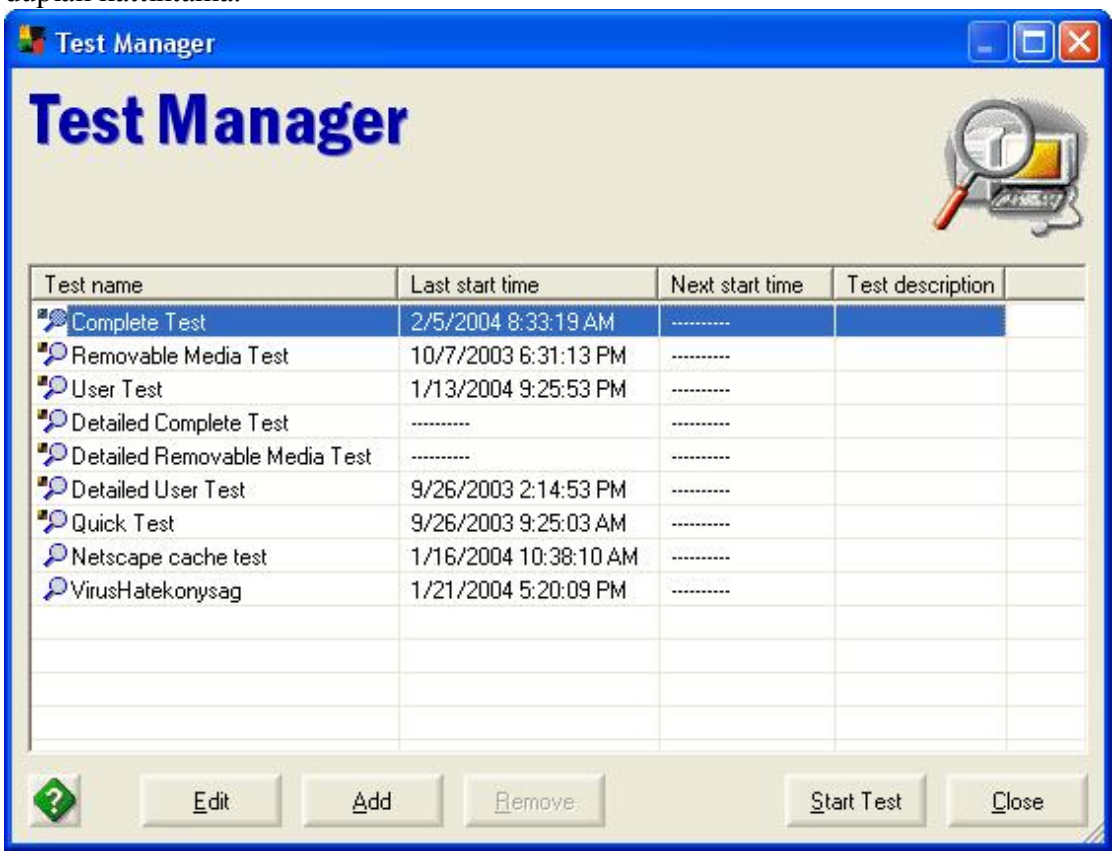
Az ablakban megjelenő sorok funkciókat és beállításokat jelentenek. Ha a sor előtt egy négyszöget ⊞ lát, akkor az azt jelenti, hogy az egy beállítás csoportot jelöl. Ha négyszögre kattint akkor a csoport kinyitható (így a tartalma hozzáférhetővé válik) illetve bezárható. Jelen dokumentációban csak az **Ellenőrzés kezelővel (Test manager)**, a **Program beállításokkal (Program settings)**, **Vírus ismertető (Virus Encyclopaedia)** és a **Jelentés kezelő (Test Results)** fejezetek tárgyaljuk. A többi menüpont csak hivatkozás a Vezérlő központ (Control Center) azonos nevű moduljaira. Beállításaikhoz kérjük, hogy tanulmányozza a korábbi fejezeteket!

Test manager (ellenőrzés kezelő)

Lehetőséget ad az ellenőrzések beállításainak módosítására, illetve az ellenőrzések futtatására.



- A csoportban lévő bármelyik ellenőrzést elindíthatja, ha a teszt nevén duplán kattint.
- Az ellenőrzések beállításainak módosítására, illetve tesztek létrehozására és törlésére is van módja, ehhez a **Test manager** (ellenőrzéskezelő) soron kell duplán kattintania.



A megjelenő ablakban felsorolva láthatja az összes, már létrehozott tesztet, az alábbi paraméterekkel:

- **Test name** – a teszt elnevezése
- **Last start time** – Az utolsó futtatás időpontja
- **Next start time** – a következő futtatás időpontja
- **Test description** – rövid magyarázat a teszthez.

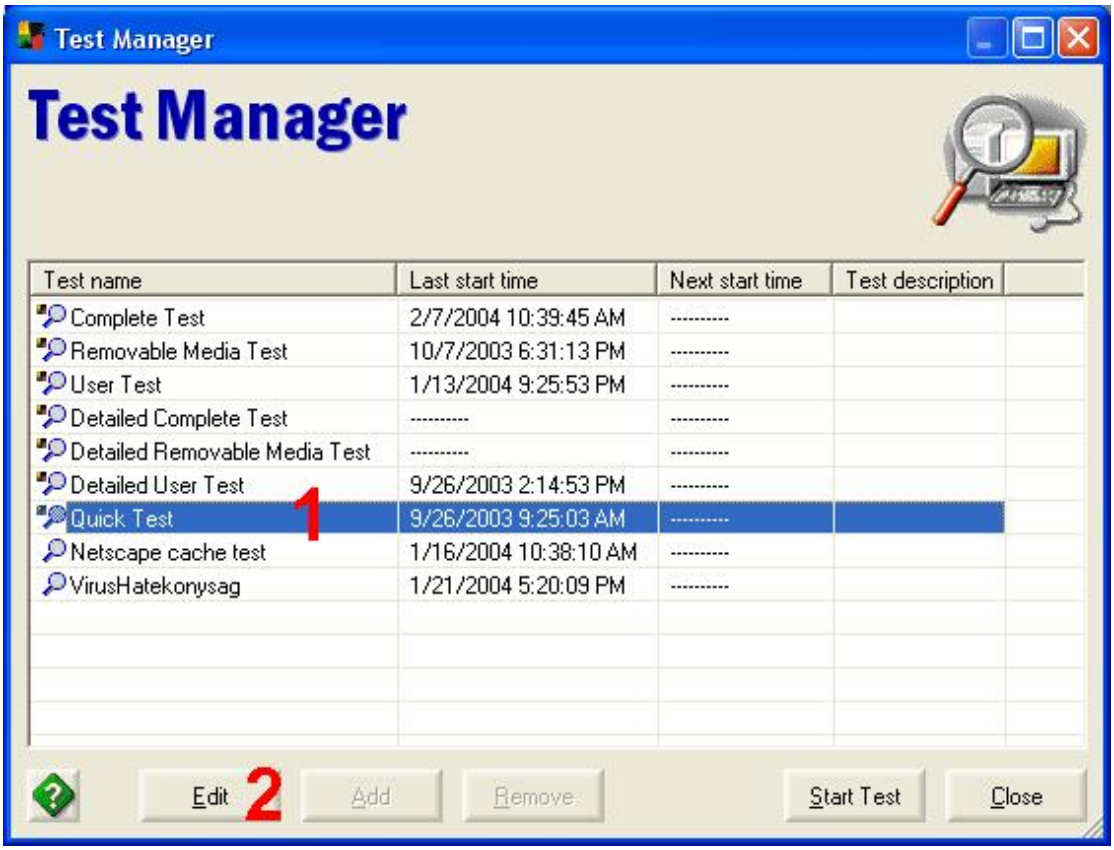
Nyomógombok:

- **Edit** – A kiválasztott teszt szerkesztése
- **Add** – Új teszt létrehozása

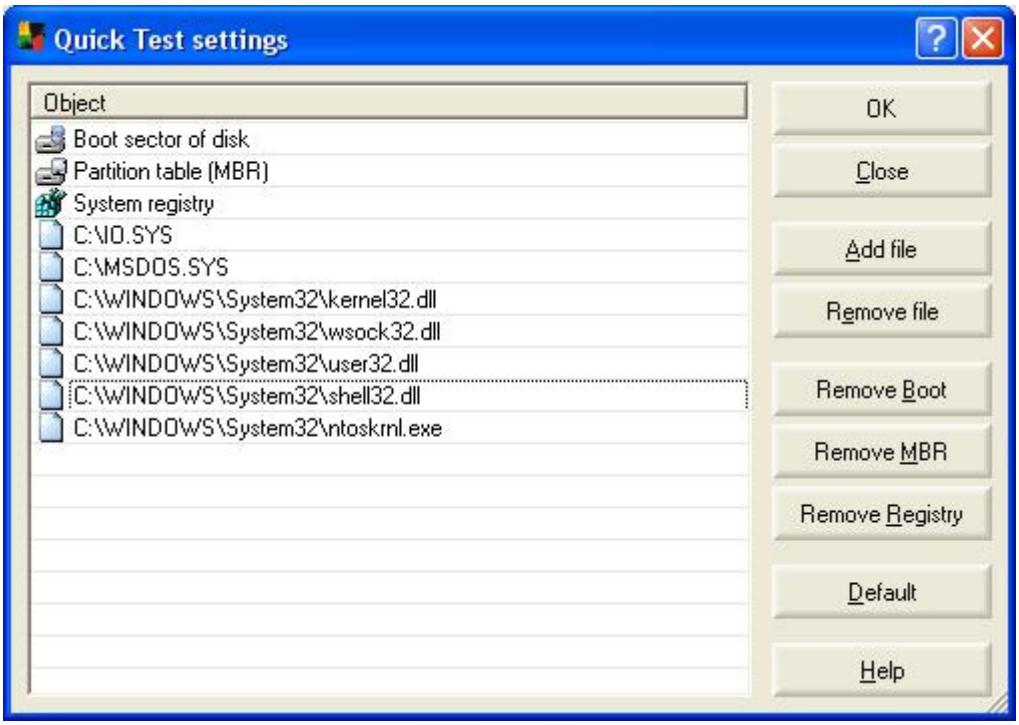
- **Remove** – A kiválasztott teszt törlése (A gyárilag elkészített tesztek nem törölhetőek)
  Gyári tesztek:
  - **Complete test** – Teljes ellenőrzés (Összes belső lemezegység)
  - **Removable media test** – hordozható lemezek ellenőrzése (hajlékony lemez, CD-ROM, stb.)
  - **User test** – felhasználói általi alap ellenőrzés típus
  - **Detailed Complete test** – Tüzetes teljes ellenőrzés (Összes belső lemezegység)
  - **Detailed Removable media test** – hordozható lemezek tüzetes ellenőrzése (hajlékony lemez, CD-ROM, stb.)
  - **Detailed User test** – felhasználói általi tüzetes ellenőrzés típus
  - **Quick test** – A számítógép operációs rendszerének gyors ellenőrzése
- **Start test** – Az ellenőrzés elindítása
- **Close** – Az ablak bezárása

Nagyon érdekes az **Add** (új ellenőrzés) létrehozásának működése. Az új teszt mindig annak az ellenőrzésnek, a beállításainak a lemásolásával kezdődik, amelyik ki van választva. Önnek csak a megfelelő módosításokat kell végrehajtania az új teszten és egy megadott néven, le kell azt mentenie. Egyetlen teszt van, amely ilyen módon nem másolható, mégpedig a **Quick test** (gyors ellenőrzés). A **Quick test** beállításai csak módosíthatók, lemásolása nem lehetséges.

Tekintsük át először a **Quick test** beállítását és azok módosítását.



A gyors ellenőrzés beállításainak módosításához az Ellenőrzés kezelőben (Test manager) kattintson egyet a **Quick test** soron, majd nyomja meg az **Edit** gombot. Ekkor a következő ablakot kell látnia:



A megjelenő képernyőn a gyors teszt által ellenőrzött rendszer összetevők listáját láthatja. A lista tetszőleges állománnyal bővíthető, illetve bármely komponens ki is vonható az ellenőrzés alól.
Az gyári beállítások a következők:

- **Boot sector of disk** – A partíció (lemezrész) Boot (indító) szektora
- **Partition table (MBR [Master Boot Record])** – Partíciós (lemezleíró) tábla
- **System registry** – A Windows operációs rendszerek és a felette futó programok beállításait tartalmazó rendszerleíró adatbázis.
- Ezt követően az operációs rendszer néhány állománya van felsorolva.

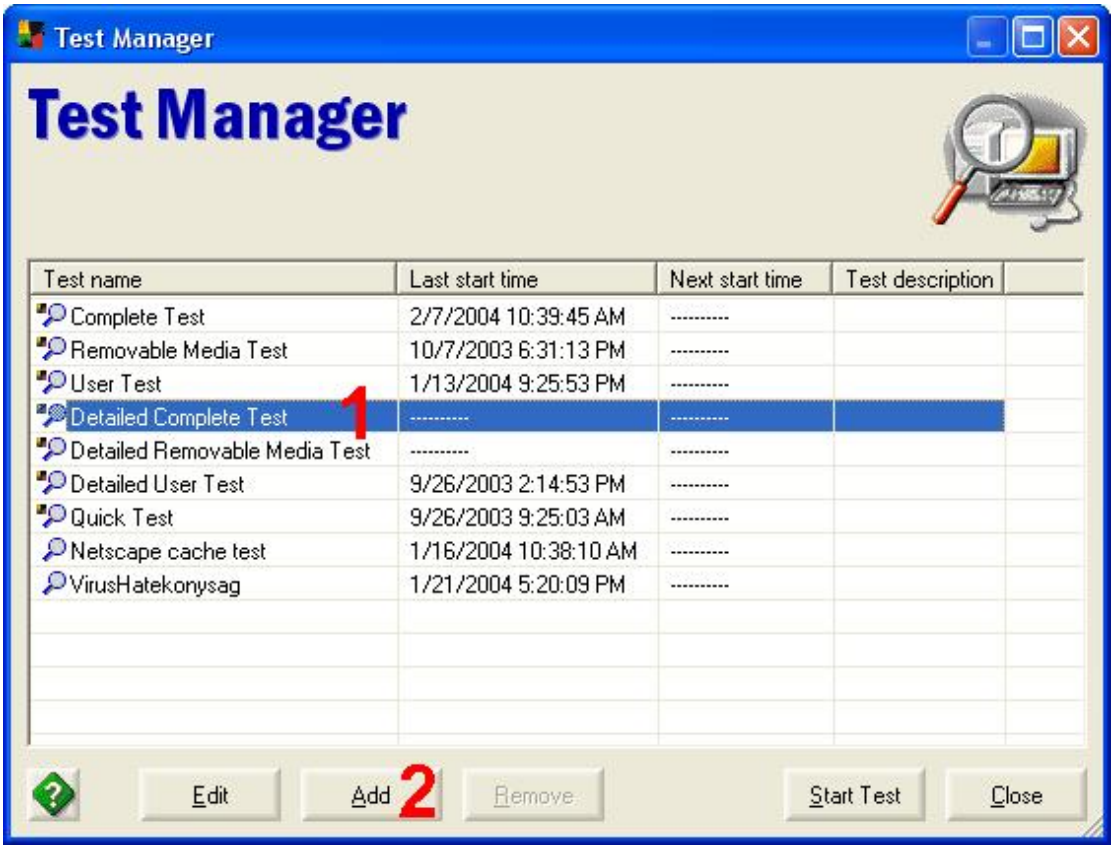
A beállító ablak nyomógombjai:

- **Ok** – a módosítások jóváhagyása
- **Close** – Az ablak bezárása
- **Add file** – új állományok hozzáadása
- **Remove file** – állomány kivonása az ellenőrzés alól
- **Add/Remove Boot** – Az indító szektor ellenőrzésének Be/Ki kapcsolása
- **Add/Remove MBR** – A lemezleíró tábla ellenőrzésének Be/Ki kapcsolása
- **Add/Remove Registry** – A rendszerleíró adatbázis ellenőrzésének Be/Ki kapcsolása
- **Default** – A gyári beállítások visszaállítása
- **Help** – Angol nyelvű súgó.

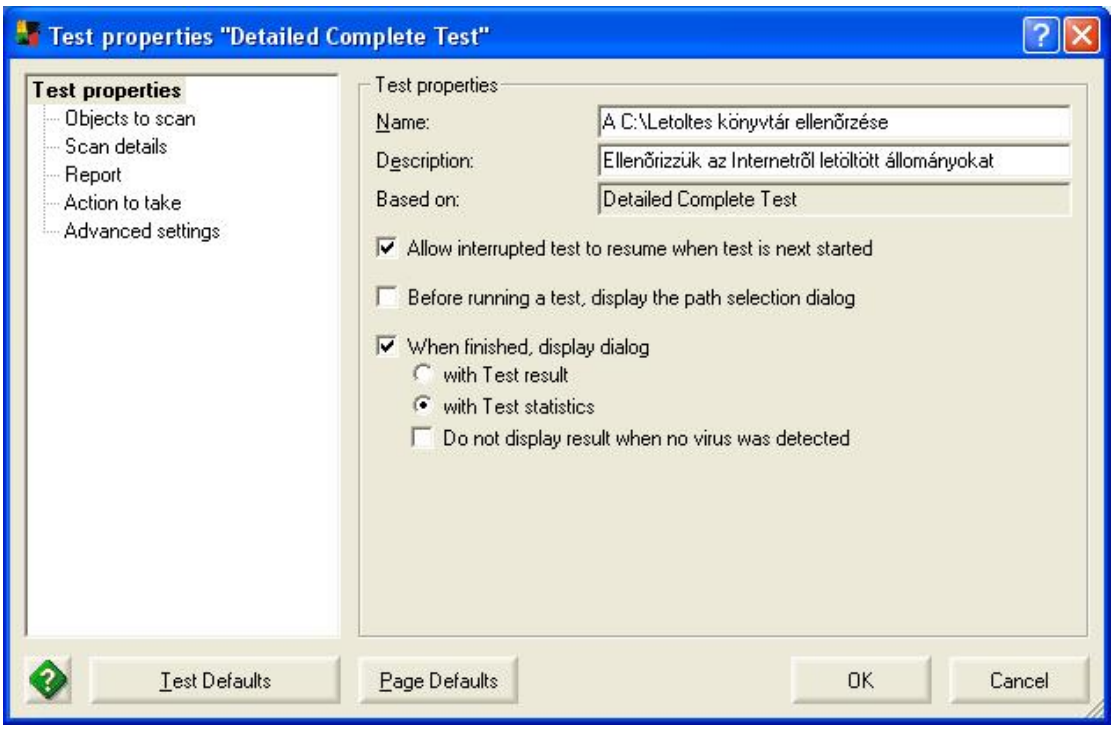
Új teszt létrehozása
Új tesztek létrehozása előtt mindig alaposan tervezze meg, hogy a lehető legjobb beállításokat készíthesse el.
Új teszt létrehozását egy példán keresztül szeretnénk bemutatni:

Adott egy számítógép, amelyet rendszeresen használnak Internetezésre. A számítógép felhasználója az Internetről letöltött állományokat a mindig a **C:\Letoltes** könyvtárba menti le.
Elvárások:

- Szeretnénk, hogy ezt a könyvtárat a többi lemezterület ellenőrzése nélkül is bármikor ellenőrizhessük.
- Szeretnénk, ezt a területet a lehető legaprólékosabban ellenőrizni, mivel az ide lementett állományok az Internetről, megbízhatatlan forrásból származnak.



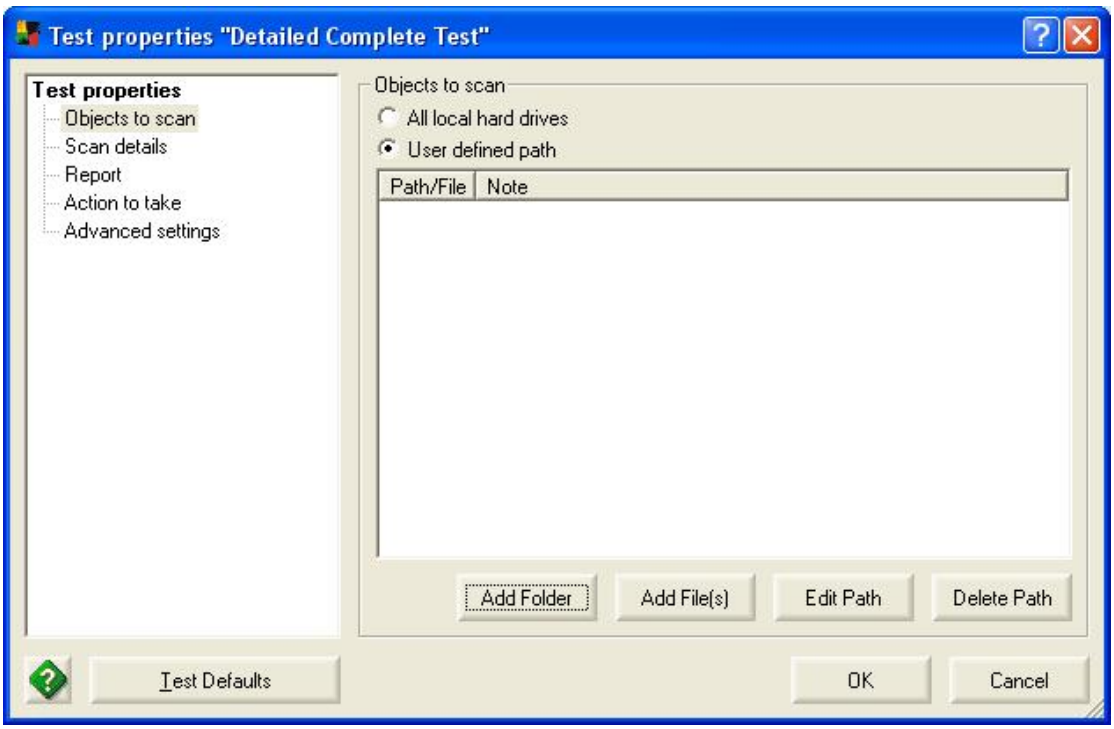
Céljainknak leginkább a **Detailed Complete test** (Tüzetes teljes ellenőrzés) felel meg kiindulásként. A teszt lemásolásához és saját teszt létrehozásához kattintson a **Detailed Complete test** sorra, majd az **Add** gombra. Ez után az alábbi ablakot kell látnia:



Elsőként a bal oldali menüben a **Test Properties (Ellenőrzés beállítások)** főadatai jelennek meg. Itt az alábbi paraméterek beállítása lehetséges:

- **Name** – Az ellenőrzés neve, amely tetszőleges szöveg lehet.
- **Description** - Az ellenőrzés rövid magyarázata, amely tetszőleges szöveg lehet.
- **Based on:** - Annak a tesztnek a neve, amely másolataként a saját ellenőrzést létrehoztuk. Jelen esetben ez a **Detailed Complete test.**
- **Allow interrupted test to resume when test is next started** – Ha Ön megszakítja az ellenőrzést, akkor ennek az opciónak kiválasztásával a teszt legközelebbi indításakor lehetősége lesz a megszakított ellenőrzés folytatására is. Ellenkező esetben az ellenőrzés elölről fog kezdődni.
- **Before runnig a test, display path selection dialog** – Az ellenőrzés indítása előtt mindig jelenjen meg egy kérdés, hogy mely könyvtárat szeretné ellenőrizni.
- **When finished, display dialog** – Az ellenőrzés után adjon információt
  - **with Test result** – az ellenőrzés végeredményéről
  - **with Test statistics** – részletes adatokkal az ellenőrzött fájlok számáról és az fájlellenőrzések eredményéről és az összes figyelmeztető üzenetről
  - **Do not display result when no virus was detected** – Csak akkor jelenjen meg információ, ha vírusfertőzést észlelt.

Az **Objects to Scan** menü

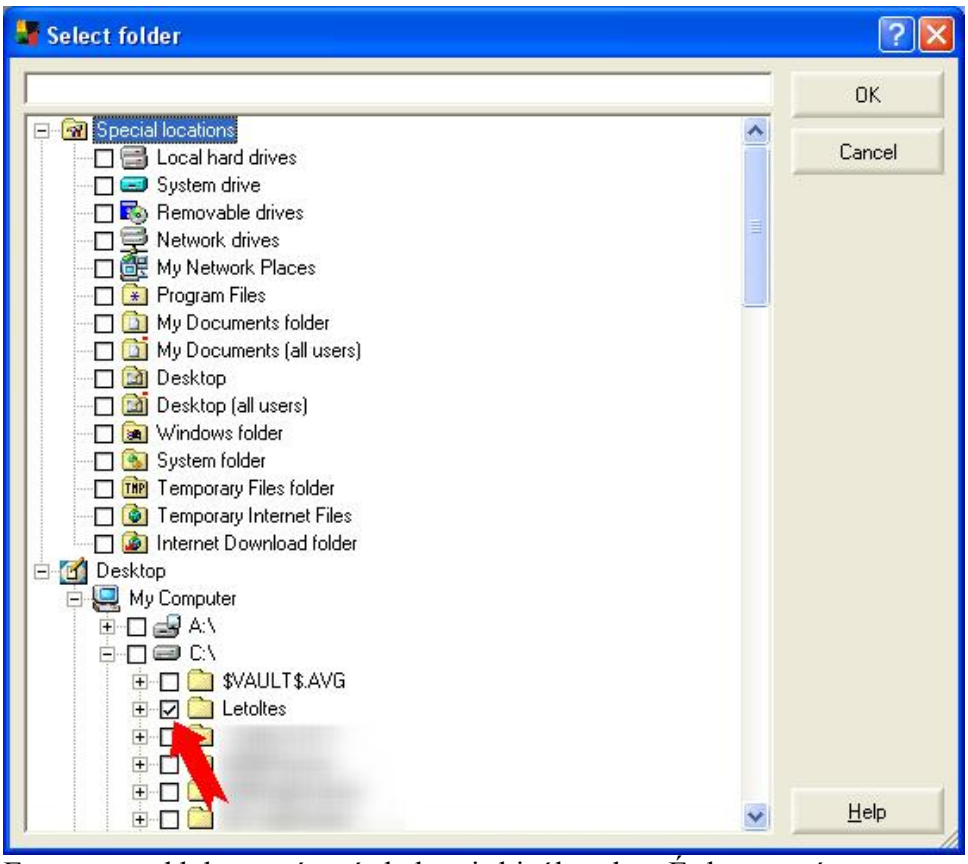


Itt kiválaszthatja azokat az objektumokat, amelyeket szeretne ellenőrizni. Beállítási lehetőségek:

- **All local hard drives** – Minden merevlemez meghajtó ellenőrzése a számítógépben
- **User defined path** – Csak a kiválasztott könyvtárak és meghajtók. Az ablakban megjelenik a kiválasztott objektumok listája.
  - **Add folder** – Könyvtár hozzáadása a listához
  - **Add files** – fájl hozzáadása a listához.
  - **Edit path** – útvonal módosítása a listában
  - **Delete path** – útvonal törlése a listából

A példánkban látható beállításokhoz:

1. Válassza ki a **User defined path** opciót
2. Az **Add folder** gomb segítségével válassza ki a c:\Letoltes könyvtárat

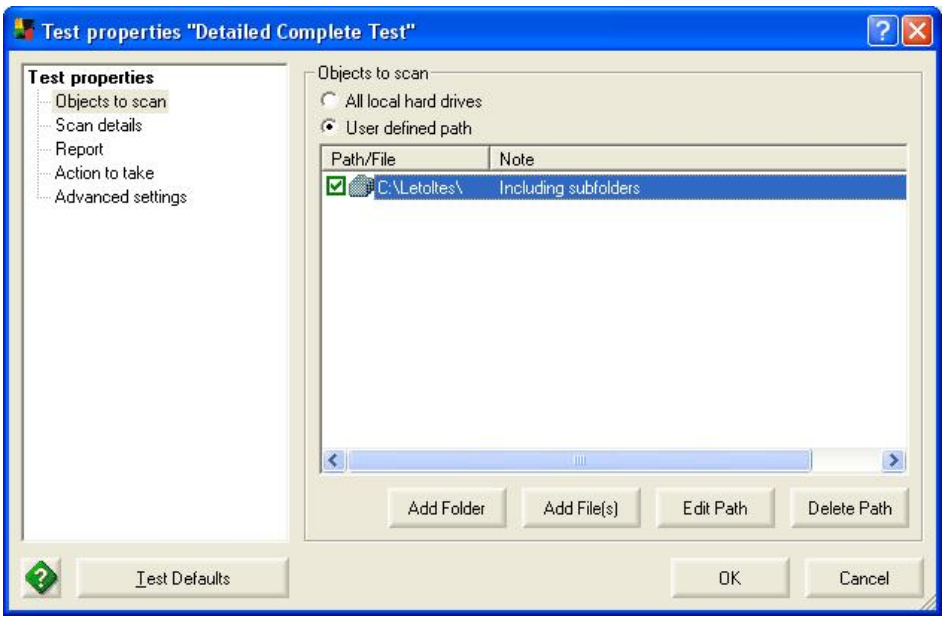


Egyszerre több könyvtárat és helyet is kiválaszthat. Érdemes még megismerni a **Special locations (Speciális helyek)** listáját, ami a lista tetején látható.

- Local hard drives – A számítógépbe épített összes merevlemez
- System drive – Az operációs rendszert tartalmazó inidító merevlemez. Általában a C: meghajtó, vagy lemezrész.
- Removable drives: Hordozható (általában a hajlékony és CD lemezek) lemezek.
- Network drives – Hálózati meghajtók, megosztások
- My Network Places – Hálózati helyek
- Program Files – Programok alapértelmezett telepítési könyvtára
- Desktop – A bejelentkezett felhasználó asztala
- Desktop (all users) – A felhasználók által közösen használt asztalrész
- Windows folder – A Windows operációs rendszerek telepítési könyvtára
- System folder - A Windows operációs rendszerek System könyvtára. Ez az operációs rendszer működéséhez szükséges fontos fájlokat és programokat tartalamaz.
- Temporary files forder – Az átmeneti állományokat tartalmazó könyvtár
- Temporary Internet files – Az Internetről letöltött állományok ideiglenes tároló helye

- Internet download folder – Az alapértelmezett könyvtár, ahová az Internetről letöltött állományok kerülnek. *(ez nem a példában szereplő c:\Letoltes könyvtár!)*

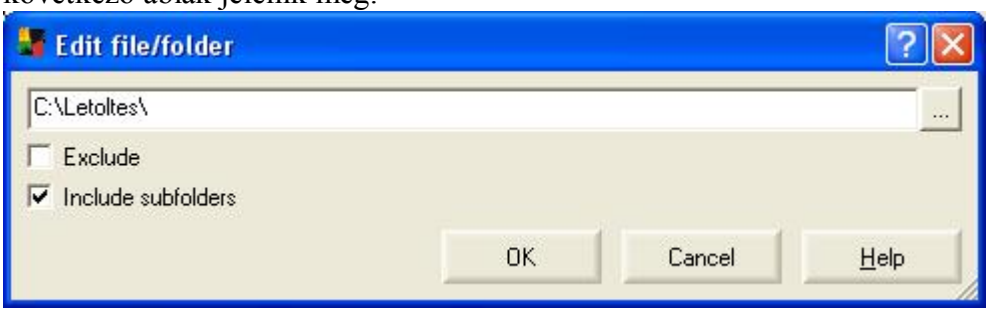
3. Az **OK** gombra kattintva a kiválasztott objektumok felkerülnek a listára:



A listában az alábbi információk jelennek meg:

- **Path/File** – A kiválasztott objektum, fájl vagy útvonal neve
- **Note** - megjegyzése
- **Include subfolders** – a kiválasztott könyvtár alkönyvtárait is ellenőrizze
- **No subfolders** – az alkönyvtárakat ne ellenőrizze

4. A beállítások finomíthatók, ha a listában a **kiválaszt** egy objektumot (példánkban csak a c:\Letoltes lehetséges), úgy hogy egyet rákattint, majd megnyomja az **Edit Path** gombot. Ekkor a következő ablak jelenik meg:

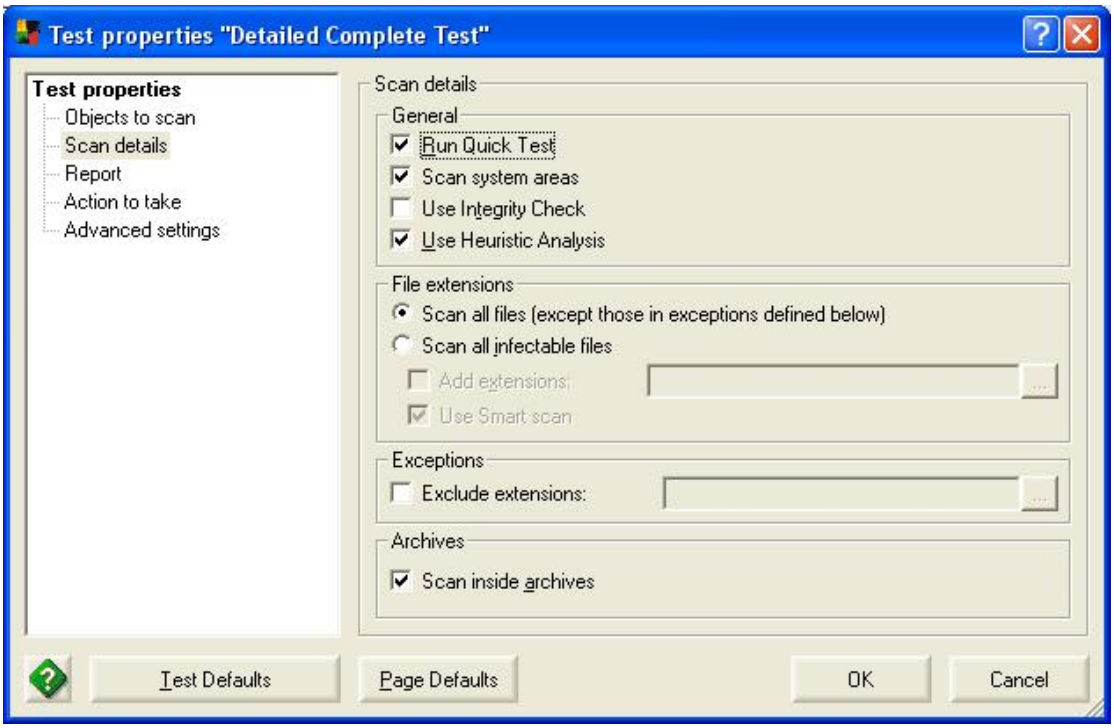


A itt megjelenő sorba a billentyűzetről maga is beképelheti az útvonalat, vagy újat választhat a sor végén látható három ponttal jelölt gomb segítségével. Itt az alábbi opciók állíthatók még be:

- **Exclude** – Felfüggesztés. Ha listába több elemet is felvett, akkor az Exclude négyzetet bejelölve, akkor a kiválasztott útvonalat az ellenőrzés alól álmenetileg kizárhatja.
- **Include subfolders** – Az alkönvtárakat is ellenőrizze. A négyzetet bejelölve a megadott könyvtár alkönyvtárai is ellenőrzésre kerülnek, míg ha üresen hagyja azt, úgy csak fenti sorban látható könyvtár, jelen esetben a c:\Letoltes\

5. A módosítások elvégzése után válassza az **OK** gombot.

A **Scan Details** menü



Itt az ellenőrzés részletei állíthatók be:

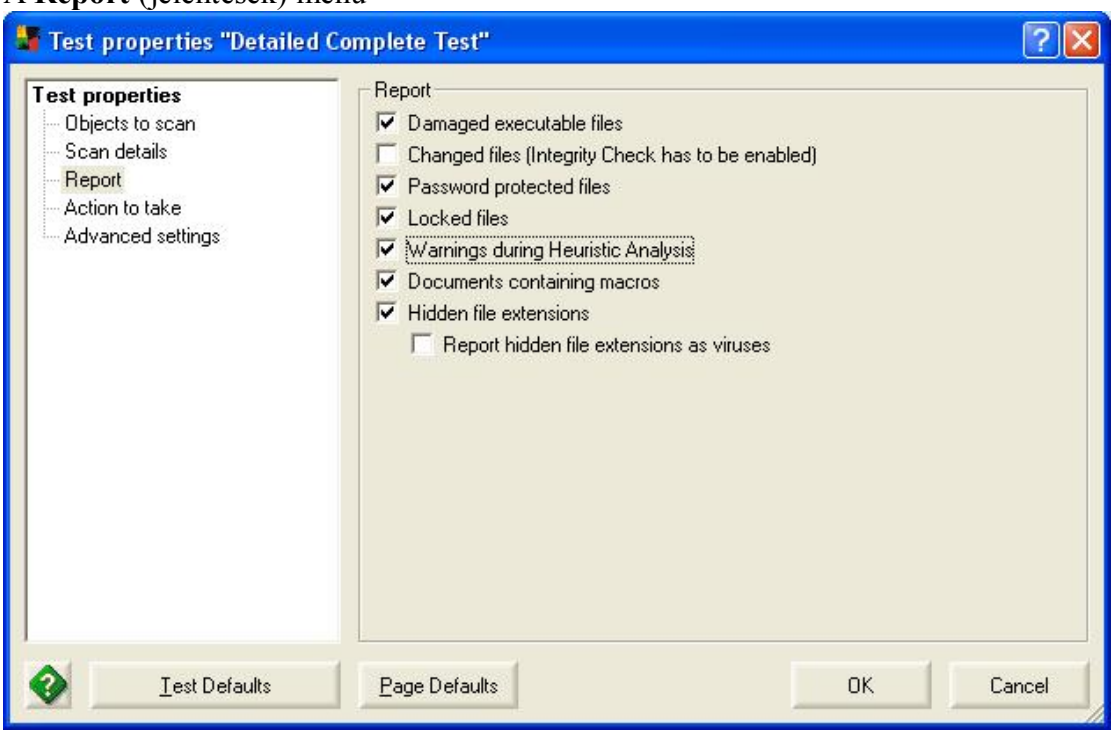
- **Run Quick test** – a program indulásakor egy igen gyors áttekintő ellenőrzést futtat a számítógépen. (Ld. **Test manager** (Ellenőrzés kezelő) **Quick Test** beállítás)
- **Scan system areas** –az operációs rendszerhez tartozó területek ellenőrzése
- **Use integrity check** – Először ellenőrzi, hogy a tesztelendő fájl módosult-e a legutóbbi ellenőrzés óta (nem dátum alapján) és csak akkor végez vírusellenőrzést, ha igen. Az opció használatával jelentős sebsségnövekedés érhető el.
- **Use Heuristic Analysis** – programszimulációs ellenőrzés. Nagyon hatékony, bizonyos esetekben a vírusok mutánsait is képes felismerni, anélkül, hogy azok különálló vírusként ismertek lennének.
- **Scan all files** – Minden fájlt ellenőriz, tekintet nélkül arra, hogy az adott fájl műszakilag tartalmazhat-e fertőzésre képes állapotban vírust.
- **Scan All infectable files** – Csak azokat a fájlokat ellenőrzi, amelyek műszakilag tartalmazhatnak fertőzésre képes állapotban vírust.
    - **Add extensions** – az AVG által ilyennek minősítetteken kívül Ön megjelölhet további fájl típusokat kiterjesztésük segítségével, amelyek ellenőrzését kéri.
    - **Use smart scan** – Intelligens keresés. Az AVG képes felismerni a fájlokat, hogy azok fertőzhetőek-e, akkor is, ha a kiterjesztésük nem utal erre. A négyzet bejelölésével engedélyezheti a kiterjesztés nélküli fájlazonosítás funkciót.
- **Exclude extensions –** kiterjesztések kihagyása. Az Ön által meghatározott kiterjesztésű fájlokat az AVG nem fogja ellenőrizni. Akkor lehet rá szüksége, ha Ön vírus kutatással foglalkozik és bizonyos állományokat ki szeretne

hagyni az ellenőrzés alól, illetve ha olyan alkalmazásokat használ, amelyek kiterjesztése megegyezik valamelyik más fertőzhető állománytípus kiterjesztésével, de az Ön által használ fájlok nem fertőzhetőek. Ezeknek a fájloknak a kihagyása gyorsabb ellenőrzést eredményez. *Élővigyázattal használja az opciót!*

- **Scan inside archives –** A tömörített fájlok tartalmát is ellenőrizze. *Figyelem! A jelszóval védett, tömörített fájlok tartalma nem ellenőrizhető!*

*Példánkban érdemes beállítani a **Run Quick Test** opciót, mivel az Internetről nem fájlként érkező támadásokra is számíthatunk, akik hátsó ajtókon az operációs rendszer hibáit és helytelen beállításait kihasználva érkeznek a számítógépre. Ez az opció kiegészítésképpen gyorsan átfésüli a számítógép érzékeny területeit. A **Scan System areas** segítségével ugyancsak a rendszerterületeket ellenőrzi, de a **Quick Test**ből a felhasználó kivehet komponenseket, itt viszont nem.*
*Az **Use Integrity Check** opciót most ne használjuk, hiszen itt esetleg kizárhatunk fájlokat a későbbi ellenőrzés alól, ha most nem találunk vírust. Márpedig az Internetről lehet a legkönnyebben megfertőzni a számítógépet olyan vírusokkal, amelyek még ismeretlenek a víruskereső programok számára.*
*A **Use Heuristic Analysis** (szimulációs keresés) opciót mindenképpen érdemes használni, hiszen a lehető legnagyobb gondossággal szeretnénk eljárni.*

A **Report** (jelentések) menü



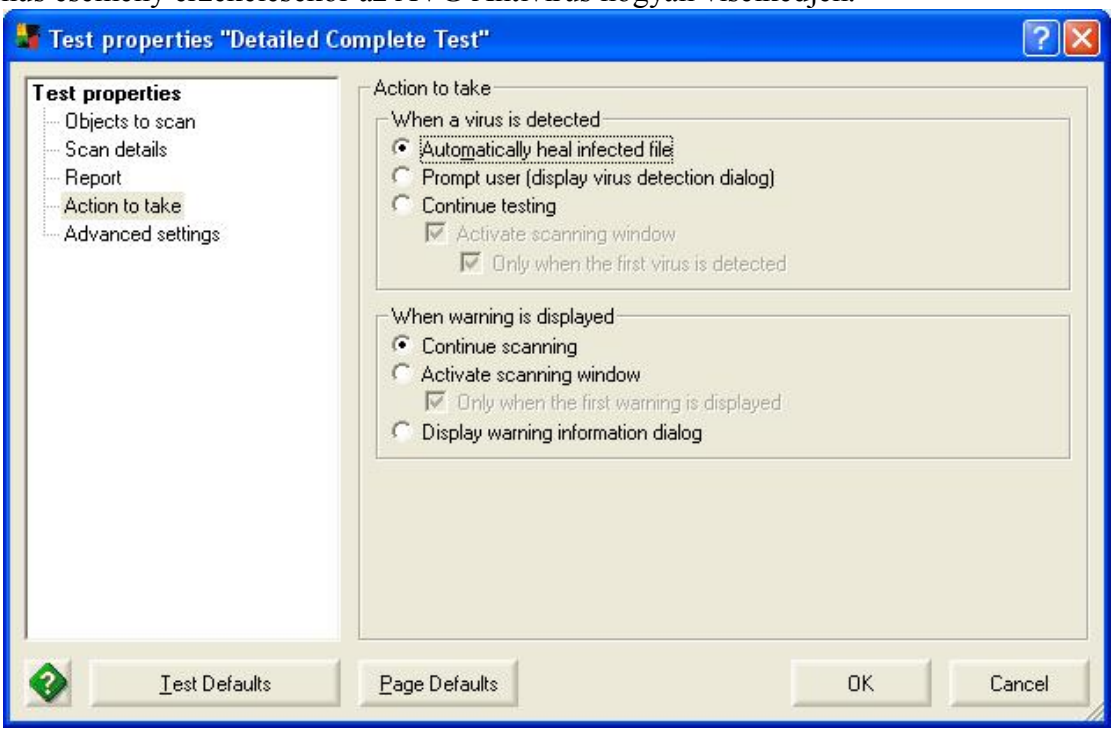
A megjelenő ablakban beállíthatja, hogy az ellenőrzés eredményéről milyen részletességű kimutat kér. Ezzel olyan problémás állományok felderítésére is lehetőség van, amelyek esetlegesen ismeretlen vírussal fertőzöttek, vagy valamilyen oknál fogva tartalmuk megváltozott. Ez az esetek többségében általában nem fertőzést jelent. Ezeknek a kimutatásoknak az értelmezése a szokásosnál magasabb szintű informatikai ismeretet igényel.
Több lehetőség egyidejű kiválasztására is mód van:

- **Damaged executable files** – Sérült futtatható állományok. Ez program fájlok sérülésére utal. Valamilyen oknál fogva a programfájl csonkolódott, tartalma megváltozott. Ha Ön programozó, előfordulhat, hogy a közelmúltban módosított programjai is megjelennek a listán.
- **Changed files (Integrity Check has to be enabled)** – Módosult fájlok. Minden olyan állomány megjelenik a riportban, amely az előző ellenőrzés óta megváltozott. Ennek oka rendszerint a napi szokásos munkavégzés. Az opció használatának előfeltétele, hogy az **Integrity Check (változás ellenőrzés)** opció az ellenőrzéseknél be legyen kapcsolva.
- **Password protected files** – Megjeleníti azokat az állományokat. Amelyek jelszóval védettek és emiatt az ellenőrzésük nem lehetséges.
- **Locked files** – Kisajátított állományok. Bizonyos állományokhoz a hozzáférést más programok, vagy az operációs rendszer saját részre lefoglalja. Ezeket az AVG Antivírus megpróbálja tesztelés miatt használatba venni. Amennyiben ez több különféle módon való próbálkozás ellenére sem sikerül, úgy a fájl megjelenik a kimutatásban.
- **Warnings during Heuristic Analysis** – Figyelmeztetések a szimulációs keresés közben. Ezek nem jelentenek feltétlenül fertőzést, de a gyanús események a kimutatásban megjelennek.
- **Documents containing macros** – Makrókat tartalmazó dokumentumok. A makrók rendszerint a felhasználók által készített az ismétlődő feladatokat segítő rövid programok. Ezek a programok rosszindulatú tevékenységeket is végezhetnek, az ilyen programkódok a makró vírusok. Ez az opció megjelenít minden olyan állományt, amely makrókat tartalmaz, akkor is ha abban egyébként vírust nem érzékelt. Ez abban lehet az Ön segítségére, ha valamelyik állománya eddig nem tartalmazott makrókat és egyszer csak megjelenik a listán, noha Ön nem változtatta meg. Ez rosszindulatú kódrészletre utaló nyom lehet.
- **Hidden file extensions** – Rejtett kiterjesztések. A vírusok igyekeznek elkerülni a lelepleződést. Erre programozójuk sokféle trükköt vet be. Gyakran kettős, rejtett kiterjesztéssel vannak ellátva amiatt, hogy másnak ismerjék fel Őket, mint amik valójában. A többszörös, rejtett kiterjesztés nem feltétlenül jelent veszélyt. A programozók, rendszergazdák sok esetben használják a fájlok tartalmának, tömörítési módjának szakemberek által értelmezhető leírására.
    - **Report hidden file extensions as viruses**– A rejtett kiterjesztéseket mindig vírusként érzékelje. Ezt az opciót csak akkor érdemes bekapcsolni, ha biztos benne, hogy az előző pontban említett lehetőségek nem állnak fenn. A fájlok nem jelölési céllal rejtett kiterjesztésűek.

A példánkban szereplő feladat megoldásához az alábbi lehetőségek beállítása célszerű:
***Damaged executeable files** - annak érdekében, hogy a rendellenes formátumú futtatható állományokról tudomást szerezzen*
***Password protected files** – Sok esetben a vírusokat személyes jellegű információként tüntetik fel, amelyet jelszóval védtek, hogy a víruskereső programok ne férjenek hozzá. Ezért fontos jelenti az ilyen állományokat is.*

Locked files *– Ha már fut a vírus, esetleg zárolhatja az Őt tartalmazó fájlt, szintén a víruskereső programok akadályozása érdekében. Ezért szintén fontos, hogy a példában szereplő esetben ellenőrizzük, hogy van-e gyanús okból zárolt állomány.*
Warnings during Heuristic Analysis *– A szimulált futtatás során jelentkező minden gyanús esemény szintén* ***fontos.***
Documents contains macros*, az Internetről letöltött, makrókat tartalmazó állományok potenciális* ***vírushordozók. Ezekkel mindig legyen elővigyázatos!***
Hidden file extensions*: Az egyik leggyakoribb elrejtési módja a vírusos fájloknak az ha elrejtik a kiterjesztését, többszörös kiterjesztést alkalmaznak. Ilyenkor az állományt más típusúként ismerhetik fel, ami miatt átsiklanak jelenlétük felett. Az Internetről letöltött állományok esetében legyünk elővigyázatosak és személyesen győződjünk meg az ilyen kiterjesztések indokoltságáról.*

Action to take (mit tegyek, ha...) menüpontban meghatározhatja, hogy vírus, illetve gyanús esemény érzékelésekor az AVG Antivírus hogyan viselkedjen.

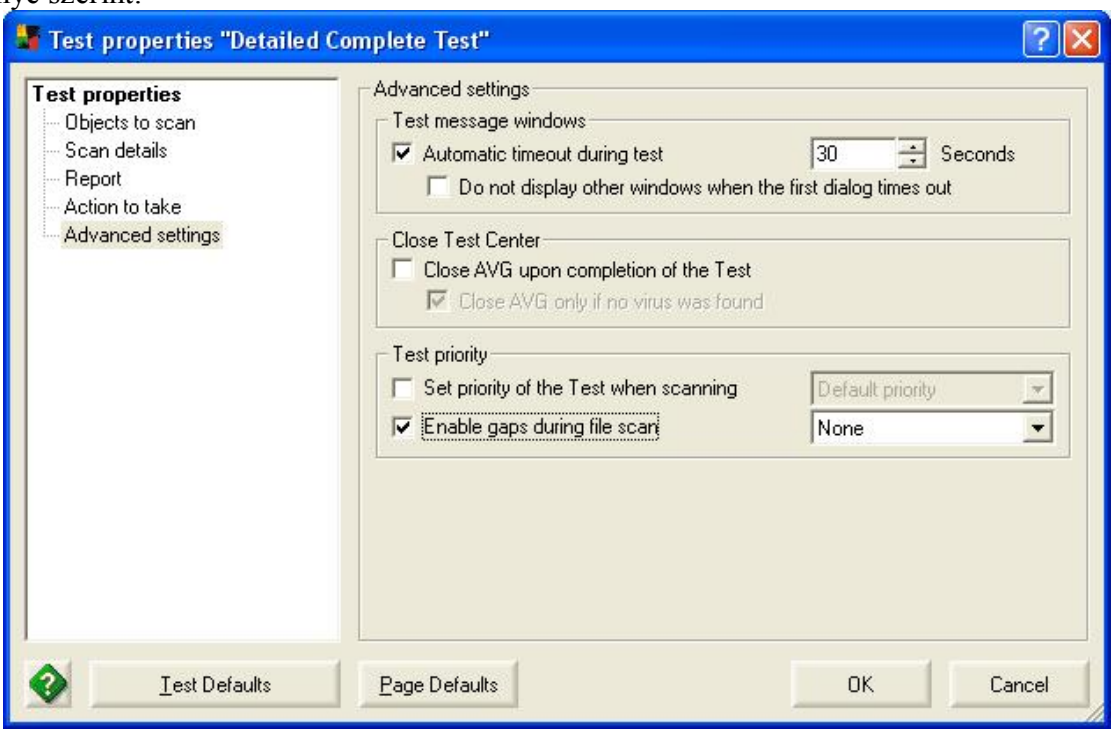


- **When a virus is detected** – Ha vírust talált
  - **Automatically heal infected files** – Automatikusan próbálja vírusmentesíteni a fájlt (ha lehetséges), az eredeti tartalom helyreállítása mellett
  - **Prompt user (display virus detection dialog)** – Kérdezze meg a felhasználót. Általában négy lehetőséget kínál fel ilyenkor: Heal – vírus mentesít, Delete: töröl, Move to virus vault: karanténba helyez, Continue: nem tesz semmit
  - **Continue testing** – ne tegyen semmit, csak jelezze
    - **Activate scanning window** – jelenítse meg az ellenőrzés képernyőjét ha nem lenne látható
      - **Only when first virus detected** – csak az első vírus esetében tegye ezt

- **When warning is displayed –** A figyelmeztető ablak jelenik meg
  - **Continue scanning –** folytassa az ellenőrzést
  - **Activate scanning window** – jelenítse meg az ellenőrzés képernyőjét ha nem lenne látható
    - § **Only when first warning displayed** – csak az első figyelmeztetés esetében tegye ezt
  - **Display warning dialog –** Külön ablakban hívja fel a figyelmet az üzenetre

A példában szereplő feladat megoldáshoz az alábbi opciókat célszerű beállítani:
When a virus is detected / Automatically heal infected files*: Próbálja meg eltávolítani az esetleges vírust.*
When warning is displayed / Continue scanning: *Figyelmeztető üzenetek ne jelenítse meg azonnal, mivel sok fájl esetén az sok megszakítást okozhat és lassítja a keresést (A jelentés beállításoknál megadottak alapján az ellenőrzés végén megjelenő riportban minden fontos információ benne lesz)*

Advanced settings - Haladó beállítások
Itt megadhatja, hogy milyen egyéb automatizmusokat kíván alkalmazni. Ezzel javíthatja számítógépe teljesítményét, gyorsíthatja az ellenőrzéseket, mindezeket igénye szerint.



- **Test message windows** – Ellenőrzés közbeni üzenetek
  - **Automatic timeout during test** – Az ellenőrzés közben üzenetek automatikusan tűnjenek el a megadott idő (másodperc) múlva, ha nem történik felhasználói beavatkozás
    - § **Do not display other windows when the first dialog times out** – Ha az első üzenetre nem érkezett felhasználói válasz, akkor a több ne jelenjen meg.
- **Close test center –** Az ellenőrző központ ablakát zárja be

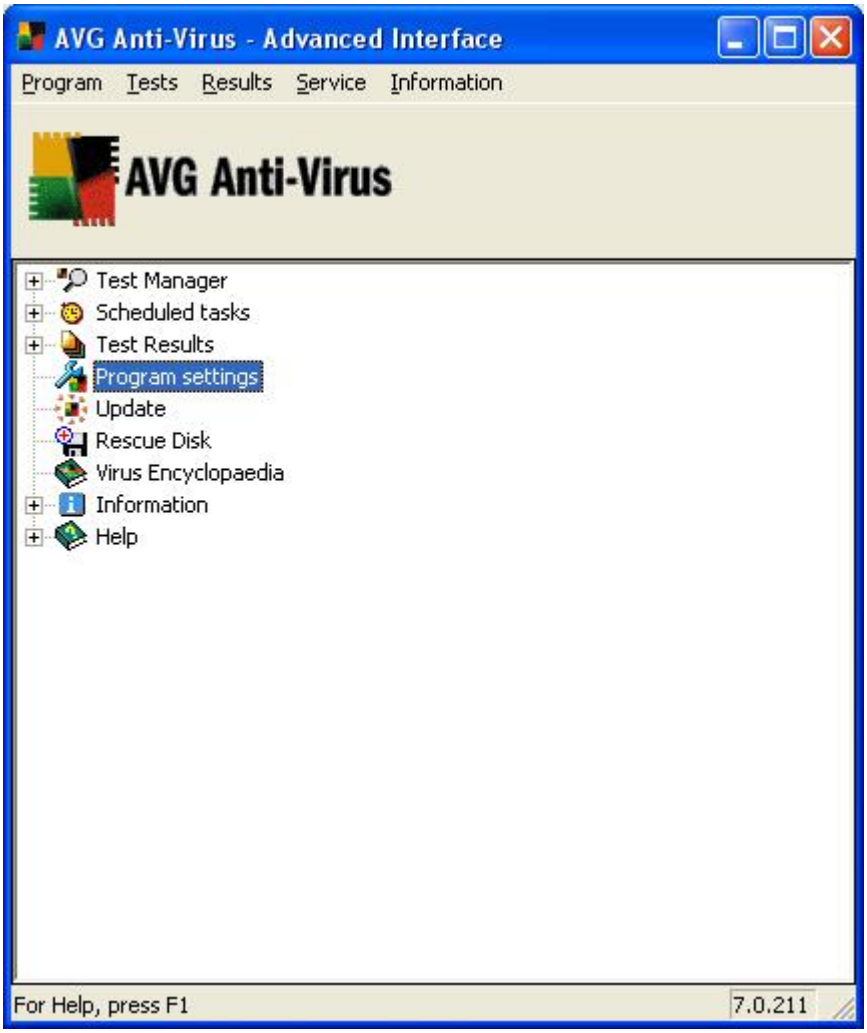
- **Close AVG upon completion of the Test –** ha az ellenőrzés befejeződött
  - **Close AVG only if no virus was found –** Csak akkor zárja be, ha nem talált vírust.

- **Test priority** – Az ellenőrzés fontossága. Ezekkel a beállításokkal befolyásolhatja, hogy számítógépe mennyire kezelje elsőbbséggel a vírusuellenőrzést. Az alacsonyabb fontosság nem jelent alacsonyabb biztonságot, csupán annyit, hogy az ellenőrzés lassabban zajlik. Így ha Ön közben dolgozik számítógépén, úgy az Ön feladataival a gép többet foglalkozik, az ellenőrzés pedig lassabb lesz. Ez természetesen fordítva is igaz, vagyis az Ön munkájával szemben is előtérbe helyezheti a vírusellenőrzés fontosságát.
  - **Set priority of the Test when scanning** – az ellenőrzés fontossága
    - **Low priority** – csekély fontosság
    - **Lower priority** – alacsony fontosság
    - **Default priority** – normál fontosság (gyári beállítás)
    - **High priority** – nagy fontosság
  - **Enable gaps during files can –** A kiválasztott fájlok ellenőrzése közötti szünet. Két fájl ellenőrzése között az AVG szünetet tart.Ennek mértékét Ön a számítógépe teljesítményének és a keresés gyorsaságának függvényében Ön állíthatja be. Az ellenőrzések közötti szünet áll az Ön rendelkezésére a beavatkozáshoz, illetve az AVG ilyenkor veszi figyelembe az Ön módosító parancsait.
    Választható lehetőségek, novekvő sorrendben:
    - **None –** nem várakozik
    - **Minimum –** minimális időt vár
    - **Default –** alapértelmezés
    - **5 milliseconds –** 5 ezredmásodperc
    - **10 milliseconds –** 10 ezredmásodperc
    - **50 milliseconds –** 50 ezredmásodperc

A példánkban szereplő feladat megoldásának hatékonyságára gyakorlatilag nincs hatással ez a beállítás.

Program beállítások (Program settings)

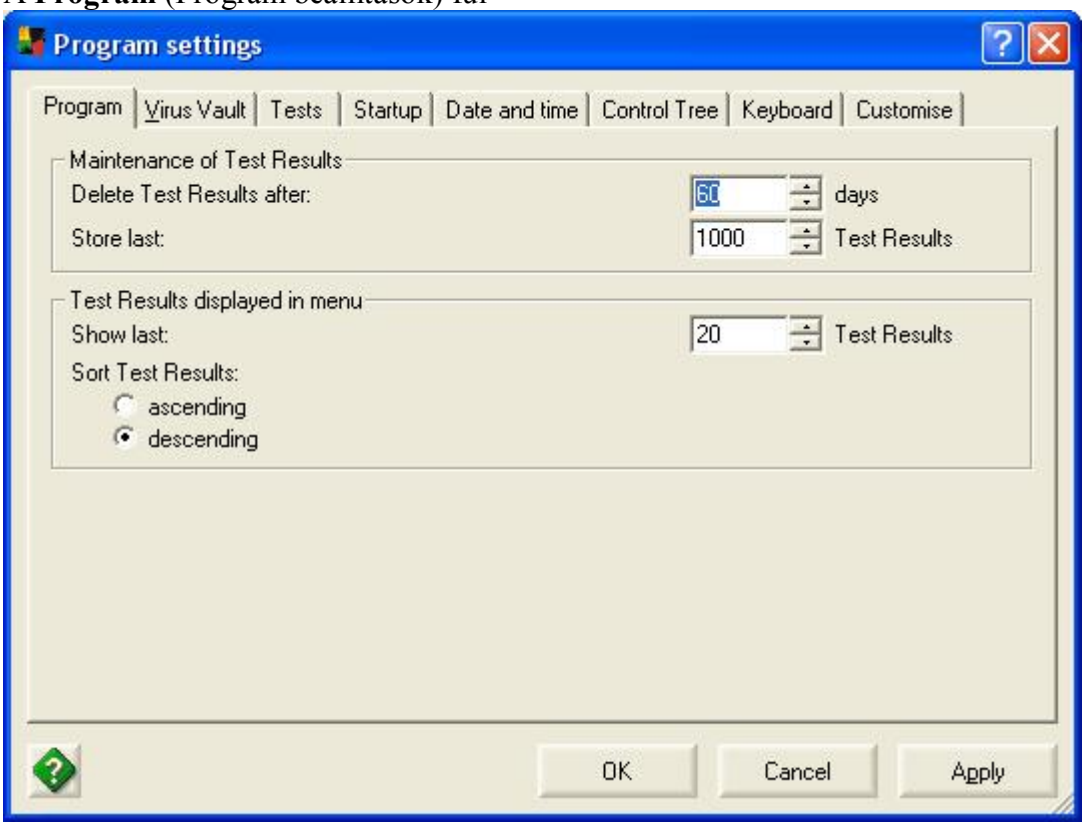
A program működését és megjelenését befolyásoló paramétereket állathatja be ezen a részen.



A párbeszédablak megjelenítéséhez kattintson duplán a **Program settings** soron.

Ekkor a következő ablakot fogja látni:

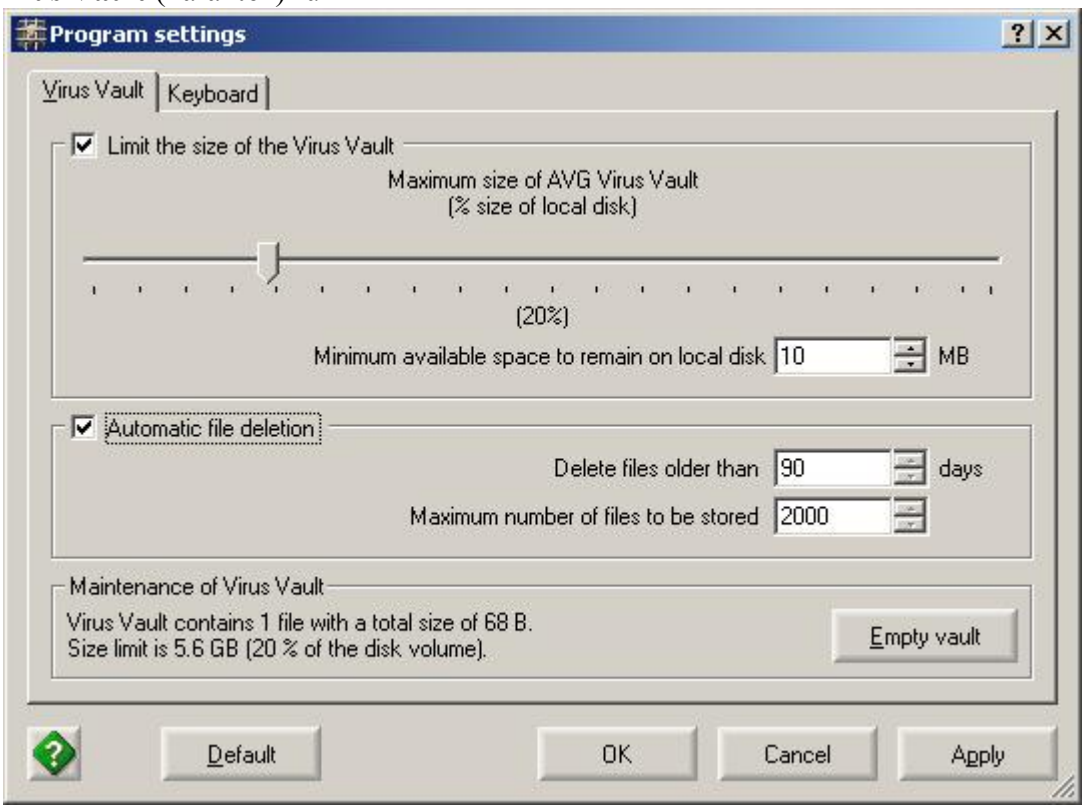
A **Program** (Program beállítások) fül



Az ablak beállításai gyakorlatilag nem befolyásolják az ellenőrzések hatékonyságát. Itt következő paraméterek módosításra van lehetősége:

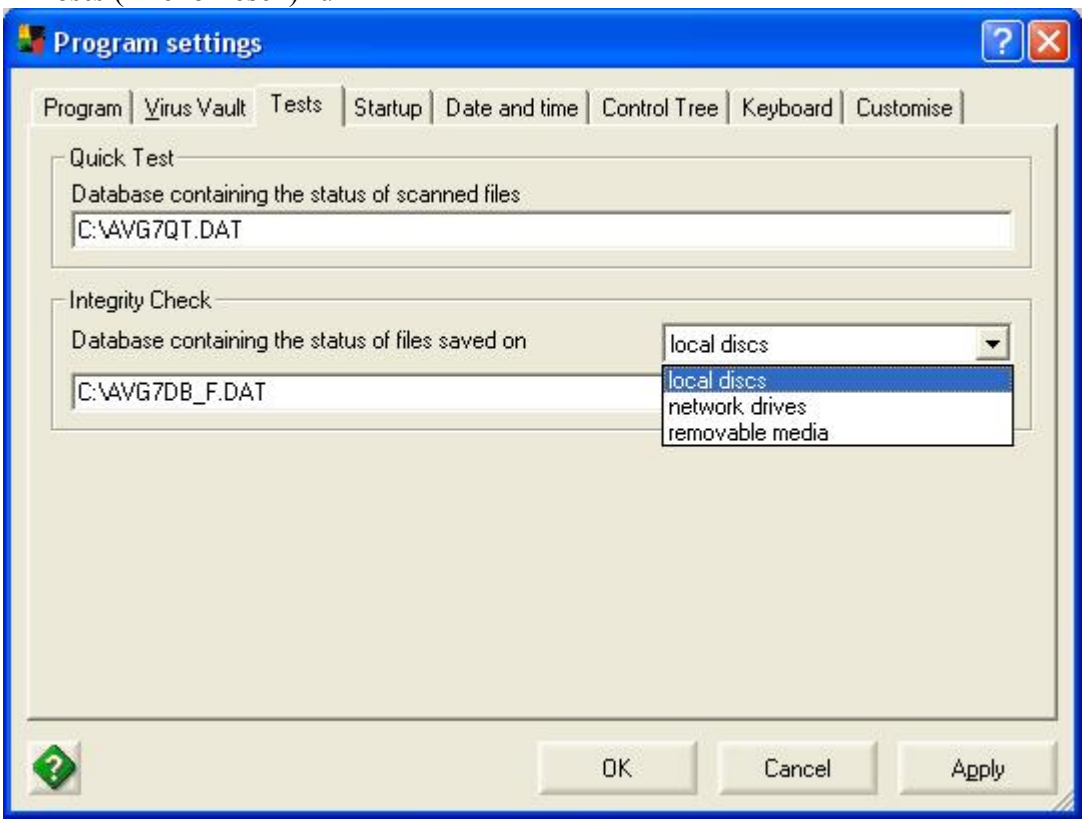
- **Maintenance of Test Results** – Az ellenőrzések jelentéseinek kezelés
  - **Delete Test Results after** – Automatikusan törölje a megadott számú napnál idősebb jelentéseket
  - **Store last** – Legfeljebb a megadott mennyiségű jelentést tárolja. Ha ezt túllépné, akkor a legrégebbiek automatikusan törlésre kerülnek
- **Test Results displayed in menu** – A menüben megjelenő ellenőrzési jelentések
  - **Show last** – Mutassa a megadott mennyiségű legfrissebb jelentést
  - **Sort Test Results** – Rendezze a jelentéseket idő szerint sorba
    - **ascending** – a legrégebbi álljon legelöl
    - **descending** – a legfrissebb álljon legelöl

A **Virus Vault** (karantén) fül



- **Limit the size of the vírus vault** – legfeljebb a lemezterület hány százalékát foglalhatja el a karantén
  - **Minimum available space to remain on local disk** – legalább hány megabájt szabad terület maradjon szabadon
- **Automatic file deletion** – automatikusan törlje a karanténből a
  - **Delete files olther than** – a megadott napnál idősebb fájlokat
  - **Maximum number of files stored to be** – a legrégebbi fájlokat, ha karantén tartalma meghaladja a 2000 db fájlt
- **Empty vault –** A gombra kattintva törölheti a karantén teljes tartalmát.

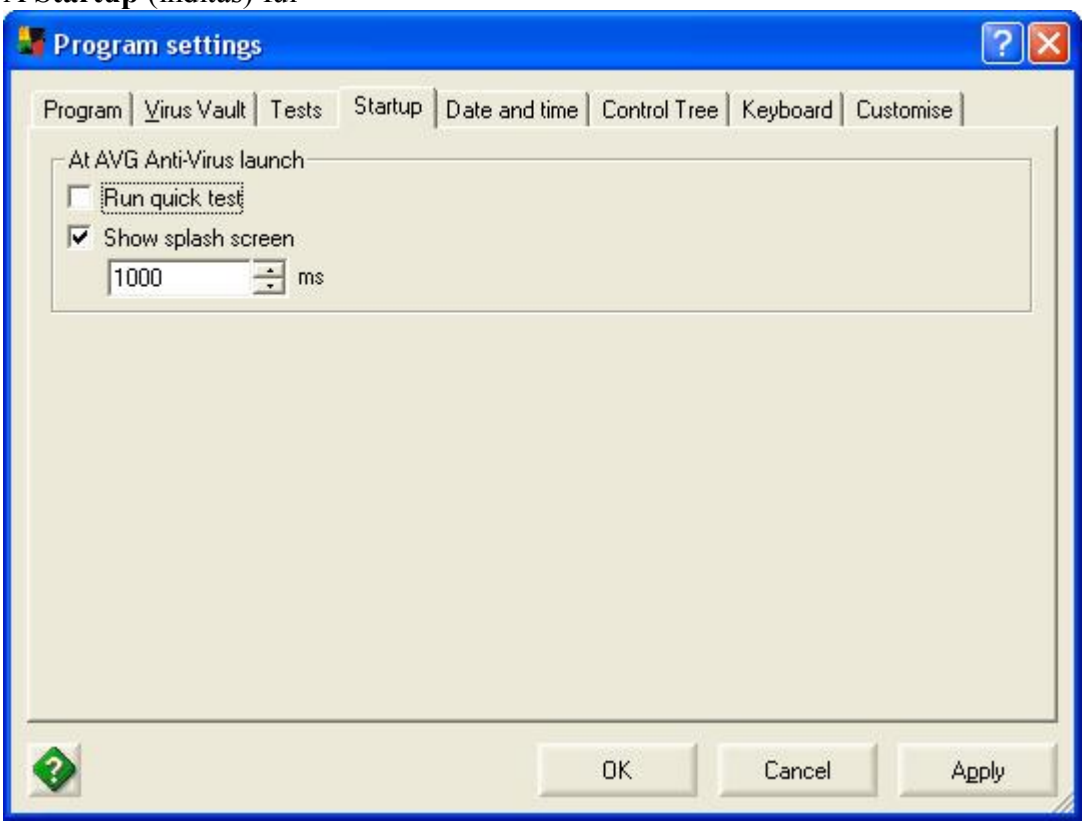
A **Tests** (Ellenőrzések) fül



Az ablakban az alábbi paraméterek beállítására van lehetőség:

- **Quick test** – Gyors ellenőrzés
  - **Database containing the status of scanned files** – A gyorsellenőrzések eredményeit a megadott állományban tárolja
- **Integrity Check** – Sértetlenség ellenőrzés
  - **Database containing the status of files saved on** – Megadhatja, hogy milyen néven és hová mentse le a sértetlenségi ellenőrzések (Integrity Check) eredményét. Korábban már olvashatta, hogy a sértetlenség ellenőrzéssel kombinált ellenőrzések során csak akkor történik vírusellenőrzés, ha a legutóbbi ellenőrzés óta a tesztelendő állomány módosult. Azonban ha egy vírus módosítja ezt az adatbázist, úgy könnyen rejtve maradhat a későbbi ellenőrzések során. Erre viszont csak akkor van lehetősége, ha ezt az adatbázist állandóan a számítógépen tartja. Mivel ez egy összetett felépítésű adatszerkezet, így kicsi esély van arra, hogy a vírus észrevétlenül megtámadja és módosítsa ezt az állományt, de fokozott biztonsági igény esetén Önnek lehetősége van ezeket az adatokat hálózati meghajtón vagy hordozható, például CD-R lemezen tárolni. Az adatállomány lemezre írását követően a lemezt (ha szükséges és lehetséges) célszerű írásvédelemmel ellátni és tartalmát csak következő sikeres ellenőrzés után, frissíteni.
    Tárolási lehetőségek:
    - **local discs** – beépített merevlemez
    - **network drives** – hálózati meghajtó, megosztás
    - **removable media** – hordozható lemez

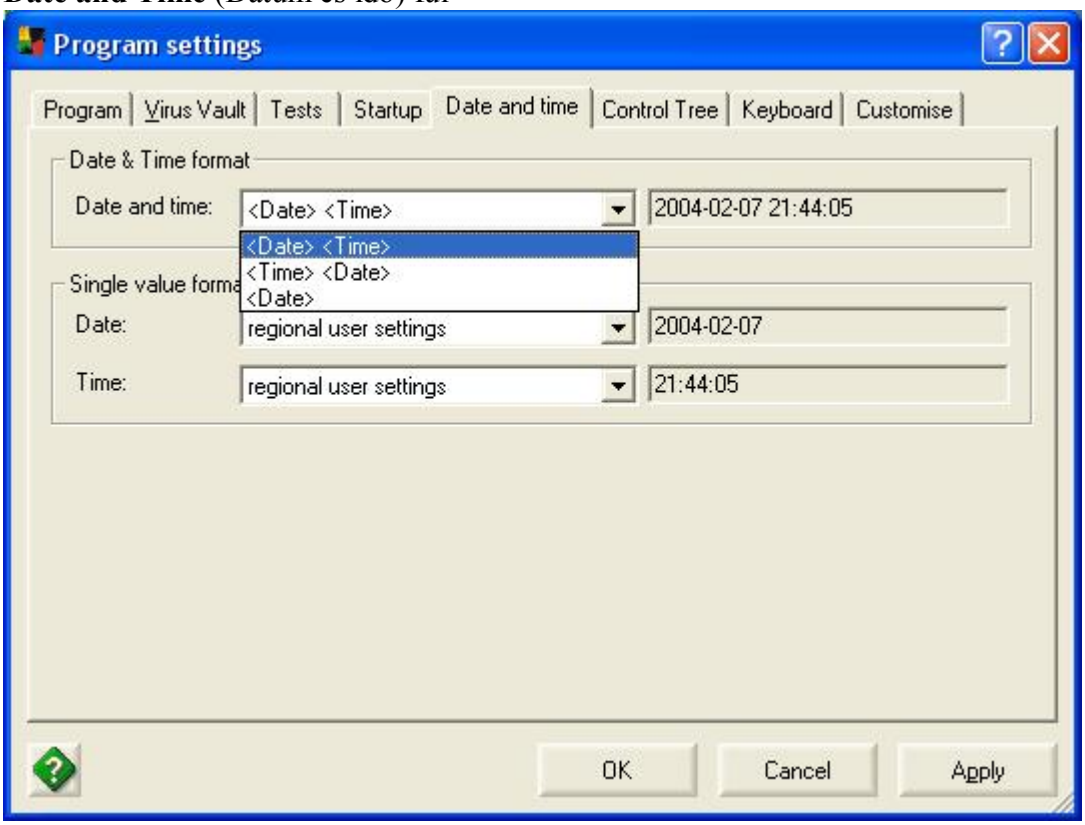
A **Startup** (indítás) fül



Ebben az ablakban a következő, az indítás befolyásoló paraméterek állíthatók be:

- **At AVG Anti-Virus launch** – Az AVG Anti-vírus indításakor
  - **Run quick test** – Futtasson le egy gyors ellenőrzést
  - **Show splash screen** – Üdvözlő képernyő megjelenítésének engedélyezése
    - A megadott ideig, az idő ezred másodpercben értendő.

Date and Time (Dátum és idő) fül



Ez a beállítás szintén csak a megjelenítést befolyásolja azokon a helyeken, ahol dátum, illetve idő adatokat kell kiírni a képernyőre vagy a riportokba.
Az dátumkezelés szabályai országonként eltérőek lehetnek ezért a testreszabhatóság ebben az esetben különösen fontos.
Az alábbi megjelenési módok állíthatók be:

- **Date & Time format** – Dátum és idő megjelenítése
  - **Date and Time:** - Ahol dátum és idő is megjelenik ott
    - **<Date> <Time>** - Először a dátum, mögötte pedig az idő jelenjen meg
    - **<Time> <Date>** - Először az idő, mögötte pedig a datum jelenjen meg
    - **<Date>** - Csak a datum jelenjen meg

- **Single value format** – A datum vagy idő önálló megjelenése esetén
  - **Date** – Dátum megjelenítésének formátuma
  - **Time** – Az idő megjelenítésének formátuma

Mindkét utóbbi esetben célszerű a **regional system settings** vagy a **regional user settings** beállítás használata. Ekkor az AVG Anti-vírus átveszi az operációs rendszer dátum és idő formátumát. Természetesen Ön ettől eltérő beállításokat is megadhat.
Jelölések az operációs rendszerben alkalmazott jelölésekhez hasonlóak.
A dátum esetében az:

- **y** – évet
- **m** – hónapot
- **d** – napot

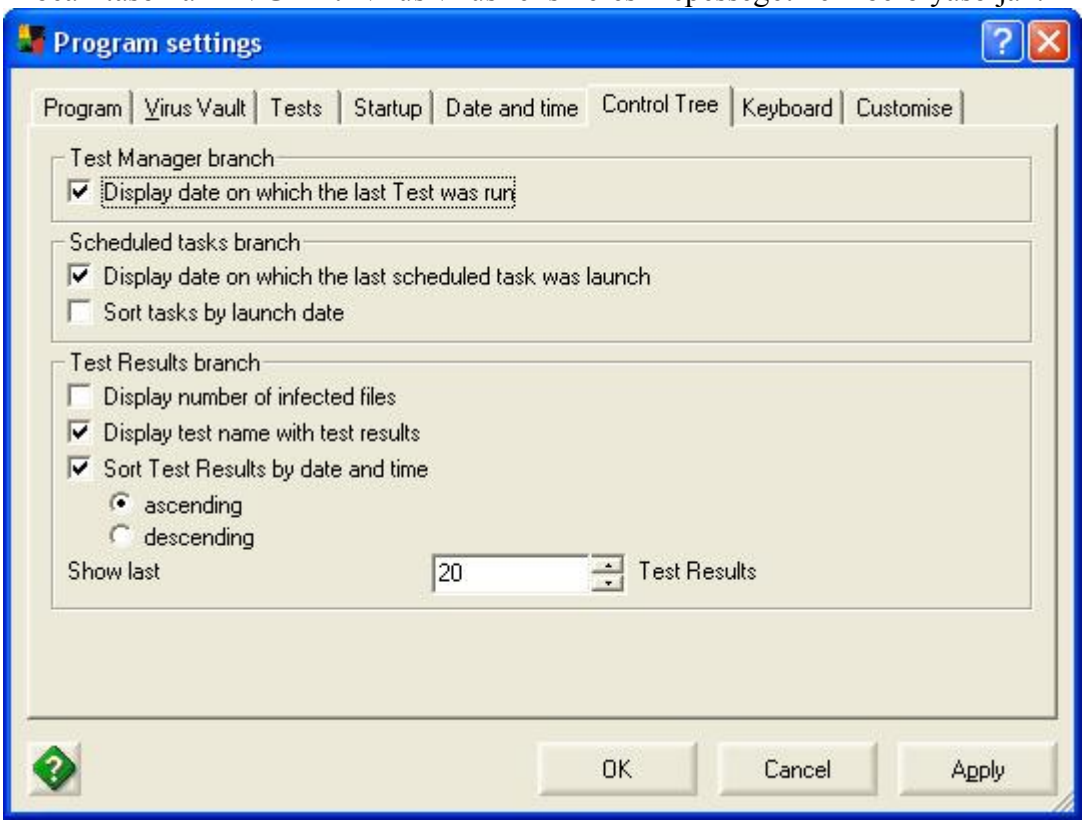
jelent

Az idő esetében a:

- **h/H** – órát
- **m** – percet
- **s** – másodpercet

jelent

A **Control Tree** (Vezérlés fa) fül
Azt állíthatja be, hogy a **haladó kezelő felületen** milyen információk jelenjenek meg. A beállítások az AVG Anti-vírus vírus felismerési képességét nem befolyásolják.

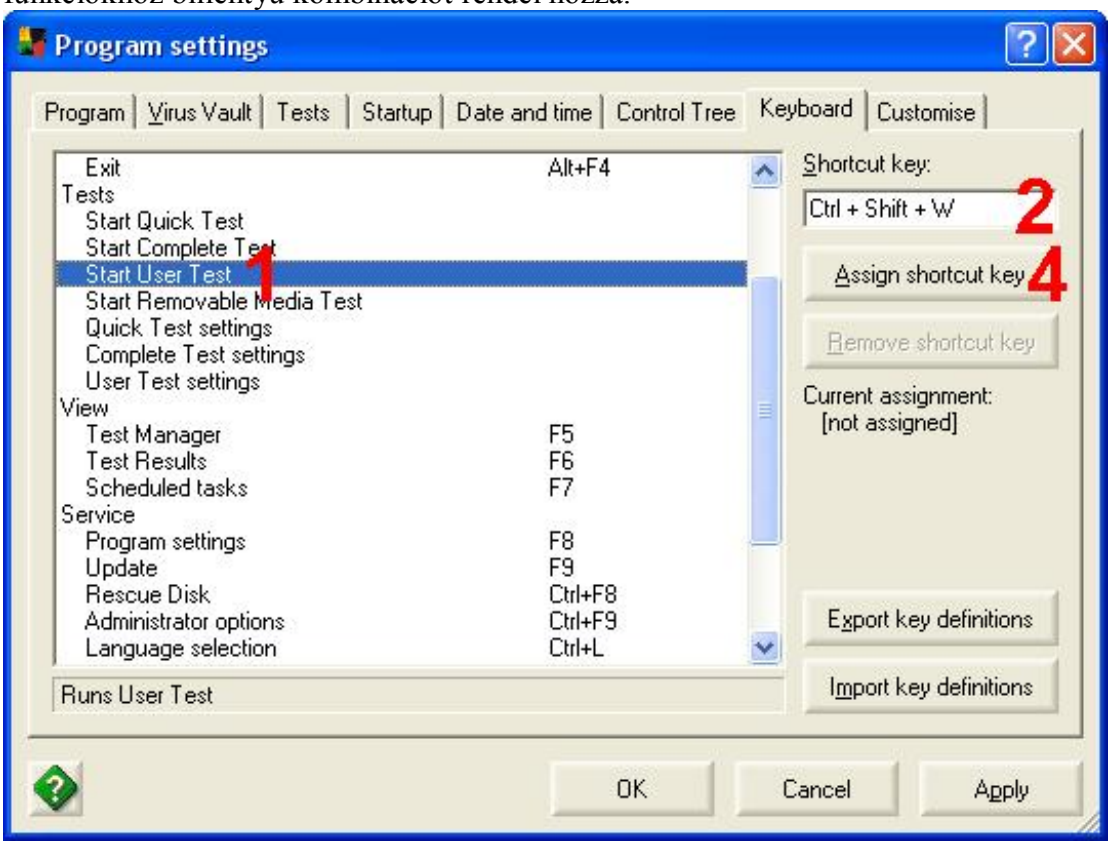


Beállítások:

- **Test Manager branch** – Az ellenőrzés kezelő csoport
  - **Display date on which the last Test was run** - A tesztek neve mellett írja ki, hogy mikor indították el utoljára
- **Scheduled tasks branch** – Ütemezett feladatok csoport
  - **Display date on which the last scheduled task was run** – az ütemezett feladatok mellé írja ki, hogy mikor futott utoljára
  - **Sort tasks by launch date** – az ütemezett feladatokat rendezze sorba futtatásuk ideje alapján

- **Test Results branch** – Ellenőrzés jelentések csoport
  - **Display number of infected file** – A jelentések mellett jelenítse meg, hogy hány fertőzött állományt talált
  - **Display test name with test result** – Jelenítse meg az ellenőrzés nevét és eredményét
  - **Sort Test Results by date and time** – rendezze a jelentéseket időrendi sorrendbe
    - **ascending** – a legrégebbi álljon legelöl
    - **descending** – a legújabb álljon legelöl
  - **Show last** – legfeljebb ennyi jelentés legyen látható

A **Keyboard** (billentyűzet) fül
A beállítás szintén nincs hatással a keresés hatékonyságára, de használatával gyorsíthatja a program funkcióinak elérését, olyan módon, hogy a gyakran használt funkciókhoz billentyű kombinációt rendel hozzá.



Használata:

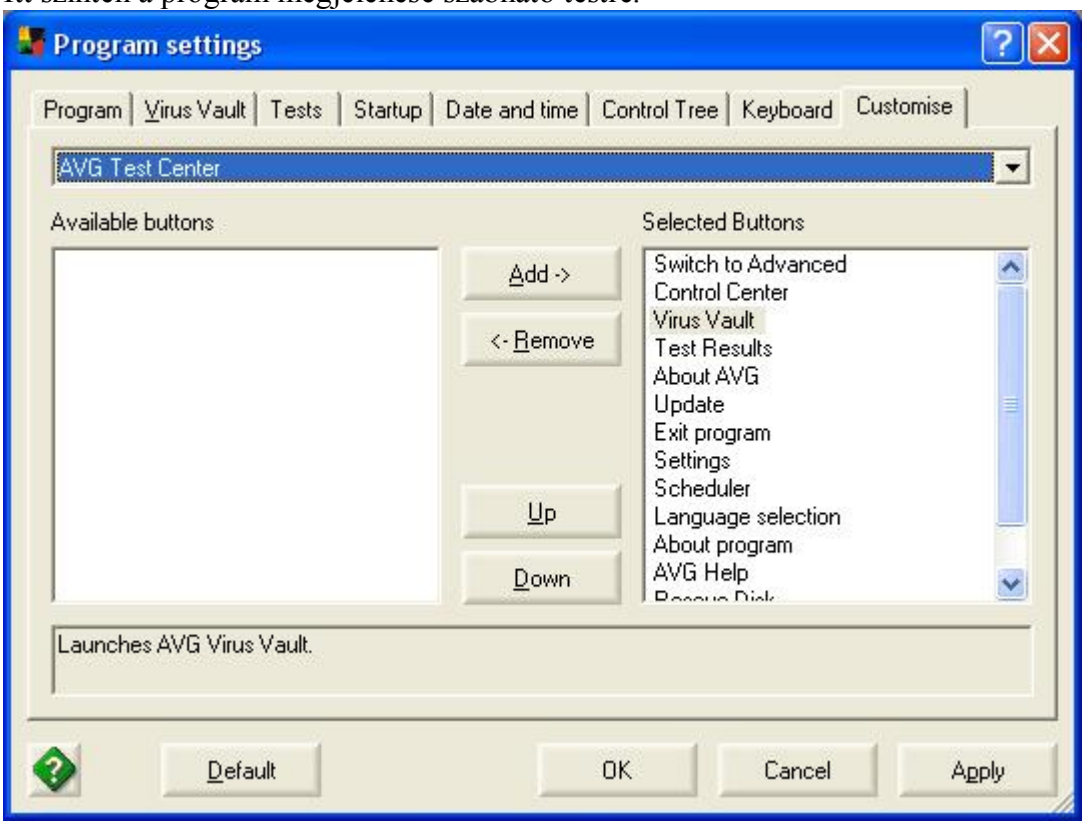
1. Válassza ki a kívánt funkciót
2. Kattintson a **Shortcut key** (billentyűzet kombináció) mezőbe (ez után ott kell villognia a kurzornak)
3. Adja meg a kívánt billentyűzet kombinációt, úgy ahogyan használni szeretné (példánkban tartsa lenyomva a Control és a Shift gombokat és nyomja le W billentyűt).
4. **Assign shortcut key** – rendelje hozzá a billentyű kombinációt a kijelölt funkcióhoz

További nyomógombok az ablakban:

- **Remove shortcut key** – A kijelölt funkciónál törli billentyűzet kombináció hozzárendelést
- **Export key definitions** – Fájlba mentheti a funkció – billentyűzet kombináció összerendeléseket
- **Import key definitions** – Fájlból betöltheti a funkció – billentyűzet kombináció összerendeléseket

A **Customize** (testreszabás) fül

Itt szintén a program megjelenése szabható testre.



A program kezelő felületén a különféle funkciókkal rendelkező gombokat jelenítheti meg, illetve rejthet el.
Két ablak választható ki:

- **AVG Test Center** – Ellenőrzés központ (példánkban)
- **AVG Control Center** – Vezérlő központ

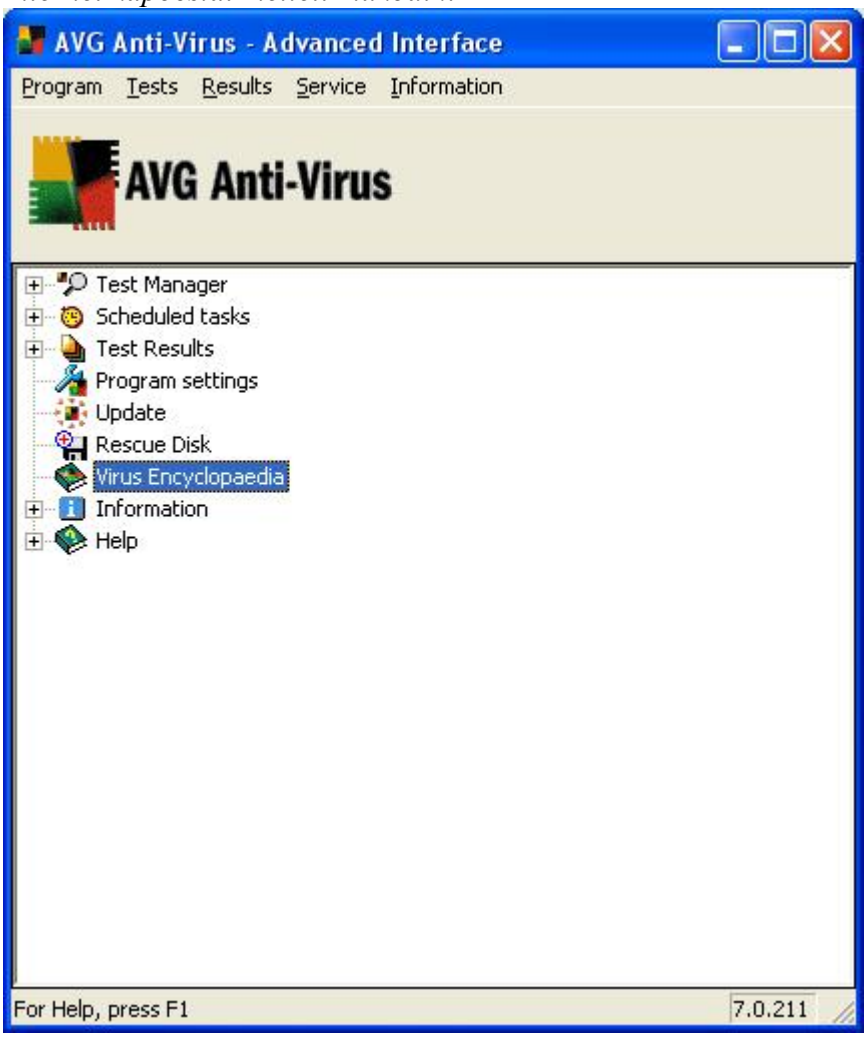
Az ablakban megjelenő további elemek:

- **Available buttons** – nem látható gombok
- **Selected buttons** – látható gombok
- **Add** – a kiválasztott nem látható gombot áthelyezi a látható csoprtba
- **Remove** – a kiválasztott látható gombot áthelyezi a nem látható csoportba
- **Up** – a kiválasztott látható gombot sorrendben a fölötte levő elé helyezi
- **Down** - a kiválasztott látható gombot sorrendben az alatta levő után helyezi
- **Default** – a gyári beállítások visszaállítása
- **OK** – a módosítások mentése és az ablak bezárása

- **Cancel** – az ablak bezárása a módosítások mentése nélkül
- **Apply** – a módosítások mentése az ablak bezárása nélkül

Vírus ismertető (Vírus Encyclopaedia)

A funkció segítségével további információkat kaphat a vírusokról. *A funkció csak elő Internet kapocslat mellett működik!*



A funkció használatához kattintson duplán a Virus Encyclopaedia sorra, ez után az alábbi ablakot kell látnia:

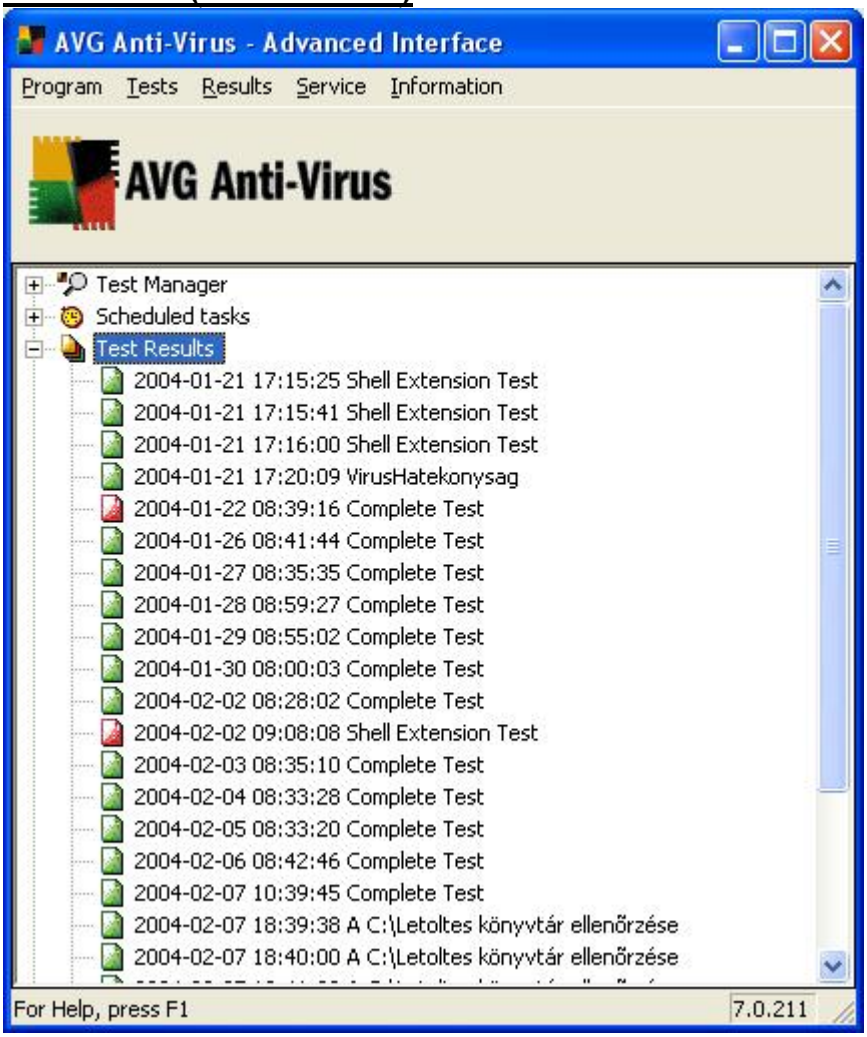
Használata:

- A **vírus name** (vírus neve) mezőbe írja be a vírus nevének töredékét. Legalább 3 karaktert (betűt, számot, írásjelet) adjon meg.
  (a **search in aliases** négyzetet bejelölve a vírusok álnevei között is keres)
- Kattintson a **search** (keresés) gombra

Ha vírus létezik, akkor az alábbi ablakot kell látnia:

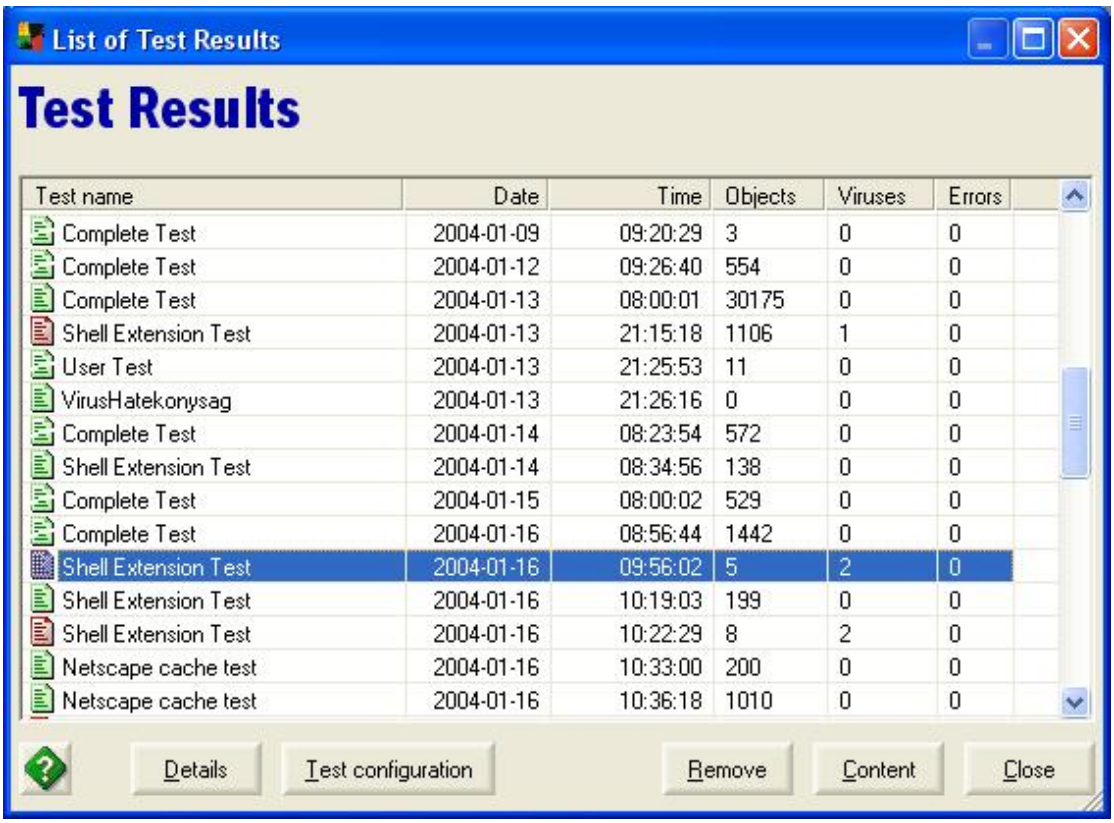
Az információk angol nyelvűek.
Az ablak a **Close** gomb megnyomásával bezárható.

Jelentések (Test results)



A Test Results (jelentések) csoportot kinyitva megjelenik a legutóbbi ellenőrzések eredménye. Az listában zöld ikon jelzi, ha az ellenőrzés nem talált vírust és piros ha igen. Listában látható továbbá az ellenőrzés időpontja és a használt teszt neve. Bármelyik ellenőrzésen az egérrel duplán kattintva megjelennek az ellenőrzés részletei. Mi azonban most egy másik módszert szeretnénk bemutatni:

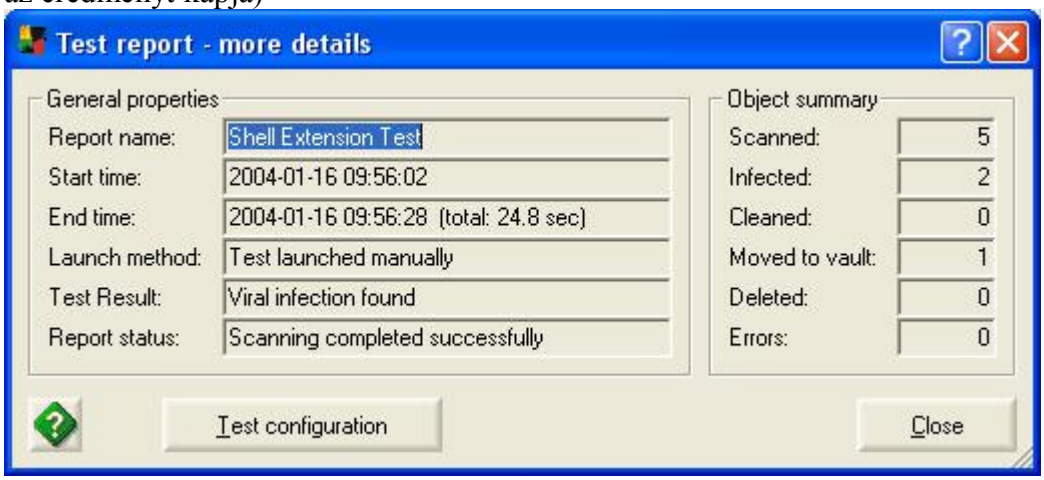
A fenti ablakban kattintson duplán a Test Results soron, ekkor részletesebb adatok jelennek meg a teszteredményekről:



- A megjelenő ablak tartalmazza a használt teszt nevét (**Test name**), amelytől a jelentés származik
- Az ellenőrzés dátumát és időpontját (**Date** és **Time** mezők).
- Az ellenőrzött objektumok, fájlok számát (**Objects**)
- Az ezekben talált vírusok számát (**Viruses**)
- A tesztelés közben fellépett hibák számát (**Errors**)

Nyomógombok:

- **Details** – Kijelölt sor részletek megjelenítése (a soron duplán kattintva is ezt az eredményt kapja)

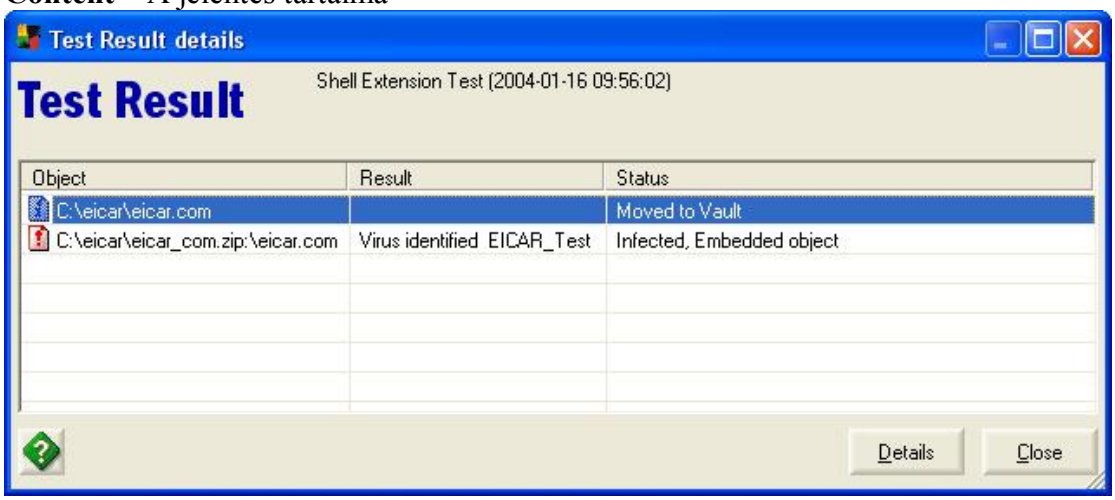


  - **Report name** – a jelentés neve (Megegyezik a teszt nevével, ami készítette)
  - **Start time** – az ellenőrzés kezdete
  - **End Time** – az ellenőrzés vége
  - **Launch method** – az indítás módja

§ **Test launched manually** – kézzel, a felhasználó által indított ellenőrzés
§ **Test launched by scheduler** – az ütemező által indított ellenőrzéz

- **Test result** – az ellenőrzés kimenetele
  - § **Viral infection found** – Talált vírus fertőzést
  - § **No viruses found** – nem talált fertőzést
- **Report status** – az ellenőrzés státusza
  - § **Scanning completed successfully – Az ellenőrzés sikeresen befejeződött**
  - § **Scanning stopped manually** – az ellenőrzést megszakították, mielőtt befejeződött volna
- **Scanned –** ellenőrzött objektumok, fájlok száma
- **Infected –** fertőzött objektumok, fájlok száma
- **Cleaned –** vírusmentesített objektumok, fájlok száma
- **Moved to vault –** karanténba helyezett objektumok, fájlok száma
- **Deleted –** törölt objektumok, fájlok száma
- **Errors –** az ellenőrzés közben történt hibák száma

- **Test configuration** – Módosíthatja annak a tesztnek a beállításait, amely a kiválasztott jelentést készítette
- **Remove** – A kiválasztott jelentés törlése
- **Content** – A jelentés tartalma



A részletezésnél az alábbi adatok láthatóak:

- **Object** – az objektum, fájl neve
- **Result** – az ellenőrzés eredménye (példánkban mindkét esetben Eicar_Test vírussal fertőződött az állomány)
- **Status** – mi történt az állománnyal? (példánkban az első állományt karanténba helyezte a program, a másodikat pedig „Embedded object”, beágyazott objektumak érzékelte, ami ha az Object oszlopra tekintünk azt jelenti, hogy az eicar_com.zip tömörített állományban található a fertőzött állomány az eicar.com. Az ilyen módon tömörített állományok kitömörítés nélkül veszélytelenek, ezért a fájlban esetlegesen még meglévő hasznos információk védelme érdekében a tömörített fájlt az AVG nem próbálta meg vírus mentesíteni)

- **Close** – az ablak bezárása