ESET SMART SECURITY 5

Felhasználói útmutató

(5.0-s és újabb termékverziókhoz)

Microsoft® Windows® 7 / Vista / XP / 2000 / Home Server

Ide kattintva letöltheti a dokumentum legújabb verzióját

ESET **SMART SECURITY**

Nemzetközi ügyfélszolgálat: www.eset.com/support

REV. 9/5/2011

Tartalom

1. ESET Smart Security 5

Az ESET Smart Security 5 egy újszerű megoldást jelentő integrált biztonsági programcsomag. A ThreatSense® keresőmotornak a Személyi tűzfal és a Levélszemétszűrő modullal kombinált legújabb verziója gyorsan és megbízhatóan védi számítógépét. Az eredmény egy olyan intelligens rendszer, amely szünet nélkül figyeli a számítógépet veszélyeztető támadási kísérleteket és kártevő szoftvereket.

Az ESET Smart Security 5 teljes körű biztonsági megoldás, mely a hosszú távú fejlesztések eredményeként minimális rendszerterhelés mellett kínál maximális védelmet. A korszerű technológia a mesterséges intelligencián alapuló elemző algoritmusok segítségével képes proaktív módon kivédeni a vírusok, kémprogramok, trójaiak, férgek, kéretlen reklámprogramok, rootkitek és más internetes károkozók támadását anélkül, hogy a rendszer teljesítményét visszafogná.

1.1 Újdonságok

Szülői felügyelet

A szülői felügyelet lehetővé teszi az esetlegesen nem kívánt tartalmú weblapok blokkolását. A szülők emellett akár 20 előre definiált webhely-kategória elérését is megtilthatják. Az eszköz célja a gyermekek és fiatal felnőttek megakadályozása abban, hogy nem megfelelő vagy káros tartalmat megjelenítő oldalakhoz férjenek hozzá.

Behatolásmegelőző rendszer

A behatolásmegelőző rendszer (HIPS, Host Intrusion Prevention System) megvédi rendszerét a kártevőktől és a számítógép biztonságát veszélyeztető minden nemkívánatos tevékenységtől. A rendszer a hálózati szűrők észlelési képességeivel párosított speciális viselkedéselemzést használ a futó folyamatok, fájlok és beállításkulcsok figyelésére, valamint aktívan blokkolja és megelőzi az ilyen kísérleteket.

Továbbfejlesztett levélszemétszűrő

Az ESET Smart Security rendszerbe integrált levélszemétszűrő alapos optimalizálási folyamaton esett át, hogy még nagyobb észlelési pontosságot nyújthasson.

ESET Live Grid

Az ESET Live Grid egy korszerű, megbízhatósági értékeléseken alapuló figyelmeztető rendszer, mely képes már korai fázisukban észlelni a terjedő kártevőket. A felhőben található kártevőadatok valós idejű letöltése révén az ESET víruslaborja folyamatosan frissen tudja tartani a védelmet, és állandó védelmi szintet képes nyújtani. A felhasználók a futó folyamatok és megnyitott fájlok megbízhatóságát közvetlenül a program felületén, illetve az ESET Live Grid rendszerből származó járulékos információkat is megjelenítő helyi menükben is megtekinthetik. A fájlok mellett megjelenik kockázati szintjük, a fájllal rendelkező felhasználók száma, valamint az első elemzés időpontja.

Cserélhető adathordozók ellenőrzése

Az ESET Smart Security lehetővé teszi a cserélhető adathordozók (CD/DVD/USB/…) vezérlését. Ez a modul lehetővé teszi a kiterjesztett szűrők/engedélyek ellenőrzését, tiltását vagy módosítását, továbbá az eszközök elérésének és használati módjának szabályozását. Ez a lehetőség különösen hasznos lehet akkor, ha a számítógép rendszergazdája meg kívánja akadályozni, hogy a felhasználók kéretlen tartalmú cserélhető adathordozót helyezzenek a számítógépbe.

Játékos üzemmód

A játékos üzemmód azoknak a játékosoknak hasznos, akiknek fontos a szoftverek megszakítás nélküli használata, és nem szeretnék, hogy előugró ablakok zavarják meg őket, illetve szeretnék minimalizálni a processzor terhelését. A játékos üzemmód prezentációs módként is használható – ilyenkor a bemutatók előadását nem zavarja meg a vírusvédelmi tevékenység. A funkció engedélyezésével letiltja az előugró ablakokat, valamint teljesen leállítja a feladatütemező tevékenységét. A rendszervédelem változatlanul működik a háttérben, felhasználói beavatkozást azonban nem igényel.

Frissítések keresése

Az ESET Smart Security a vírusdefiníciós adatbázisok és a programmodulok frissítése mellett beállítható a legújabb termékverziók rendszeres keresésére is. A telepítés során akkor is letöltheti és telepítheti az ESET Smart Security legújabb verzióját, ha régebbi telepítőcsomaggal indítja a telepítést.

Új kivitel

Az ESET Smart Security fő ablakát is teljes mértékben átterveztük, míg a További beállítások párbeszédpanel intuitívabbá és áttekinthetőbbé vált.

1.2 Rendszerkövetelmények

Az ESET Smart Security zavartalan működéséhez a rendszernek meg kell felelnie az alábbi hardver- és szoftverkövetelményeknek:

Windows 2000, XP,

400 MHz 32 bites (x86) / 64 bites (x64)
128 MB RAM rendszermemória
320 MB szabad lemezterület
Super VGA (800 × 600 képpont felbontással)

Windows 7, Vista,

1 GHz 32 bites (x86) / 64 bites (x64)
512 MB RAM rendszermemória
320 MB szabad lemezterület
Super VGA (800 × 600 képpont felbontással)

1.3 Megelőzés

Amikor számítógépen dolgozik – de különösen internetes böngészés közben – folyton tartsa szem előtt azt a tényt, hogy a világon egyetlen vírusvédelmi szoftver sem képes teljesen megszüntetni a kártevők és támadások jelentette kockázatot. A maximális védelem és kényelem érdekében a vírusvédelmi rendszert megfelelően, számos hasznos szabály figyelembevételével kell alkalmazni.

Rendszeres frissítés

Az ESET Live Grid statisztikája szerint nap mint nap új, egyedi kártevő kódok ezrei készülnek azzal a szándékkal, hogy megkerüljék a meglévő biztonsági rendszereket, és hasznot hajtsanak szerzőiknek – mindezt mások rovására. Az ESET víruslaborjának specialistái naponta elemzik ezeket a kódokat, majd frissítéseket állítanak össze és adnak ki, hogy folyamatosan emeljék a vírusvédelmi program felhasználóinak védelmi szintjét. A helytelenül konfigurált frissítések csökkentik a program hatékonyságát. Ide kattintva további információkat olvashat a frissítések konfigurálásáról.

Biztonsági javítócsomagok letöltése

A kártékony szoftverek szerzői előszeretettel használják ki a rendszer különféle biztonsági réseit, hogy kódjaik terjesztését megkönnyítsék. A szoftvergyártók ezért alaposan figyelemmel követik, hogy alkalmazásaikban milyen új biztonsági réseket fedeznek fel, és biztonsági frissítések kibocsátásával rendszeresen igyekeznek elejét venni a lehetséges veszélyeknek. Fontos, hogy ezeket a biztonsági frissítéseket megjelenésükkor töltse le. Az ilyen szoftverek közé tartozik a Windows operációs rendszer vagy a széles körben használt böngésző, az Internet Explorer.

Fontos adatok biztonsági mentése

A kártékony szoftverek előállítói általában nem foglalkoznak a felhasználók igényeivel, és az ilyen programok tevékenysége gyakran az operációs rendszer tönkretételével, a fontos adatok szándékos megrongálásával jár együtt. Lényeges, hogy fontos vagy bizalmas adatairól rendszeresen készítsen biztonsági másolatot egy külső forrásra, például DVD-re vagy külső merevlemezre. Az efféle elővigyázatosság megkönnyíti és meggyorsítja az adatok helyreállítását egy esetleges rendszerhiba bekövetkezésekor.

Víruskereső rendszeres futtatása a számítógépen

Ha rendszeresen, helyes beállításokkal futtat automatikus ellenőrzéseket a számítógépen, kiszűrheti azokat a fertőzéseket, amelyeket a program a vírusdefiníciós adatbázis elavult volta miatt korábban esetleg átugrott.

Alapvető biztonsági szabályok betartása

Ez a leghasznosabb és leghatékonyabb szabály mind közül – legyen mindig elővigyázatos. Manapság sok kártékony szoftver csak felhasználói beavatkozásra lép működésbe vagy terjed el. Ha körültekintően jár el az új fájlok megnyitásakor, megtakaríthatja a számítógép későbbi megtisztítására fordított jelentős időmennyiséget. Néhány hasznos tanács:

- Ne keressen fel gyanús webhelyeket, ahol sok előugró ablak nyílik meg, vagy hirdetések villognak.
- Legyen óvatos, amikor „freeware" programokat (szabadszoftvereket), kodekcsomagokat és más hasonló szoftvereket telepít. Csak biztonságos programokat telepítsen, és csak biztonságos webhelyekre látogasson.
- Legyen óvatos, amikor e-mail mellékleteket nyit meg, különösen, ha tömeges címre küldték őket, vagy feladójuk ismeretlen.
- A napi rutinmunka során ne használja a Rendszergazda fiókot a számítógépen.

2. Telepítés

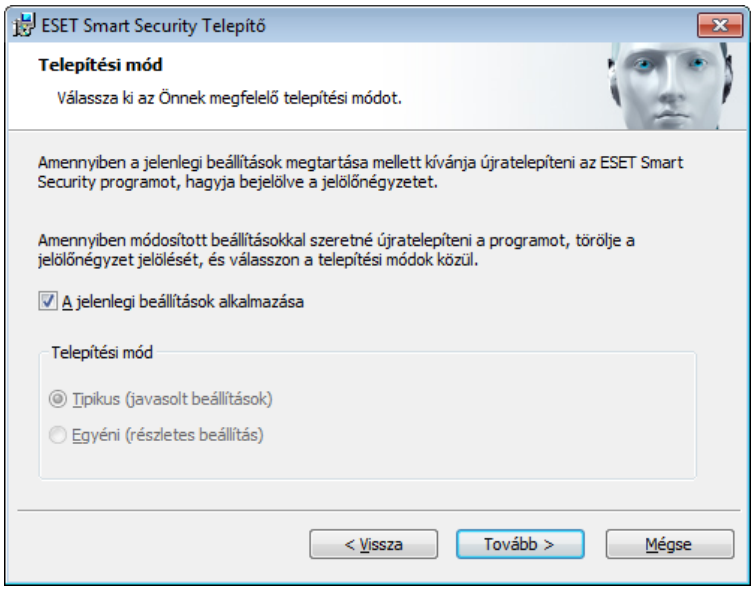
A telepítő elindítása után a telepítővarázsló végigvezeti Önt a telepítés alaplépésein.

Fontos: Győződjön meg arról, hogy a számítógépen nincs másik víruskereső program telepítve. Ha több vírusvédelmi megoldás üzemel egy számítógépen, megzavarhatják egymás tevékenységét. Ajánlatos az esetleges további víruskereső programokat eltávolítani a rendszerből. További információkért tanulmányozza tudásbázisunk cikkét (csak angolul és néhány más nyelven érhető el).

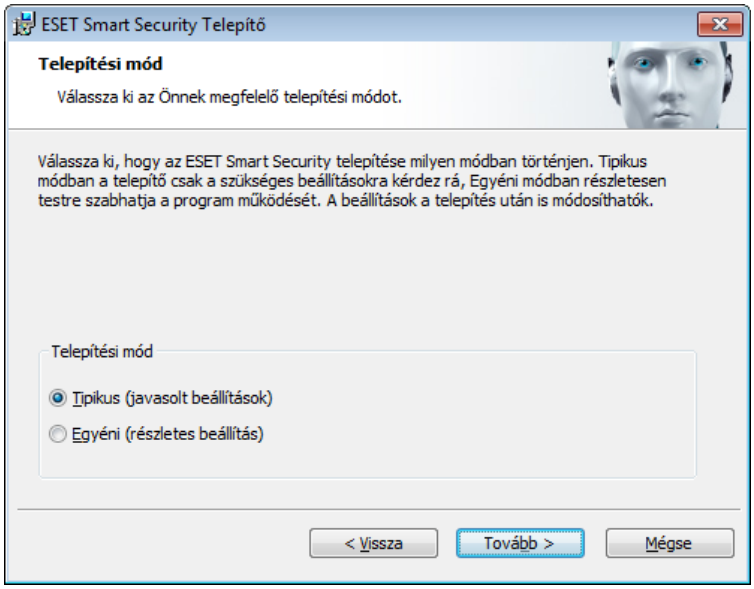
A program először is ellenőrzi, hogy van-e frissebb verzió az ESET Smart Security rendszerből.

A **Töltse le, és telepítse a legújabb alkalmazásverziót** lehetőséget választva letöltődik az új verzió, és folytatódik a telepítés. A következő lépésben megjelenik a végfelhasználói licencszerződés. A szerződés tanulmányozását követően az **Elfogadom** lehetőség választásával jelezheti, hogy elfogadja az abban foglaltakat. A szerződés elfogadását követően kétféleképp folytatódhat a telepítés:

1. Az ESET Smart Security telepítése a termék korábbi verziójára. Az alább látható ablakban eldöntheti, hogy megtartja-e a program jelenlegi beállításait. Ha törli a jelet **A jelenlegi beállítások alkalmazása** jelölőnégyzetből, választhat a tipikus telepítési mód és az egyéni telepítési mód közül.



2. Ha a számítógépen nincs telepítve az ESET Smart Security korábbi verziója, az alábbi képernyő jelenik meg a **Végfelhasználói licencszerződés** elfogadása után. Ebben az ablakban választhat a tipikus telepítési mód és az egyéni telepítési mód közül.



2.1 Tipikus telepítés

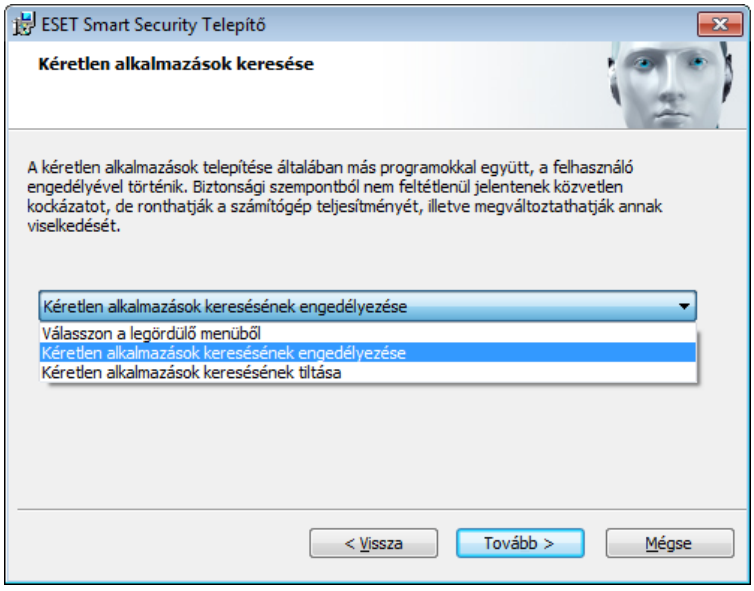
A tipikus telepítési mód a legtöbb felhasználónak megfelelő beállítási lehetőségeket biztosít. A beállítások nagy biztonságot nyújtanak, amihez könnyű használat és magas fokú rendszerteljesítmény társul. A tipikus telepítési mód az alapértelmezett beállítás, amely abban az esetben ajánlott, ha adott beállítások esetén nincs szükség különleges követelményekre.

A következő lépés az ESET Live Grid összetevő beállítása. Az ESET Live Grid rendszerrel biztosítható, hogy az ESET azonnal és folyamatosan értesüljön az új fertőzésekről, így biztosítva gyors védelmet a felhasználók számára. A rendszer lehetővé teszi, hogy a felhasználó elküldje az új kártevőket az ESET víruslaborjába, ahol elemzik és feldolgozzák az adatokat, és felveszik azokat a vírusdefiníciós adatbázisba.

Alapértelmezés szerint be van jelölve a **Részvétel az ESET Live Grid szolgáltatásban** jelölőnégyzet, ami aktiválja ezt a szolgáltatást.

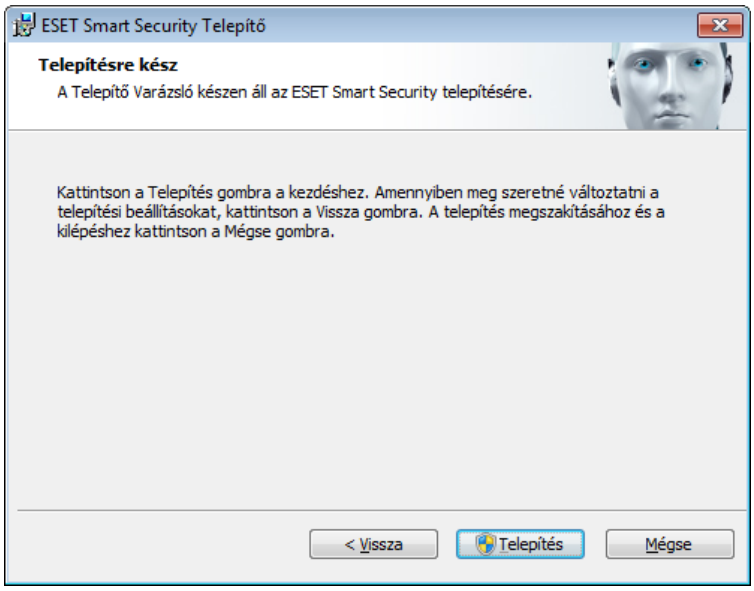
A következő telepítési lépés a kéretlen alkalmazások felismerésének beállítása. A kéretlen alkalmazások nem feltétlenül kártevők, azonban kedvezőtlen hatással lehetnek a számítógép teljesítményére.

Ezeket az alkalmazásokat gyakran más programokkal csomagolják egybe, így előfordulhat, hogy a telepítési folyamat során nehéz őket észrevenni. Bár az alkalmazások a telepítés során általában megjelenítenek egy értesítést, a beleegyezése nélkül is könnyedén telepíthetők.



Jelölje be a **Kéretlen alkalmazások keresésének engedélyezése** választógombot, ha azt szeretné, hogy az ESET Smart Security észlelje az ilyen típusú kártevőket (ajánlott).

A tipikus telepítési mód utolsó lépésében a **Telepítés** gombra kattintva erősítse meg a telepítést.



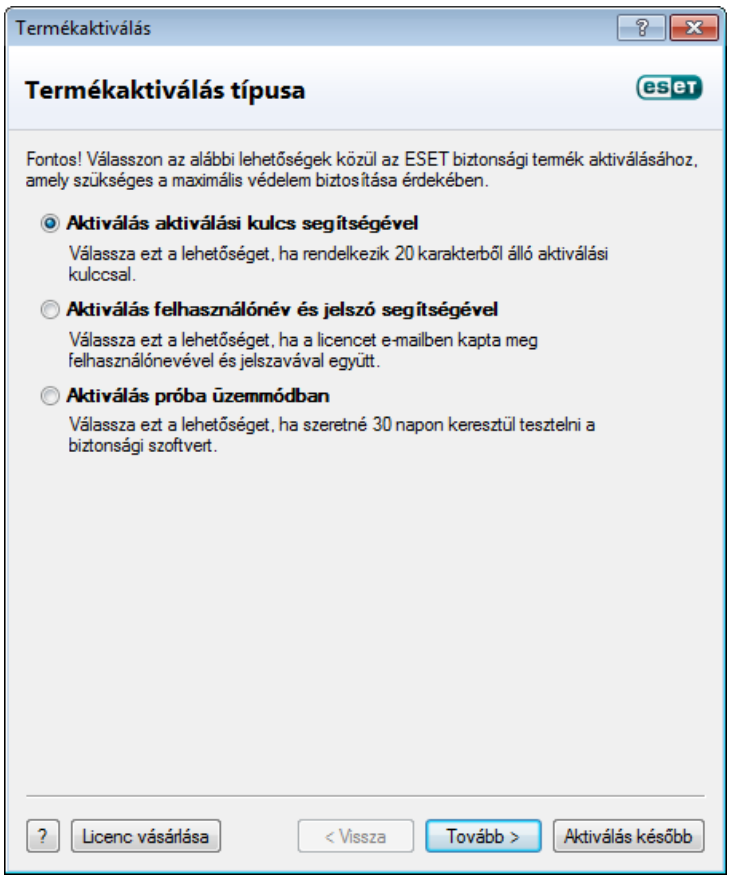
A telepítés végeztével a rendszer megkéri a termék aktiválására.

Ha kiskeresekedelmi forgalomban kapható dobozos változatot vásárolt, akkor már rendelkezik aktiválási kulccsal, és az aktiválási folyamat részletes ismertetését is megtalálja a dobozban. Az aktiválási kulcs általában a termék dobozában vagy a csomagolás hátoldalán található. A sikeres aktiváláshoz pontosan kell megadni az aktiválási kulcsot.

Ha már megkapta a felhasználónevét és jelszavát, jelölje be a **Felhasználónév és jelszó** választógombot, majd írja be a licencadatokat a megfelelő mezőkbe.

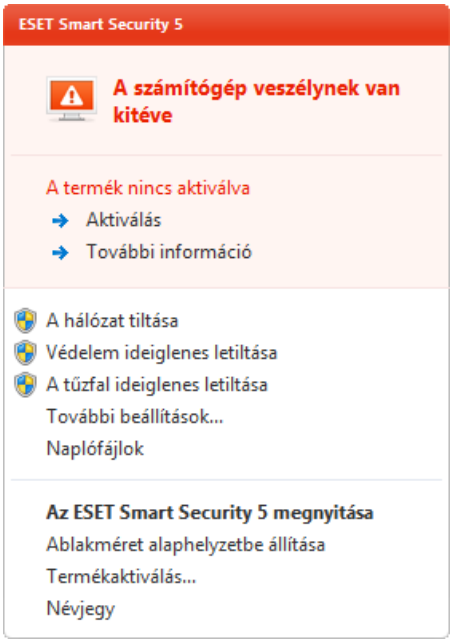
Amennyiben vásárlás előtt szeretné kipróbálni az ESET Smart Security programot, jelölje be a **Aktiválás próba üzemmódban** választógombot. Az ESET Smart Security korlátozott idejű használatát lehetővé tévő aktiváláshoz adja meg e-mail címét és tartózkodási helyének országát. A próbaverzióhoz tartozó licencet e-mailben küldjük el Önnek. Minden kliens csak egyszer aktiválhatja a próbaverzió licencét.

Amennyiben még nincs licence, és szeretne vásárolni egyet, kattintson a **Licenc vásárlása** gombra. A program ekkor átirányítja az ESET helyi forgalmazójának a weboldalára.



Válassza az **Aktiválás később** lehetőséget, ha szeretné gyorsan kipróbálni a terméket, és nem igényli az azonnali aktiválást.

Az ESET Smart Security programot közvetlenül az alkalmazásból aktiválhatja. Kattintson a tálcán az ESET Smart Security ikonjára, vagy kattintson a jobb gombbal az ESET Smart Security értesítési területen megjelenő ikonjára, és válassza a **Termékaktiválás** parancsot.



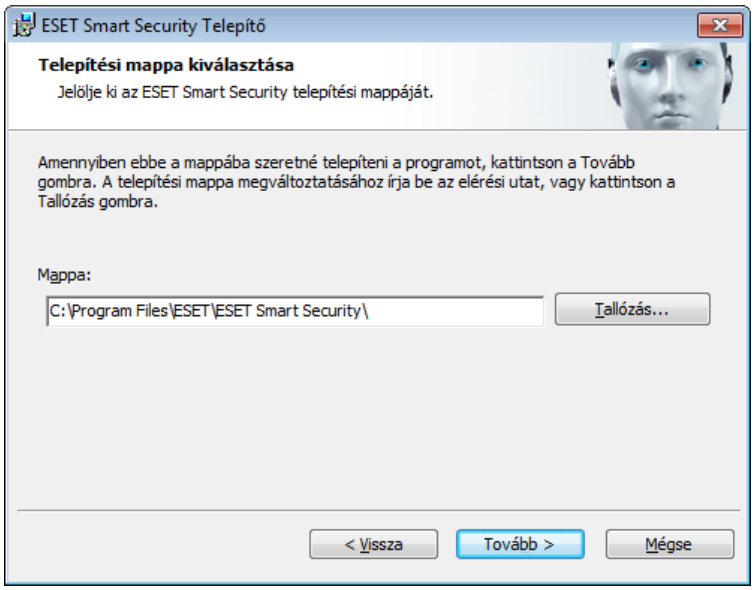
2.2 Egyéni telepítés

Az egyéni telepítési módot azoknak javasoljuk, akik tapasztalattal rendelkeznek a programok finomhangolása terén, és a telepítés közben módosítani szeretnék a további beállításokat.

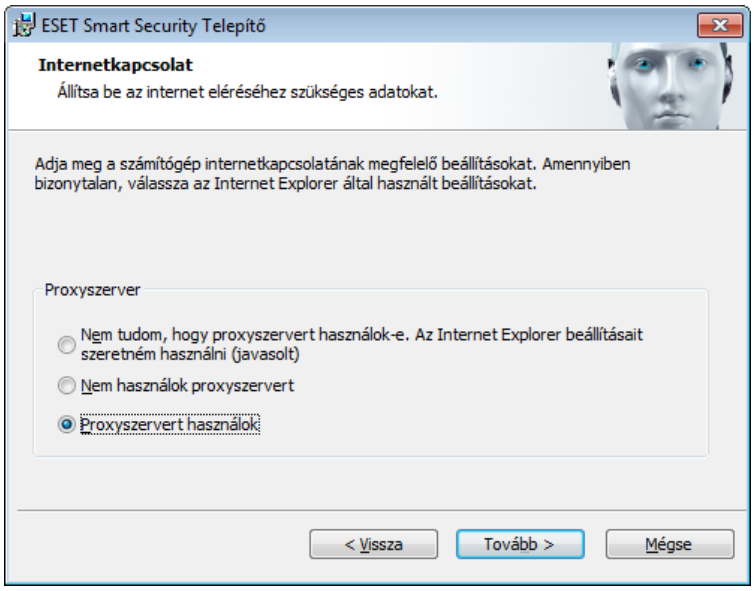
A telepítési mód kiválasztása és a **Tovább** gombra kattintást követően a program kérni fogja a telepítési mappa megadását. Alapértelmezés szerint ez a hely a következő:

C:*Program Files*\ESET*ESET Smart Security*\

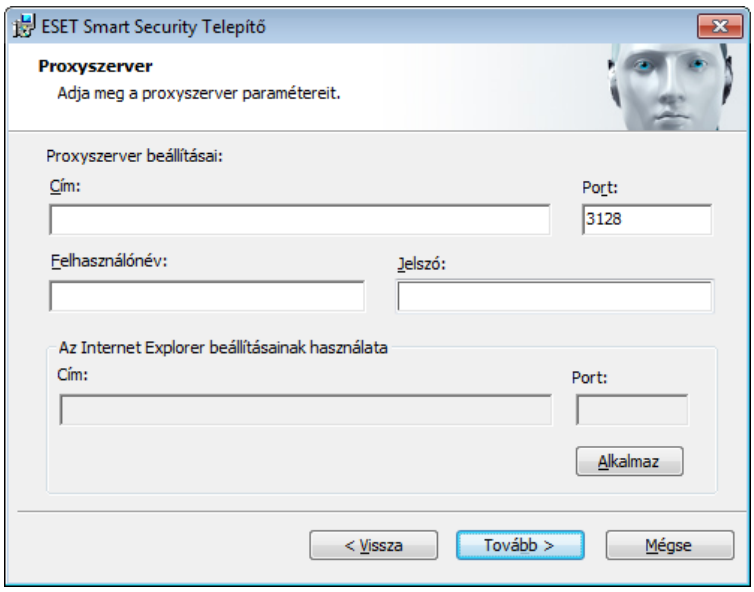
Kattintson a **Tallózás** gombra, ha módosítani szeretné a helyet (nem ajánlott).



Amennyiben nem kívánja módosítani a telepítési könyvtárat kattintson a **Tovább** gombra.

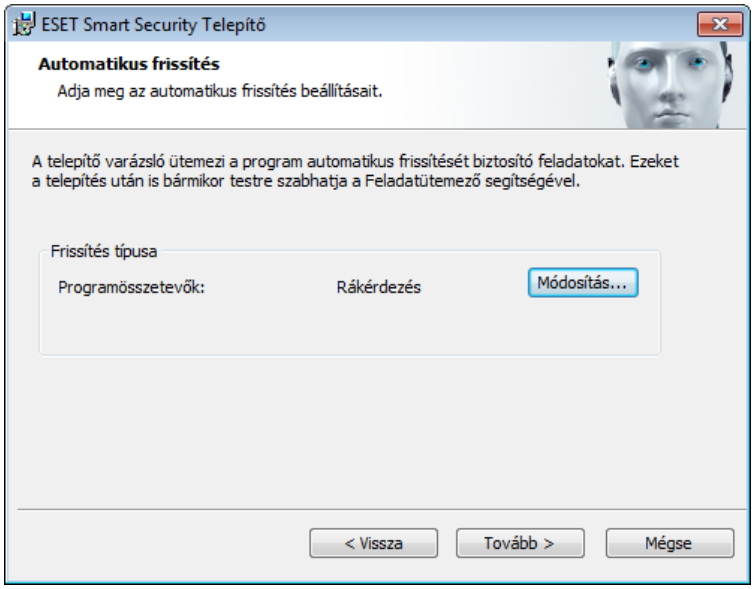


Proxyszerver használata esetén állítsa be azt helyesen annak érdekében, hogy a vírusdefiníciós adatbázis frissítése megfelelően működjön. Ha nem biztos abban, hogy használ-e proxyszervert az internetkapcsolathoz, válassza a **Nem tudom biztosan, hogy az internetkapcsolatom proxyszerverrel működik-e. Az Internet Explorer beállításait szeretném használni (javasolt)** lehetőséget, és kattintson a **Tovább** gombra. Ha nem használ proxyszervert, a **Nem használok proxyszervert** lehetőséget válassza.

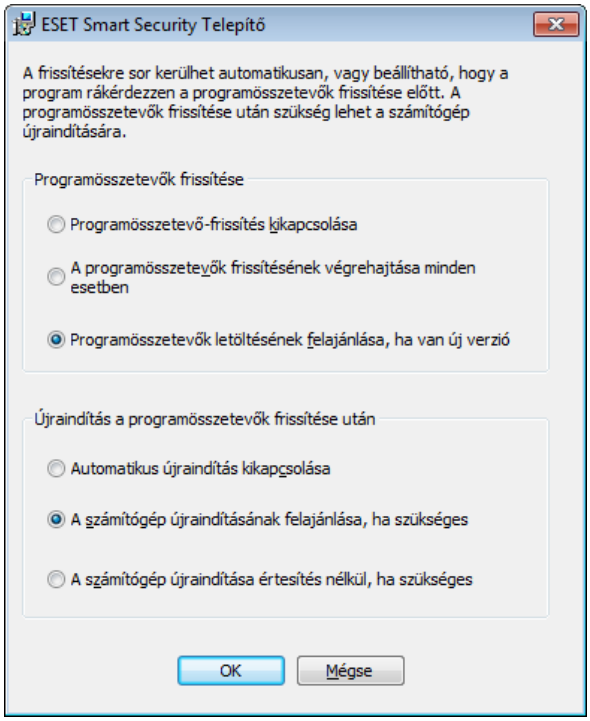


A proxyszerver beállításainak megadásához jelölje be a **Proxyszervert használok** választógombot, és kattintson a **Tovább** gombra. Írja be a proxyszerver IP- vagy URL-címét a **Cím** mezőbe. A **Port** mezőben adja meg azt a portot, amelyen a proxyszerver fogadja a kapcsolatokat (alapértelmezés szerint a 3128-as port). Hitelesítést kérő proxyszerver esetén be kell írnia egy érvényes **felhasználónevet** és **jelszót**, mert csak így lesz jogosult a szerver használatára. Szükség esetén az Internet Explorer böngészőből is átmásolhatja a proxyszerver beállításait: ehhez kattintson az **Alkalmaz** gombra, és hagyja jóvá a megadott beállításokat.

Ezzel a telepítési lépéssel adhatja meg az automatikus programfrissítések kezelési módját. A **Módosítás** gombra kattintva megjelenítheti a további beállításokat.

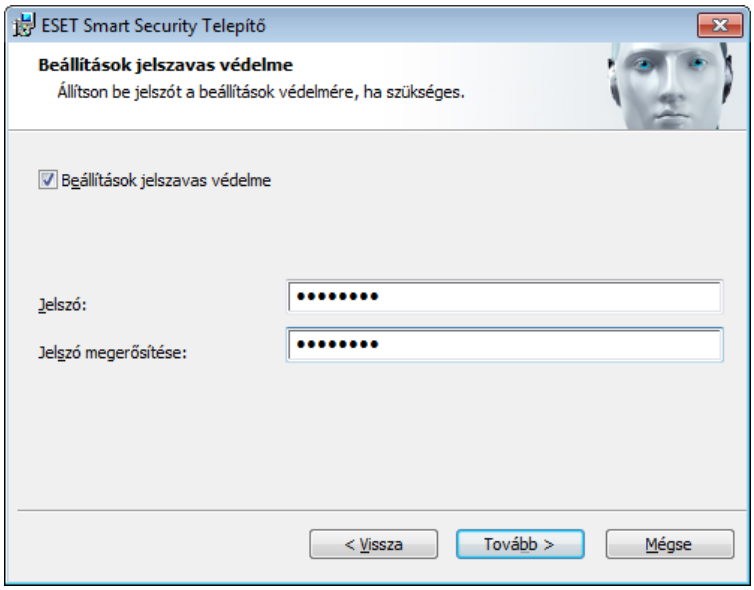


Ha nem szeretné frissíteni a programösszetevőket, jelölje be a **Programösszetevő-frissítés kikapcsolása** választógombot. A **Programösszetevők letöltésének felajánlása, ha van új verzió** lehetőséget választva egy megerősítést kérő párbeszédpanel fog megjelenni, mielőtt a rendszer a programösszetevők letöltéséhez hozzákezdene. A programösszetevők frissítésének automatikus letöltéséhez jelölje be **A programösszetevők frissítésének végrehajtása minden esetben** választógombot.



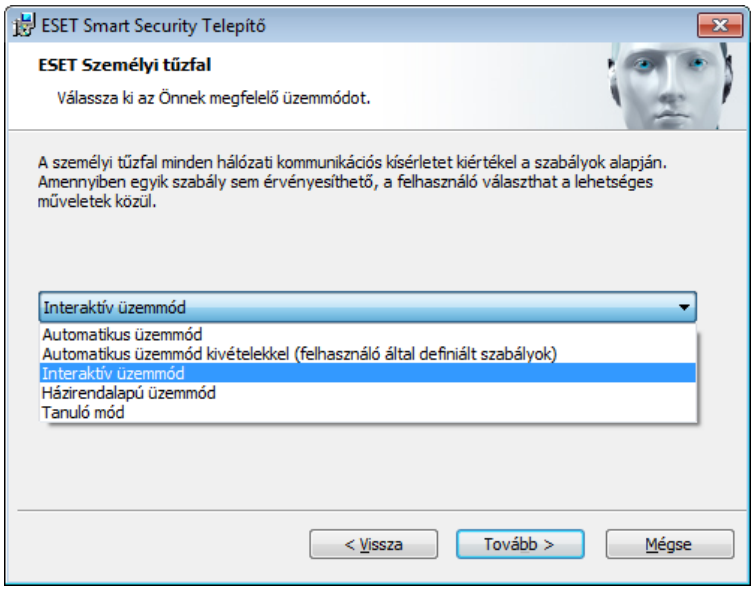
Megjegyzés: A programösszetevők frissítését követően rendszerint újra kell indítani a számítógépet. Ajánlott **A számítógép újraindítása értesítés nélkül, ha szükséges** választógombot bejelölni.

A következő telepítési ablakban megadhat egy jelszót a programbeállítások védelmének biztosításához. Jelölje be a **Beállítások jelszavas védelme** jelölőnégyzetet, és adja meg az ESET Smart Security beállításainak módosításához szükséges jelszót az **Új jelszó** és az **Új jelszó megerősítése** mezőben. Ha a két mezőben azonos jelszót adott meg, kattintson a **Tovább** gombra.



A következő két telepítési lépés, az **ESET ESET Live Grid közösségi online szolgáltatás** és a **Kéretlen alkalmazások keresése** megegyezik a tipikus telepítést ismertető témakörben leírttal (lásd Tipikus telepítés).

Ezután válasza ki az ESET Személyi tűzfal szűrési üzemmódját. Az ESET Smart Security Személyi tűzfalban öt szűrési üzemmód alkalmazható. A választott módtól függően változik a tűzfal működése. A szűrési módok a szükséges felhasználói beavatkozás szintjét is meghatározzák.



A telepítés befejezéséhez kattintson a **Telepítés** gombra a **Telepítésre kész** ablakban. A telepítés végeztével a rendszer megkéri a termék aktiválására. Az aktiválásról a Tipikus telepítés című témakörben olvashat.

2.3 Frissítés újabb verzióra

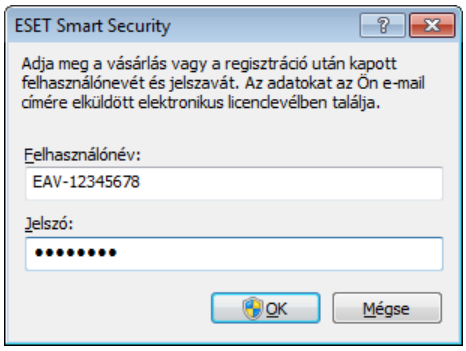
Az ESET Smart Security új verziói továbbfejlesztett funkciókat tartalmaznak, és a programmodulok automatikus frissítésével nem megszüntethető problémákat orvosolnak. Az újabb verzióra frissítés számos módon elvégezhető:

1. Automatikusan, a program frissítésével.
   Mivel a programfrissítések minden felhasználóra vonatkoznak, és hatással lehetnek a rendszerkonfigurációkra, kibocsátásukat megelőzően hosszú tesztelésen esnek át, hogy minden lehetséges rendszerkonfiguráción zavartalanul telepíthetők legyenek. Ha a kibocsátását követően azonnal újabb verzióra kell frissítenie, használja az alábbi módszerek egyikét.
2. Manuálisan, a fő ablak **Frissítés** lapján, **Az ESET Smart Security elérhető verziója** felirat melletti **Telepítés/ Ellenőrzés** hivatkozásra kattintva.
3. Manuálisan, az új verzió letöltésével és telepítésével (az előző verzióra).
   Ha a telepítés elkezdésekor bejelöli **A jelenlegi beállítások alkalmazása** jelölőnégyzetet, megőrizheti az aktuális programbeállításokat.

2.4 Felhasználónév és jelszó megadása

Az optimális működéshez fontos a program rendszeres, automatikus frissítése. Erre csak akkor van lehetőség, ha a **frissítési beállítások** lapján megadja a helyes felhasználónevet és jelszót.

Ha a program telepítésekor nem adta meg felhasználónevét és jelszavát, most megteheti. A program fő ablakában kattintson a **Frissítés** fülre, majd a **Termékaktiválás** műveletre, és adja meg az ESET biztonsági termékkel kapott licencadatokat a Termékaktiválás ablak mezőiben.



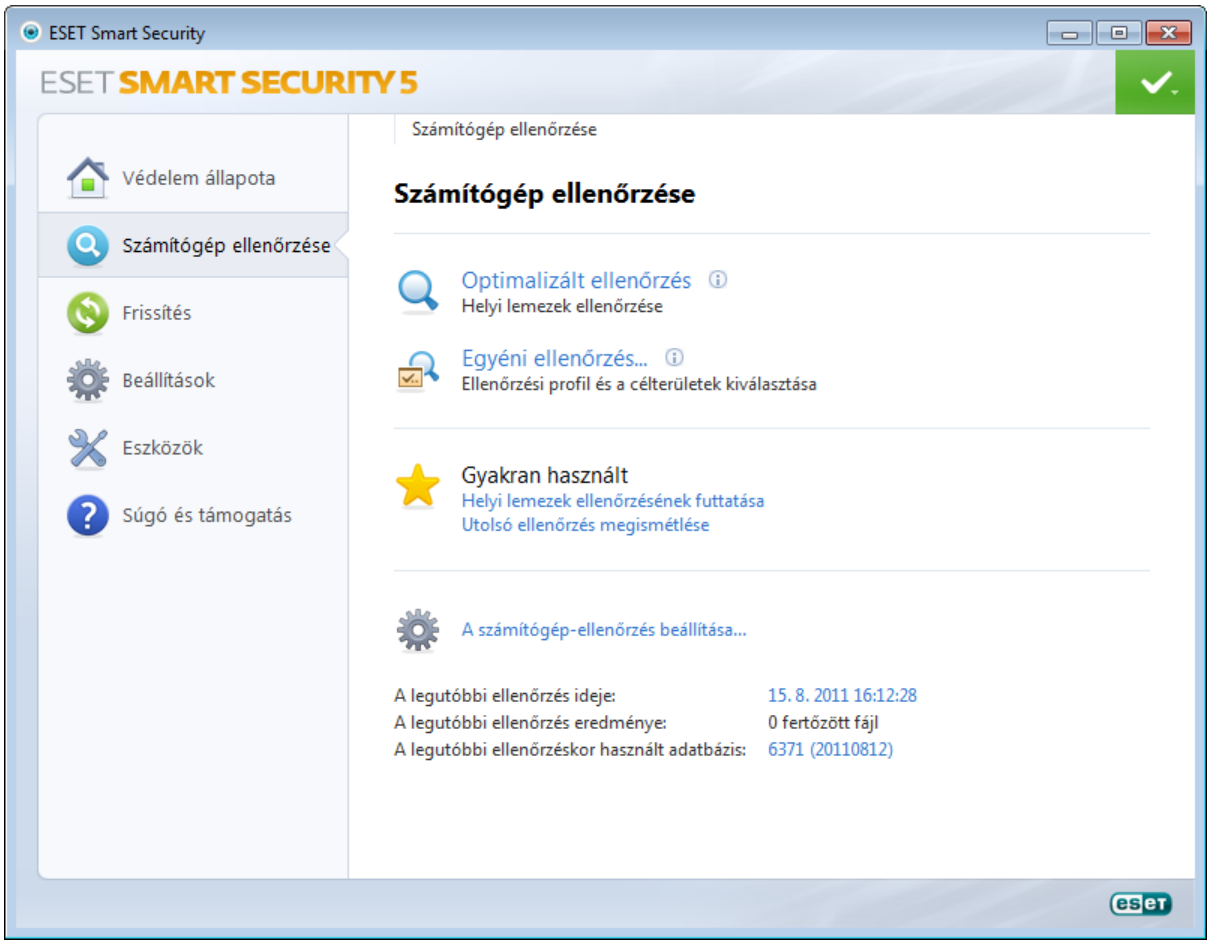
A **felhasználónév** és a **jelszó** megadásakor fontos, hogy pontosan írja be azokat:

- A felhasználónév és a jelszó beírásakor meg kell különböztetni a kis- és a nagybetűket, valamint szükség esetén a felhasználónévben ki kell tenni a kötőjelet.
- A jelszó tíz karakterből áll, amelyek mindegyike kisbetűs.
- A jelszavakban nem használjuk az L betűt (használja helyette az egy (1) számot).
- Egy nagy „O” a nulla (O), egy kis „o” a kisbetűs o betű.

Javasoljuk, hogy a legnagyobb pontosság érdekében a regisztrációs e-mailből másolja és illessze be az adatokat.

2.5 Számítógép ellenőrzése

Az ESET Smart Security telepítése után célszerű végrehajtani egy számítógép-ellenőrzést a kártevőkódok észlelésére. A program fő ablakában kattintson a **Számítógép ellenőrzése** fülre, majd az **Optimalizált ellenőrzés** műveletre. A számítógép ellenőrzéséről a Számítógép ellenőrzése című témakörben részletesebben olvashat.



3. Útmutató kezdő felhasználók számára

Ez a témakör az ESET Smart Security és alapbeállításainak az áttekintését tartalmazza.

3.1 A felhasználói felület ismertetése

Az ESET Smart Security fő ablaka két fő részre oszlik. A jobb oldali elsődleges ablakban a bal oldalon kiválasztott beállításnak megfelelő információk jelennek meg.

Az alábbi szakaszok a főmenüben található lehetőségeket ismertetik.

Védelem állapota – Az ESET Smart Security védelmi állapotáról jelenít meg adatokat.

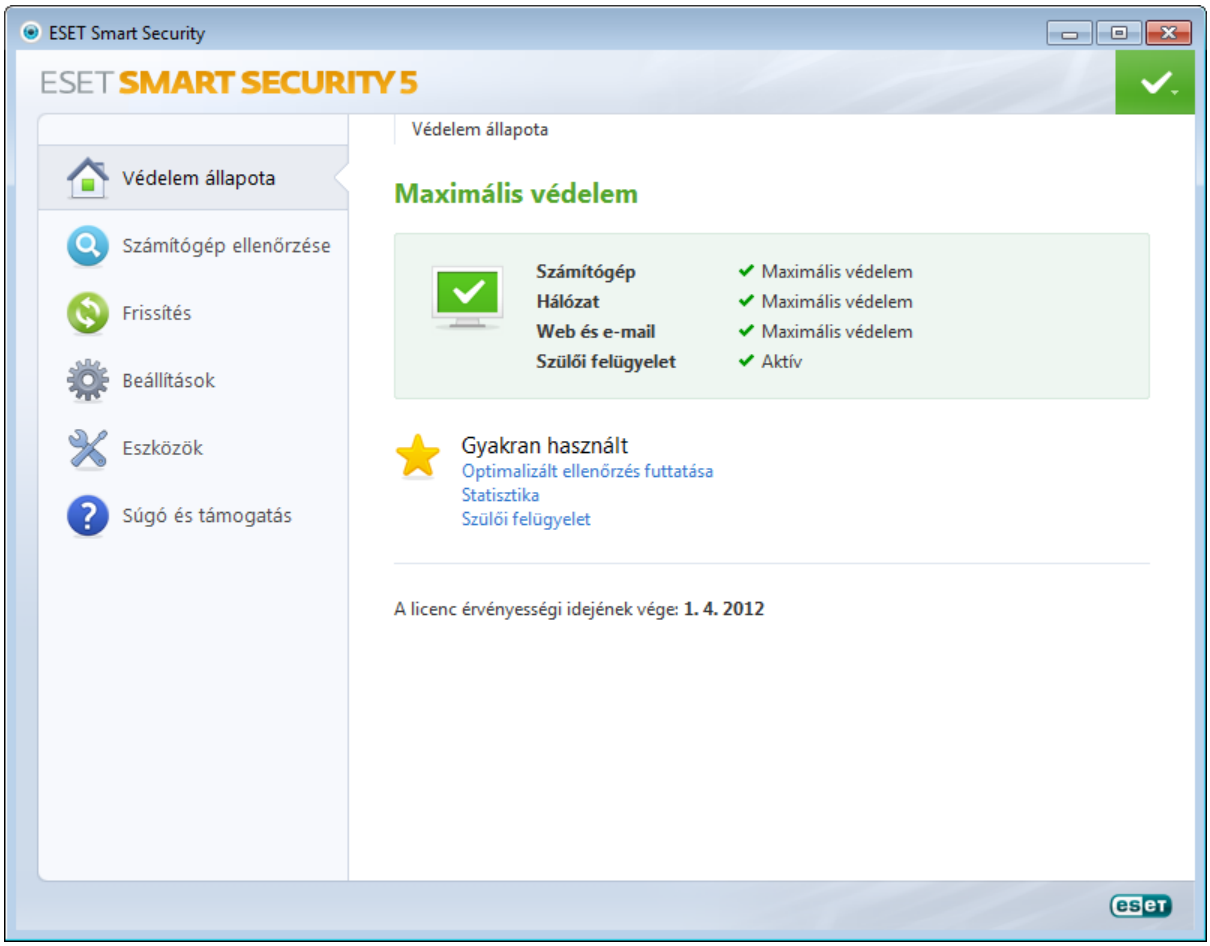
Számítógép ellenőrzése – Ezen a lapon optimalizált vagy egyéni ellenőrzést tud beállítani és indítani.

Frissítés – A vírusdefiníciós adatbázis frissítéseiről jelenít meg információkat.

Beállítások – Itt konfigurálhatja a számítógép, a web és a levelezés, valamint a hálózat és a szülői felügyelet biztonsági szintjét.

Eszközök – A lapon megjelenítheti a naplófájlokat, a védelmi statisztikákat, az aktivitást és a futó folyamatokat,a hálózati kapcsolatokat, a feladatütemezőt, a karantént, valamint elindíthatja az ESET SysInspector és az ESET SysRescue eszközt.

Súgó és támogatás – Erről a lapról elérheti a súgót, az ESET tudástárának cikkeit, az ESET weboldalát és a terméktámogatási kérelmekre mutató hivatkozásokat.

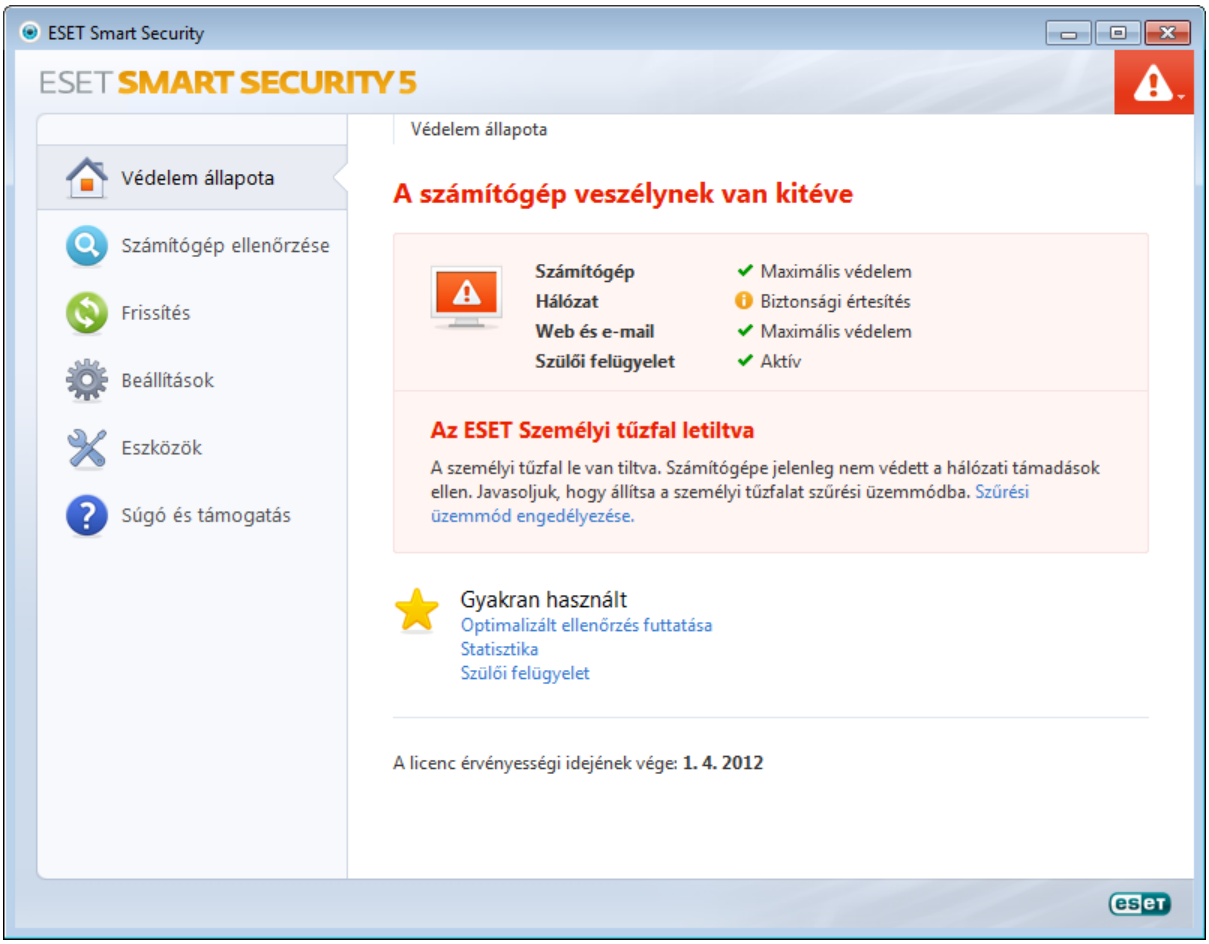


A **Védelem állapota** lap a számítógép biztonságáról és aktuális védelmi szintjéről nyújt tájékoztatást. A védelem állapotát jelző zöld ikon azt jelöli, hogy biztosított a **maximális védelem**.

Az állapotablakban láthatók az ESET Smart Security gyakran használt funkciói, valamint a program lejárati dátuma is.

3.2 Teendők, ha a program nem működik megfelelően

Ha az engedélyezett modulok megfelelően működnek, nevük mellett egy zöld pipa látható, ha nem, ezt egy piros felkiáltójel vagy egy sárga értesítő ikon jelzi, és ebben az esetben az ablak felső részében további információk is olvashatók. A szoftver javaslatot is ad a modulok működésének helyreállításához. Az egyes modulok állapotának megváltoztatásához kattintson a főmenüben a **Beállítások** lehetőségre, majd a kívánt modul nevére.



A vörös ikon kritikus problémákat jelez – ekkor nem biztosított a számítógép maximális védelme. A lehetséges okok:

- Le van tiltva a valós idejű fájlrendszervédelem
- Le van tiltva a személyi tűzfal
- Elavult a vírusdefiníciós adatbázis
- A termék nincs aktiválva
- Lejárt a terméklicenc

A sárga ikon azt jelzi, hogy a webhozzáférés vagy a levelezőprogramok védelme le van tiltva, probléma történt a program frissítése során (nem frissíthető egy elavult vírusdefiníciós adatbázis), vagy a licenc a közeljövőben lejár.

A termék nincs aktiválva – A problémát az ablak piros háttere, illetve a **Számítógép** ikon melletti biztonsági értesítés jelzi. Az ESET Smart Security a programmenü **Termékaktiválás** parancsával aktiválható. Az programmenü az ablak jobb felső részén helyezkedik el.

A vírus- és kémprogramvédelem le van tiltva – A problémát az ablak piros háttere, illetve a **Számítógép** ikon melletti biztonsági értesítés jelzi. A vírusvédelem engedélyezéséhez kattintson **Az összes vírus- és kémprogramvédelmi modul indítása** műveletre.

A webhozzáférés-védelem le van tiltva – A problémát egy i betűt ábrázoló sárga ikon, illetve a **Biztonsági értesítés** állapotfelirat jelzi. A webhozzáférés-védelem ismételt engedélyezéséhez kattintson a biztonsági értesítésre, majd a **Webhozzáférés-védelem engedélyezése** hivatkozásra.

Az ESET Személyi tűzfal letiltva – A problémát az ablak piros háttere, illetve a **Számítógép** ikon melletti biztonsági értesítés jelzi. A hálózati védelem ismételt engedélyezéséhez kattintson a **Szűrési üzemmód engedélyezése** hivatkozásra.

Az Ön licence hamarosan lejár – Ezt a tényt a védelmi állapot ikonján megjelenő felkiáltójel jelzi. A licenc lejárta után a

program nem frissül, és a védelem állapota ikon vörös lesz.

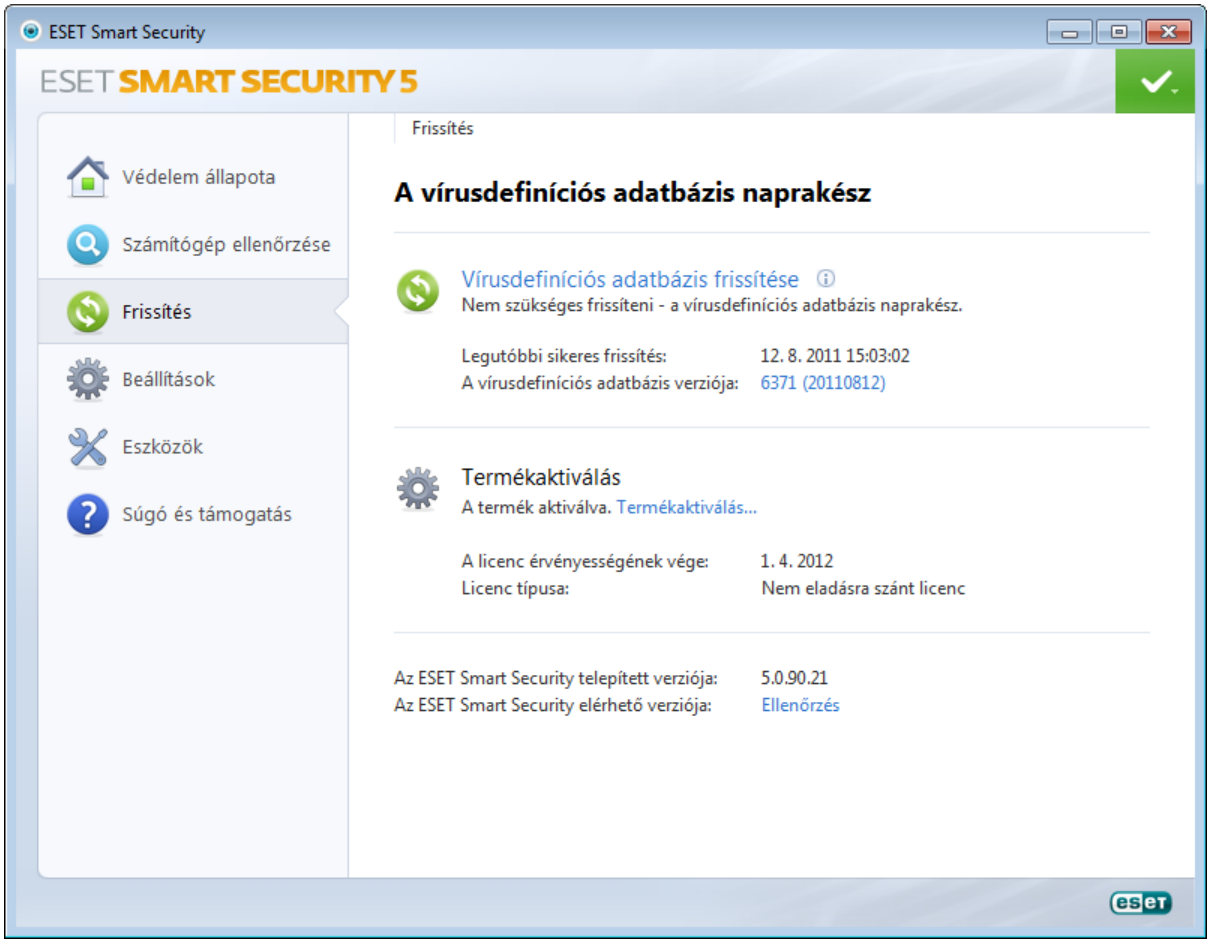
A licenc lejárt – Ezt jelzi, ha a védelem állapota ikon vörösre változik. Ettől kezdve a program nem frissül. Javasoljuk, hogy a licenc megújításához kövesse a riasztási ablakban látható utasításokat.

Ha a javasolt megoldásokkal nem szüntethető meg a probléma, kattintson a **Súgó és támogatás** fülre a súgófájlok megtekintéséhez és a tudásbázisbeli kereséshez. Ha további segítségre van szüksége, küldjön el egy kérelmet az ESET terméktámogatásának. Az ESET terméktámogatási munkatársa gyorsan válaszol a kérdéseire, és segít a probléma megoldásában.

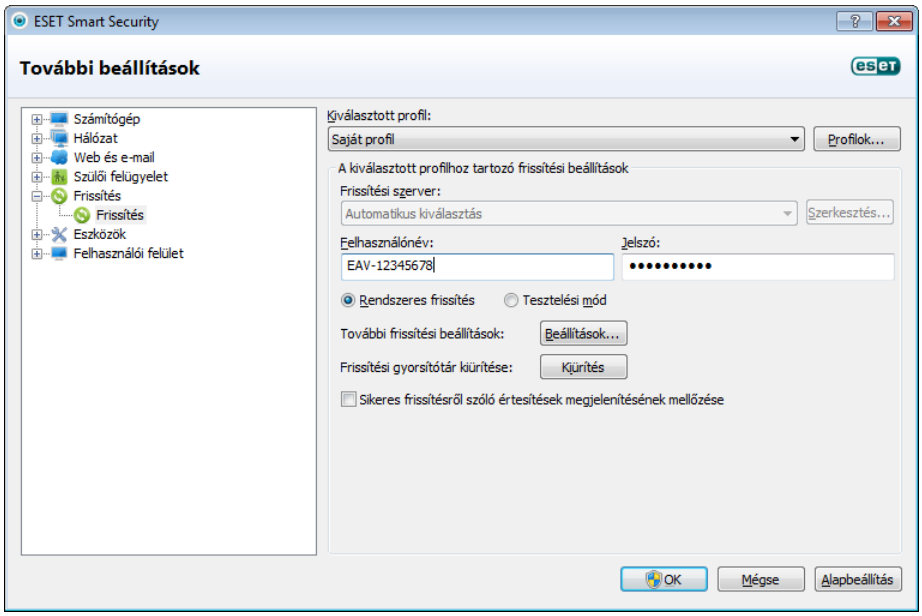
3.3 Frissítési beállítások

A kártevők elleni maradéktalan védelem fontos összetevője a vírusdefiníciós adatbázis és a programösszetevők frissítése, ezért beállításukra és működésükre különösen oda kell figyelni. Válassza a főmenü **Frissítés** parancsát, és kattintson a fő ablak **A vírusdefiníciós adatbázis frissítése** hivatkozására az újabb adatbázis-frissítések kereséséhez.

Ha az ESET Smart Security telepítése vagy aktiválása során nem adott meg felhasználónevet és jelszót, azokat ebben a lépésben kell megadnia.

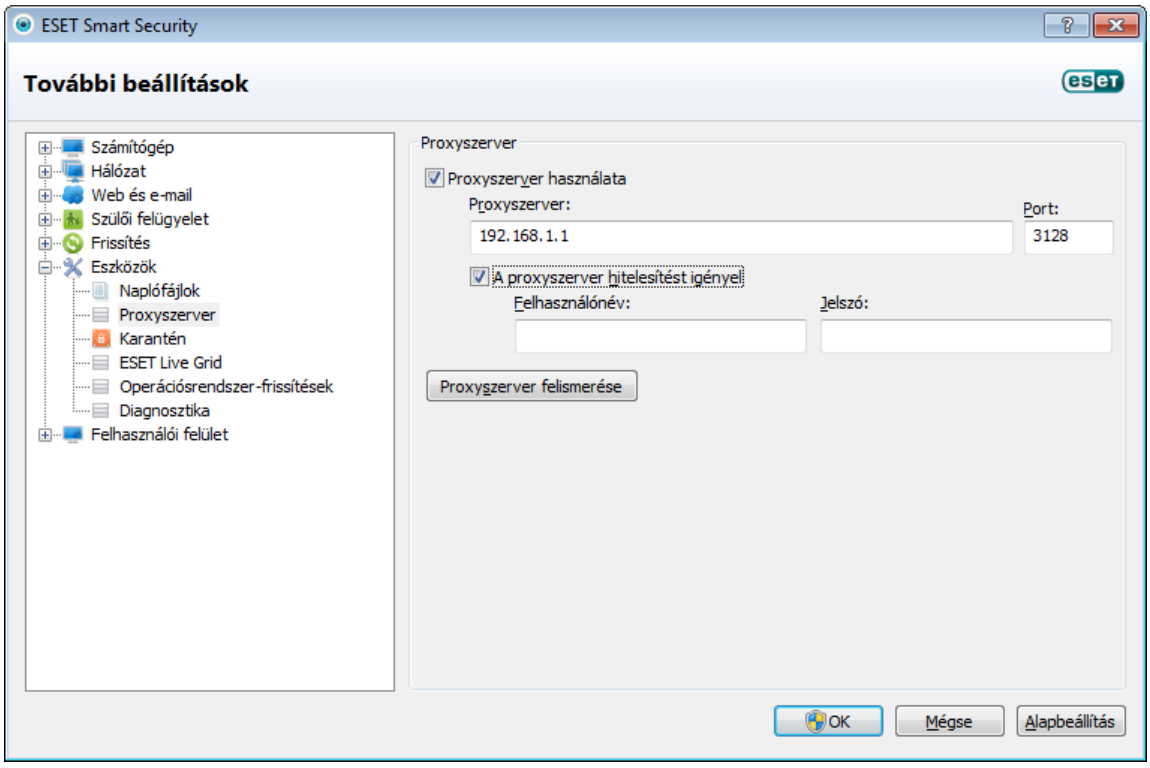


A További beállítások ablakban – amit a főmenü **Beállítások** parancsára, majd a **További beállítások megnyitása** lehetőségre kattintva, vagy az F5 billentyűt lenyomva érhet el – további frissítési beállítások találhatók. A további beállításokat tartalmazó bal oldali listában kattintson a **Frissítés** lehetőségre. A **Frissítési szerver** legördülő listában az **Automatikus kiválasztás** lehetőséget ajánlott kijelölni. A további beállítások – például a frissítési mód, a proxyszerver elérhetőségi adatai és a helyi hálózati kapcsolatok – beállításához kattintson a **Beállítások** gombra.



3.4 A proxyszerver beállításai

Ha proxyszerveren keresztül kapcsolódik az internethez az ESET Smart Security programot használó rendszeren, azt a További beállítások között kell megadnia. A proxyszerver beállításainak megnyitásához az F5 billentyű lenyomásával nyissa meg a További beállítások párbeszédpanelt, és jelölje ki a beállításfa **Eszközök** > **Proxyszerver** elemét. Jelölje be a **Proxyszerver használata** jelölőnégyzetet, majd töltse ki a **Proxyszerver** (IP-cím) és a **Port** mezőt. Szükség szerint jelölje be **A proxyszerver hitelesítést igényel** jelölőnégyzetet, és töltse ki a **Felhasználónév** és a **Jelszó** mezőt is.



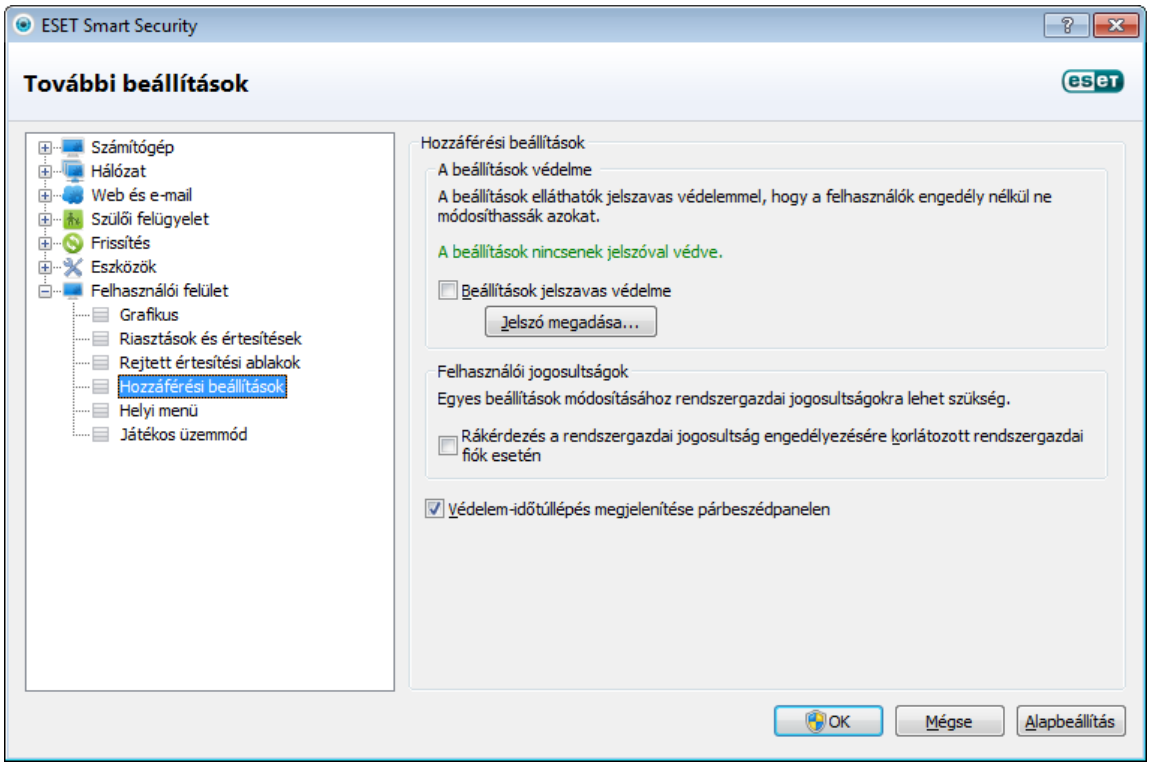
Ha nincs birtokában ezeknek az információknak, megpróbálkozhat a proxyszerver beállításainak automatikus észlelésével is, ha a **Proxyszerver felismerése** gombra kattint.

Megjegyzés: A különféle frissítési profilokhoz eltérő proxyszerver-beállítások tartozhatnak. Ebben az esetben a további beállítások listájában kattintson a Frissítés lehetőségre, és adja meg a különböző frissítési profilokat a további

beállítások között.

3.5 Védelmi beállítások

Az ESET Smart Security beállításai igen fontosak a biztonsági rend szempontjából. A jogosulatlan módosítások veszélyeztethetik a rendszer stabilitását és védelmét. A beállítási paraméterek védelméhez a főablakból indulva válassza a **Beállítások** > **További beállítások megnyitása** > **Felhasználói felület** > **Hozzáférési beállítások** lehetőséget, jelölje be a **Beállítások jelszavas védelme** jelölőnégyzetet, és kattintson a **Jelszó megadása** gombra.

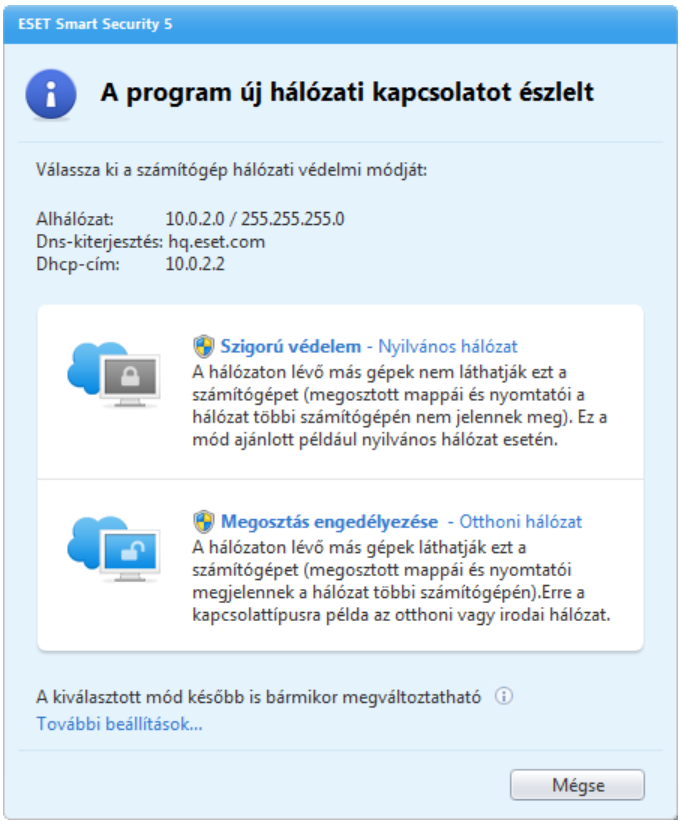


Írjon be egy jelszót az **Új jelszó** mezőbe, majd ismételje ezt meg a **Jelszó megerősítése** mezőben, és kattintson az **OK** gombra. Erre a jelszóra lesz szükség az ESET Smart Security minden jövőbeli módosításához.

3.6 Megbízható zóna beállításai

A megbízható zónát be kell állítani, hogy a számítógép hálózatos környezetben is védett legyen. A megbízható zóna megfelelő beállításával és a megosztás engedélyezésével lehetővé teheti másoknak a számítógéphez való hozzáférést. Válassza a **Beállítások** > **Hálózat** > **Válassza ki a számítógép hálózati védelmi módját** lehetőséget. Egy ablakban megjelennek a beállítások, amelyek közül kiválaszthatja a számítógép kívánt védelmi módját.

A megbízható zónák észlelése az ESET Smart Security telepítése vagy a számítógép új hálózathoz történő hozzáadása után történik meg. Ennek következtében általában nincs szükség a megbízható zóna definiálására. Az új zónák észlelésekor a szoftver alapértelmezés szerint egy párbeszédpanelt jelenít meg, amely lehetővé teszi az adott zóna védelmi szintjének a megadását.



Figyelmeztetés: Ha helytelenül adja meg a megbízható zónák beállításait, számítógépét biztonsági kockázatnak teszi ki.

Megjegyzés: A program alapértelmezés szerint engedélyezi a megbízható zónákban lévő munkaállomásoknak a megosztott fájlok és nyomtatók elérését, a bejövő távoli eljáráshívásokat, valamint a távoli asztalok megosztását is.

4. Az ESET Smart Security

Az ESET Smart Security beállításai lehetővé teszik a számítógépek és hálózatok védelmi szintjének megadását.

A **Beállítások** csoport az alábbi lehetőségeket tartalmazza:

- **Számítógép**
- **Hálózat**
- **Web és e-mail**
- **Szülői felügyelet**

Az egyes elemekre kattintva megadhatók a megfelelő védelmi modul további beállításai.

A **Számítógép** a csoport védelmi beállításai között engedélyezheti vagy tilthatja le az alábbi összetevőket:

- **Valós idejű fájlrendszervédelem** – A program a fájlok megnyitásakor, létrehozásakor vagy a számítógépen történő futtatásakor ellenőrzi, hogy nem tartalmaznak-e kártevő kódot.
- **Dokumentumvédelem** - A dokumentumvédelmi szolgáltatás a megnyitásuk előtt ellenőrzi a Microsoft Office-dokumentumokat, valamint az Internet Explorer által automatikusan letöltött fájlokat, például a Microsoft ActiveX-összetevőket.
- **Behatolásmegelőző rendszer** – A behatolásmegelőző rendszer felügyeli az operációs rendszeren belüli eseményeket, és a testreszabott szabályegyüttesek alapján reagál rájuk.
- **Játékos üzemmód** – Engedélyezi vagy letiltja a játékos üzemmódot. A játékos üzemmód engedélyezése biztonsági kockázatot hordoz, ezért a védelmi állapot ikonja a tálcán sárgára vált, és egy figyelmeztetés jelenik meg rajta.

A **Hálózat** részen engedélyezheti vagy tilthatja le a **személyi tűzfalat**.

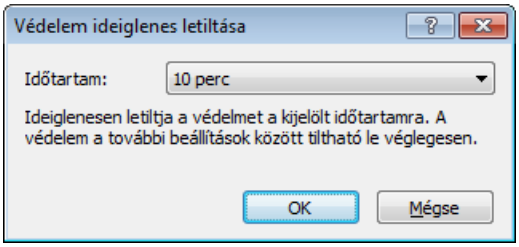
A **Web és e-mail** csoport védelmi beállításai lehetővé teszik az alábbi összetevők engedélyezését vagy letiltását:

- **Webhozzáférés-védelem** – Ha bejelöli ezt a jelölőnégyzetet, a program a HTTP és a HTTPS protokoll teljes forgalmát ellenőrzi kártevő szoftvereket keresve.
- **E-mail védelem** – Az e-mail védelem biztosítja a POP3 és IMAP protokollon keresztül érkező e-mail kommunikáció szabályozását.
- **Levélszemétszűrő** – Kiszűri a kéretlen e-maileket, azaz a levélszemetet.

A Szülői felügyelet szakaszban a szülői felügyelet engedélyezésére és letiltására van mód. A szülői felügyelet lehetővé teszi az esetlegesen nem kívánt tartalmú weblapok blokkolását. A szülők emellett akár 20 előre definiált webhely-kategória elérését is megtilthatják.

MEGJEGYZÉS: A Dokumentumvédelem a **További beállítások megnyitása** (F5) > **Számítógép** > **Vírus- és kémprogramvédelem** > **Dokumentumvédelem** > **Integrálás a rendszerbe** lehetőség választása után jelenik meg. Ugyanez igaz a szülői felügyeletre, csak a fenti lépéssorozatban a **Szülői felügyelet** lehetőséget kell választani.

Az **Engedélyezve** hivatkozásra kattintva megjelenik **A vírusvédelem ideiglenes kikapcsolása** párbeszédpanel. A kijelölt biztonsági összetevő letiltásához kattintson az **OK** gombra. Az **Időtartam** legördülő listában választhatja ki, hogy milyen időtartamra tiltja le a kijelölt összetevőt.



A letiltott biztonsági összevető ismételt engedélyezéséhez kattintson a **Letiltva** hivatkozásra.

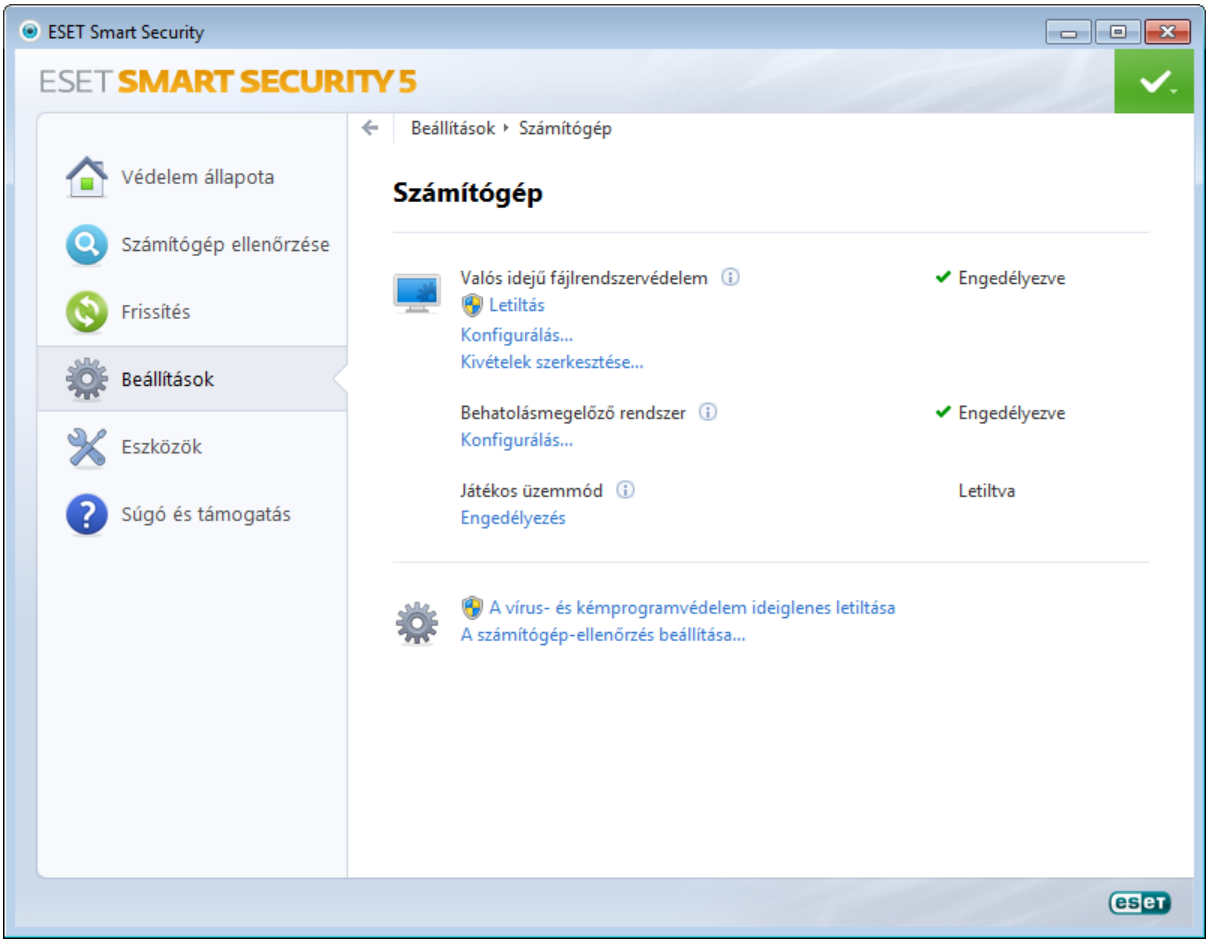
MEGJEGYZÉS: Ha ezzel a módszerrel tiltja le a védelmet, a számítógép újraindítása után a védelem összes letiltott eleme engedélyezett lesz.

A beállítási ablak alsó részén további lehetőségek találhatók. A **Termékaktiválás** hivatkozással megnyithat egy regisztrációs űrlapot, amelyet használva aktiválhatja az ESET biztonsági terméket, és egy e-mailt küldhet a hitelesítési adataival (felhasználónévvel és jelszóval). Egy *.xml* konfigurációs fájl segítségével betöltheti a beállítási paramétereket, illetve a **Beállítások importálása és exportálása** hivatkozást használva egy konfigurációs fájlba mentheti az aktuális beállítási paramétereket.

4.1 Számítógép

A számítógép konfigurációja a **Számítógép** hivatkozásra kattintva megnyitható **Beállítások** lapon található. A lapon az összes védelmi modul áttekintése látható. Az egyes modulok ideiglenes letiltásához kattintson a kívánt modul neve alatt található **Letiltás** hivatkozásra. Ne feledje, hogy ez gyengítheti a számítógép védelmét. Az egyes modulok részletes beállításainak megjelenítéséhez kattintson a **Konfigurálás** hivatkozásra.

A vírusellenőrzésből kizárandó fájlok és mappák **A kivételek szerkesztése** lehetőségre kattintva megnyitható Kivételek párbeszédpanelen adhatók meg.



A vírus- és kémprogramvédelem ideiglenes letiltása – Letiltja az összes vírus- és kémprogramvédelmi modult. Megjelenik **A vírusvédelem ideiglenes kikapcsolása** párbeszédpanel az **Időtartam** legördülő listával. Az **Időtartam** legördülő listában választhatja ki, hogy milyen hosszú időre tiltja le a kijelölt összetevőt. A megerősítéshez kattintson az **OK** gombra.

A számítógép-ellenőrzés beállítása – Kattintson a hivatkozásra a kézi indítású víruskereső paramétereinek módosításához (manuálisan végrehajtott ellenőrzéshez).

4.1.1 Vírus- és kémprogramvédelem

A Vírus- és kémprogramvédelem modul a fájlok, az e-mailek és az internetes kommunikáció ellenőrzésével akadályozza meg a kártékony kódok bejutását a rendszerbe. Ha a program kártékony kódot észlel, a víruskereső modul először letiltja, majd megtisztítja, törli vagy karanténba helyezi a hordozó fájlt.

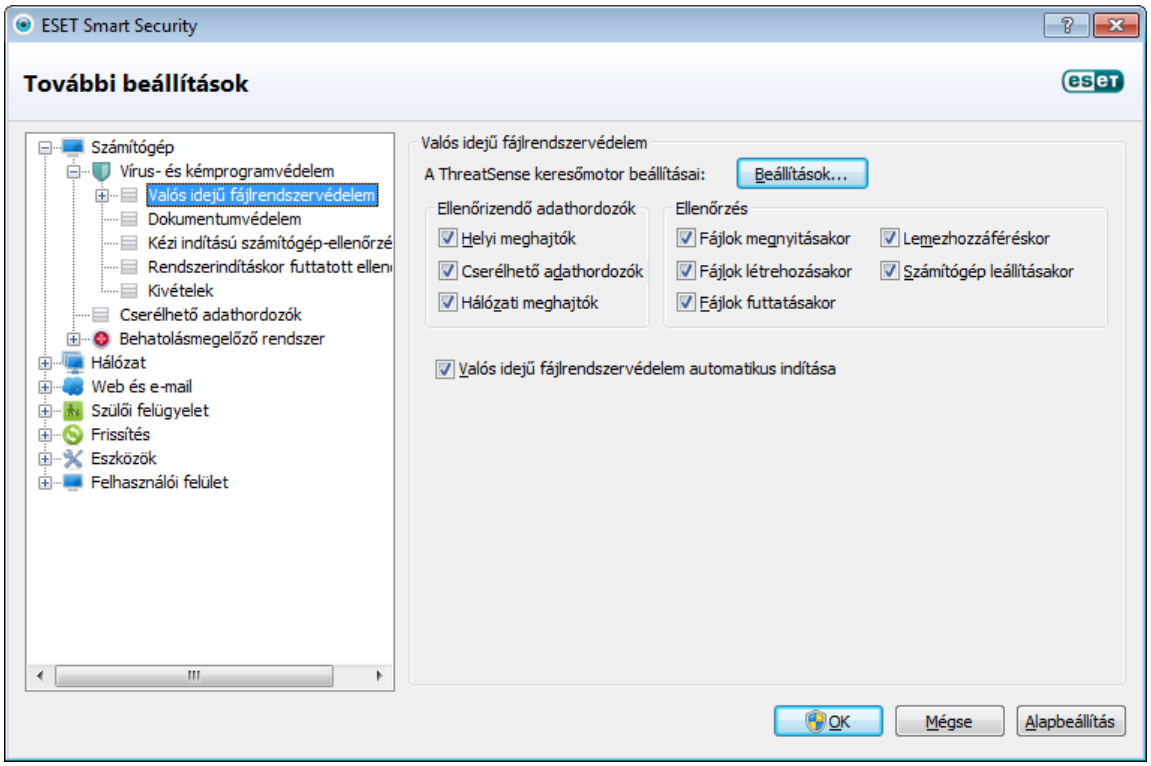
4.1.1.1 Valós idejű fájlrendszervédelem

A valós idejű fájlrendszervédelem a rendszer összes, a vírusvédelemhez köthető eseményét ellenőrzi. A program minden fájl megnyitásakor, létrehozásakor vagy a számítógépen történő futtatásakor ellenőrzi, hogy a fájl nem tartalmaz-e kártékony kódot. A valós idejű fájlrendszervédelem a számítógép indításakor automatikusan elindul.

A valós idejű fájlrendszervédelem a különböző rendszeresemények – például a fájlokhoz való hozzáférések – hatására ellenőrzi a különféle típusú adathordozókat. Az ellenőrzés az ThreatSense technológia észlelési módszereit alkalmazza (ezek leírása Az ThreatSense keresőmotor beállításai című témakörben található). Előfordulhat, hogy a valós idejű fájlrendszervédelem működése eltér az újonnan létrehozott, illetve a meglévő fájlok esetén. Új fájlok létrehozásakor lehetőség van mélyebb szintű ellenőrzés alkalmazására.

Az alacsony rendszerterhelés biztosítása érdekében a valós idejű védelem során a program csak akkor ellenőrzi újra a már ellenőrzött fájlokat, ha módosítják azokat. A fájlok újbóli ellenőrzése a vírusdefiníciós adatbázis minden frissítése után azonnal megtörténik. Ennek működése az **Optimalizálás** segítségével állítható be. Ha a szolgáltatás le van tiltva, a fájlok ellenőrzése a hozzájuk való minden egyes hozzáférés esetén megtörténik. A beállítás módosításához az F5 billentyű lenyomásával nyissa meg a További beállítások párbeszédpanelt, és válassza a beállításfa **Számítógép** > **Vírus- és kémprogramvédelem** > **Valós idejű fájlrendszervédelem** csomópontját. Kattintson a **Beállítások** gombra **Az ThreatSense keresőmotor beállításai** felirat mellett, jelölje ki az **Egyéb** csomópontot, végül jelölje be az **Optimalizálás engedélyezése** jelölőnégyzetet, vagy törölje belőle a jelet.

Alapértelmezés szerint a valós idejű védelem indítása a rendszerindításkor történik, és folyamatos ellenőrzés biztosít. Különleges esetekben – például ha a rendszer ütközik egy másik valós idejű víruskeresővel – a valós idejű védelem kikapcsolható a **Valós idejű fájlrendszervédelem automatikus indítása** jelölőnégyzet bejelölésével.



4.1.1.1.1 Ellenőrizendő adathordozók

A program alapértelmezés szerint minden típusú adathordozót ellenőriz a lehetséges veszélyek felderítése érdekében.

Helyi meghajtók – Az összes helyi meghajtó ellenőrzése

Cserélhető adathordozók – Hajlékonylemezek, USB-tárolóeszközök stb. ellenőrzése

Hálózati meghajtók – Az összes csatlakoztatott meghajtó ellenőrzése

Ajánlott az alapértelmezett beállításokat megtartani, és csak bizonyos esetekben módosítani – például amikor egyes adathordozók ellenőrzése jelentősen lassítja az adatátvitelt.

4.1.1.1.2 Ellenőrzés (esemény hatására történő ellenőrzés)

A program alapértelmezés szerint minden fájlt ellenőriz azok megnyitásakor, létrehozásakor vagy végrehajtásakor. Ajánlott az alapértelmezett beállítások megtartása, amelyek maximális szintű valós idejű védelmet biztosítanak a számítógép számára.

Fájlok megnyitásakor – Ezzel a beállítással engedélyezheti vagy letilthatja a megnyitott fájlok ellenőrzését.

Fájlok létrehozásakor – Ezzel a beállítással engedélyezheti vagy letilthatja az újonnan létrehozott vagy módosított fájlok ellenőrzését.

Fájlok futtatásakor – Ezzel a beállítással engedélyezheti vagy letilthatja a futtatott fájlok ellenőrzését.

Lemezhozzáférés – Ezzel a beállítással engedélyezheti vagy letilthatja a hajlékonylemezes meghajtóhoz való hozzáféréskor történő ellenőrzést.

A **Számítógép leállításakor** – Ezzel a jelölőnégyzettel engedélyezheti vagy letilthatja a merevlemez rendszerindítási szektorainak ellenőrzését a számítógép leállítása során. Habár a rendszerindítási szektorban manapság már ritkán találhatók vírusok, ajánlatos e beállításokat engedélyezett állapotban hagyni, mivel különböző forrásokban még mindig előfordulhatnak ilyen típusú fertőzések.

4.1.1.1.3 További ellenőrzési beállítások

A **Számítógép** > **Vírus- és kémprogramvédelem** > **Valós idejű fájlrendszervédelem** > **További beállítások** lapon részletesebb beállítási lehetőségek is találhatók.

További ThreatSense-paraméterek az új és módosított fájlokhoz – A fertőzés valószínűsége az újonnan létrehozott vagy módosított fájloknál nagyobb, mint a meglévő fájlok esetében, ezért a program további ellenőrzési paraméterekkel ellenőrzi a fájlt. A szokásos vírusdefiníció-alapú ellenőrzési módszerek mellett a szoftver kiterjesztett heurisztikát is alkalmaz, ami nagymértékben javítja az észlelési arányokat, mivel a heurisztikák új kártevők észlelésére is alkalmasak, még a vírusdefiníciós adatbázis frissítésének a megjelenése előtt. Az újonnan létrehozott fájlok mellett az ellenőrzés kiterjed az önkicsomagoló (.sfx) fájlokra és a futtatás közbeni tömörítőkre (belsőleg tömörített végrehajtható fájlokra) is. A tömörített fájlokat a program alapértelmezés szerint a 10. maximális szintig ellenőrzi, és ez az ellenőrzés a fájlok méretétől függetlenül megtörténik. A tömörített fájlok ellenőrzési beállításainak a módosításához törölje az **Alapbeállítások használata a tömörített fájlok ellenőrzéséhez** jelölőnégyzet jelölését.

További ThreatSense-paraméterek a futtatott fájlokhoz – Alapértelmezés szerint a program nem használ kiterjesztett heurisztikát a fájlok futtatásakor. Bizonyos esetekben azonban célszerű lehet ennek a lehetőségnek az engedélyezése (a **Kiterjesztett heurisztika a fájlok futtatásakor** beállítás segítségével). Ne feledje, hogy a kiterjesztett heurisztika következtében megnövekedett rendszerkövetelmények miatt néhány program futása lelassulhat. Ha a **Kiterjesztett heurisztika a fájlok cserélhető adathordozóról történő futtatásakor** jelölőnégyzet be van jelölve, és egyes cserélhető adathordozók (USB-) portját ki szeretné zárni a fájlok futtatásakor végzett kiterjesztett heurisztikai ellenőrzésből, kattintson a **Kivételek** gombra. Ekkor megjelenik a cserélhető adathordozók kizárására szolgáló ablak. Itt az egyes portokat képviselő jelölőnégyzetek bejelölésével vagy a jelölések törlésével testre szabhatja a beállításokat.

4.1.1.1.4 Megtisztítási szintek

A valós idejű védelem három megtisztítási szinttel rendelkezik (elérésükhöz kattintson a **Beállítások** gombra a **Valós idejű fájlrendszervédelem** párbeszédpanellapon, majd kattintson a **Megtisztítás** fülre).

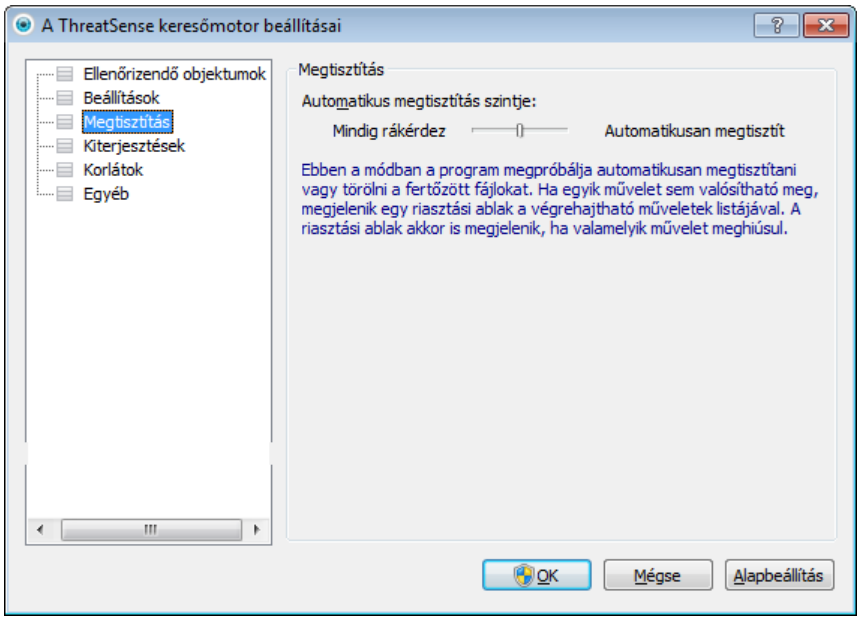
Mindig rákérdez – A program nem tisztítja meg automatikusan a fertőzött fájlokat, hanem megjelenít egy figyelmeztető ablakot, és a felhasználó választhat a műveletek közül. Ez a szint a tapasztalt felhasználóknak ajánlott, akik tisztában vannak azzal, hogy mi a teendő a fertőzések esetén.

Alapértelmezett szint – A program megkísérli a fertőzött fájlok automatikus megtisztítását vagy törlését. A tényleges műveletet a fertőzés függvényében határozza meg a rendszer. A fertőzött fájlok észlelését és törlését a program egy, a képernyő jobb alsó sarkában megjelenő tájékoztató üzenettel jelzi. Ha a megfelelő művelet automatikus kiválasztására nincs lehetőség, felkínál néhány utóműveletet. Ugyanez történik akkor is, ha az előre beállított műveletet nem lehet elvégezni.

Automatikusan megtisztít – A program megtisztítja vagy törli az összes fertőzött fájlt. A rendszerfájlok ez alól kivételt képeznek. Ha nem lehetséges a megtisztítás, a program egy figyelmeztető ablakban ajánl fel egy műveletet.

Figyelmeztetés: Ha egy tömörített fájl fertőzött fájlt tartalmaz, két alternatíva lehetséges: normál módban (**Alapértelmezett szint**) a program csak akkor törli a tömörített fájlt, ha a benne lévő összes fájl fertőzött; míg az **Automatikusan megtisztít** üzemmódban a program már akkor is törli a tömörített fájlt, ha csak egyetlen fertőzött fájlt

tartalmaz (tehát függetlenül a többi fájl állapotától).



4.1.1.1.5 Mikor érdemes módosítani a valós idejű védelem beállításain?

A valós idejű védelem a biztonságos rendszerek fenntartásának legfontosabb összetevője, ezért a paramétereket csak körültekintően módosítsa. Azt javasoljuk, hogy ezt csak különleges esetekben tegye, például akkor, ha a beállítások miatt a program ütközik egy másik alkalmazással vagy egy másik vírusvédelmi program valós idejű víruskeresőjével.

Telepítése után az ESET Smart Security minden beállítást optimalizál, hogy a lehető legmagasabb szintű védelmet biztosítsa a rendszer számára. Az alapértelmezett beállítások visszaállításához kattintson a **További beállítások** > **Számítógép** > **Vírus- és kémprogramvédelem** > **Valós idejű fájlrendszervédelem** lehetőség választásával elérhető **Valós idejű fájlrendszervédelem** párbeszédpanellap jobb alsó részén található **Alapbeállítás** gombra.

4.1.1.1.6 A valós idejű védelem ellenőrzése

Ha meg szeretne bizonyosodni arról, hogy a valós idejű védelem működik és képes a vírusok észlelésére, használja az eicar.com nevű tesztfájlt. A tesztfájl egy ártalmatlan, az összes víruskereső program által felismerhető speciális fájl. A fájlt az EICAR (European Institute for Computer Antivirus Research) vállalat hozta létre a víruskereső programok működésének tesztelése céljából. Az eicar.com fájl a következő helyről tölthető le: http://www.eicar.org/download/eicar.com

Megjegyzés: A valós idejű védelem ellenőrzésének végrehajtása előtt le kell tiltani a tűzfalat. Az engedélyezett tűzfal észleli a fájlt, és így megakadályozza a tesztfájlok letöltését.

4.1.1.1.7 Teendők, ha a valós idejű védelem nem működik

Ez a témakör a valós idejű védelem használata során előforduló problémákat és azok elhárítási módját ismerteti.

A valós idejű védelem le van tiltva

Ha a valós idejű védelmet egy felhasználó akaratlanul letiltotta, akkor újra kell aktiválni. A valós idejű védelem újbóli aktiválásához kattintson a **Beállítások** gombra, majd a program főablakában a **Valós idejű fájlrendszervédelem** fülre.

Ha a valós idejű védelem nem indul el a rendszer indításakor, valószínűleg nincs bejelölve a **Valós idejű fájlrendszervédelem automatikus indítása** jelölőnégyzet. A beállítás engedélyezéséhez válassza a További beállítások (F5) lehetőséget, és a beállításfában kattintson a **Számítógép** > **Vírus- és kémprogramvédelem** > **Valós idejű fájlrendszervédelem** csomópontra. A **További beállítások** párbeszédpanelen ellenőrizze, hogy be van-e jelölve a **Valós idejű fájlrendszervédelem automatikus indítása** jelölőnégyzet.

Ha a valós idejű védelem nem észleli és nem tisztítja meg a fertőzéseket

Győződjön meg arról, hogy a számítógépen nincs másik víruskereső program telepítve. Ha egyszerre két valós idejű védelmi szolgáltatást nyújtó eszköz van engedélyezve, azok ütközésbe kerülhetnek egymással. Ajánlatos az esetleges további víruskereső programokat eltávolítani a rendszerből.

A valós idejű védelem nem indul el

Ha a valós idejű védelem nem indul el rendszerindításkor (és be van jelölve a **Valós idejű fájlrendszervédelem automatikus indítása** jelölőnégyzet), akkor ennek valószínűleg más programokkal való ütközés az oka. Ilyen esetben forduljon az ESET terméktámogatási szakembereihez.

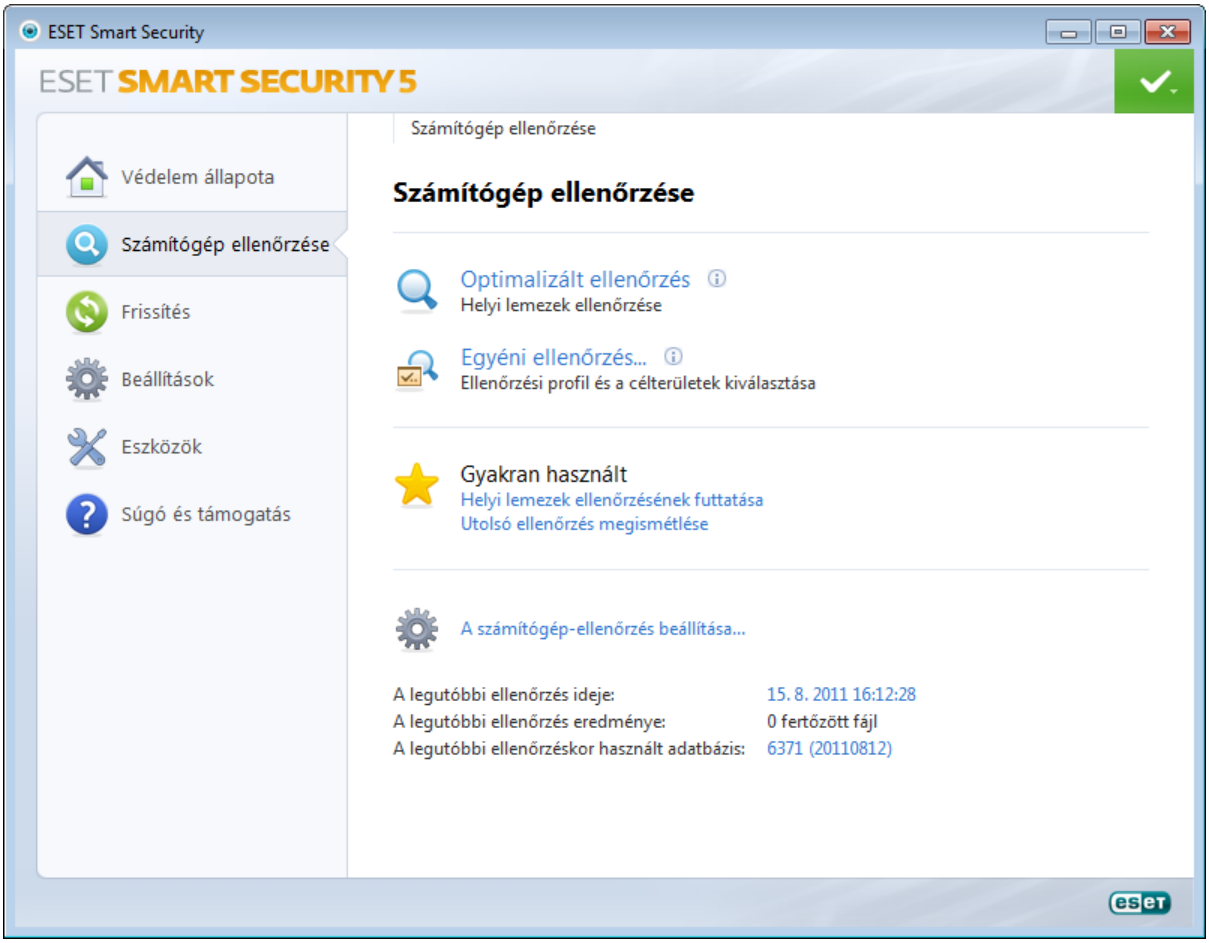
4.1.1.2 Dokumentumvédelem

A dokumentumvédelmi szolgáltatás a megnyitásuk előtt ellenőrzi a Microsoft Office-dokumentumokat, valamint az Internet Explorer által automatikusan letöltött fájlokat, például a Microsoft ActiveX-összetevőket. A védelmi rendszert az **Integrálás a rendszerbe** beállítás aktiválja. A beállítás módosításához az F5 billentyű lenyomásával nyissa meg a További beállítások párbeszédpanelt, és válassza a beállításfa **Számítógép** > **Vírus- és kémprogramvédelem** > **Dokumentumvédelem** csomópontját. Aktiválása esetén a dokumentumvédelmi funkció az ESET Smart Security főablakának **Beállítások** lapján, a **Számítógép** szakaszban tekinthető meg.

A szolgáltatást a Microsoft Antivirus API-t használó alkalmazások (például a Microsoft Office 2000 vagy újabb, illetve a Microsoft Internet Explorer 5.0-s vagy újabb verziói) aktiválják.

4.1.1.3 Számítógép ellenőrzése

A kézi indítású víruskereső a vírus- és kémprogramvédelem fontos része. Használatával ellenőrizheti a számítógépen lévő fájlokat és mappákat. Biztonsági szempontból fontos, hogy a számítógép-ellenőrzések futtatása ne csak akkor történjen meg, ha fertőzés gyanítható, hanem rendszeres időközönként, a szokásos biztonsági intézkedések részeként. Ajánlott a rendszer alapos és rendszeres ellenőrzése a **Valós idejű fájlrendszervédelem** által nem észlelt lehetséges vírusok kiszűrése céljából. Vírusok akkor lehetnek jelen, ha a Valós idejű fájlrendszervédelem ki volt kapcsolva az adott időben, a vírusdefiníciós adatbázis elavult volt, illetve a lemezre íráskor a program nem ismerte fel vírusként a fájlt.



A **Számítógép ellenőrzése** lap kétféle ellenőrzési lehetőséget kínál – az **Optimalizált ellenőrzés** lehetőséget választva gyorsan, az ellenőrzési paraméterek konfigurálása nélkül ellenőrizheti a rendszert; míg az **Egyéni ellenőrzés** lehetőség esetén választhat az előre definiált ellenőrzési profilok közül, illetve ellenőrizendő célterületeket jelölhet ki.

Az ellenőrzési folyamatról olvashat bővebben Az ellenőrzés folyamata című fejezetben.

Javasolt legalább havonta egyszer ellenőrizni a számítógépet. Az ellenőrzés az **Eszközök** lapon lévő **Feladatütemező** lehetőséget választva állítható be.

4.1.1.3.1 Az ellenőrzés típusa

4.1.1.3.1.1 Optimalizált ellenőrzés

Az optimalizált ellenőrzéssel gyorsan elindítható a számítógép ellenőrzése, és felhasználói beavatkozás nélkül megtisztíthatók a fertőzött fájlok. Az optimalizált ellenőrzés előnye az egyszerű használhatóság, mely nem igényli az ellenőrzési beállítások részletes megadását. Az optimalizált ellenőrzés a helyi meghajtókon lévő összes fájlt ellenőrzi, és automatikusan megtisztítja vagy törli az észlelt fertőzéseket. A megtisztítás szintje automatikusan az alapértelmezett értékre van állítva. A megtisztítás típusairól a Megtisztítás című témakörben olvashat bővebben.

4.1.1.3.1.2 Egyéni ellenőrzés

Az egyéni ellenőrzés optimális megoldás, ha be szeretné állítani az ellenőrzés paramétereit (például a célterületeket vagy az ellenőrzési módszereket). Az egyéni ellenőrzés előnye a paraméterek részletes konfigurálásának lehetősége. A beállított paraméterek felhasználó által definiált ellenőrizési profilokba menthetők, ami az ugyanazon beállításokkal végzett gyakori ellenőrzések során lehet hasznos.

Az ellenőrizendő célterületek kiválasztásához a **Számítógép ellenőrzése** lapon kattintson az **Egyéni ellenőrzés** hivatkozásra, és válasszon egy lehetőséget az **Ellenőrizendő célterületek** legördülő listában, vagy a fastruktúrában jelöljön ki adott célterületeket. Az ellenőrizendő célterületek az ellenőrzésben szerepeltetni kívánt mappa vagy fájl(ok) elérési útjának megadásával is meghatározhatók. Ha csak információszerzés céljából, változtatás nélkül szeretné ellenőrizni a rendszert, jelölje be a **Csak ellenőrzés megtisztítás nélkül** jelölőnégyzetet. A **Beállítások** > **Megtisztítás** lehetőséget választva három megtisztítási szint közül választhat.

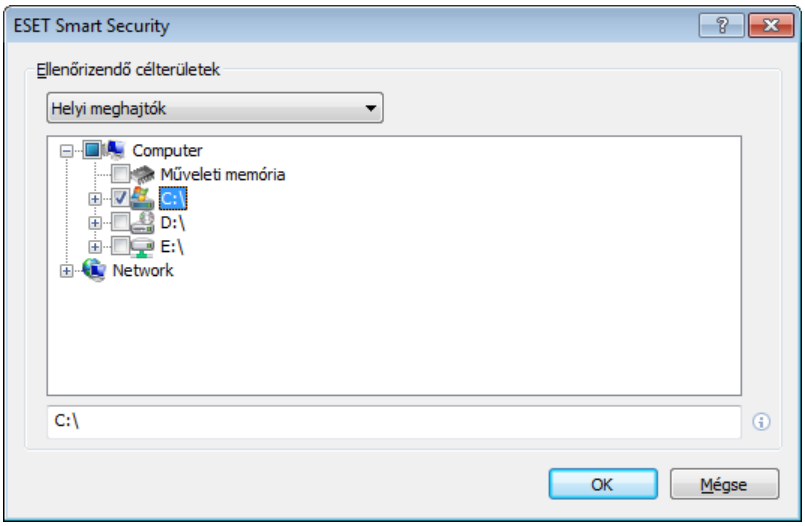
A számítógép egyéni ellenőrzése a víruskereső programokkal kapcsolatban tapasztalattal rendelkező felhasználóknak ajánlott.

4.1.1.3.2 Ellenőrizendő célterületek

Az Ellenőrizendő célterületek kiválasztása párbeszédpanelen definiálhatók azok a célterületek (memória, meghajtók, szektorok, fájlok és mappák), amelyeken vírusellenőrzést szeretne végrehajtani. Az **Ellenőrizendő célterületek** legördülő listában előre definiált célterületeket választhat ki.

- **Profilbeállítások alapján** – A kijelölt ellenőrzési profilban meghatározott célterületeket ellenőrzi.
- **Cserélhető adathordozók** – A hajlékonylemezeket, USB-tárolóeszközöket, CD és DVD lemezeket ellenőrzi.
- **Helyi meghajtók** – Valamennyi helyi meghajtót ellenőrzi.
- **Hálózati meghajtók** – Valamennyi csatlakoztatott hálózati meghajtót ellenőrzi.
- **Nincs kiválasztás** – Nem ellenőriz egyetlen célterületet sem.

Az ellenőrizendő célterületek az ellenőrzésben szerepeltetni kívánt mappa vagy fájl(ok) elérési útjának megadásával is meghatározhatók. Az ellenőrizendő objektumokat a számítógépen rendelkezésre álló összes eszközt felsoroló, fa szerkezetű listából választhatja ki.



Ha gyorsan szeretne egy kiválasztott ellenőrizendő célterülethez navigálni, vagy közvetlenül szeretne hozzáadni egy kívánt célterületet, írja be azt a mappalista alatti üres mezőbe. Erre csak akkor van lehetősége, ha a mappalistában nincs kijelölve objektum, illetve ha a fastruktúrás listából nem választott ki célterületet, és az **Ellenőrizendő célterületek** legördülő listában a **Nincs kiválasztás** elem van kijelölve.

4.1.1.3.3 Ellenőrzési profilok

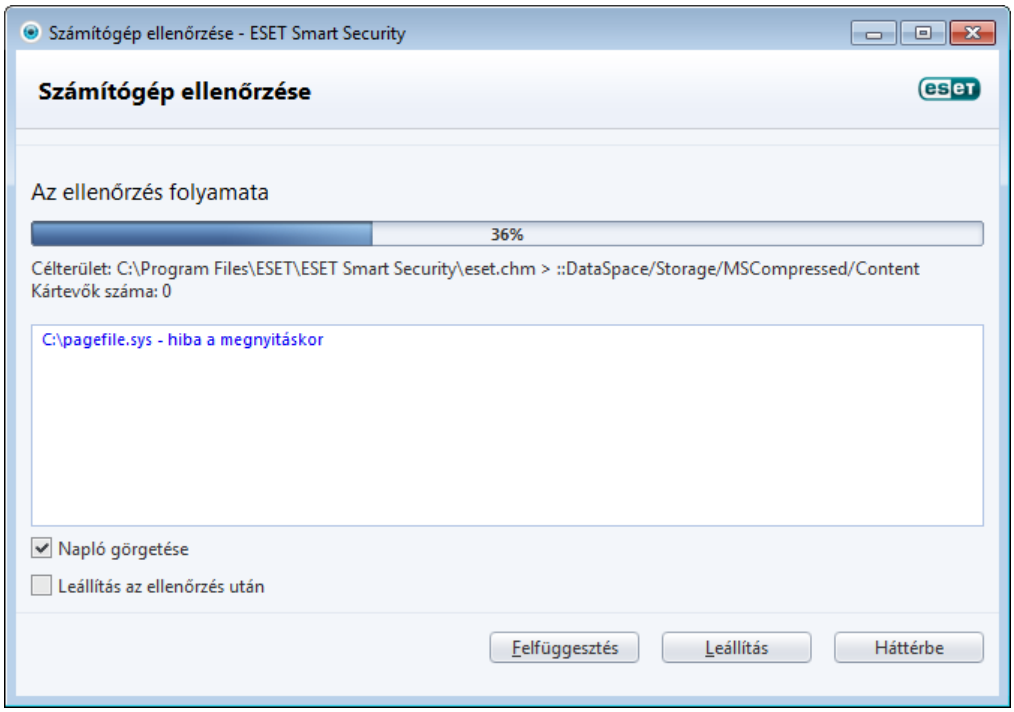
Az előnyben részesített ellenőrzési paramétereket mentheti, és a későbbi ellenőrzésekhez használhatja. A rendszeresen használt ellenőrzésekhez ajánlott különböző profilt létrehozni (különféle ellenőrizendő célterületekkel, ellenőrzési módszerekkel és más paraméterekkel).

Új profil létrehozásához nyissa meg a További beállítások ablakot (F5), és kattintson a **Számítógép-ellenőrzés** lehetőségre, majd a **Profilok** gombra. A **Konfigurációs profilok** ablakban látható a meglévő ellenőrzési profilok legördülő listája és egy új profil létrehozására szolgáló gomb. Ha segítségre van szüksége az igényeinek megfelelő ellenőrzési profil létrehozásával, Az ThreatSense keresőmotor beállításai című részben megtalálja az ellenőrzési beállítások egyes paramétereinek a leírását.

Példa: Tegyük fel, hogy saját ellenőrzési profilt szeretne létrehozni, és az Optimalizált ellenőrzés konfigurációja részben megfelel az elképzeléseinek, nem kívánja azonban ellenőrizni a futtatás közbeni tömörítőket vagy a veszélyes alkalmazásokat, emellett **automatikus megtisztítást** szeretne alkalmazni. A **Konfigurációs profilok** ablakban kattintson a **Hozzáadás** gombra. Írja be az új profil nevét a **Profil neve** mezőbe, és jelölje ki az **Intelligens ellenőrzés** profilt a **Beállítások másolása a következő profilból** legördülő listából. Ezt követően a fennmaradó paraméterek szükség szerinti módosításával az igényeinek megfelelően alakíthatja a profilt.

4.1.1.3.4 Az ellenőrzés folyamata

Az ellenőrzés folyamatát jelző ablakban látható az ellenőrzés jelenlegi állapota, valamint a kártékony kódokat tartalmazó fájlok száma.



MEGJEGYZÉS: A program rendes működése mellett előfordulhat, hogy bizonyos – például jelszóval védett vagy kizárólag a rendszer által használt – fájlok (jellemzően a *pagefile.sys* és egyes naplófájlok) ellenőrzése nem lehetséges.

Az ellenőrzés folyamata – A folyamatjelző sáv a már ellenőrzött és az ellenőrzésre váró objektumok egymáshoz viszonyított százalékos arányát jelzi. A program ezt az értéket az ellenőrzésbe felvett objektumok teljes számából számítja ki.

Célterület – Az aktuálisan ellenőrzött objektum neve és helye.

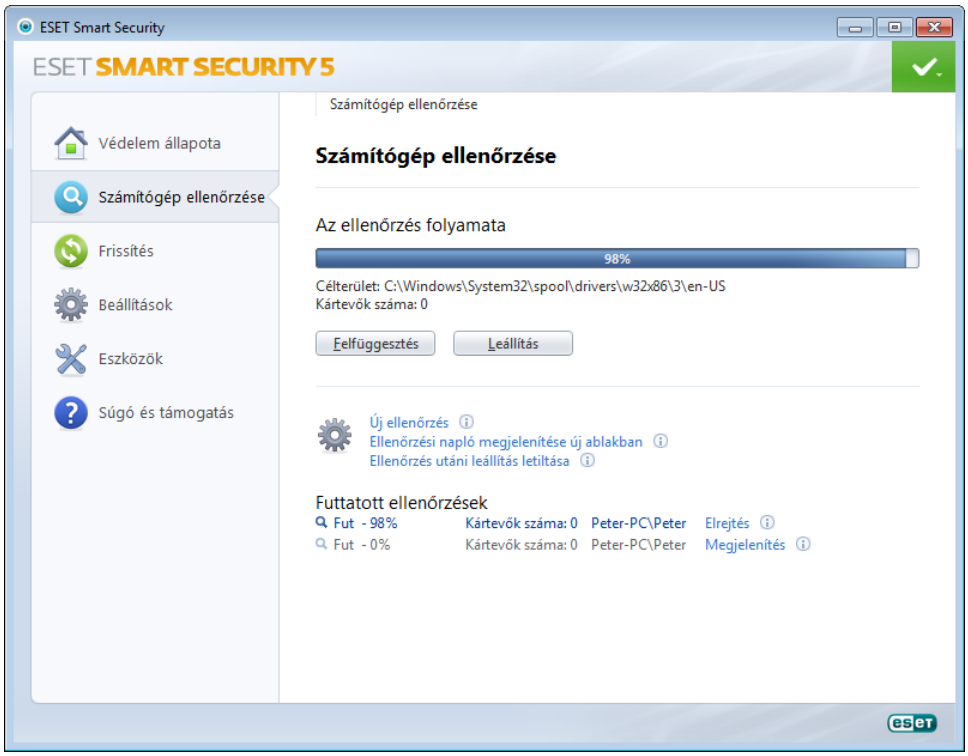
Kártevők száma – Itt látható a program által az ellenőrzés során észlelt kártevők száma.

Felfüggesztés – Felfüggeszti az ellenőrzést.

Folytatás – Ez a gomb akkor látható, ha felfüggesztette az ellenőrzést. Az ellenőrzés folytatásához kattintson a **Folytatás** gombra.

Leállítás – Megszakítja az ellenőrzést.

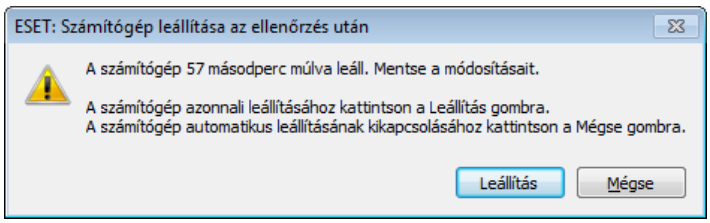
Háttérbe – Egy másik ellenőrzést is futtathat párhuzamosan. A folyamatban lévő ellenőrzés a háttérbe kerül.



Az ellenőrzési folyamathoz való visszatéréshez kattintson **Az ellenőrzés előtérbe hozása** hivatkozásra.

Napló görgetése – A jelölőnégyzet bejelölése esetén a víruskeresési napló az új bejegyzések hozzáadásával automatikusan legördül, láthatóvá téve a legfrissebb bejegyzéseket.

Ellenőrzés utáni leállítás engedélyezése – Engedélyezi a számítógép ütemezett leállítását a kézi indítású számítógép-ellenőrzés befejezését követően. Ebben az esetben a leállítás megerősítését kérő párbeszédablak jelenik meg, amely 60 másodperc elteltével automatikusan bezárul. A számítógép leállításának megszakításához kattintson a **Mégse** gombra.

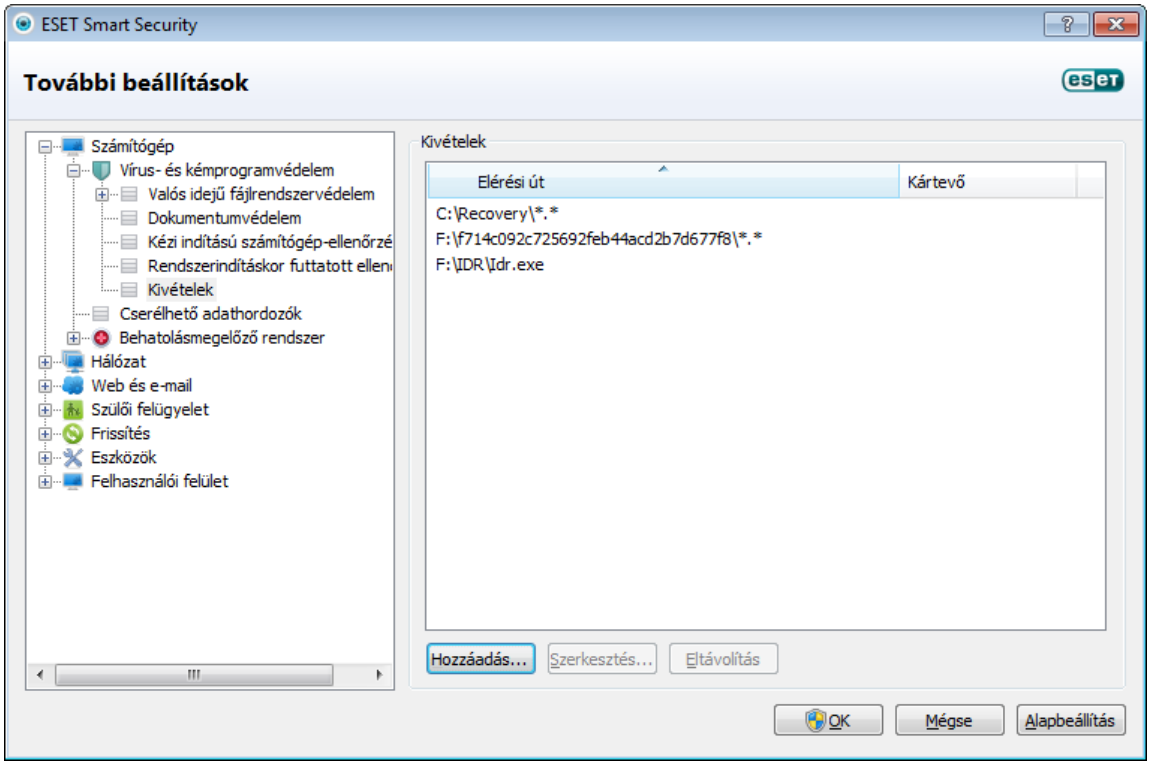


4.1.1.4 Rendszerindításkor futtatott ellenőrzés

A valós idejű fájlrendszervédelem engedélyezése esetén a program rendszerindításkor vagy a vírusdefiníciós adatbázis frissítésekor elvégzi a rendszerindításkor automatikusan futtatott fájlok ellenőrzését. Az ellenőrzés a **Feladatütemezőben** meghatározott beállításoktól és feladatoktól függ.

4.1.1.5 Kivételek

Ebben a részben fájlokat és mappákat zárhat ki az ellenőrzésből. Ha azt szeretné, hogy a program minden objektumot megvizsgáljon az esetleges kártevők kiszűrése érdekében, azt javasoljuk, hogy ne módosítsa ezeket a beállításokat. Bizonyos esetekben azonban szükség lehet egy-egy objektum kizárására. A nagy adatbázis-bejegyzések ellenőrzése például lelassíthatja a számítógép működését, akárcsak az olyan szoftverek, amelyek ütköznek az ellenőrzéssel.



Elérési út – A kizárt fájlok és mappák elérési útját írja le.

Kártevő – Ha a kizárt fájl mellett egy kártevő neve látható, akkor az azt jelenti, hogy a fájlt nem teljesen, hanem csak az adott kártevőt érintő ellenőrzésből zárja ki. Ha a fájlt később egy másik kártevő is megfertőzi, a vírusvédelmi modul ezt észlelni fogja. Ez a kizárástípus csak egyes fertőzéstípusok esetén használható, és vagy a fertőzést jelentő riasztási ablakban hozható létre (kattintson a **További beállítások megjelenítése**, majd az **Ellenőrzésből kizárva** lehetőségre) vagy a **Beállítások** > **Karantén** ablakban (kattintson a jobb gombbal a karanténba helyezett fájlon, majd válassza a helyi menüből a **Visszaállítás és kizárás az ellenőrzésből** parancsot).

Hozzáadás – Ezzel a gombbal zárhat ki objektumokat az ellenőrzésből.

Szerkesztés – A kijelölt bejegyzések szerkesztését teszi lehetővé.

Eltávolítás – A kijelölt bejegyzéseket távolítja el.

Objektumok ellenőrzésből való kizárásához:

1. Kattintson a **Hozzáadás**,
2. Írja be az objektum elérési útját, vagy jelölje ki az objektumot a fastruktúrában.

A kivételek definiálásához helyettesítő karaktereket, vagyis * és ? szimbólumot is használhat.

Példák

- Ha egy mappa összes fájlját ki szeretné zárni, akkor írja be a mappa elérési útját, és fűzze a végére a „*.*” maszkot.
- Ha csak a .doc fájlokat szeretné kizárni, a „*.doc” maszkot kell megadnia.
- Ha tudja, hogy egy programfájl neve hány (a példában 5) karaktert tartalmaz, de csak az elsőt ismeri biztosan (legyen ez a példában D), akkor ezt a „D????.exe” maszkkal fejezheti ki. Minden kérdőjel egy ismeretlen karaktert helyettesít.

4.1.1.6 Az ThreatSense keresőmotor beállításai

Az ThreatSense technológia számos összetett kártevő-észlelési módszer együttese, amely az új kártevők elterjedésének korai szakaszában is védelmet nyújt. Számos módszer (kódelemzés, kódemuláció, általános definíciók, vírusdefiníciók) összehangolt alkalmazásával jelentős mértékben növeli a rendszer biztonságát. A keresőmotor több adatfolyam egyidejű ellenőrzésére képes a hatékonyság és az észlelési arány maximalizálása érdekében. Az ThreatSense technológia sikeresen eltávolítja a rootkiteket is.

Az ThreatSense technológia beállítási lehetőségeivel több ellenőrzési paraméter megadható, többek között az alábbiak:

- Az ellenőrizendő fájltípusok és kiterjesztések
- Különböző észlelési módszerek kombinációja
- A megtisztítás mértéke stb.

A beállítási ablak megnyitásához kattintson a **Beállítások** gombra az ThreatSense technológiát alkalmazó bármely modul beállítási ablakában (lásd alább). A különböző biztonsági körülmények eltérő konfigurációkat igényelhetnek. Ennek érdekében az ThreatSense külön beállítható az alábbi védelmi modulokhoz:

- Valós idejű fájlrendszervédelem
- Dokumentumvédelem
- E-mail védelem
- Webhozzáférés-védelem
- Számítógép ellenőrzése

Az ThreatSense keresőmotor beállításai minden modulhoz nagymértékben optimalizáltak, és módosításuk jelentősen befolyásolhatja a rendszer működését. Ha például engedélyezi, hogy a program mindig ellenőrizze a futtatás közbeni tömörítőket, vagy bekapcsolja a kiterjesztett heurisztikát a Valós idejű fájlrendszervédelem modulban, a rendszer lelassulhat (a program normál esetben ezekkel a módszerekkel csak az újonnan létrehozott fájlokat ellenőrzi). Ezért a Számítógép ellenőrzése modul kivételével az összes modul esetében ajánlott az ThreatSense paramétereit az alapértelmezett értékeken hagyni.

4.1.1.6.1 Ellenőrizendő objektumok

Az **Ellenőrizendő objektumok** részben állítható be, hogy a rendszer mely elemeit, illetve milyen típusú fájlokat ellenőrizzen a keresőmotor.

Műveleti memória – E beállítással a rendszer műveleti memóriáját megtámadó kártevők ellenőrizhetők.

Rendszerindítási szektorok – A rendszerindítási szektorok ellenőrzése.

E-mail fájlok – A program a következő kiterjesztéseket ellenőrzi: DBX (Outlook Express) és EML.

Tömörített fájlok – A program a következő kiterjesztéseket ellenőrzi: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE stb.

Önkicsomagoló tömörített fájlok – Az önkicsomagoló tömörített fájlok olyan fájlok, amelyek kicsomagolásához nincs szükség külön programra, mert önmagukat csomagolják ki.

Futtatás közbeni tömörítők – Elindításuk után a futtatás közbeni tömörítők (a normál tömörített fájloktól eltérően) a memóriába csomagolják ki a fájlokat. A szokásos statikus tömörítők (UPX, yoda, ASPack, FSG stb.) mellett a víruskereső (a kódemuláció révén) számos más típusú tömörítőt is támogat.

4.1.1.6.2 Beállítások

A rendszer fertőzésekkel kapcsolatos ellenőrzésének módjait a **Beállítások** csoportban választhatja ki. A választható lehetőségek az alábbiak:

Alapheurisztika használata – Az alapheurisztika a programok kártevő tevékenységének a felismerésére szolgáló algoritmus. Fő előnye, hogy a korábbi vírusdefiníciós adatbázisban még nem létező, illetve nem ismert kártevő szoftvereket is képes felismerni. Hátránya, hogy (nagyon ritkán) téves riasztásokat is küldhet.

Kiterjesztett heurisztika/DNA/Elektronikus aláírások – A kiterjesztett heurisztika az ESET saját, a számítógépes férgek és trójai programok felismerésére optimalizált, magas szintű programozási nyelveken fejlesztett heurisztikus algoritmusa. A kiterjesztett heurisztikával a program vírusfelismerési képessége jelentősen megnő. A vírusdefiníciók alapján a program megbízhatóan felismeri és azonosítja a vírusokat. Az automatizált frissítési rendszeren keresztül a definíciós frissítések a kártevők felfedezése után mindössze néhány órával elérhetővé válnak. A vírusdefiníciók hátránya, hogy csak az ismert vírusok (vagy azok alig módosított változatai) ismerhetők fel velük.

A **kéretlen alkalmazások** nem feltétlenül kártevők, de hátrányosan befolyásolhatják a számítógép teljesítményét. Ezek az alkalmazások általában engedélyt kérnek a telepítésükhöz. Miután a számítógépre kerülnek, a rendszer a telepítésük előtti állapotához képest eltérően kezd viselkedni. A lényegesebb változások az alábbiak:

- Korábban nem látott új ablakok nyílnak meg (előugró ablakok, hirdetések).
- Rejtett alkalmazások aktiválódnak és futnak.
- Megnő a rendszererőforrások terhelése.
- Módosulnak a keresési eredmények.
- Az alkalmazások távoli szerverekkel kommunikálnak.

Veszélyes alkalmazások keresése – A veszélyes alkalmazások a kereskedelmi forgalomban kapható, legitim szoftverek egyik osztályát alkotják – ilyenek például a távoli hozzáférést biztosító eszközök, a jelszófeltörő alkalmazások, valamint a billentyűzetfigyelők (a felhasználó minden billentyűleütését rögzítő programok). Ez a beállítás alapértelmezés szerint le van tiltva.

ESET Live Grid – Az ESET megbízhatósági értékeléseken alapuló technológiája révén az ellenőrzött fájlok adatai összehasonlíthatók az ESET Live Grid felhőbeli adataival, és ez egy olyan gyors figyelmeztető rendszert eredményez, amellyel fokozható az észlelés és az ellenőrzés sebessége.

4.1.1.6.3 Megtisztítás

A tisztítási beállítások határozzák meg, hogy a víruskereső mit tegyen a fertőzött fájlok tisztítása során. A megtisztításnak az alábbi három szintje létezik:

Mindig rákérdez – A program nem tisztítja meg automatikusan a fertőzött fájlokat, hanem megjelenít egy figyelmeztető ablakot, és a felhasználó választhat a műveletek közül. Ez a szint a tapasztalt felhasználóknak ajánlott, akik tisztában vannak azzal, hogy mi a teendő a fertőzések esetén.

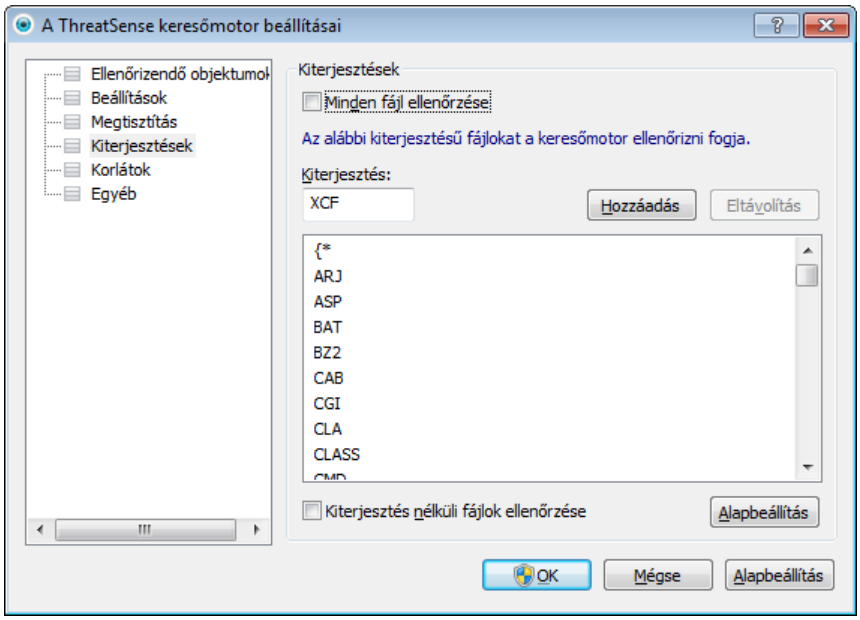
Alapértelmezett szint – A program megkísérli a fertőzött fájlok automatikus megtisztítását vagy törlését. A tényleges műveletet a fertőzés függvényében határozza meg a rendszer. A fertőzött fájlok észlelését és törlését a program egy, a képernyő jobb alsó sarkában megjelenő tájékoztató üzenettel jelzi. Ha a megfelelő művelet automatikus kiválasztására nincs lehetőség, felkínál néhány utóműveletet. Ugyanez történik akkor is, ha az előre beállított műveletet nem lehet elvégezni.

Automatikusan megtisztít – A program megtisztítja vagy törli az összes fertőzött fájlt. A rendszerfájlok ez alól kivételt képeznek. Ha nem lehetséges a megtisztítás, a program egy figyelmeztető ablakban ajánl fel egy műveletet.

Figyelmeztetés: Ha egy tömörített fájl fertőzött fájlt tartalmaz, két alternatíva lehetséges: normál módban (**Alapértelmezett szint**) a program csak akkor törli a tömörített fájlt, ha a benne lévő összes fájl fertőzött; míg az **Automatikusan megtisztít** üzemmódban a program már akkor is törli a tömörített fájlt, ha csak egyetlen fertőzött fájlt tartalmaz (tehát függetlenül a többi fájl állapotától).

4.1.1.6.4 Kiterjesztés

A kiterjesztés a fájlnév ponttal elválasztott része. A kiterjesztés határozza meg a fájl típusát és tartalmát. Az ellenőrizendő fájlok típusai az ThreatSense keresőmotor beállításait tartalmazó lap alábbi részén definiálhatók.



A program alapértelmezés szerint kiterjesztéstől függetlenül ellenőrzi az összes fájlt. Az ellenőrzésből kizárt fájlok listájára bármilyen kiterjesztés felvehető. Ha nincs bejelölve a **Minden fájl ellenőrzése** jelölőnégyzet, a lista az összes aktuálisan ellenőrzött fájlkiterjesztést megjeleníti.

A kiterjesztés nélküli fájlok ellenőrzéséhez jelölje be a **Kiterjesztés nélküli fájlok ellenőrzése** jelölőnégyzetet. A **Minden fájl ellenőrzése** jelölőnégyzet bejelölésének hatására elérhetővé válik a **Ne ellenőrizze a kiterjesztés nélküli fájlokat** jelölőnégyzet is.

A fájlok kizárása az ellenőrzésből akkor lehet hasznos, ha bizonyos típusú fájlok ellenőrzése a velük társított programokban működési hibákat eredményez. MS Exchange-szerver használata esetén érdemes lehet például kizárni az ellenőrzésből az .edb, az .eml és a .tmp kiterjesztésű fájlokat.

A **Hozzáadás** és az **Eltávolítás** gombbal engedélyezheti és megtilthatja az egyes fájlkiterjesztésekkel rendelkező fájlok ellenőrzését. Egy **kiterjesztés** beírása aktiválja a **Hozzáadás** gombot, amellyel az új kiterjesztést felveheti a listára. Egy kiterjesztés törléséhez jelölje ki a kiterjesztést a listában, és kattintson az **Eltávolítás** gombra.

A * (csillag) és a ? (kérdőjel) speciális szimbólumok használhatók. A csillaggal tetszőleges karaktersor, a kérdőjellel pedig bármilyen szimbólum helyettesíthető. Az ellenőrzésből kizárt címek megadásakor különös figyelemmel járjon el, mert a listában csak megbízható és biztonságos címek szerepelhetnek. Szintén fontos, hogy a * és a ? szimbólumot megfelelően használja a listában.

Ha csak az alapértelmezett kiterjesztéskészletet szeretné ellenőrizni, kattintson az **Alapbeállítás** gombra, és erősítse meg szándékát.

4.1.1.6.5 Korlátok

A Korlátok csoportban adhatja meg az ellenőrizendő objektumok maximális méretét és a többszörösen tömörített fájlok maximális szintjét:

Maximális objektumméret – Itt adhatja meg az ellenőrizendő objektumok maximális méretét. Az adott víruskereső modul csak a megadott méretnél kisebb objektumokat fogja ellenőrizni. A beállítás módosítása csak olyan tapasztalt felhasználóknak javasolt, akik megfelelő indokkal rendelkeznek a nagyobb méretű objektumok ellenőrzésből való kizárásához. Alapértelmezett érték: *korlátlan*.

Objektumok ellenőrzésének maximális időtartama (mp.) – Itt az objektumok ellenőrzésének maximális időtartamát adhatja meg. A felhasználó által megadott érték esetén a víruskereső modul leállítja az objektum ellenőrzését, függetlenül attól, hogy az ellenőrzés befejeződött-e, vagy sem. Alapértelmezett érték: *korlátlan*.

Többszörösen tömörített fájlok maximális szintje – Itt adhatja meg a tömörített fájlok ellenőrzésének maximális mélységét. Alapértelmezett érték: *10*.

Tömörített fájlok maximális mérete – Itt adhatja meg az ellenőrizendő tömörített fájlok között található fájlok (kibontás utáni) maximális méretét. Alapértelmezett érték: *korlátlan*.

Ha egy tömörített fájl ellenőrzése ennek következtében idő előtt megszakad, a tömörített fájl jelölőnégyzete be nem jelölt marad.

Megjegyzés: Nem javasoljuk az alapértelmezett érték módosítását, mivel erre a szokásos körülmények között nincs szükség.

4.1.1.6.6 Egyéb

Az **Egyéb** részben az alábbi beállításokat adhatja meg:

Minden objektum naplózása – Ha bejelöli ezt a jelölőnégyzetet, a program nemcsak a fertőzött fájlokat, hanem az összes ellenőrzött fájlt meg fogja jeleníteni a naplóban – ha például fertőzést talál egy tömörített fájlban, a naplóban megjelennek a tömörített fájlban lévő nem fertőzött fájlok is.

Optimalizálás engedélyezése – A jelölőnégyzet bejelölése esetén a program a legoptimálisabb beállításokat használja a leghatékonyabb ellenőrzési szint, ugyanakkor a leggyorsabb ellenőrzési sebesség biztosításához. A különböző védelmi modulok intelligensen végzik az ellenőrzést, kihasználják és az adott fájltípusokhoz alkalmazzák a különböző ellenőrzési módszereket. Az optimalizálás letiltása esetén a program csak a felhasználók által az egyes modulok ThreatSense-alapbeállításaiban megadott beállításokat alkalmazza az ellenőrzések végrehajtásakor.

A számítógép-ellenőrzés beállítása során az ThreatSense keresőmotor beállításai mellett az alábbi lehetőségeket is megadhatja:

Változó adatfolyamok (ADS) ellenőrzése – Az NTFS fájlrendszer által használt változó adatfolyamok olyan fájl- és mappatársítások, amelyek a szokásos ellenőrzési technikák számára láthatatlanok maradnak. Számos fertőzés azzal

próbálja meg elkerülni az észlelést, hogy változó adatfolyamként jelenik meg.

Háttérben futó ellenőrzések indítása alacsony prioritással – Minden ellenőrzés bizonyos mennyiségű rendszererőforrást használ fel. Ha a használt programok jelentősen leterhelik a rendszererőforrásokat, az alacsony prioritású háttérellenőrzés aktiválásával erőforrásokat takaríthat meg az alkalmazások számára.

Utolsó hozzáférés időbélyegének megőrzése – Jelölje be ezt a jelölőnégyzetet, ha a frissítés helyett meg szeretné őrizni az ellenőrzött fájlok eredeti hozzáférési idejét (például az adatok biztonsági mentését végző rendszerekkel való használathoz).

Napló görgetése – Ezzel a beállítással engedélyezheti, illetve letilthatja a napló görgetését. Ha engedélyezi, az adatokat függőleges irányban görgetheti a megjelenítési ablakban.

4.1.1.7 A program fertőzést észlelt

A fertőzések számos különböző ponton keresztül juthatnak be a rendszerbe, például weboldalakról, megosztott mappákból, e-mailen keresztül vagy cserélhető számítógépes eszközökről (USB-eszközökről, külső lemezekről, CD, DVD vagy hajlékonylemezekről stb.).

Ha a számítógép fertőzés jeleit mutatja, azaz működése lelassul, gyakran lefagy stb., ajánlatos elvégeznie az alábbiakat:

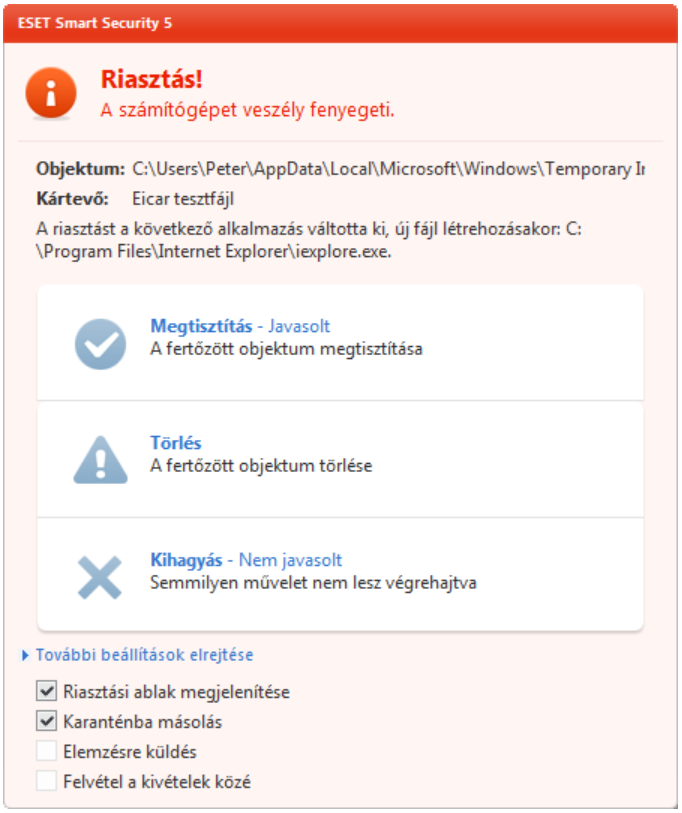
- Nyissa meg az ESET Smart Security programot, és kattintson a Számítógép ellenőrzése ikonra.
- Kattintson az **Optimalizált ellenőrzés** műveletre (erről az Optimalizált ellenőrzés című témakörben olvashat).
- Az ellenőrzés végeztével a naplóban megtekintheti az ellenőrzött, a fertőzött és a megtisztított fájlok számát.

Ha csak a lemez egy bizonyos részét kívánja ellenőrizni, kattintson az **Egyéni ellenőrzés** hivatkozásra, és a víruskereséshez jelölje ki az ellenőrizendő célterületeket.

Ha meg szeretnénk nézni, hogy miként kezeli az ESET Smart Security a fertőzéseket, általános példaként tegyük fel, hogy az alapértelmezett megtisztítási szintet alkalmazó valós idejű fájlrendszerfigyelő egy fertőzést talál. Ilyenkor az eszköz megkísérli a fájl megtisztítását vagy törlését. Ha nincs előre meghatározva, hogy a valós idejű védelmi modul milyen műveletet hajtson végre, a program egy riasztási ablakban kéri a felhasználót egy művelet megadására. Rendszerint a **Megtisztítás**, a **Törlés** és a **Kihagyás** közül választhat. Nem ajánlott a **Kihagyás** lehetőséget választani, mert a fertőzött fájlok ebben az esetben változatlanok maradnak. Kivételnek számít az a helyzet, ha az adott fájl biztosan ártalmatlan, és a program hibásan észlelte azt fertőzöttnek.

Megtisztítás és törlés

Megtisztítást akkor érdemes alkalmazni, ha egy fájlt megtámadott egy olyan vírus, amely kártékony kódot csatolt a fájlhoz. Ilyen esetben először a fertőzött fájlt megtisztítva kísérelje meg visszaállítani annak eredeti állapotát. Ha a fájl kizárólag kártékony kódból áll, akkor a program törli azt.



Ha egy fertőzött fájl „zárolva" van, vagy azt éppen egy rendszerfolyamat használja, annak törlése rendszerint csak a feloldás után történik meg (ez általában a rendszer újraindítása után megy végbe).

Tömörített fájlokban lévő fájlok törlése

Az alapértelmezett megtisztítási szint használata esetén a program csak akkor törli a kártevőt tartalmazó teljes tömörített fájlt, ha kizárólag fertőzött fájlokat tartalmaz. Más szóval a program nem törli a tömörített fájlokat abban az esetben, ha azok ártalmatlan, nem fertőzött fájlokat is tartalmaznak. Az automatikus megtisztítással járó ellenőrzés végrehajtásakor azonban körültekintően kell eljárni, ekkor ugyanis a program a tömörített fájlt a benne lévő többi fájl állapotától függetlenül akkor is törli, ha csak egyetlen fertőzött fájlt tartalmaz.

4.1.2 Cserélhető adathordozók ellenőrzése és letiltása

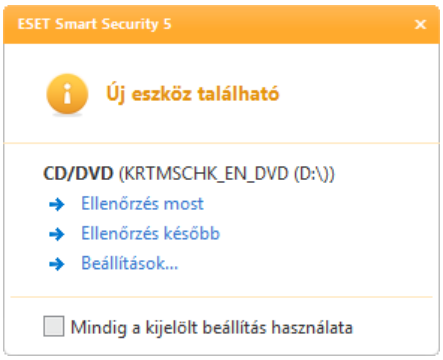
Az ESET Smart Security lehetővé teszi a cserélhető adathordozók automatikus (CD, DVD, USB stb) felügyeletét. Ez a modul lehetővé teszi a kiterjesztett szűrők/engedélyek ellenőrzését, tiltását vagy módosítását, valamint annak megadását, hogy a felhasználó hogyan érhet el és használhat egy adott eszközt. Ez a lehetőség különösen hasznos lehet akkor, ha a számítógép rendszergazdája meg kívánja akadályozni, hogy a felhasználók kéretlen tartalmú cserélhető adathordozót helyezzenek a számítógépbe.

Támogatott cserélhető adathordozók

- CD/DVD/Blu-ray
- USB-kulcs
- USB-meghajtó
- FireWire

A cserélhető adathordozó behelyezése után szükséges művelet – Válassza ki a cserélhető adathordozó (CD/DVD/USB) számítógépbe történő behelyezését követően végrehajtandó alapértelmezett műveletet. Az **Ellenőrzési beállítások megjelenítése** lehetőség kiválasztása esetén egy értesítés jelenik meg, amely segítségével kiválaszthatja a kívánt műveletet:

- **Ellenőrzés most** – Elvégzi a behelyezett cserélhető adathordozó eszköz kézi indítású számítógép-ellenőrzését.
- **Ellenőrzés később** – Nem végez műveletet, és az **Új eszköz található** ablak bezárul.
- **Beállítások** – Megnyitja a Cserélhető adathordozók részt.



Cserélhető adathordozók letiltásának szabályai – Jelölje be ezt a jelölőnégyzetet a számítógéphez csatlakoztatott valamennyi cserélhető adathordozó letiltásához. Amennyiben egyes adathordozókat elérhetővé kíván tenni, azokat zárja ki a letiltás alól.

A **Szabályok** gombra kattintással engedélyezheti vagy tilthatja le a kiválasztott cserélhető adathordozóhoz való hozzáférést. Az ablakban a cserélhető adathordozókra vonatkozó további szabályokat kezelheti. Lehetősége van a szabályok – például az adathordozó mérete, sorozatszáma, és az eszköz típusa szerinti – szűrésére. Minden szabályhoz saját engedélyek tartoznak, így engedélyezheti, korlátozhatja, vagy letilthatja a kiválasztott cserélhető adathordozóhoz való hozzáférést.

4.1.3 Behatolásmegelőző rendszer (HIPS)

A **behatolásmegelőző rendszer** (HIPS, Host Intrusion Prevention System) megvédi rendszerét a kártevőktől és a számítógép biztonságát veszélyeztető minden nemkívánatos tevékenységtől. A behatolásmegelőző rendszer a hálózati szűrési algoritmusok észlelési képességeivel párosított fejlett viselkedéselemzési mechanizmusokkal figyeli a futó folyamatokat, a fájlokat és a beállításkulcsokat, és aktívan blokkolja, illetve megelőzi a támadási kísérleteket.

A behatolásmegelőző rendszer beállításainak megjelenítéséhez nyissa meg a **További beállítások** párbeszédpanelt az F5 billentyű lenyomásával, és válassza a **Számítógép** ág **Behatolásmegelőző rendszer** beállításcsoportját. A rendszer engedélyezettségi állapota (engedélyezett vagy letiltott) az ESET Smart Security fő ablakának **Beállítások** lapján, a **Számítógép** szakaszban, a jobb oldalon látható.

Figyelmeztetés: A behatolásmegelőző rendszer beállításainak módosítását csak tapasztalt felhasználóknak javasoljuk.

Az ESET Smart Security beépített *önvédelmi* technológiával rendelkezik, mely megakadályozza a kártevőprogramokat a vírusvédelmi és kémprogramvédelmi szoftverek manipulálásában és letiltásában, így biztosítva a felhasználók számára a folyamatos védelmet. A **Behatolásmegelőző rendszer engedélyezése** és az **Önvédelem engedélyezése** beállítások módosítása a Windows újraindításakor lép érvénybe. A teljes behatolásmegelőző rendszer letiltása szintén a számítógép újraindítását igényli. A behatolásmegelőző rendszer működése az alábbiakban ismertetett szűrési módokra állítható be.

Automatikus üzemmód szabályokkal – A műveletek a rendszer védelmét biztosító gyári szabályokban megadott tiltások kivételével engedélyezettek.

Interaktív üzemmód – A felhasználónak minden műveletet meg kell erősítenie.

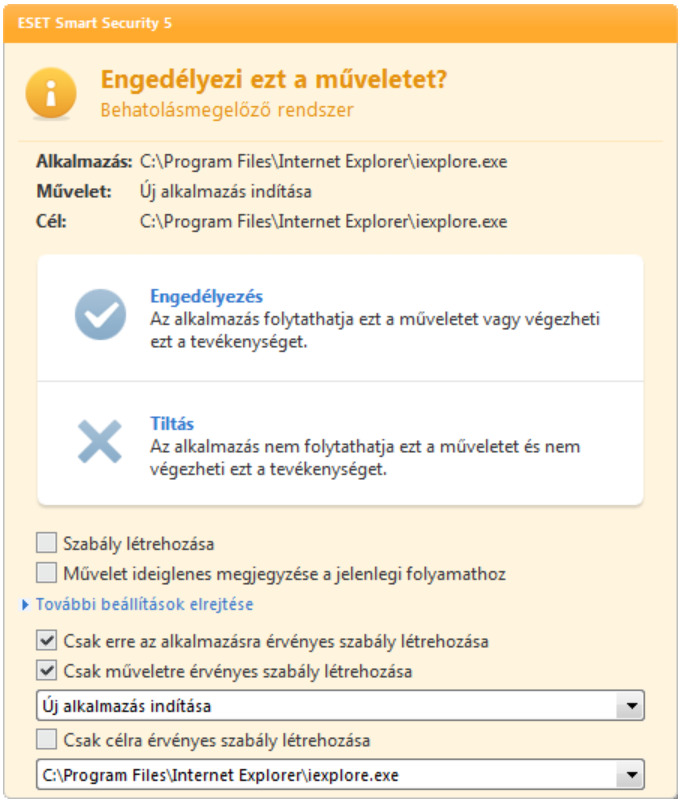
Házirendalapú üzemmód – A műveletek blokkoltak.

Tanuló mód – A műveletek engedélyezettek, és mindegyikhez létrejön egy szabály. Az ebben a módban létrehozott szabályok megtekinthetők a **Szabályszerkesztő** párbeszédpanelen, azonban prioritásuk alacsonyabb a manuálisan és az automatikus módban létrehozott szabályokénál. A **Tanuló mód** szűrésmód választása után elérhetővé válik az **Értesítés a tanuló mód lejáratáról** mező. Az ebben megadott idő lejárta után a program letiltja a tanuló módot. A legnagyobb engedélyezett időtartam 14 nap. Ezt követően megjelenik egy előugró ablak, melyben szerkesztheti a szabályokat, és másik szűrési módot választhat.

A behatolásmegelőző rendszer figyeli az operációs rendszerben zajló eseményeket, és a szabályoknak megfelelően reagál rájuk. A szabályok hasonlóak a személyi tűzfal szabályaihoz.

A **Szabályok konfigurálása** gombra kattintva megnyithatja a behatolásmegelőző rendszer szabálykezelési párbeszédpaneljét, melyen megtekintheti, létrehozhatja, szerkesztheti és törölheti a szabályokat.

Ha az alapértelmezett művelet a **Rákérdezés**, a szabály minden aktiválódásakor megjelenik egy párbeszédpanel. Ezen a párbeszédpanelen a **Tiltás** és az **Engedélyezés** lehetőségekkel letiltható és engedélyezhető az adott művelet. Ha a felhasználó nem választ műveletet adott időn belül, a rendszer a szabályok alapján dönt a végrehajtandó műveletről.



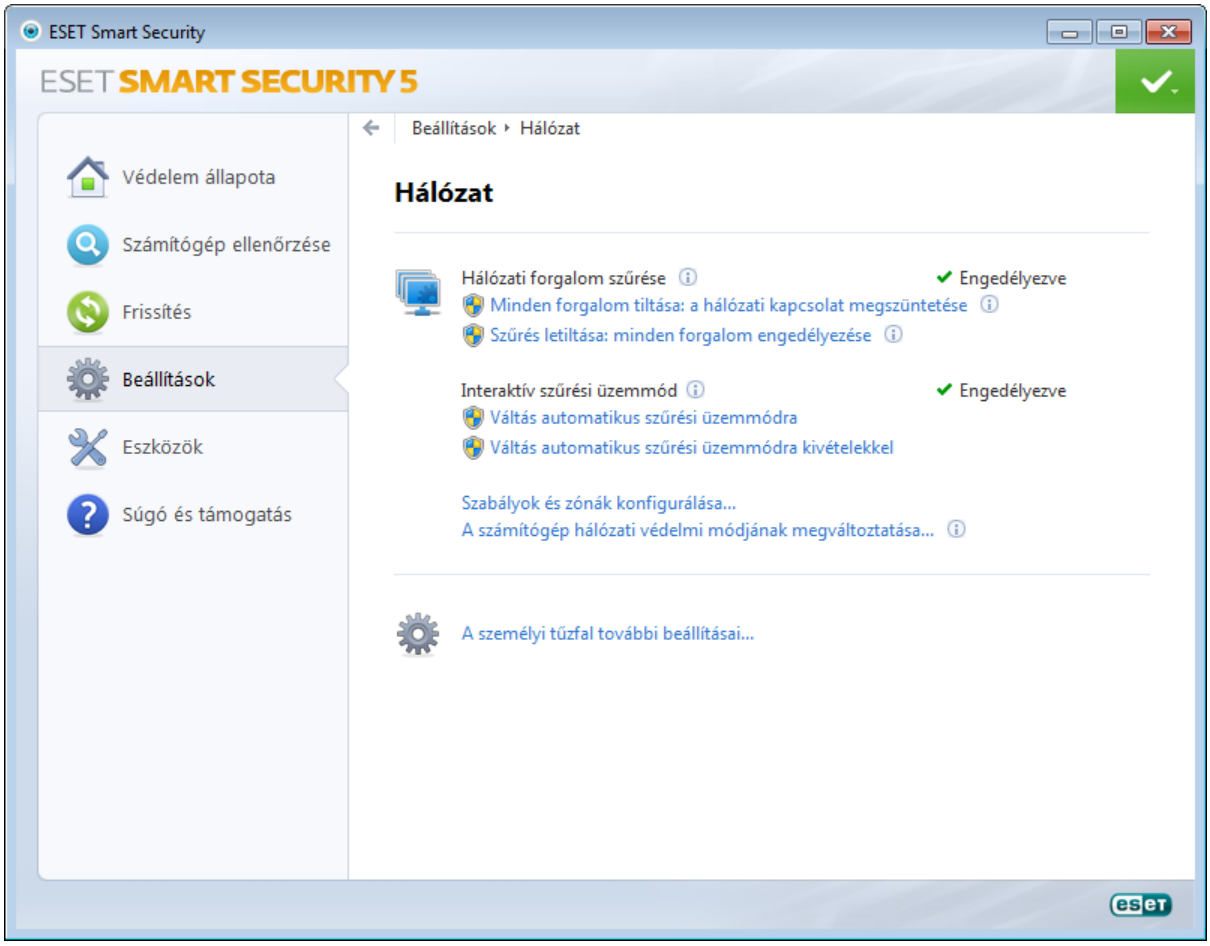
A párbeszédpanelen a panel megjelenését kiváltó művelet és a művelethez kapcsolódó feltételek alapján új szabály is létrehozható. A paraméterek pontos megadásához a **További beállítások megjelenítése** parancsra kell kattintania. Az így létrehozott szabályokat a program a manuálisan létrehozott szabályokkal azonos prioritással látja el, azaz a párbeszédpanelen létrehozott szabályoknak nem kell olyan specifikusnak lenniük, mint a párbeszédpanel megjelenítését kiváltó szabálynak. Ez azt jelenti, hogy egy ilyen szabály létrehozása után ugyanaz a művelet megjelenítheti ugyanazt a párbeszédpanelt.

A **Művelet ideiglenes megjegyzése a jelenlegi folyamathoz** jelölőnégyzet bejelölése esetén a program megjegyzi a választott műveletet (**Engedélyezés** vagy **Tiltás**), és az érintett folyamat esetén mindig ezt fogja választani, ha a művelet kiváltaná a párbeszédpanel megjelenítését. Ezek a beállítások csak ideiglenesek – és a szabályok vagy a szűrési mód megváltoztatása, a behatolásmegelőző rendszer frissítése, illetve az operációs rendszer újraindítása után törlődnek.

4.2 Hálózat

A személyi tűzfal ellenőrzi a számítógép teljes bejövő és kimenő hálózati forgalmát. A megadott szűrési szabályok alapján engedélyezi vagy letiltja az egyes hálózati kapcsolatokat. A tűzfal védelmet nyújt a távoli számítógépekről kezdeményezett támadások ellen, és lehetővé teszi egyes szolgáltatások letiltását. A HTTP, a POP3 és az IMAP protokollnak vírusvédelmet is nyújt. A személyi tűzfal a számítógép-védelem igen fontos összetevője.

A személyi tűzfal konfigurációja a **Hálózat** hivatkozásra kattintva megnyitható **Beállítások** lapon található. Itt adható meg a szűrés üzemmódja, illetve leállítható az összes kapcsolat, vagy engedélyezhető minden kommunikáció. A tűzfal részletesebb beállításai is elérhetők innen.



A teljes hálózati forgalom letiltásának egyetlen lehetősége a **Minden forgalom tiltása: a hálózati kapcsolat megszüntetése** beállítás. Ebben az esetben a személyi tűzfal figyelmeztetés megjelenítése nélkül letiltja az összes bejövő és kimenő kapcsolatot. Ezt a lehetőséget csak olyan különleges biztonsági kockázat felmerülése esetén alkalmazza, amely megköveteli a rendszer leválasztását a hálózatról.

A **Szűrés letiltása: minden forgalom engedélyezése** az ellenkező hatással jár, mint a fent ismertetett minden forgalom tiltása. Ha ezt a lehetőséget választja, a személyi tűzfal összes szűrési beállítását kikapcsolja, és minden bejövő, illetve kimenő kapcsolatot engedélyez. Ez olyan hatással jár, mintha nem is lenne tűzfal a számítógépen. Mialatt a hálózati forgalom szűrése **Letiltás** állapotban van, a **Váltás szűrési üzemmódra** beállítás engedélyezi a tűzfalat.

Az automatikus szűrési üzemmód engedélyezése esetén az alábbi beállítások érhetők el:

- **Automatikus szűrési üzemmód** – A szűrési üzemmód módosításához kattintson a **Váltás interaktív szűrési üzemmódra** hivatkozásra.
- **Zóna beállításai** – Erre kattintva jeleníthetők meg a megbízható zóna beállítási lehetőségei.

Az interaktív szűrési üzemmód engedélyezése esetén az alábbi beállítások érhetők el:

- **Interaktív szűrési üzemmód** – A szűrési üzemmód módosításához kattintson a **Váltás automatikus szűrési üzemmódra** vagy a **Váltás automatikus szűrési üzemmódra kivételekkel** hivatkozásra attól függően, hogy melyik szűrési üzemmód van beállítva.
- **Szabályok és zónák konfigurálása** – Megnyitja a Szabályok és zónák beállításai ablakot, ahol meghatározhatja, hogy a tűzfal hogyan kezelje a hálózati kommunikációt.

A számítógép hálózati védelmi módjának megváltoztatása – Itt választhat a szigorú és az engedélyezett védelmi mód közül.

A személyi tűzfal további beállításai – Erre kattintva megjelennek a tűzfal további beállításai.

4.2.1 Szűrési módok

Az ESET Smart Security személyi tűzfala öt szűrési módot támogat. A szűrési módokat a **További beállítások** képernyőn tekintheti meg. Ennek megjelenítéséhez nyomja le az F5 billentyűt, vagy válassza a **Hálózat** > **Személyi tűzfal** lehetőséget. A választott módtól függően változik a tűzfal működése. A szűrési üzemmódok a szükséges felhasználói beavatkozás szintjét is meghatározzák.

Az öt szűrési módot az alábbi szakaszok ismertetik.

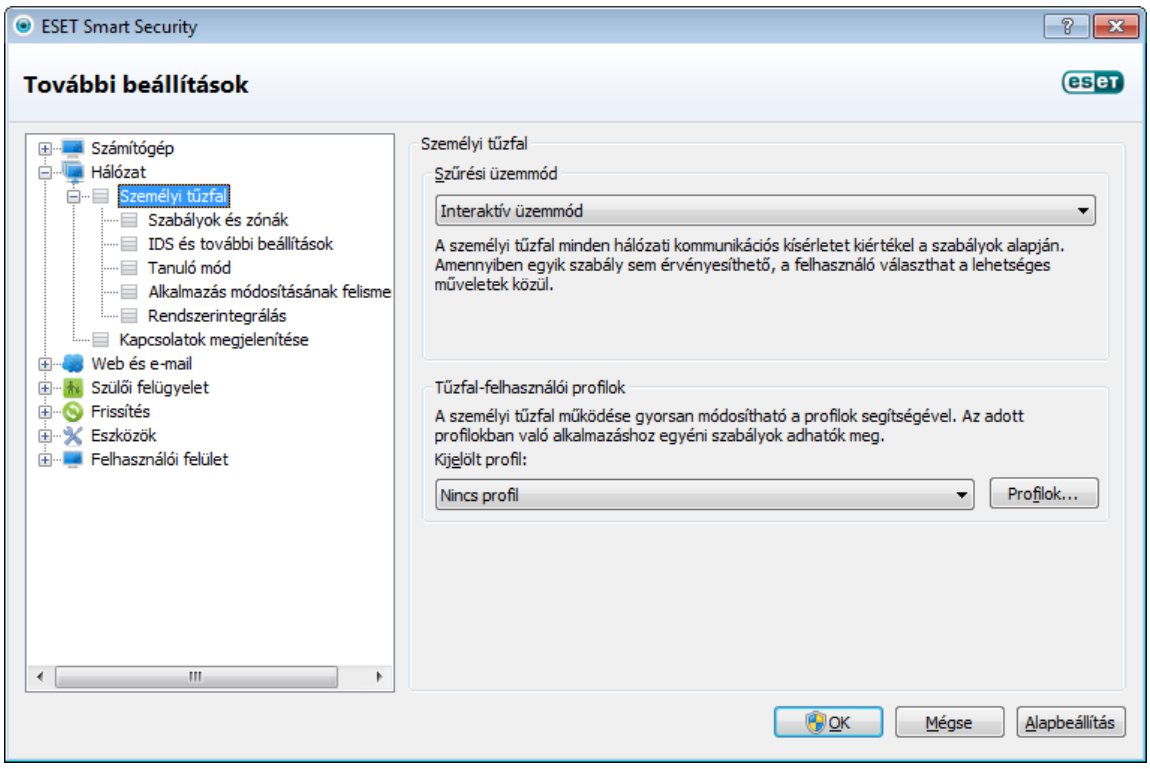
Automatikus üzemmód – Az alapértelmezett üzemmód. Ez az üzemmód azoknak a felhasználóknak ajánlott, akik a tűzfal egyszerű és kényelmes használatát részesítik előnyben, és nincs szükségük szabályok definiálására. Az automatikus mód nem korlátozza a kimenő forgalmat, de letiltja a hálózati oldalról kezdeményezett új kapcsolatokat.

Automatikus üzemmód kivételekkel (felhasználó által definiált szabályok) – Az automatikus üzemmód kínálta lehetőségek mellett ebben a módban egyéni szabályokat is megadhat.

Interaktív üzemmód – Ez az üzemmód lehetővé teszi a személyi tűzfal egyéni konfigurációjának a kialakítását. Ha a program olyan kommunikációt észlel, amelyhez nincs szabály definiálva, egy párbeszédpanelen jelenti az ismeretlen kapcsolatot. A párbeszédpanelen engedélyezheti vagy letilthatja a kommunikációt, döntését pedig a személyi tűzfal új szabályaként is mentheti. Ha a párbeszédpanelen új szabály létrehozása mellett dönt, a program a szabály alapján az összes hasonló típusú kommunikációt engedélyezi vagy letiltja a jövőben.

Házirendalapú üzemmód – A házirendalapú üzemmódban a program csak a szabályokban kifejezetten engedélyezett kapcsolatokat engedélyezi, minden más kapcsolatot letilt. Ez az üzemmód lehetővé teszi, hogy a tapasztalt felhasználók szabályok definiálásával csak a kívánt és biztonságos kapcsolatokat engedélyezzék. A személyi tűzfal az összes többi kapcsolatot letiltja.

Tanuló mód – A program automatikusan létrehozza és menti a szabályokat. Ez a mód alkalmas a személyi tűzfal kezdeti konfigurálására. Ebben a folyamatban nincs szükség felhasználói beavatkozásra, mert az ESET Smart Security előre definiált paraméterek szerint menti a szabályokat. A tanuló mód nem biztonságos, és csak addig tanácsos használni, amíg a program a szükséges kommunikációkhoz létre nem hozza az összes szabályt.

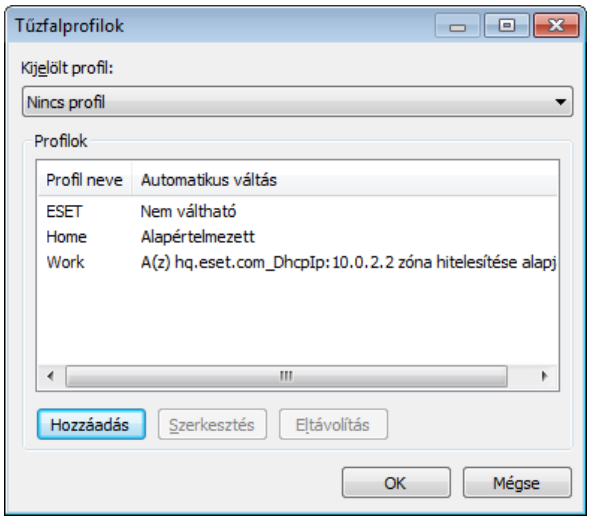


Az ESET Smart Security személyi tűzfalának működését szabályozó eszközök egyikét alkotják a profilok. A tűzfalszabályok létrehozásakor és szerkesztésekor megadhatja, hogy az adott szabály minden profilban érvényes legyen-e, vagy csak egy adott profilban. Ha választ egy profilt, a program csak a profilhoz nem rendelt globális szabályokat és a választott profillal társított szabályokat alkalmazza. A személyi tűzfal működésének egyszerű módosításához létrehozhat több profilt különböző szabályokkal.

4.2.2 Profilok

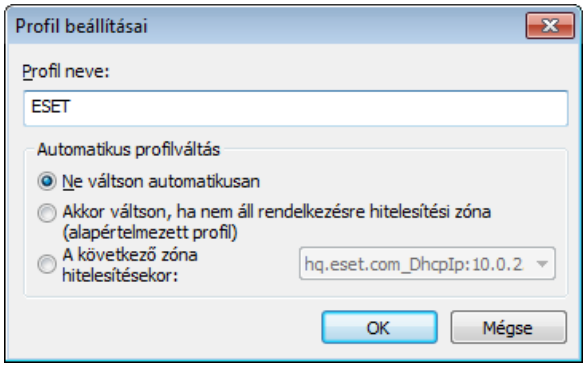
A profilok az ESET Smart Security működését szabályozó eszközök egyikét alkotják. A tűzfalszabályok létrehozásakor és szerkesztésekor megadhatja, hogy az adott szabály minden profilban érvényes legyen-e, vagy csak egy adott profilban. Ha választ egy profilt, a program csak a profilhoz nem rendelt globális szabályokat és a választott profillal társított szabályokat alkalmazza. A személyi tűzfal működése különböző szabályokat tartalmazó profilok kialakításával egyszerűen módosítható.

Kattintson a **Profilok** gombra (lásd: a Szűrési módok című szakasz képernyőmetszetét) a **Tűzfalprofilok** párbeszédpanel megnyitásához. A párbeszédpanel **Hozzáadás**, **Szerkesztés** és **Eltávolítás** gombjával készíthet, módosíthat és törölhet profilokat. A **Szerkesztés** és az **Eltávolítás** gomb nem érhető el, ha a profillistában és a felette található **Kiválasztott profil** legördülő listában ugyanaz a profil van kijelölve. A profilok létrehozásakor és szerkesztésekor megadhatja az adott profilt aktiváló feltételt is.



A profilok létrehozásakor megadhatja, hogy mely események indítsák el az adott profilt. A választható lehetőségek az alábbiak:

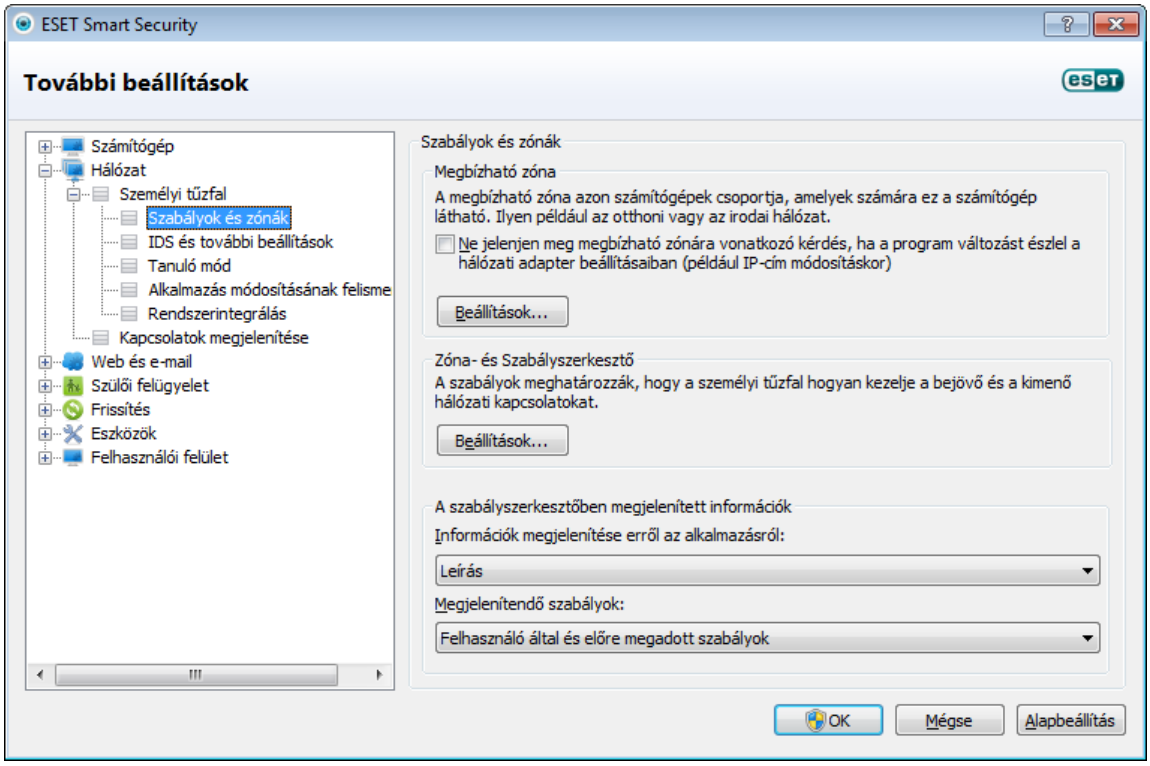
- **Ne váltson automatikusan** – Az automatikus indítás ki van kapcsolva (a profilt kézzel kell aktiválni).
- **Az automatikus profil érvénytelenné válása esetén, amikor nem aktiválódik automatikusan másik profil (alapértelmezett profil)** – Ha az automatikus profil érvénytelenné válik (mert például a számítógép egy nem megbízható hálózathoz csatlakozik – további információ: Hálózati hitelesítés), és nem aktiválódik helyette másik (a számítógép nem csatlakozik másik megbízható hálózathoz), a személyi tűzfal erre a profilra vált. Csak egy profil használhatja ezt az indítási módot.
- **A következő zóna hitelesítésekor** – A profilt a megadott zóna hitelesítése aktiválja. (Erről a Hálózati hitelesítés című témakörben talál további információt.)



A jobb alsó sarokban, a rendszeróra mellett egy értesítés jelzi, ha a személyi tűzfal másik profilra vált.

4.2.3 Szabályok beállítása és használata

A szabályok feltételegyüttesek, melyek célja a hálózati kapcsolatok ellenőrzése, és a feltételekkel társított műveletek végrehajtása. A személyi tűzfalban meghatározhatja, hogy a tűzfal milyen műveletet hajtson végre egy szabályban definiált kapcsolat létrehozásakor. A szabályszűrési beállítások megjelenítéséhez válassza a **További beállítások** (F5) > **Hálózat** > **Személyi tűzfal** > **Szabályok és zónák** lehetőséget.



A **Megbízható zóna** szakasz **Beállítás** gombjára kattintva megjelenítheti a Megbízható zóna beállításai párbeszédpanelt. A **Ne jelenjen meg a megbízhatózóna-beállításokat tartalmazó párbeszédpanel, ha a program változást (például IP-címmódosítást) észlel a hálózati adapter beállításaiban** jelölőnégyzet bejelölése esetén letilthatja, hogy a megbízható zóna beállítására szolgáló ablak minden alkalommal megjelenjen, amikor a program új alhálózatot észlel. Ebben az esetben a program automatikusan az aktuálisan érvényes zónabeállításokat alkalmazza.

MEGJEGYZÉS: Ha a személyi tűzfal automatikus szűrési módra van állítva (**Automatikus üzemmód** beállítás), akkor ezek a beállítások nem érhetők el.

A **Zóna- és Szabályszerkesztő** szakasz Beállítás gombjára kattintva megnyithatja a **Szabályok és zónák beállításai** párbeszédpanelt. A párbeszédpanel két lapján a szabályok és a zónák áttekintése jelenik meg. Az ablak két részre oszlik: a felső részen egy egyszerűsített nézetben megjelenik az összes szabály, míg alul a felső részen kijelölt szabály részletes adatai láthatók. Az ablak alsó részén található **Új**, **Szerkesztés** és **Törlés** gombbal konfigurálhatja a szabályokat.

A kapcsolatok bejövő és kimenő kapcsolatokra oszthatók. A bejövő kapcsolatokat egy távoli számítógép kezdeményezte, és a távoli számítógép szeretne a helyi számítógéphez csatlakozni. A kimenő kapcsolatok ezek ellentettjei – a helyi oldal kezdeményez kapcsolatot egy távoli számítógéppel.

Ha ismeretlen új kapcsolatot észlel, alaposan gondolja meg, hogy engedélyezi vagy megtagadja-e azt. A kéretlen, nem biztonságos vagy ismeretlen kapcsolatok biztonsági kockázatot jelentenek a számítógépen. Ha ilyen kapcsolat jön létre, javasoljuk, hogy szenteljen megkülönböztetett figyelmet a távoli oldalnak és a számítógéphez csatlakozni próbáló alkalmazásnak. Sok kártevő tesz kísérletet a magánjellegű adatok megszerzésére és továbbítására, vagy más kártékony alkalmazásoknak a munkaállomásokra való letöltésére. A személyi tűzfallal észlelheti és bonthatja az ilyen kapcsolatokat.

Információk megjelenítése erről az alkalmazásról – A legördülő listával szabályozhatja az alkalmazások megjelenési módját a szabálylistákban. A választható lehetőségek az alábbiak:

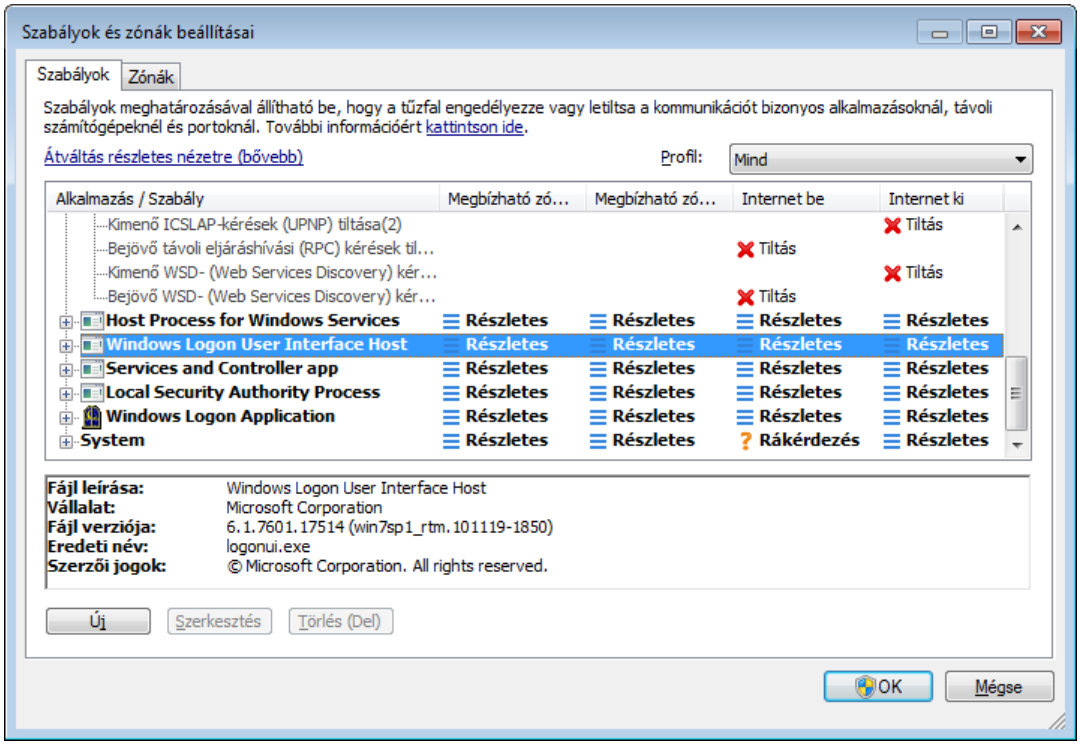
- **Teljes elérési út** – Az alkalmazásokhoz tartozó végrehajtható fájlok (az alkalmazásokat indító programfájlok) nevének megjelenítése teljes elérési úttal.
- **Leírás** – Az alkalmazás leírásának megjelenítése.
- **Név** – Az alkalmazás nevének megjelenítése.

A **Megjelenítendő szabályok** legördülő listában a megjelenítendő szabályok körét adhatja meg:

- **Csak felhasználó által megadott szabályok** – Ezt a lehetőséget választva csak a felhasználó által létrehozott szabályok jelennek meg.
- **Felhasználó által és előre megadott szabályok** – Ebben az esetben a felhasználó által definiált és az alapértelmezettként előre megadott szabályok jelennek meg.
- **Minden szabály (beleértve a rendszerszabályokat is)** – Ezt a lehetőséget választva az összes szabály megjelenik.

4.2.3.1 Szabályok beállítása

A szabályok beállítási párbeszédpanellapján megtekintheti az egyes alkalmazások által a megbízható zónában és az interneten generált forgalomra vonatkozó összes szabályt. A szabályokat a program alapértelmezés szerint automatikusan, a felhasználó új kommunikációs kísérletekre adott válaszai alapján hozza létre. Ha egy alkalmazásról további információkat szeretne megjeleníteni az ablak alján, jelölje ki az alkalmazást a listában.



A szabályokat tartalmazó sorok elején lévő ikonokkal (+/-) kibonthatók és összecsukhatók az információk. Ha az **Alkalmazás/Szabály** oszlopban kijelöl egy alkalmazást, az ablak alján további információk jelennek meg a szabályról. A helyi menüben beállítható a megjelenítési mód, továbbá lehetőség van szabályok felvételére, szerkesztésére és törlésére is.

Megbízható zóna be/ki – A megbízható zóna bejövő és kimenő irányú kommunikációja esetén esedékes műveletek megjelenítése.

Internet be/ki – A bejövő és kimenő irányú internetes kommunikáció esetén esedékes műveletek megjelenítése.

Valamennyi kommunikációs típushoz (irányhoz) az alábbi műveletek közül választhat:

- **Engedélyezés** – A kommunikáció engedélyezése.
- **Rákérdezés** – A program minden egyes kommunikációs kapcsolat létesítésekor üzenetet jelenít meg a felhasználónak.
- **Tiltás** – A kommunikáció tiltása.
- **Részletes** – Nem sorolható a fenti kategóriákba. Ha például egy IP-cím és vagy port engedélyezett a személyi tűzfalon, nem dönthető el teljes bizonyossággal, hogy egy kapcsolódó alkalmazás bejövő vagy kimenő kommunikációja engedélyezett-e.

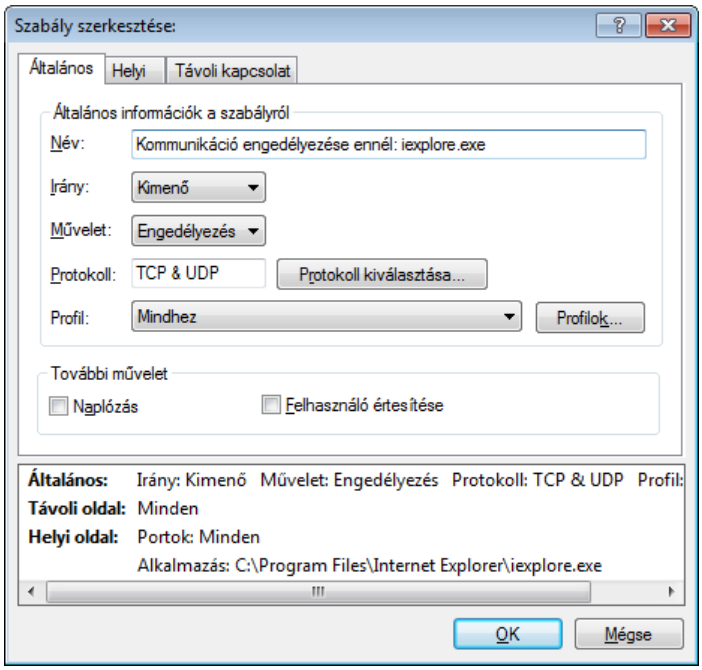
Ha hálózati hozzáféréssel rendelkező új alkalmazást telepít, vagy egy meglévő kapcsolatot (távoli oldalt, portszámot stb.) módosít, új szabályt kell létrehoznia. Ha módosítani szeretne egy szabályt, jelölje ki a **Szabályok** lapon, és kattintson a **Szerkesztés** gombra.

4.2.3.2 Szabályok szerkesztése

Ha egy szabály valamelyik figyelt paramétere változik, módosítani kell a szabályt, ugyanis a változás után már nem teljesülnek az eredeti feltételek, ezért a szabállyal társított műveletek sem hajthatók végre a megfelelő szituációkban. A paraméterek módosítása esetén a program letilthatja az adott kapcsolatot, ami zavart okozhat az érintett alkalmazás működésében. Ilyen esetre példa egy távoli oldali hálózati cím vagy portszám változása.

A párbeszédpanel három lapból áll:

- **Általános** – A szabály neve, a szabályozott kapcsolat iránya, a társított művelet, valamint a szabállyal felügyelt protokoll és profil.
- **Helyi** – A kapcsolat helyi oldalának adatai, beleértve a helyi portszámot vagy porttartományt, valamint a kommunikációt folytató alkalmazás nevét.
- **Távoli** – Ezen a lapon a távoli port (vagy porttartomány) adatai találhatók. Ugyanitt van lehetőség a szabályban érintett távoli IP-címek vagy zónák listájának megadására.



Protokoll legördülő listában a szabállyal felügyelt átviteli protokoll adható meg. A **Protokoll kiválasztása** gombra kattintva megnyithatja a Protokoll kiválasztása párbeszédpanelt.

Alapértelmezés szerint **Minden** profilban engedélyezett minden szabály. Ha ez nem megfelelő, a **Profilok** gombra kattintva módosíthatja a profilok körét.

A **Naplózás** jelölőnégyzet bejelölése esetén a program naplózza a szabállyal kapcsolatos műveleteket. A **Felhasználó értesítése** jelölőnégyzet bejelölése esetén a program értesítésben jelzi, ha alkalmazta a szabályt.

A mindhárom lap alján megjelenő információs mező a szabály összefoglalását tartalmazza. Ugyanezek az információk a szabályok fő ablakában is megjeleníthetők. Ehhez válassza az **Eszközök** > **Hálózati kapcsolatok** lehetőséget, kattintson a jobb gombbal a szabályra, végül kattintson a **Részletek megjelenítése** parancsra (további információt talál a Hálózati kapcsolatok című témakörben).

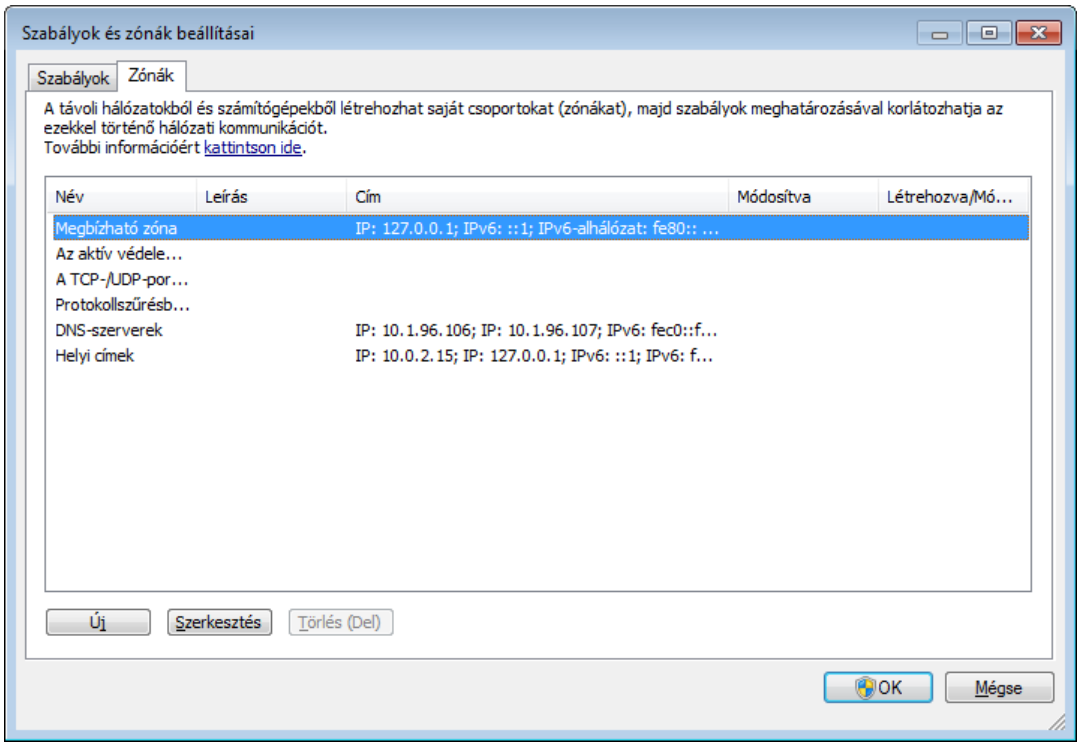
Ha új szabályt hoz létre, a **Név** mezőben el kell neveznie. Az **Irány** legördülő listában jelölheti ki, hogy milyen irányú kommunikációra vonatkozik a szabály. A **Művelet** legördülő listában a szabály feltételeinek megfelelő kommunikációra alkalmazandó műveletet kell megadnia.

Egy új szabály felvételére jó példa a hálózati elérés engedélyezése egy internetböngésző számára. Ebben az esetben az alábbiakat kell megadni:

- Az **Általános** lapon engedélyezni kell a TCP és UDP protokollon keresztüli kimenő irányú kommunikációt.
- A **Helyi** lapon meg kell adni a böngészőalkalmazás programfájlját (például Internet Explorer esetén az iexplore.exe fájlt).
- Ha csak a szabványos internetböngészési tevékenységeket szeretné engedélyezni, a **Távoli kapcsolat** lapon engedélyezze a 80-as számú portot.

4.2.4 Zónák konfigurálása

A **Zóna beállításai** párbeszédpanelen megadhatja egy zóna nevét, leírását, hálózati címeinek listáját és a zónahitelesítési adatokat (erről a Zónahitelesítés – Klienskonfiguráció című témakörben talál további tudnivalókat).



A zónák hálózati címek logikai csoportjai. Egy csoport minden címére hasonló, a teljes csoport számára központilag definiált szabályok vonatkoznak. A Megbízható zóna például egy olyan címcsoport, amelybe a teljes mértékben megbízhatónak ítélt, és ezért a személyi tűzfal által semmilyen módon nem korlátozott hálózati címek tartoznak.

A zónák a **Szabályok és zónák beállításai** párbeszédpanel **Zónák** lapján konfigurálhatók – csak jelölje ki a módosítani kívánt zónát, és kattintson a **Szerkesztés** gombra. A megjelenő párbeszédpanel **Név** mezőjében a zóna nevét, **Leírás** mezőjében a zóna rövid ismertetését kell megadnia. A zónához tartozó távoli IP-címeket az **IPv4-cím hozzáadása / IPv6-cím hozzáadása** gombbal és paranccsal adhatja meg.

4.2.4.1 Hálózati hitelesítés

A hordozható számítógépek esetében ajánlott ellenőrizni annak a hálózatnak a megbízhatóságát, amelyhez kapcsolódik. A megbízható zónát a hálózati adapter helyi IP-címe azonosítja. A hordozható számítógépek gyakran a megbízható hálózathoz hasonló IP-címekkel lépnek be a hálózatokra. Ha a megbízható zóna beállításait nem állítja át kézzel **Szigorú védelem** módra, a személyi tűzfal továbbra is a **Megosztás engedélyezése** módot használja.

Az ilyen szituációk zónahitelesítéssel elkerülhetők.

4.2.4.1.1 Zónahitelesítés – Klienskonfiguráció

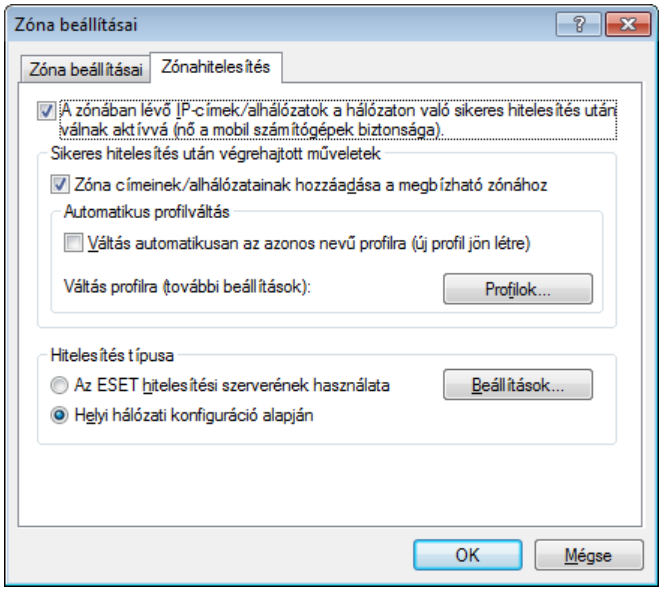
Kattintson a **Szabályok és zónák beállításai** párbeszédpanel **Zónák** fülére, és hozzon létre egy új zónát, a szerver által hitelesített zóna nevét adva meg névként. Ezután kattintson az **IPv4-cím hozzáadása** gombra, jelölje be az **Alhálózat** választógombot, és adja meg a hitelesítési szerver címét is magában foglaló alhálózati maszkot.

Kattintson a **Zónahitelesítés** fülre. Minden zónában beállítható a szerverhitelesítés. A zóna (annak IP-címe és alhálózata) a sikeres hitelesítés után válik érvényessé, vagyis a különböző műveletek – például átváltás egy másik tűzfalprofilra, vagy a zóna valamelyik IP-címének vagy alhálózatának felvétele a megbízható zónába – csak a sikeres hitelesítés után válik lehetségessé.

Ha bejelöli **A zónában lévő IP-címek/alhálózatok a hálózaton való sikeres hitelesítés után válnak aktívvá (nő a mobil számítógépek biztonsága)** jelölőnégyzetet, a zóna sikertelen hitelesítés esetén érvénytelenné válik. A sikeres zónahitelesítés után aktiválandó tűzfalprofil megadásához kattintson a **Profilok** gombra.

Ha bejelöli a **Zóna címeinek/alhálózatainak hozzáadása a megbízható zónához** jelölőnégyzetet, a sikeres hitelesítés után a zóna címei és alhálózatai a megbízható zónába fognak tartozni. Ha a hitelesítés sikertelen, a címek nem kerülnek

a megbízható zónába. Ha a **Váltás automatikusan az azonos nevű profilra (új profil jön létre)** jelölőnégyzetet bejelöli, a sikeres hitelesítés után új profil jön létre. Kattintson a **Profilok** gombra a Tűzfalprofilok párbeszédpanel megnyitásához.



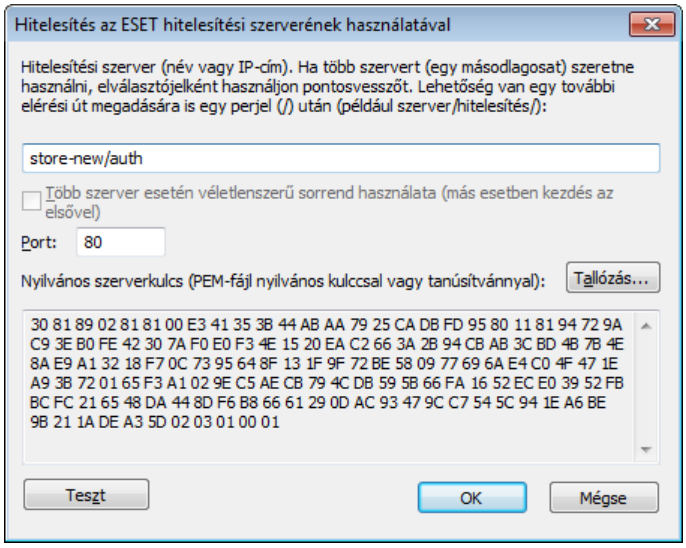
Az alább ismertetett kétféle hitelesítési típus közül választhat.

1) Az ESET hitelesítési szerverének használata

Kattintson a **Beállítások** gombra, és adja meg a szerver nevét és figyelőportját, valamint a titkos szerverkulcsnak megfelelő nyilvános kulcsot (erről további információt talál a Zónahitelesítés – Szerverkonfiguráció című témakörben). A szervernév DNS-név, NetBios-név és IP-cím formájában is megadható. A szerveren tárolt fájl nevét a szervernév után írt elérési úttal adhatja meg (példa: *szervernév/könyvtár1/könyvtár2/hitelesítés*). További szerverek is megadhatók (egymástól pontosvesszővel elválasztva). Ezek helyettesítő szerverként fognak üzemelni az első szerver elérhetetlensége esetén.

A nyilvános kulcs az alábbi típusú fájlok valamelyike lehet:

- Titkosított nyilvános kulcsot tartalmazó, PEM formátumú (.pem) fájl
  Az ilyen kulcsokat az ESET hitelesítési szerverével lehet előállítani. További információkért tanulmányozza a Zónahitelesítés – Szerverkonfiguráció).
- Titkosított nyilvános kulcsot tartalmazó fájl
- Nyilvános kulcsú tanúsítványt tartalmazó (.crt) fájl



A beállítások ellenőrzéséhez kattintson a **Teszt** gombra. Sikeres hitelesítéskor *A szerverhitelesítés sikeres* üzenet jelenik meg. Ha a hitelesítés nincs megfelelően beállítva, az alábbi üzenetek valamelyike jelenik meg.

Nem sikerült a szerverhitelesítés. Letelt a maximális hitelesítési idő.
A hitelesítési szerver nem érhető el. Ellenőrizze a szerver nevét és IP-címét, a kliens tűzfalbeállításait, valamint a szerverbeállításokat.

Hiba történt a szerverrel való kommunikáció során.

A hitelesítési szerver nem fut. Indítsa el a hitelesítési szerverhez tartozó szolgáltatást. További tudnivalókért tekintse meg a Zónahitelesítés – Szerverkonfiguráció című témakört.

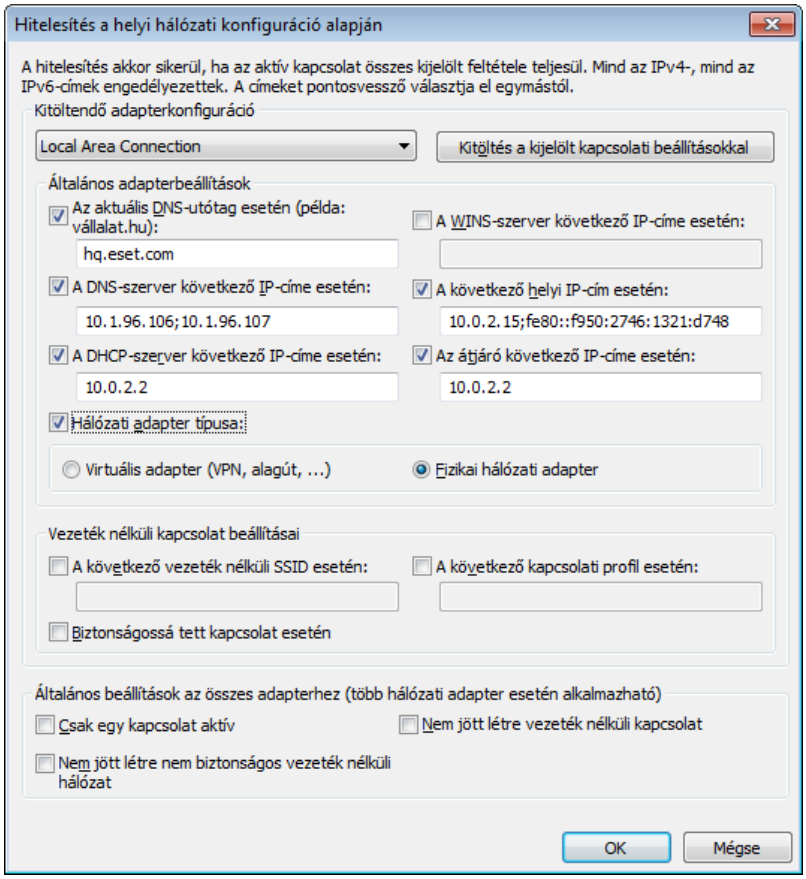
A hitelesítési zóna neve nem egyezik meg a szerver zónájával.
A megadott zónanév nem egyezik meg a hitelesítési szerver zónájával. Ellenőrizze mindkét zónát, és állítson be azonos nevet számukra.

Nem sikerült a szerverhitelesítés. A szerver címe nem található a megadott zóna címlistájában.
A hitelesítési szervert futtató számítógép IP-címe nem tartozik az aktuális zónakonfigurációban megadott IP-címek tartományába.

Nem sikerült a szerverhitelesítés. A megadott nyilvános kulcs valószínűleg érvénytelen.
Ellenőrizze, hogy a megadott nyilvános kulcs megfelel-e a titkos szerverkulcsnak. Ellenőrizze nyilvános kulcsot tartalmazó fájl épségét is.

2) Helyi hálózati konfiguráció alapján

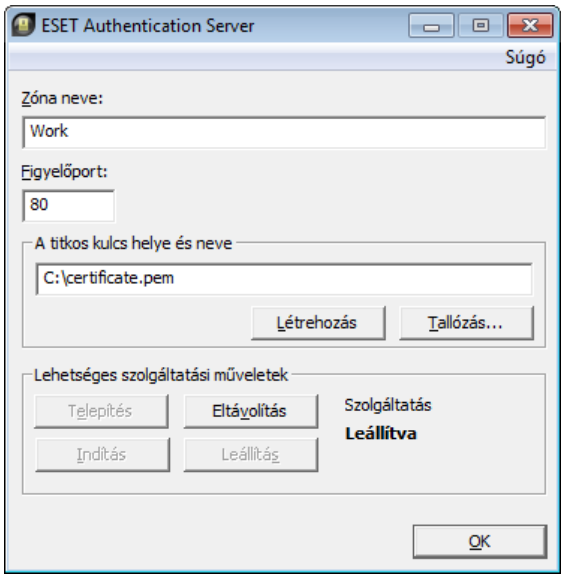
A hitelesítés a helyi hálózati adapter paramétereinek megfelelően történik. A zónahitelesítés sikerességéhez az aktív kapcsolat összes kijelölt paraméterének érvényesnek kell lennie.



4.2.4.1.2 Zónahitelesítés – Szerverkonfiguráció

A hitelesítési eljárás a hitelesítendő hálózathoz csatlakoztatott bármely számítógép vagy szerver által végrehajtható. Az ESET hitelesítési szerver alkalmazást olyan számítógépen vagy szerveren kell telepíteni, amely mindig elérhető a hitelesítéshez, valahányszor egy kliens megpróbál a hálózathoz csatlakozni. Az ESET hitelesítési szerverének telepítőfájlja az ESET weboldaláról tölthető le.

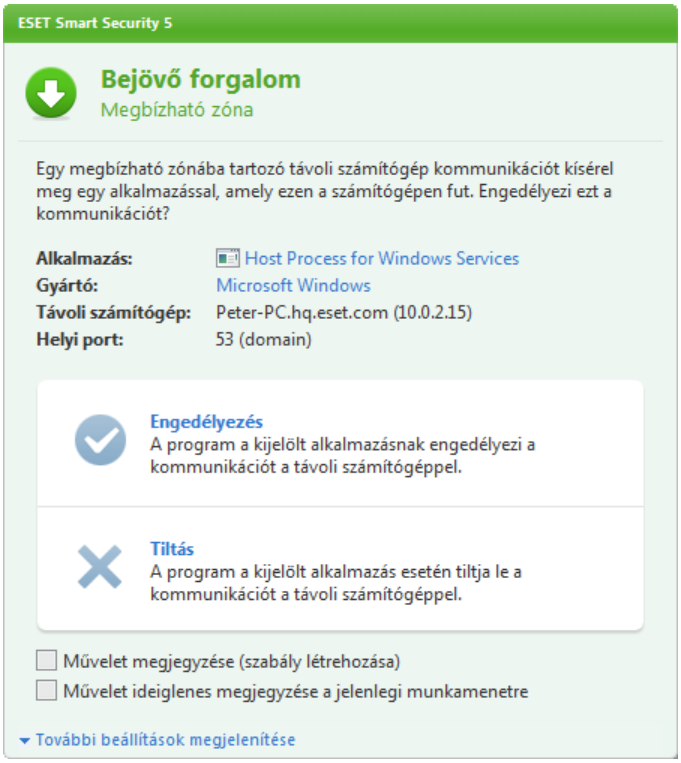
Az ESET hitelesítésszerver-alkalmazásának letöltését követően egy párbeszédpanel jelenik meg (az alkalmazás bármikor elindítható a **Start** > **Programok** > **ESET** > **ESET Authentication Server** parancsokkal).



A hitelesítési szerver konfigurálásához írja be a hitelesítési zóna nevét, a szerver figyelőportját (alapértelmezés szerint a 80-as), valamint a nyilvános és titkos kulcspár tárolási helyét. Ezután hozza létre a hitelesítési eljárásban használandó nyilvános és titkos kulcsot. A titkos kulcs a szerveren marad, míg a nyilvános kulcsot importálni kell a kliensoldalon a Zónahitelesítés részben, amikor a tűzfal beállításaiban beállít egy zónát.

4.2.5 Kapcsolat létesítése – észlelés

A személyi tűzfal minden újonnan létesített hálózati kapcsolatot észlel. A tűzfal aktív üzemmódja határozza meg, hogy a program milyen műveleteket alkalmazzon az új szabályhoz. Az **automatikus** vagy a **házirendalapú** üzemmód használatakor a személyi tűzfal előre megadott műveleteket fog végrehajtani, felhasználói beavatkozás nélkül. Interaktív üzemmódban a program egy tájékoztató ablakban értesítést küld az új kapcsolat észleléséről, és részletes információkat nyújt erről a kapcsolatról. Eldöntheti, hogy engedélyezi vagy elutasítja (letiltja) a kapcsolatot. Ha többször engedélyezi ugyanazt a kapcsolatot a párbeszédpanelen, ajánlatos új szabályt létrehozni a kapcsolathoz. Ehhez jelölje be a **Művelet megjegyzése (szabály létrehozása)** jelölőnégyzetet, és a személyi tűzfal új szabályaként mentse a műveletet. Ha a tűzfal a jövőben ugyanezt a kapcsolatot észleli, a meglévő szabályt alkalmazza rá.



Új szabályok létrehozásakor legyen körültekintő, és csak biztonságos kapcsolatokat engedélyezzen. Ha minden kapcsolatot engedélyez, a személyi tűzfal nem tölti be a rendeltetését. A kapcsolatok fontos jellemzői az alábbiak:

- **Távoli** – Csak megbízható és ismert címekkel engedélyezzen kapcsolatot.
- **Helyi alkalmazás** – Nem ajánlott ismeretlen alkalmazásoknak és folyamatoknak kapcsolatot engedélyezni.
- **Portszám** – A szokásos portokon (például webes kapcsolatok esetében a 80-as számú porton) zajló kommunikáció általában engedélyezhető.

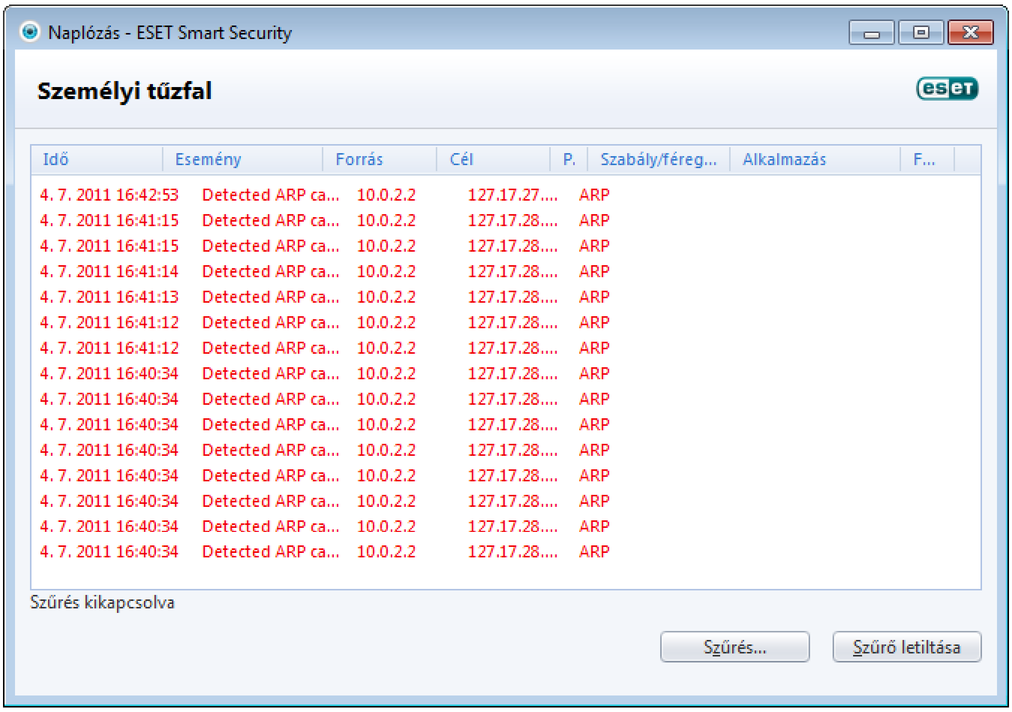
A számítógépes kártevők a terjedésükhöz gyakran az internetet és rejtett kapcsolatokat használnak, így próbálnak megfertőzni távoli rendszereket. Helyesen konfigurált szabályokkal a személyi tűzfal hasznos eszközzé válhat a különféle kártékony kódok támadása elleni védelemben.

4.2.6 Naplózás

Az ESET Smart Security Személyi tűzfal a fontos eseményeket egy naplófájlba menti, amely közvetlenül a fő menüből megtekinthető. Kattintson az **Eszközök** > **Naplófájlok** hivatkozásra, majd a **Napló** legördülő listában válassza **A személyi tűzfal naplója** elemet.

A naplófájlok a hibák javítását és a behatolási kísérletek észlelését nagyban segítő eszközök. A személyi tűzfal naplója az alábbi adatokat tartalmazza:

- Az esemény dátuma és időpontja
- Az esemény neve
- A forrás
- A cél hálózati címe
- A hálózati kommunikációs protokoll
- Az alkalmazott szabály, illetve a féreg neve (ha talált ilyet a program)
- Az érintett alkalmazás
- Felhasználó



Ezeknek az adatoknak az alapos elemzésével felderítheti a rendszerbiztonság megsértésére tett kísérleteket. Számos tényező utal a lehetséges biztonsági kockázatokra, amelyek negatív hatását így a lehető legkisebbre csökkentheti. Ilyen például, ha ismeretlen helyek túl gyakran kezdeményeznek kapcsolatot, egyidejűleg több kapcsolatra tesznek kísérletet, ismeretlen alkalmazások kommunikálnak vagy szokatlan portok vannak használatban.

4.2.7 Rendszerintegrálás

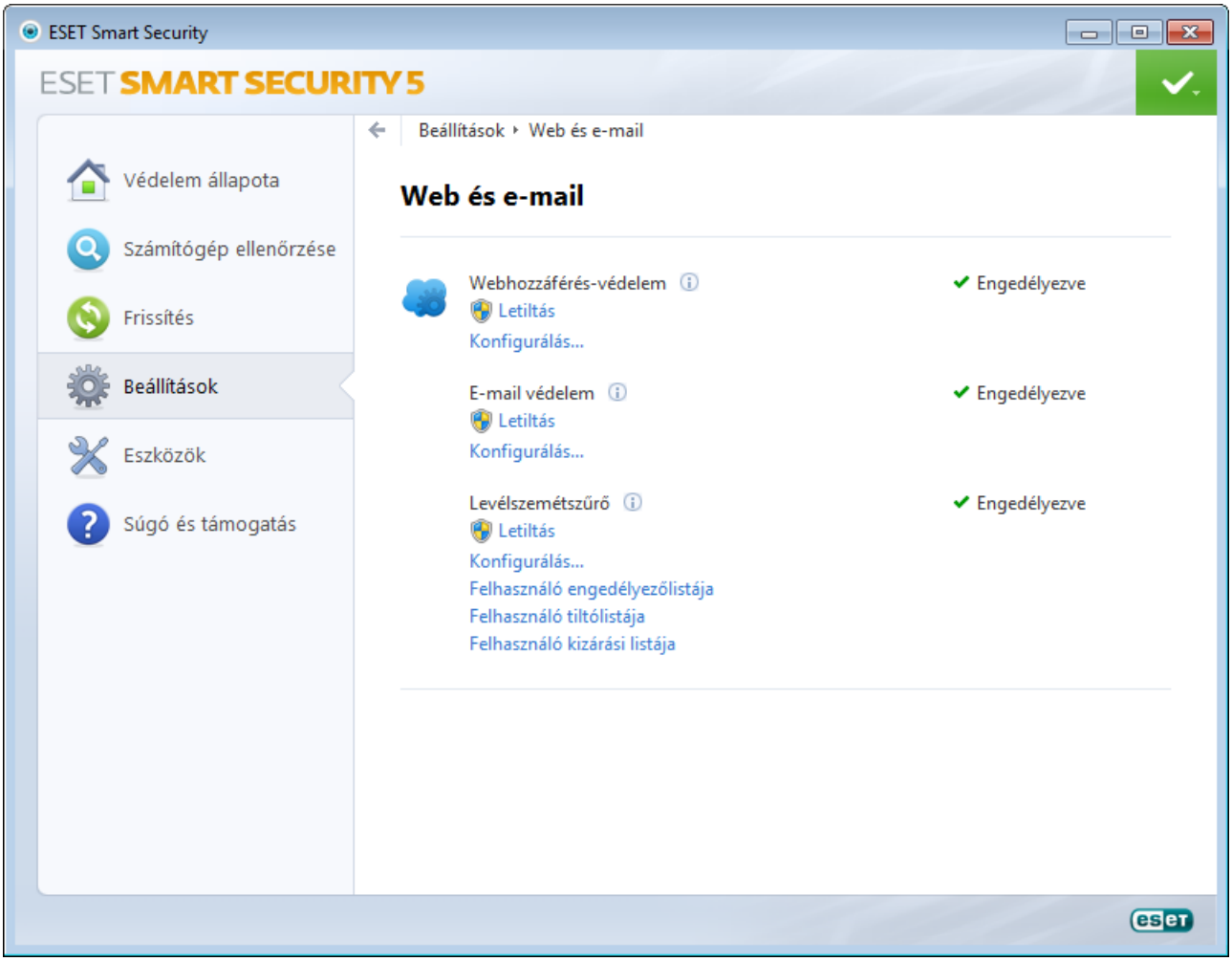
Az ESET Smart Security személyi tűzfala többféle szinten üzemelhet:

- **Minden szolgáltatás aktív** – A személyi tűzfal teljes integrációban üzemel, összetevői aktívak (ez az alapértelmezett üzemmód). Ha a számítógép nagyobb méretű hálózathoz vagy az internethez csatlakozik, javasolt ezt az üzemmódot választani, ugyanis a rendszer teljes körű védelme révén ez nyújtja a legnagyobb biztonságot.
- **A személyi tűzfal inaktív** – A rendszerbe integrálódó személyi tűzfal részt vesz a kommunikáció közvetítésében, kártevőszűrést azonban nem végez.
- **Csak az alkalmazásprotokollok szűrése** – A személyi tűzfalnak csak az alkalmazásprotokollok (HTTP, POP3, IMAP és ezek biztonságos verziói) szűrését biztosító összetevői aktívak. Az alkalmazásprotokoll-szintű szűrés mellőzése esetén a védelmet a fájlrendszerszintű valós idejű védelem és a kézi indítású számítógép-ellenőrzés biztosítja.
- **A személyi tűzfal ki van kapcsolva** – A személyi tűzfal kikapcsolása a rendszerben. Ebben az esetben a tűzfal nem végez szűrést. Ez az üzemmód például tesztelési célokra lehet hasznos – ha egy alkalmazás blokkolt, ellenőrizheti, hogy a tűzfal blokkolja-e. Mivel ez a legkevésbé biztonságos üzemmód, legyen körültekintő a tűzfal teljes kikapcsolása esetén.

A személyi tűzfal modul frissítésének elhalasztása a számítógép újraindításáig – A frissítések letöltődnek, de csak a számítógép újraindításakor fognak települni.

4.3 Web és e-mail

A web és e-mail konfigurációja a **Web és e-mail** hivatkozásra kattintva megnyitható **Beállítások** lapon található. A tűzfal részletesebb beállításai is elérhetők innen.



Az internetkapcsolatra való képesség a személyi számítógépek szabványos funkciója. Sajnos a kártevők is ezt használják ki a terjedéshez. Emiatt nagyon fontos a **webhozzáférés-védelem** engedélyezése.

E-mail védelem – A POP3 és az IMAP protokollon keresztül érkező e-mail kommunikáció szabályozását biztosítja. A levelezőprogramba beépülő modul segítségével az ESET Smart Security a levelezőprogramtól érkező minden kommunikáció (POP3, MAPI, IMAP, HTTP) ellenőrzésére képes.

A **Levélszemétszűrő** kiszűri a kéretlen e-maileket.

Letiltás – Kikapcsolja a levelezőprogramok webes/e-mail/levélszemétszűrő védelmét.

Konfigurálás – Megnyitja a webes/e-mail/levélszemétszűrő védelem további beállításait.

Felhasználó engedélyezőlistája – Megnyit egy párbeszédpanelt, ahol felveheti, szerkesztheti, illetve törölheti a biztonságosnak tartott e-mail címeket. Az engedélyezőlistán található feladói címekről érkező e-maileket nem ellenőrzi a program.

Felhasználó tiltólistája – Megnyit egy párbeszédpanelt, ahol felveheti, szerkesztheti, illetve törölheti a nem biztonságosnak tartott e-mail címeket. A tiltólistán szereplő feladói címekről érkező e-maileket a program levélszemétnek tekinti.

Felhasználó kizárási listája – Megnyit egy párbeszédpanelt, ahol felveheti, szerkesztheti, illetve törölheti az esetleg hamisított és kéretlen levelek küldésére használt e-mail címeket. A kizárási listán található feladói címekről érkező e-maileket a program mindig ellenőrzi. Alapértelmezés szerint a kizárási lista a meglévő levelezőfiókokról származó e-mail címeket tartalmazza.

4.3.1 Webhozzáférés-védelem

Az internetelérés a személyi számítógépek alapvető szolgáltatásaihoz tartozik. Sajnos a kártevők is ezt használják ki a terjedéshez. Emiatt nagyon fontos a webhozzáférés-védelem engedélyezése.

Kifejezetten javasoljuk, hogy engedélyezze a Webhozzáférés-védelem funkciót. A beállítás helye: **Beállítások** > **Web és e-mail** > **Webhozzáférés-védelem**.

4.3.1.1 HTTP, HTTPS

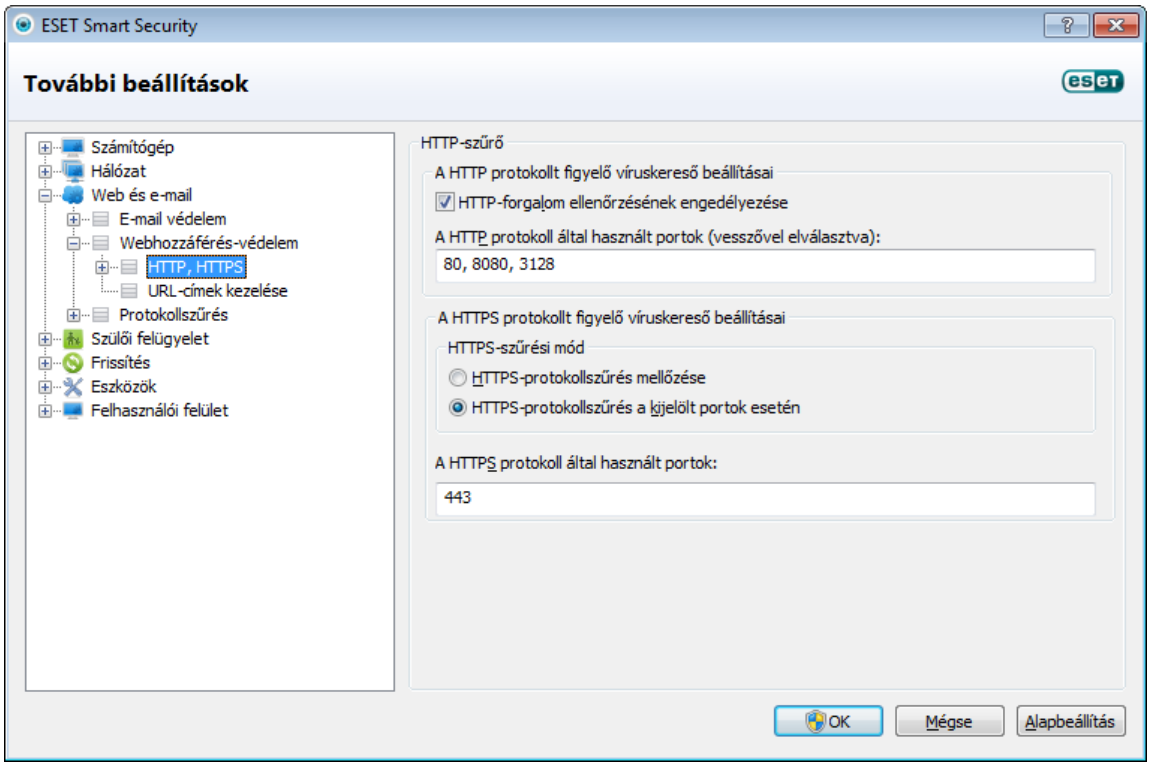
A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP és a HTTPS (titkosított kommunikáció) protokollon alapuló szabályokat. A ESET Smart Security támogatja a HTTPS-kapcsolatok ellenőrzését is. Ez a kommunikációtípus titkosított csatornán keresztül továbbítja az adatokat a szerver és a kliens között. Az ESET Smart Security képes az SSL és TLS protokollon alapuló kommunikáció ellenőrzésére. Az ESET Smart Security alapértelmezett konfigurációjában támogatja a legtöbb böngésző szabványait. A HTTP-szűrő beállításai azonban módosíthatók is a **További beállítások** (F5) > **Vírus- és kémprogramvédelem** > **Webhozzáférés-védelem** > **HTTP, HTTPS** szakaszban. A HTTP-szűrő fő ablakában bejelölheti a **HTTP-forgalom ellenőrzésének engedélyezése** jelölőnégyzetet, illetve törölheti a jelölést. A HTTP-kommunikáció által használt portszámokat is definiálhatja. Alapértelmezés szerint a 80-as, a 8080-as és a 3128-as portszám van beállítva. A HTTPS-ellenőrzésre az alábbi beállítások vonatkoznak.

HTTPS-protokollszűrés mellőzése – Ha bejelöli ezt a választógombot, a program nem ellenőrzi a titkosított kommunikációt.

HTTPS-protokollszűrés a kijelölt portok esetén – Akkor jelölje be ezt a választógombot, ha a HTTPS-ellenőrzést csak **A HTTPS protokoll által használt portok** listában megadott portokhoz szeretné engedélyezni.

HTTPS-protokollszűrés a kijelölt portok esetén – Ha ezt a beállítást választja, a program csak a böngészők szakaszban megadott alkalmazásokat, illetve **A HTTPS protokoll által használt portok** listában definiált portokat használó alkalmazásokat ellenőrzi. és alapértelmezés szerint csak a 443-as port szerepel rajta.

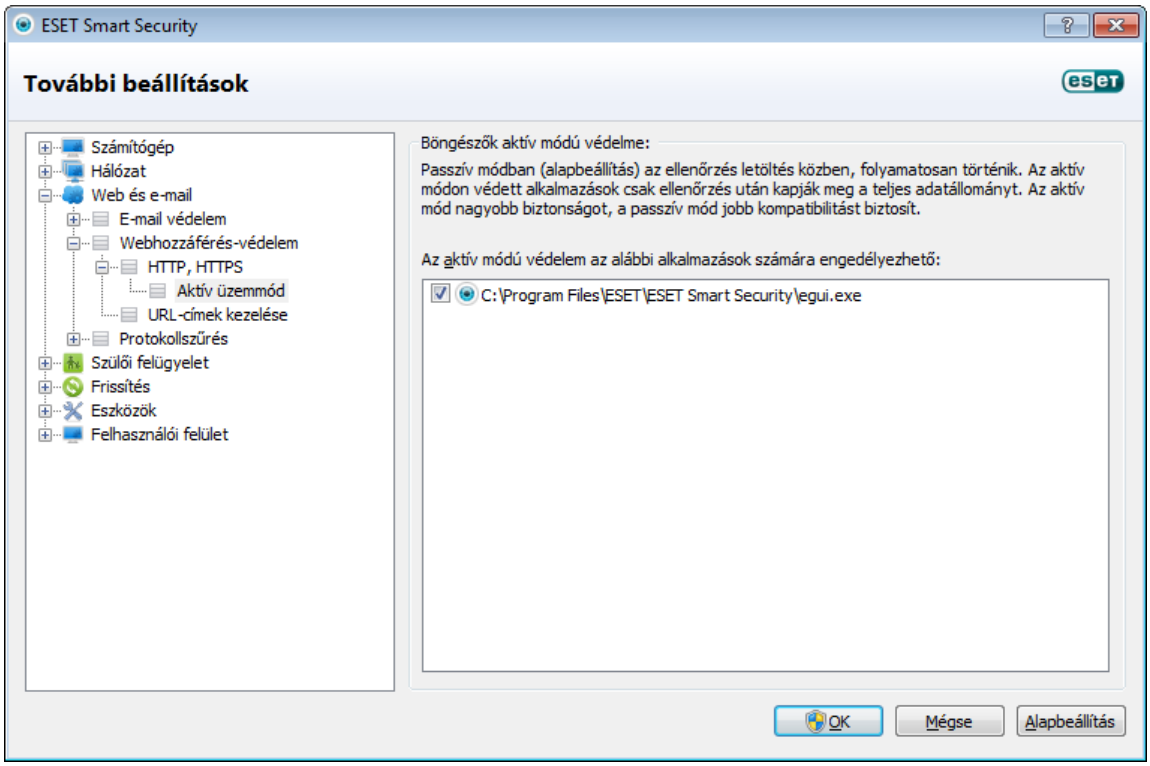
A titkosított adatokat a program nem ellenőrzi. A titkosított kommunikáció ellenőrzésének engedélyezéséhez és a víruskereső beállításához a További beállítások részen keresse meg az SSL-protokollszűrés csoportot (**Web és e-mail** > **Protokollszűrés** > **SSL**), és jelölje be **Az SSL protokoll ellenőrzése minden esetben** választógombot.



4.3.1.1.1 Böngészők aktív módú védelme

Az ESET Smart Security **Aktív üzemmód** almenüjében határozható meg a webböngészők ellenőrzési módja.

A program teljes egészében vizsgálja az internetkapcsolattal rendelkező, aktív üzemmódú ellenőrzésre beállított alkalmazásokból eredő adatforgalmat, akár böngészőként van megjelölve egy ilyen alkalmazás, akár nem (erről további információt talál az Internetböngészők című témakörben). Ha a beállítás nincs engedélyezve, az alkalmazások kommunikációját fokozatosan, kötegek formájában ellenőrzi a program. Ezzel csökken az adat-ellenőrzési folyamat hatékonysága, ugyanakkor magasabb fokú kompatibilitás biztosítható a megjelölt alkalmazásokhoz. Ha a beállítás használata problémamentes, az adott alkalmazás mellett található jelölőnégyzet bejelölésével ajánlott engedélyezni az aktív ellenőrzési üzemmódot. Az aktív üzemmód működésének áttekintése: Amikor egy ellenőrzött alkalmazás adatokat tölt le az internetről, az ESET Smart Security először egy ideiglenes fájlba helyezi a letöltött adatokat. Ezek ebben a fázisban még nem érhetők el az alkalmazás számára. Amikor a letöltés befejeződik, a program ellenőrzi az adatokat, hogy nem tartalmaznak-e kártékony kódot. Ha nem észlel fertőzést, átadja az adatokat az eredeti alkalmazásnak. Ez a folyamat teljes ellenőrzést biztosít az adott alkalmazás által folytatott kommunikáció felett. Passzív üzemmódban a program az időtúllépés elkerülésére folyamatosan, kisebb adagokban adja át az adatokat az eredeti alkalmazásnak.

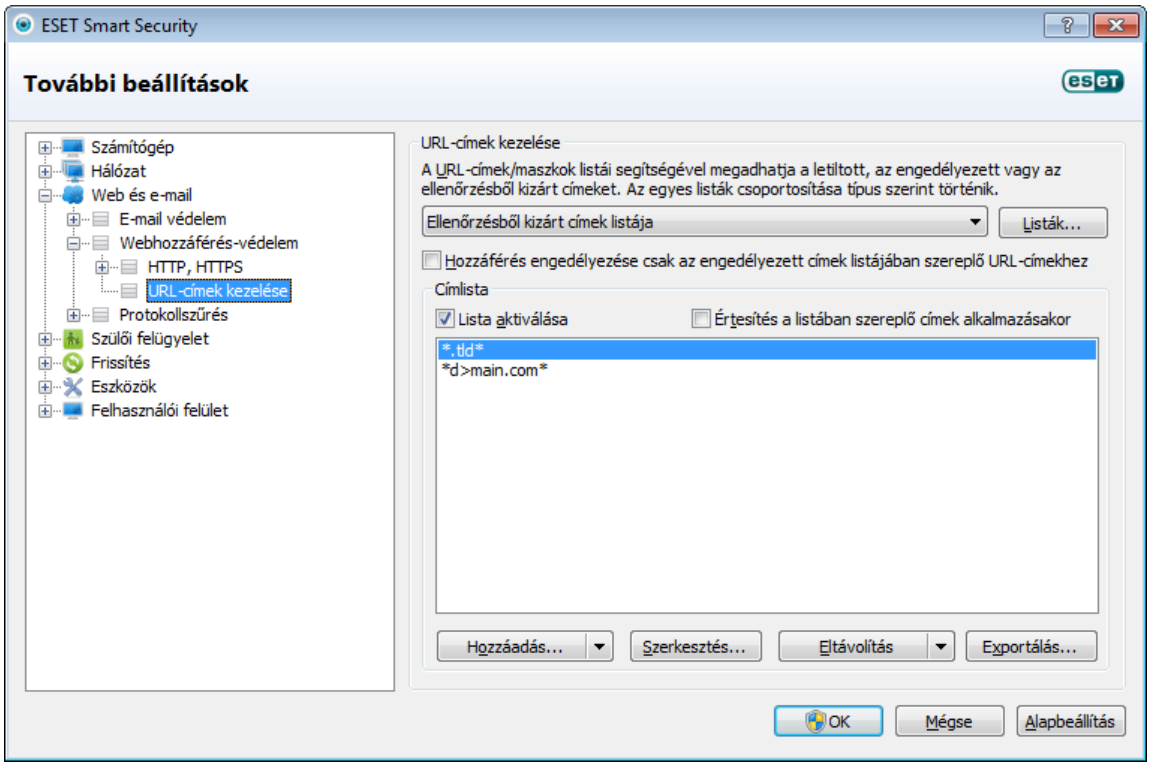


4.3.1.2 URL-címek kezelése

A témakörből megtudhatja, miként tilthat le, engedélyezhet és zárhat ki az ellenőrzésből HTTP-címeket. A címlisták a **Hozzáadás**, a **Szerkesztés**, az **Eltávolítás** és az **Exportálás** gombbal kezelhetők. A tiltólistán szereplő webhelyeket nem fogja tudni elérni. A kizárt címek listáján szereplő webhelyek elérése közben a program nem keres kártékony kódokat. Ha bejelöli a **Hozzáférés engedélyezése csak az engedélyezett címek listájában szereplő HTTP-címekhez** jelölőnégyzetet, akkor csak az engedélyezett címek listáján szereplő címek lesznek elérhetők; minden más HTTP-címet blokkolni fog a program.

Az **Ellenőrzésből kizárt címek listája** nevű listára felvett címeket a program kihagyja az ellenőrzésből. Az egyes címek engedélyezéséhez és blokkolásához az érintett címeket felveheti az **Engedélyezett címek listája** és a **Letiltott címek listája** nevű listára. A **Listák** gombra kattintva megjelenik a **HTTP-címek/maszkok listái** párbeszédpanel, melyen a **Hozzáadás** és az **Eltávolítás** gombra kattintva lehet címet felvenni és eltávolítani. Ha HTTPS-címeket szeretne felvenni a listára, az SSL protokoll beállítási szakaszában **Az SSL protokoll ellenőrzése minden esetben** választógombot kell bejelölnie.

Mindegyik listában használhatók speciális szimbólumok, nevezetesen a * (csillag) és a ? (kérdőjel). A csillaggal tetszőleges karaktersor, a kérdőjellel pedig bármilyen szimbólum helyettesíthető. A szűrés alól kizárt címek megadásakor különös figyelemmel járjon el, mert a listába csak megbízható és biztonságos címeket ajánlott felvenni. Szintén fontos, hogy a * és a ? szimbólumot megfelelően használja a listában. Ha aktiválni szeretne egy listát, jelölje be a **Lista aktiválása** jelölőnégyzetet. Ha értesítést szeretne megjeleníteni az aktuális listán szereplő címek beírásakor, jelölje be az **Értesítés a listában szereplő címek alkalmazásakor** jelölőnégyzetet.



Hozzáadás / Beolvasás fájlból – A **Hozzáadás** paranccsal manuálisan vehet fel egy címet a listára. A **Beolvasás fájlból** parancsra kattintva választhat egy szövegfájlt, hogy az abban lévő e-mail címeket felvegye a listára.

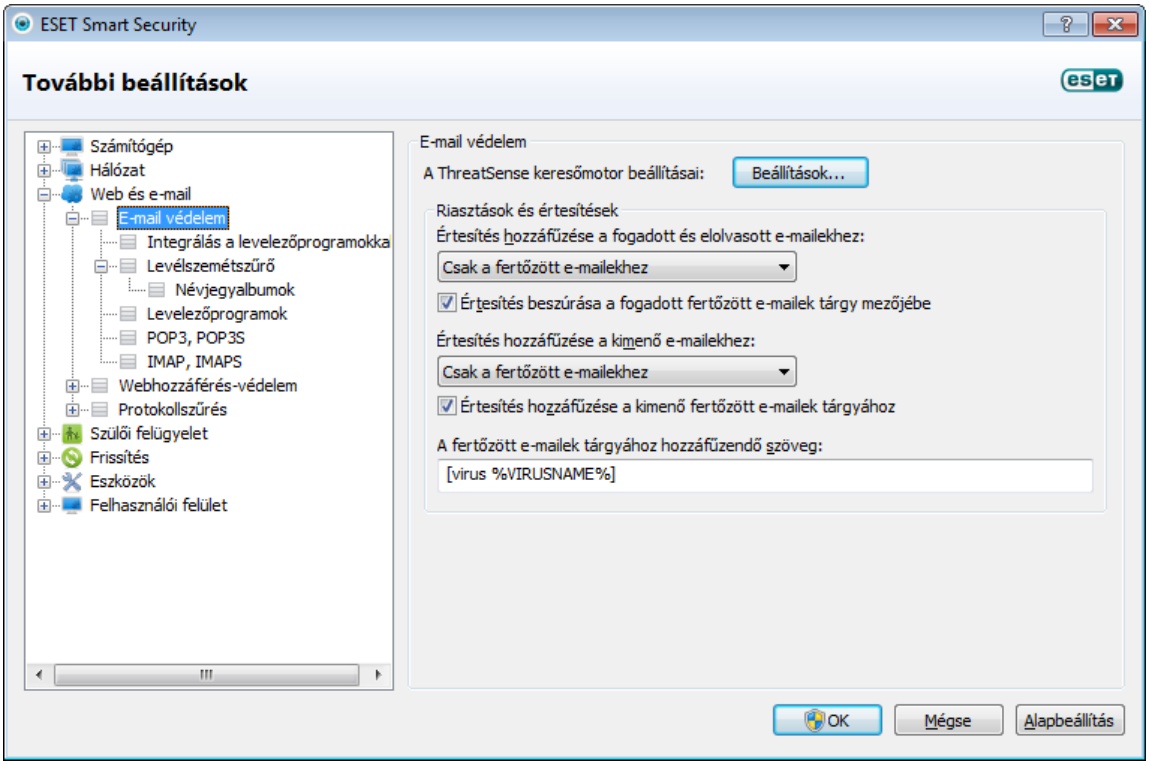
Szerkesztés – A gombra kattintva kézzel szerkesztheti a címeket (például kiegészíthet egy címet egy * vagy ? maszkkal).

Eltávolítás / Összes eltávolítása – Az **Eltávolítás** paranccsal a listában kijelölt címeket törölheti a listáról, míg az **Összes eltávolítása** paranccsal az összes címet eltávolíthatja.

Exportálás – A gombra kattintva az aktuális listából egy egyszerű szöveges fájlba mentheti a címeket.

4.3.2 E-mail védelem

Az e-mail védelem biztosítja a POP3 és az IMAP protokollon keresztül érkező e-mail kommunikáció ellenőrzését. A Microsoft Outlook alkalmazásba és más levelezőprogramokba beépülő modul segítségével az ESET Smart Security a levelezőprogramok által folytatott teljes kommunikációt képes ellenőrizni (beleértve a POP3, a MAPI, az IMAP és a HTTP protokollt is). A bejövő üzenetek vizsgálatakor a program az ThreatSense keresőmotor által biztosított összes speciális ellenőrzési módszert alkalmazza. Ez azt jelenti, hogy a kártékony programok észlelése még azelőtt megtörténik, hogy a program összevetné azokat a vírusdefiníciós adatbázissal. A POP3 és az IMAP protokollon keresztül folytatott kommunikáció ellenőrzése a beépülő modultól függetlenül minden levelezőprogram esetén megtörténik.



A funkciókhoz tartozó beállítások eléréséhez válassza a **További beállítások** > **Web és e-mail** > **E-mail védelem** lehetőséget.

Az **ThreatSense keresőmotor beállításai** – A speciális víruskeresési beállításokkal megadhatja az ellenőrizendő célterületek körét, az észlelési módszereket stb. Kattintson a **Beállítások** gombra a részletes vírusellenőrzési beállításokat tartalmazó ablak megnyitásához.

Miután a program ellenőriz egy-egy levelet, az ellenőrzés eredményét ismertető értesítést is hozzáfűzhet. Az **Értesítés hozzáfűzése a fogadott és elolvasott e-mailekhez**, illetve az **Értesítés hozzáfűzése a kimenő e-mailekhez** jelölőnégyzet bejelölésével értesítéseket fűzhet a levelekhez. Ezek az értesítések azonban nem tekinthetők megkérdőjelezhetetlennek, mivel a hibásan formázott HTML-üzenetekben eltűnhetnek, illetve egyes vírusok képesek meghamisítani. Az értesítés a beérkezett/elolvasott üzenetekhez és a kimenő levelekhez (vagy mindkét típushoz) egyaránt hozzáadható. A választható lehetőségek az alábbiak:

- **Soha** – A program nem fűz értesítő szöveget az üzenetekhez.
- **Csak a fertőzött e-mailekhez** – A program csak a kártékony szoftvert tartalmazó levelekhez fűz értesítést (alapértelmezett).
- **Az összes ellenőrzött e-mailhez** – A program minden ellenőrzött levélhez értesítést fűz.

Értesítés beszúrása a fogadott fertőzött e-mailek tárgy mezőjébe – Jelölje be ezt a jelölőnégyzetet, ha azt szeretné, hogy az e-mailek védelmét ellátó funkció vírusra utaló figyelmeztetést fűzzön a fertőzött levelek tárgyához. Ezzel a módszerrel egyszerűen, a tárgy alapján szűrheti a fertőzött leveleket (ha ezt a használt levelezőprogram támogatja). Így a címzett számára megnő az üzenetek hitelességi szintje, és fertőzés észlelése esetén értékes információk nyerhetők az adott üzenet vagy feladója veszélyességi szintjéről.

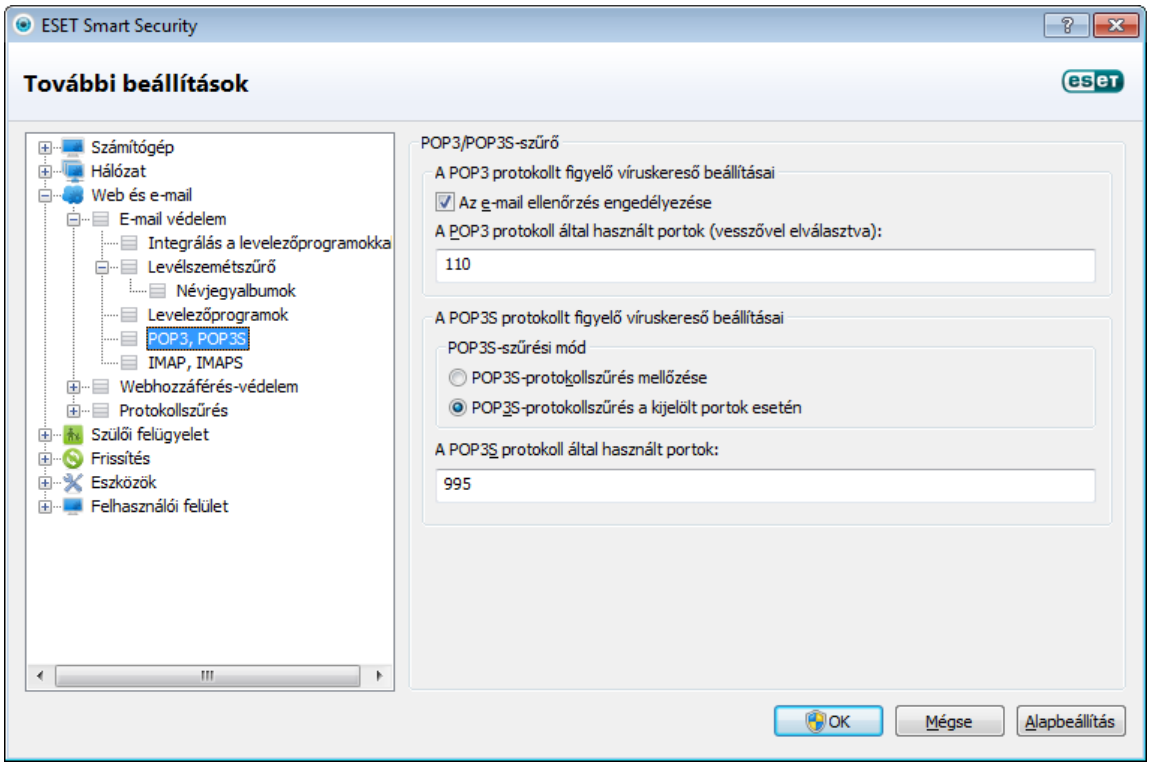
A fertőzött e-mailek tárgyához hozzáfűzendő szöveg – A szöveg szerkesztésével módosíthatja a fertőzött e-mail tárgyában szereplő előtag formátumát. Ez a funkció az üzenet tárgyában szereplő *"Hello"* szót a *"[vírus]"* előtagra cseréli a következő formátumban: *"[vírus] Hello"*. A(z) *%VIRUSNAME%* változó az észlelt kártevőt jelöli.

4.3.2.1 POP3/POP3S-szűrő

A POP3 a levelezőprogramok által a legszélesebb körben használt levélfogadási protokoll. Az ESET Smart Security a levelezőprogramtól függetlenül képes védeni a POP3 protokollon keresztüli kommunikációt.

Az ellenőrzést biztosító védelmi modul automatikusan elindul az operációs rendszer indításakor, és aktív marad a memóriában. A megfelelő működéshez győződjön meg arról, hogy a modul engedélyezett. Az automatikus POP3-ellenőrzéshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 110-es porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. A portszámokat vesszővel elválasztva kell megadni.

A titkosított adatokat a program nem ellenőrzi. A titkosított kommunikáció ellenőrzésének engedélyezéséhez és a víruskereső beállításához a További beállítások részen keresse meg az SSL-protokollszűrés csoportot (**Web és e-mail** > **Protokollszűrés** > **SSL**), és jelölje be **Az SSL protokoll ellenőrzése minden esetben** választógombot.



Ebben a szakaszban a POP3 és a POP3S protokollon keresztüli kommunikáció ellenőrzése szabályozható.

Az e-mail ellenőrzés engedélyezése – A jelölőnégyzet bejelölése esetén a program a POP3 protokollon zajló teljes forgalmon végez kártevőkeresést.

A POP3 protokoll által használt portok – A POP3 protokoll által használt portok listája (az alapértelmezett port a 110-es).

Az ESET Smart Security a POP3S protokoll ellenőrzését is támogatja. Ez a kommunikációtípus titkosított csatornán keresztül továbbítja az adatokat a szerver és a kliens között. Az ESET Smart Security képes az SSL és TLS protokollon alapuló kommunikáció ellenőrzésére.

POP3S-protokollszűrés mellőzése – Ha bejelöli ezt a választógombot, a program nem ellenőrzi a titkosított kommunikációt.

POP3S-protokollszűrés a kijelölt portok esetén – Jelölje be ezt a választógombot, ha a POP3S-ellenőrzést csak **A POP3S protokoll által használt portok** listában megadott portokhoz szeretné engedélyezni.

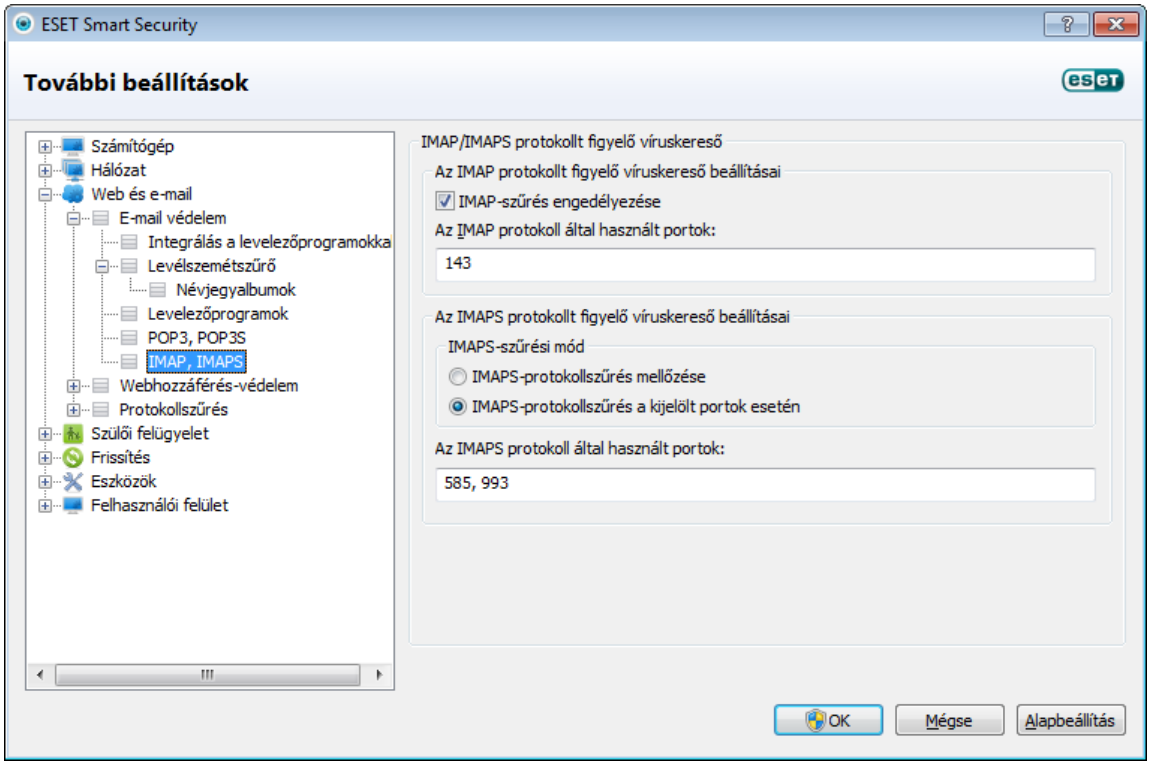
A POP3S protokoll által használt portok – A POP3S protokoll által használt portok listája (mely alapértelmezés szerint a 995-ös portból áll).

4.3.2.2 IMAP-, IMAPS-protokollellenőrzés

Az IMAP egy e-mailek fogadására szolgáló protokoll. Az IMAP a POP3 protokollnál fejlettebb funkciókkal rendelkezik – például több levelezőprogram is csatlakozhat ugyanahhoz a postaládához egy időben, miközben az üzenetek állapota (például az olvasottság, a megválaszoltság és a töröltség) megőrződik és egységesen látszik. Az ESET Smart Security a levelezőprogramtól függetlenül képes az IMAP protokoll védelmére.

Az ellenőrzést biztosító védelmi modul automatikusan elindul az operációs rendszer indításakor, és aktív marad a memóriában. A megfelelő működéshez győződjön meg arról, hogy a modul engedélyezett. Az automatikus IMAP-ellenőrzéshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 143-as porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. A portszámokat vesszővel elválasztva kell megadni.

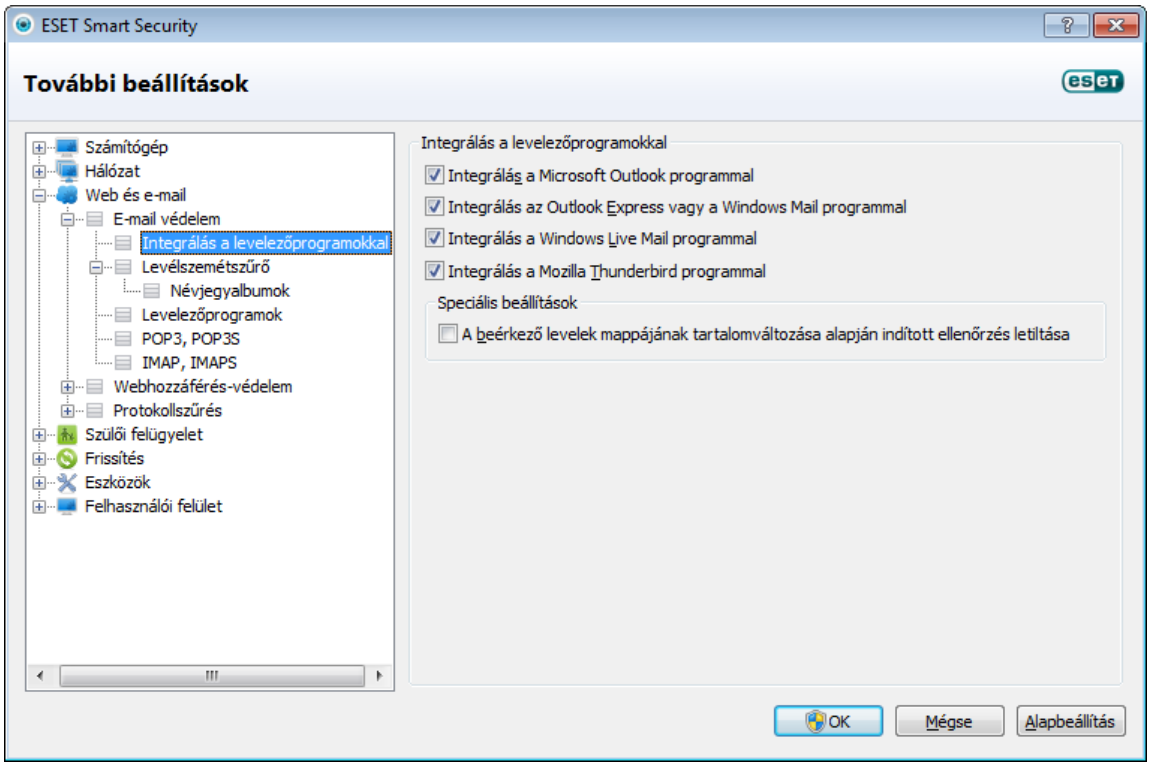
A titkosított adatokat a program nem ellenőrzi. A titkosított kommunikáció ellenőrzésének engedélyezéséhez és a víruskereső beállításához a További beállítások részen keresse meg az SSL-protokollszűrés csoportot (**Web és e-mail** > **Protokollszűrés** > **SSL**), és jelölje be **Az SSL protokoll ellenőrzése minden esetben** választógombot.



4.3.2.3 Integrálás a levelezőprogramokkal

Az ESET Smart Security levelezőprogramokkal való integrálásával növelhető az e-mailekben terjesztett kártékony kódok elleni aktív védelem. A támogatott levelezőprogramok integrálása az ESET Smart Security programban engedélyezhető. Ha az integráció engedélyezett, az ESET Smart Security eszköztára közvetlenül a levelezőprogramban jelenik meg, ezzel még hatékonyabb e-mail védelmet nyújtva. Az integrálási beállítások eléréséhez válassza a **Beállítások** > **További beállítások megnyitása** > **Web és e-mail** > **E-mail védelem** > **Integrálás a levelezőprogramokkal** lehetőséget. A jelenleg támogatott levelezőprogramok: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail és Mozilla Thunderbird.

Ha a levelezőprogram használatakor a rendszer lassulását tapasztalja, jelölje be **A beérkező levelek mappájának tartalomváltozása alapján indított ellenőrzés letiltása** jelölőnégyzetet. Ilyen helyzet fordulhat elő, amikor a Kerio Outlook Connector tárolójából tölt le e-mailt.



4.3.2.3.1 Az e-mail védelem beállításai

Az E-mail védelem modul az alábbi levelezőprogramokat támogatja: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail és Mozilla Thunderbird. Az E-mail védelem a fenti programok beépített moduljaként működik. A beépülő modul legfőbb előnye az, hogy független a használt protokolltól. Amikor a levelezőprogram egy titkosított üzenetet fogad, a modul visszafejti és a víruskeresőhöz küldi azt.

Ellenőrizendő e-mailek

Fogadott e-mailek – Ha bejelöli ezt a jelölőnégyzetet, a program ellenőrzi a beérkező üzeneteket.
Küldendő e-mailek – Ha bejelöli ezt a jelölőnégyzetet, a program ellenőrzi a küldeni kívánt üzeneteket.
Olvasott e-mailek – Ha bejelöli ezt a jelölőnégyzetet, a program ellenőrzi az elolvasott üzeneteket.

A fertőzött e-maileken végrehajtandó művelet

Kihagyás – Engedélyezése esetén a program felismeri a fertőzött mellékleteket, de semmilyen műveletet nem hajt végre rajtuk.
E-mail törlése – A program értesíti a felhasználót a fertőzésről, és törli az üzenetet.
E-mail áthelyezése a Törölt elemek mappába – A program a fertőzött e-maileket automatikusan a **Törölt elemek** mappába helyezi át.
E-mail áthelyezése a következő mappába – E lehetőség választása esetén megadhatja, hogy melyik mappába kerüljenek a fertőzött e-mailek a fertőzések észlelése után.

Egyéb

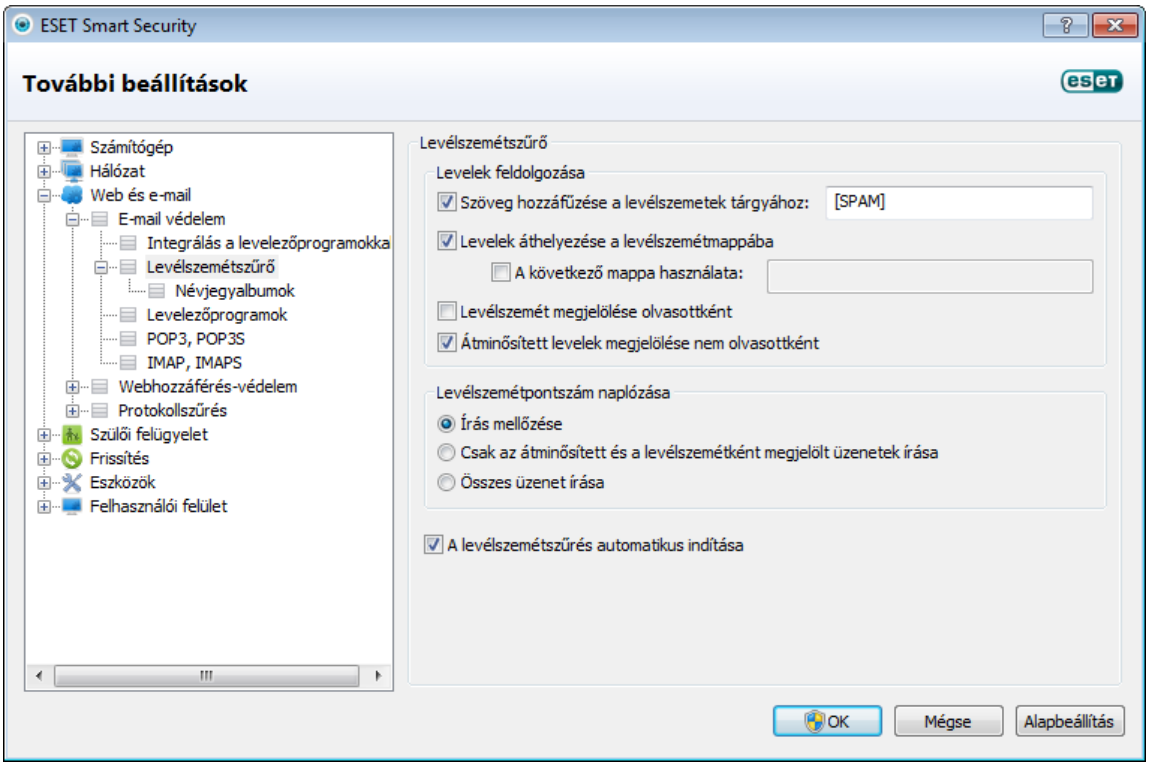
Ellenőrzés megismétlése frissítés után – Ha bejelöli ezt a jelölőnégyzetet, a program megismétli az ellenőrzést a vírusdefiníciós adatbázis frissítése után.
Más modulok által végrehajtott ellenőrzések eredményeinek elfogadása – Ha bejelöli ezt a jelölőnégyzetet, az E-mail védelem modul elfogadja a többi védelmi modul ellenőrzési eredményeit.

4.3.2.4 Fertőzések eltávolítása

Fertőzött e-mail érkezése esetén a program megjelenít egy riasztási ablakot. A riasztási ablakban szerepel a feladó neve, az e-mail és a fertőzés neve. Az ablak alsó részén a **Megtisztítás**, a **Törlés** vagy a **Kihagyás** gombra kattintással választhatja ki az észlelt objektumra vonatkozó műveletet. A legtöbb esetben ajánlatos a **Megtisztítás** vagy a **Törlés** lehetőséget választani. Speciális esetekben, ha meg szeretné kapni a fertőzött fájlt, választhatja a **Kihagyás** lehetőséget is. Ha az **Automatikusan megtisztít** beállítás van engedélyezve, a program csak egy tájékoztató ablakot jelenít meg, amelyben nincsenek a fertőzött objektumokra vonatkozó lehetőségek.

4.3.3 Levélszemétszűrő

Az elektronikus kommunikáció egyik legnagyobb problémáját a kéretlen levelek, más néven levélszemét áradata jelenti. A kéretlen levelek a teljes levelezés mintegy 80 százalékát teszik ki. A levélszemétszűrés megoldást nyújt e problémára. A számos hatékony alapelvet kombináló Levélszemétszűrő modul egyedülálló szűrési képességekkel tartja tisztán postaládáját.



A levélszemét észlelésének egyik fontos elve a kéretlen levél felismerése az előre definiált, megbízható címeket (engedélyezőlista), illetve a tiltott címeket (tiltólista) tartalmazó listák alapján. A névjegyzékében található címeket a program automatikusan hozzáadja az engedélyezőlistához, illetve további címeket is megjelölhet biztonságosként.

A levélszemét észlelésének elsődleges módszere az e-mail tulajdonságainak ellenőrzése. A beérkezett üzeneteket a program különböző alapvető feltételek (üzenetdefiníciók, statisztikai heurisztika, felismerőalgoritmusok és egyéb egyedi módszerek) alapján ellenőrzi, és az eredményként kapott indexérték határozza meg, hogy az üzenet levélszemét-e.

Az ESET Smart Security levélszemétszűrője lehetővé teszi, hogy a levelezőlisták kezelése érdekében különböző paramétereket állítson be. A beállítások az alábbiak:

A levélszemétszűrés automatikus indítása – A jelölőnégyzet segítségével be- vagy kikapcsolhatja az e-mail védelmet.

Levelek feldolgozása

Szöveg hozzáfűzése a levélszemetek tárgyához – A jelölőnégyzet bejelölésekor egyéni szöveges előtagot fűzhet a levélszemétként azonosított levelek tárgyához. Az alapértelmezett előtag a „[SPAM]”.

Levelek áthelyezése a levélszemétmappába – Ha a jelölőnégyzet be van jelölve, a program automatikusan áthelyezi a levélszemétként azonosított leveleket az alapértelmezett levélszemétmappába.

A következő mappa használata – Ezzel a beállítással a levélszemetet egy egyénileg megadott mappába helyezheti.

Levélszemét megjelölése olvasottként – Ezt a jelölőnégyzetet bejelölve automatikusan olvasottként jelölheti meg a levélszemetet. Így gyorsabban kiszűrheti a jó leveleket.

Átminősített levelek megjelölése nem olvasottként – Az eredetileg levélszemétként megjelölt, később jó levéllé átminősített levelek nem olvasottként jelennek meg.

Levélszemétpontszám naplózása

Az ESET Smart Security levélszemétszűrő motorja minden ellenőrzött üzenethez levélszemétpontszámot rendel. A program a levélszemétszűrő naplójában rögzíti az üzenetet (**ESET Smart Security** > **Eszközök** > **Naplófájlok** > **Levélszemétszűrő**).

- **Írás mellőzése** – A **Pontszám** cella a levélszemétszűrő naplójában üres marad.
- **Csak az átminősített és a levélszemétként megjelölt üzenetek írása** – A választógomb bejelölésével rögzítheti a levélszemétként megjelölt üzenetek levélszemétpontszámát.
- **Összes üzenet írása** – A választógomb bejelölése esetén a program minden üzenetet – levélszemétpontszámmal együtt – rögzít a naplóban.
- **A levélszemétszűrés automatikus indítása** – A jelölőnégyzet bejelölése esetén a levélszemétszűrés rendszerindításkor automatikusan aktiválódik.

Az ESET Smart Security támogatja a Microsoft Outlook, az Outlook Express, a Windows Mail, a Windows Live Mail és a Mozilla Thunderbird levélszemét elleni védelmét.

4.3.3.1 Tanítható levélszemétszűrő

A tanítható levélszemétszűrő a Bayes-féle szűrőhöz kapcsolódik. Az üzenetek levélszemétként vagy jó levélként megjelölésével létrehozza a bennük használt szavak adatbázisát. Minél több üzenetet sorol be (levélszemétként vagy jó levélként megjelölve), annál pontosabb lesz a *Bayes-féle szűrő*. Az ismert e-mail címeket vegye fel az engedélyezőlistára, így kizárja azokat a szűrésből.

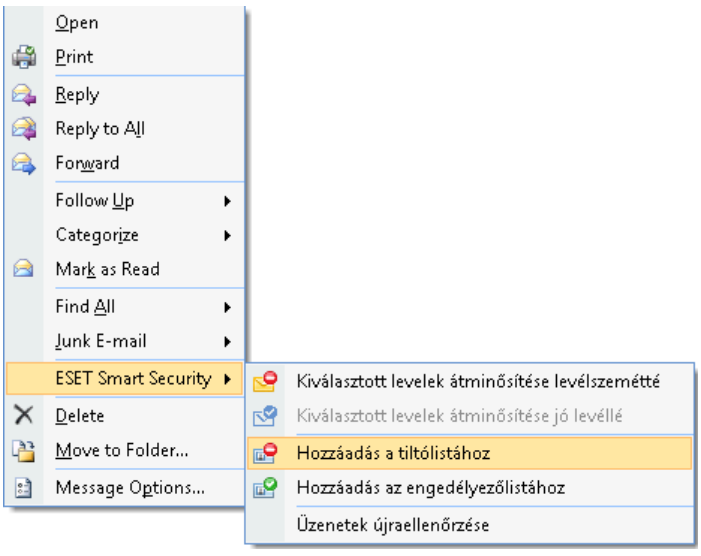
4.3.3.1.1 Címek felvétele engedélyező- és tiltólistára

Felveheti az engedélyezőlistára az olyan személyek e-mail címét, akikkel gyakran kommunikál, így a listán szereplő címről érkező üzeneteket a program soha nem minősíti levélszemétnek. Az ismert levélszemétküldő címeket felveheti a tiltólistára, így az arról érkező levelek levélszemétnek minősülnek. Ha új címet szeretne felvenni az engedélyező- vagy a tiltólistára, kattintson a jobb gombbal az e-mailre, és válassza az **ESET Smart Security** menüpontban a **Hozzáadás az engedélyezőlistához** vagy a **Hozzáadás a tiltólistához** parancsot; vagy az ESET Smart Security levélszemétszűrő eszköztárán kattintson a **Megbízható cím** vagy a **Levélszemétküldő cím** gombra.

A levélszemétküldő címeket hasonló módszerrel jelölheti meg. Ha egy e-mail cím a tiltólistán szerepel, a program az adott címről érkező összes üzenetet levélszemétnek minősíti.

4.3.3.1.2 Levelek megjelölése levélszemétként

A levelezőprogramban megtekintett bármely levelet megjelölheti levélszemétként. Ehhez kattintson a jobb gombbal az üzenetre, és válassza az **ESET Smart Security** menüpont **Kiválasztott levelek átminősítése levélszeméttévé** parancsát; vagy kattintson a **Levélszemétküldő cím** gombra az ESET Smart Security Levélszemétszűrő eszköztárán, a levelezőprogram ablakának felső részén.



Az átminősített leveleket a program automatikusan áthelyezi a Levélszemét mappába, de a feladó e-mail címét nem adja hozzá a tiltólistához. A levelek ugyanígy átminősíthetők „jó levél" megjelöléssel. Ha a **Levélszemét** mappában

található leveleket jó levélként jelöli meg, a program visszahelyezi őket az eredeti mappába. A levelek jó levélként való megjelölésével a program a feladó címét nem adja hozzá automatikusan az engedélyezőlistához.

4.3.4 Protokollszűrés

Az alkalmazásprotokollok vírusvédelmét az összes fejlett kártevőkereső technológiát zökkenőmentesen integráló ThreatSense keresőmotor biztosítja. Az ellenőrzés az alkalmazott internetböngészőtől és levelezőprogramtól függetlenül, automatikusan működik. A titkosított SSL-kommunikáció beállításai a **Protokollszűrés** > **SSL** szakaszban tekinthetők meg.

Protokollszűrés engedélyezése – A jelölőnégyzet bejelölése esetén a víruskereső minden HTTP(S), POP3(S) és IMAP(S) protokollon keresztüli forgalmat ellenőriz.

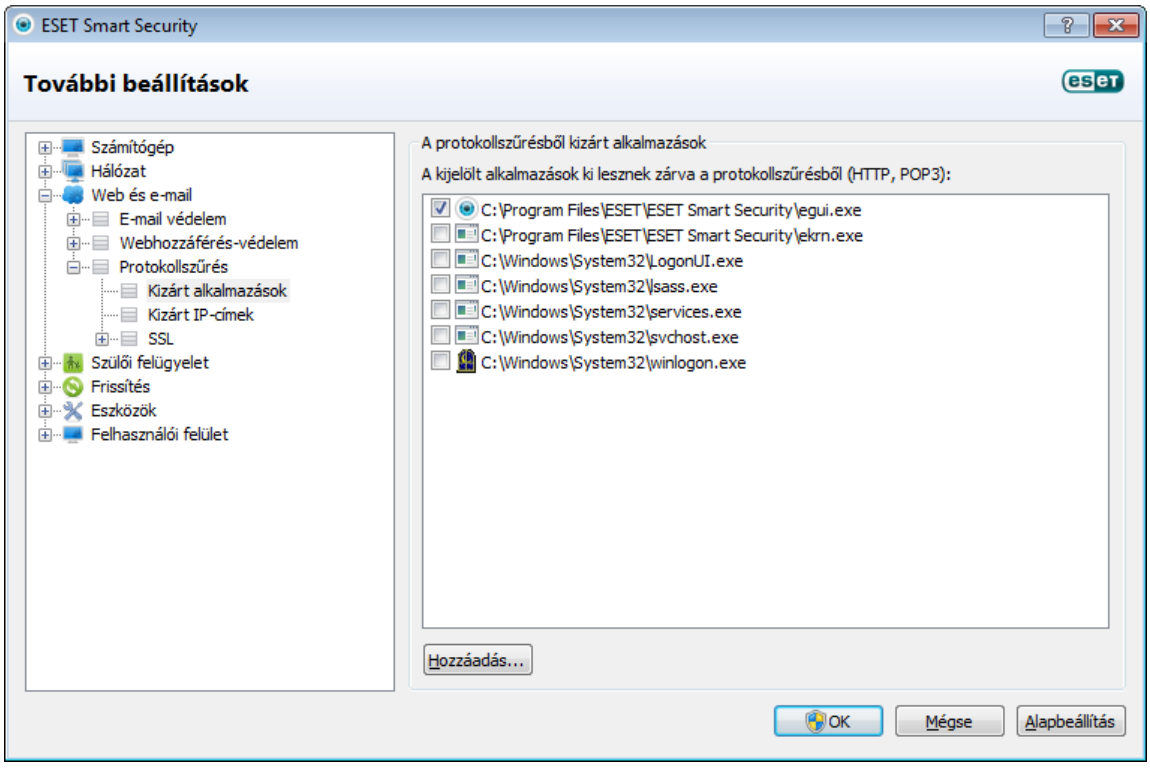
MEGJEGYZÉS: A Windows Vista SP1, a Windows 7 és a Windows Server 2008 rendszerrel kezdődően a hálózati kommunikáció ellenőrzése az új Windows szűrőplatform (WFP) architektúrájára épül. Mivel a Windows szűrőplatform saját figyelési technikákat használ, az alábbi beállítások nem érhetők el.

- **HTTP- és POP3-portok** – Ezt a lehetőséget választva a program csak a HTTP- és a POP3-portok forgalmát irányítja a belső proxyszerverhez.
- **Böngészőként és levelezőprogramként megjelölt alkalmazások** – Ezt a lehetőséget választva a program csak a böngészőként és levelezőprogramként megjelölt alkalmazások forgalmát irányítja a belső proxyszerverhez. (Az alkalmazások efféle megjelölésére a **Web és e-mail** > **Protokollszűrés** > **Böngészők és levelezőprogramok** szakaszban van mód).
- **Böngészőként és levelezőprogramként megjelölt alkalmazások és portok** – Ezt a lehetőséget választva a program mind a HTTP- és POP3-portok, mind a böngészőként és levelezőprogramként megjelölt alkalmazások forgalmát a belső proxyszerverhez irányítja.

4.3.4.1 Kizárt alkalmazások

A rendszer nem végez tartalomszűrést a listán szereplő azon hálózati alkalmazások adatforgalmán, melyek jelölőnégyzetét bejelöli. Az adott alkalmazásokhoz irányuló és általuk kezdeményezett HTTP- és POP3-alapú adatforgalmon a program nem végez kártevő-ellenőrzést. Csak azon alkalmazásokat ajánlott kizárni az ellenőrzésből, melyek a kommunikáció ellenőrzése esetén nem működnek megfelelően.

A listában automatikusan megjelennek a futó alkalmazások és szolgáltatások. A **Hozzáadás** gombra kattintva a protokollszűrési listában meg nem jelenített alkalmazások közül is választhat.

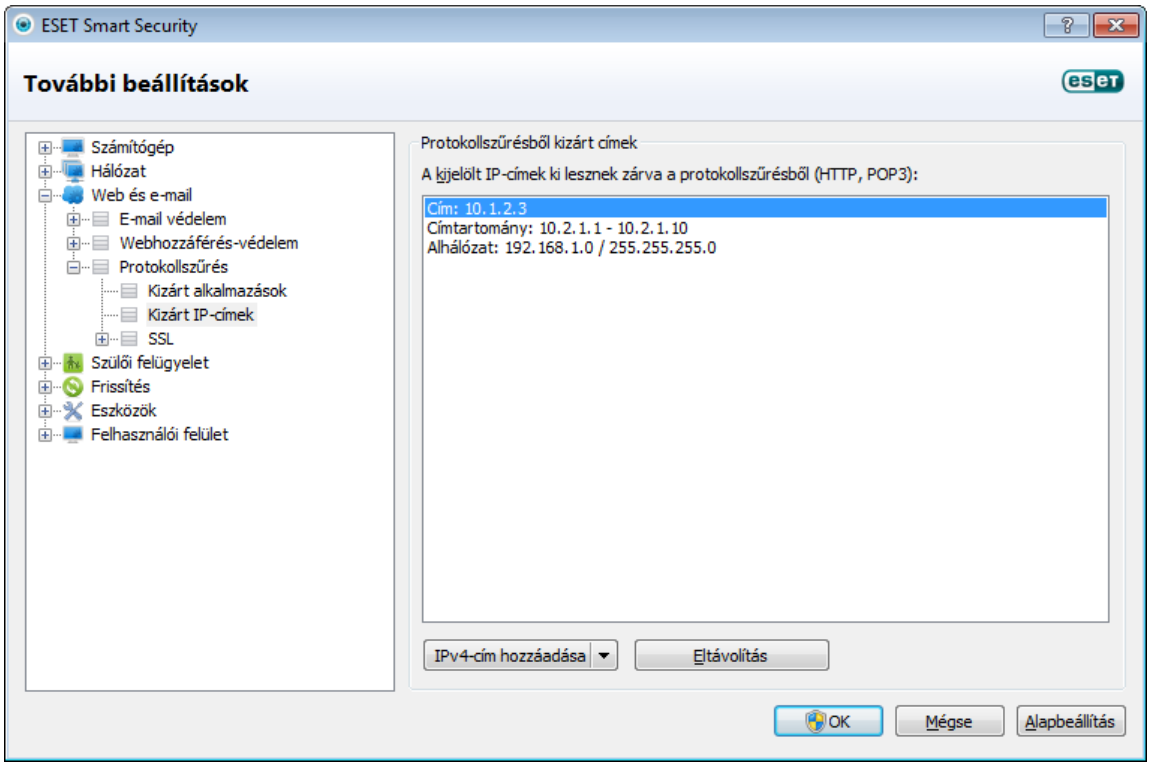


4.3.4.2 Kizárt címek

A listában szereplő címeken nem végez tartalomszűrést a rendszer. Az adott címekhez irányuló és onnan eredő HTTP- és POP3-alapú adatforgalmon a program nem végez kártevő-ellenőrzést. A listára csak megbízható címeket ajánlott felvenni.

IPv4-cím hozzáadása – A gombra kattintva felvehet egy újabb olyan távoli IP-címet, -címtartományt vagy -alhálózatot, amelyre alkalmazni szeretné ezt a szabályt.

Eltávolítás – A kijelölt bejegyzések eltávolítása a listáról.



4.3.4.3 SSL-protokollszűrés

Az ESET Smart Security lehetővé teszi az SSL protokollba burkolt más protokollok ellenőrzését. Az SSL protokollal védett kommunikáció ellenőrzése többféleképp is beállítható. Az ellenőrzés a megbízható, az ismeretlen és az SSL protokollal védett kommunikáció ellenőrzéséből kizárt tanúsítványokon alapul.

Az SSL protokoll ellenőrzése minden esetben – Jelölje be ezt a választógombot, ha az ellenőrzésből kizárt tanúsítványokkal védett kommunikáció kivételével az SSL protokoll által védett összes kommunikációt ellenőrizni szeretné. Az ismeretlen, aláírt tanúsítványokat használó új kapcsolatok létesítésekor a felhasználó nem kap értesítést az új tanúsítványról, és a kommunikációt a program automatikusan szűrni fogja. Ha a felhasználó saját maga által megbízhatóként megjelölt (a megbízható tanúsítványok listájához hozzáadott), enélkül azonban nem megbízható tanúsítvánnyal rendelkező szervert ér el, a program engedélyezi a kommunikációt a szerverrel, és szűri a kommunikációs csatornát.

Rákérdezés a nem látogatott helyekre (kivételek megadhatók) – Ha SSL protokollal védett, de ismeretlen tanúsítvánnyal rendelkező webhelyet látogat meg, megjelenik egy műveletválasztási párbeszédpanel. Ez a mód lehetővé teszi, hogy tanúsítványokat helyezzen az ellenőrzésből kizárt SSL-tanúsítványok listájára.

Az SSL protokoll ellenőrzésének mellőzése – Ha ezt a választógombot jelöli be, a program nem ellenőrzi az SSL protokollon keresztül zajló kommunikációt.

Létrehozott kivételek alkalmazása tanúsítványok alapján – A jelölőnégyzet bejelölésével engedélyezheti az SSL-alapú kommunikációban kivételként megadott kizárt és megbízható tanúsítványok figyelembevételét. A jelölőnégyzet engedélyezéséhez fentebb **Az SSL protokoll ellenőrzése minden esetben** választógombot kell bejelölni.

A 2-es verziójú elavult SSL protokollt használó titkosított kommunikáció tiltása – A program automatikusan letiltja az SSL protokoll korábbi verzióit használó kommunikációt.

4.3.4.3.1 Tanúsítványok

Az SSL-alapú kommunikáció böngészőkben vagy levelezőprogramokban való megfelelő működéséhez az ESET, spol s r. o. legfelső szintű tanúsítványát hozzá kell adni az ismert legfelső szintű tanúsítványok (kibocsátók) listájához. Erre szolgál a **Legfelső szintű tanúsítvány hozzáadása az ismert böngészőkhöz** jelölőnégyzet, melynek bejelölésével a program automatikusan hozzáadja az ESET legfelső szintű tanúsítványát az ismert böngészőkhöz (például Opera, Firefox). A rendszer tanúsítványtárolóját használó böngészők (például az Internet Explorer) esetén a tanúsítvány hozzáadása automatikusan történik. Ha a tanúsítványt nem támogatott böngészőben szeretné beállítani, válassza a **Tanúsítvány megtekintése** > **Részletek** > **Másolás fájlba** lehetőséget, majd importálja manuálisan a böngészőbe a fájlba exportált tanúsítványt.

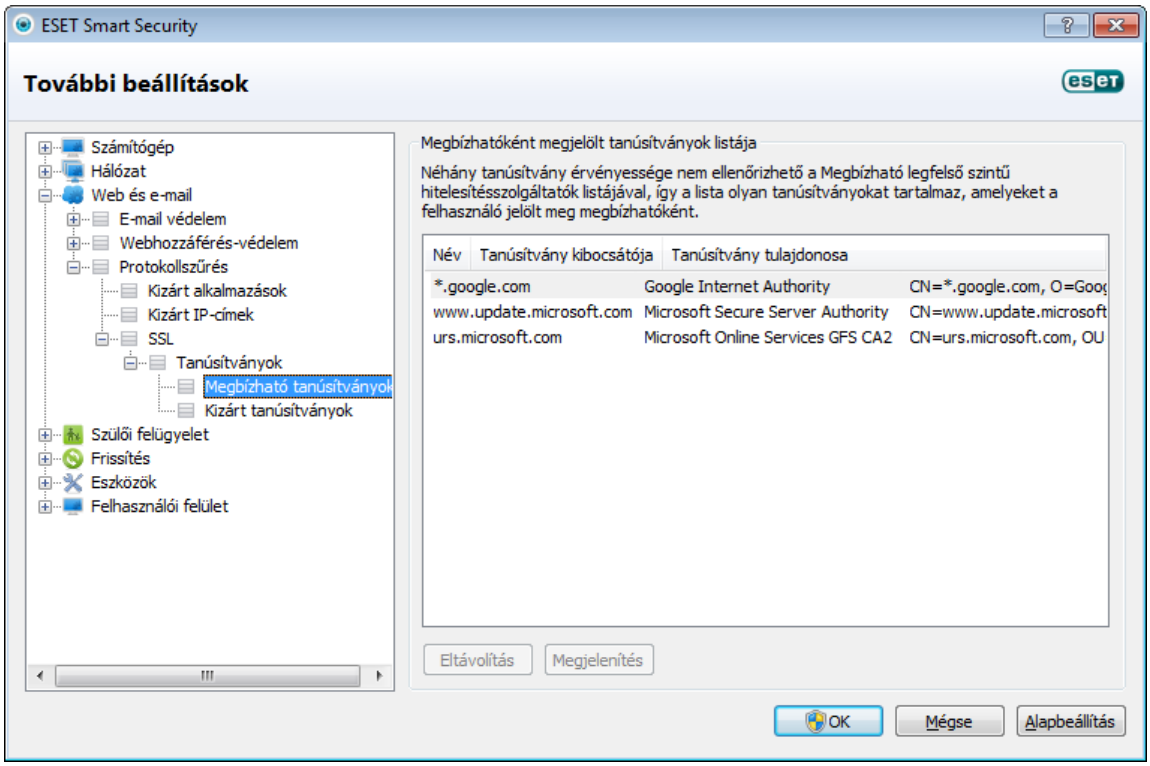
Egyes tanúsítványok nem ellenőrizhetők a megbízható legfelső szintű hitelesítésszolgáltatók listájával (például a VeriSign hitelesítésszolgáltató által). Ezek a tanúsítványok egy webszerver vagy egy kisebb cég rendszergazdája által készített, önaláírt tanúsítványok, és nem jelentenek feltétlenül kockázatot. A legtöbb nagy szervezet (például a bankok) legfelső szintű hitelesítésszolgáltató által aláírt kibocsátott tanúsítványokat használ. Ha a **Kérdezzen rá a tanúsítvány érvényességére** választógomb van bejelölve (ez az alapértelmezett beállítás), a titkosított kapcsolatok létesítésekor választania kell egy műveletet. A műveletválasztó párbeszédpanelen eldöntheti, hogy megbízhatóként vagy kizártként jelöl-e meg egy tanúsítványt. Ha egy tanúsítvány nem szerepel a megbízható legfelső szintű tanúsítványok listájában, az ablak színe piros lesz, ellenkező esetben zöld.

Amennyiben a **Tiltsa le a tanúsítványt használó kommunikációt** választógombot jelöli be, a program automatikusan blokkolja a nem ellenőrzött tanúsítványokat használó webhelyek titkosított kapcsolatait.

Az érvénytelen vagy sérült tanúsítványok lejártak, vagy helytelenül lettek önaláírva. Az ilyen tanúsítványokon alapuló kommunikációt ajánlott letiltani.

4.3.4.3.1.1 Megbízható tanúsítványok

Az ESET Smart Security által a megbízható tanúsítványok tárolására használt, integrált Megbízható legfelső szintű hitelesítésszolgáltatók tároló mellett saját listát is készíthet a megbízható tanúsítványokról. Ezeket a **További beállítások** (F5) > **Web és e-mail** > **Protokollszűrés** > **SSL** > **Tanúsítványok** > **Megbízható tanúsítványok** lehetőséget választva tekintheti meg. Az ESET Smart Security az ebben a listában szereplő tanúsítványokat is felhasználja a titkosított kommunikáció tartalmának ellenőrzéséhez.



Az **Eltávolítás** gombra kattintva törölheti a listában kijelölt tanúsítványt. A **Megjelenítés** gombra kattintva (vagy a tanúsítványra duplán kattintva) megtekintheti a kijelölt tanúsítvány adatait.

4.3.4.3.1.2 Kizárt tanúsítványok

A Kizárt tanúsítványok szakasz tartalmazza a biztonságosnak tartott tanúsítványokat. A listabeli tanúsítványokkal hitelesített titkosított kommunikáció tartalmán a program nem végez kártevőkeresést. Csak azokat a bizonyíthatóan biztonságos webes tanúsítványokat ajánlott kizárni, melyek esetében nincs szükség a kommunikáció ellenőrzésére. Az **Eltávolítás** gombra kattintva törölheti a listában kijelölt tanúsítványt. A **Megjelenítés** gombra kattintva (vagy a tanúsítványra duplán kattintva) megtekintheti a kijelölt tanúsítvány adatait.

4.4 Szülői felügyelet

A **Szülői felügyelet** részben adhatja meg a szülői felügyeletre vonatkozó beállításokat, amelyek automatizált eszközök nyújtásával segítik a szülőket, hogy védelmezzék gyermekeiket és az eszközök, szolgáltatások használatával kapcsolatos korlátozásokat határozzanak meg. A cél a gyermekek és fiatal felnőttek megakadályozása abban, hogy nem megfelelő vagy káros tartalmat megjelenítő oldalakhoz férjenek hozzá. A szülői felügyelet lehetővé teszi az esetlegesen nem kívánt tartalmú weblapok blokkolását. A szülők emellett akár 20 előre definiált webhely-kategória elérését is megtilthatják.

A **Szülői felügyelet** hivatkozásra kattintva a fő ablak három szakaszra bomlik.

Szülői felügyelet letiltása – A műveletre kattintva megjelenik A vírusvédelem ideiglenes kikapcsolása párbeszédpanel, ahol megadhatja, hogy mennyi ideig legyen tiltott ez a fajta védelem. A művelet helyén pedig a **Szülői felügyelet engedélyezése** művelet fog megjelenni, amire kattintva azonnal visszaállítható a védelem.

Megjegyzés: Fontos az ESET Smart Security beállításainak jelszavas védelme. A jelszót a Hozzáférési beállítások részben állíthatja be. Ha nem adott meg jelszót a beállítások védelméhez, a **Szülői felügyelet letiltása** hivatkozás alatt megjelenik *A szülői felügyelethez nincs megadva jelszavas védelem!* figyelmeztetés és a **Jelszó megadása** gomb. A **Szülői felügyelet** beállításcsoportban tett módosítások csak a normál felhasználói fiókokra vonatkoznak. Mivel az adminisztrátorok (a Rendszergazdák csoport tagjai) minden megszorítást mellőzhetnek, rájuk nincs hatással.

A második rész a fiókokra vonatkozik. Ha a **További beállítások > Szülői felügyelet > Fiókok > Hozzáadás** gombra kattintva már hozott létre új fiókot, az tartomány\fióknév formában jelenik meg, az Engedélyezve felirat társaságában. Az **Engedélyezve** feliratra kattintva megváltoztathatja a fiók felügyeleti módját. Az aktív fiókok alatt található egy Beállítások lehetőség. Itt láthatja a fiókhoz tartozó **Engedélyezett kategóriák listája**, **Tiltott és engedélyezett weboldalak** és **Gyors kijelölés** lehetőséget.

- **Engedélyezett kategóriák listája** – A bejelölt kategóriák engedélyezve vannak. Ha valamely kategóriát a választott fiók számára le kíván tiltani, szüntesse meg a hozzá tartozó jelölőnégyzet bejelölését. Ha egy kategória fölé viszi az egér mutatóját, megjelenik az adott kategóriába tartozó weboldalak listája.
- **Tiltott és engedélyezett weboldalak** – Az engedélyezett weboldalak listája a bal oldalon, a tiltott weboldalak listája pedig a jobb oldalon látható. Mindkét listához tartozik egy **Hozzáadás** és egy **Eltávolítás** gomb. Ha egy címet fel szeretne venni valamelyik listába, írja be az URL-címet a lista alatt található üres mezőbe, és kattintson a **Hozzáadás** gombra. A cím törléséhez jelölje ki az URL-címet a listában, majd kattintson az **Eltávolítás** gombra.
- **Gyors kijelölés** – Az egyes fiókokhoz tartozó **Engedélyezett kategóriák listája** másolásához válassza ki az egyik előre meghatározott profilt (**Gyermek**, **Szülő** és **Tizenéves**) vagy egy felhasználó által létrehozott fiókot, majd kattintson a **Másolás** gombra

Megjegyzés: Az egyes weboldalak tiltása és engedélyezése pontosabb szabályozást tesz lehetővé a teljes weboldal-kategóriák letiltásánál és engedélyezésénél. E beállítások megváltoztatásakor és valamely kategória/weboldal listára történő felvételekor legyen elővigyázatos.

Az utolsó csoportban két hivatkozás található:

Kivétel beállítása weboldalhoz – Itt állíthat be gyorsan kivételt a kiválasztott fiókhoz az egyes weboldalak számára. Írja be a weboldal URL-címét az **URL-cím** mezőbe, és az alatta látható listából válassza ki a fiókot. A **Letiltás** jelölőnégyzet bejelölésével letilthatja a weboldalt a megadott fiók számára. A jelölőnégyzet üresen hagyásával engedélyezheti a weboldalt. Az itt meghatározott kivételek elsőbbséget élveznek a kiválasztott fiók(ok) számára meghatározott kategóriákkal szemben. Ha például a **Hírek** kategória az adott fiók számára tiltott, de később egy engedélyezett híroldalt kivételként határoz meg, a fiók hozzáférhet a szóban forgó weboldalhoz.

Napló megjelenítése – Itt tekintheti meg a szülői felügyeleti tevékenység részletes naplóját (letiltott oldalak, a letiltott oldalhoz tartozó fiók, indok stb.). A naplóban a kiválasztott szempontok szerint **szűrést** is végezhet.

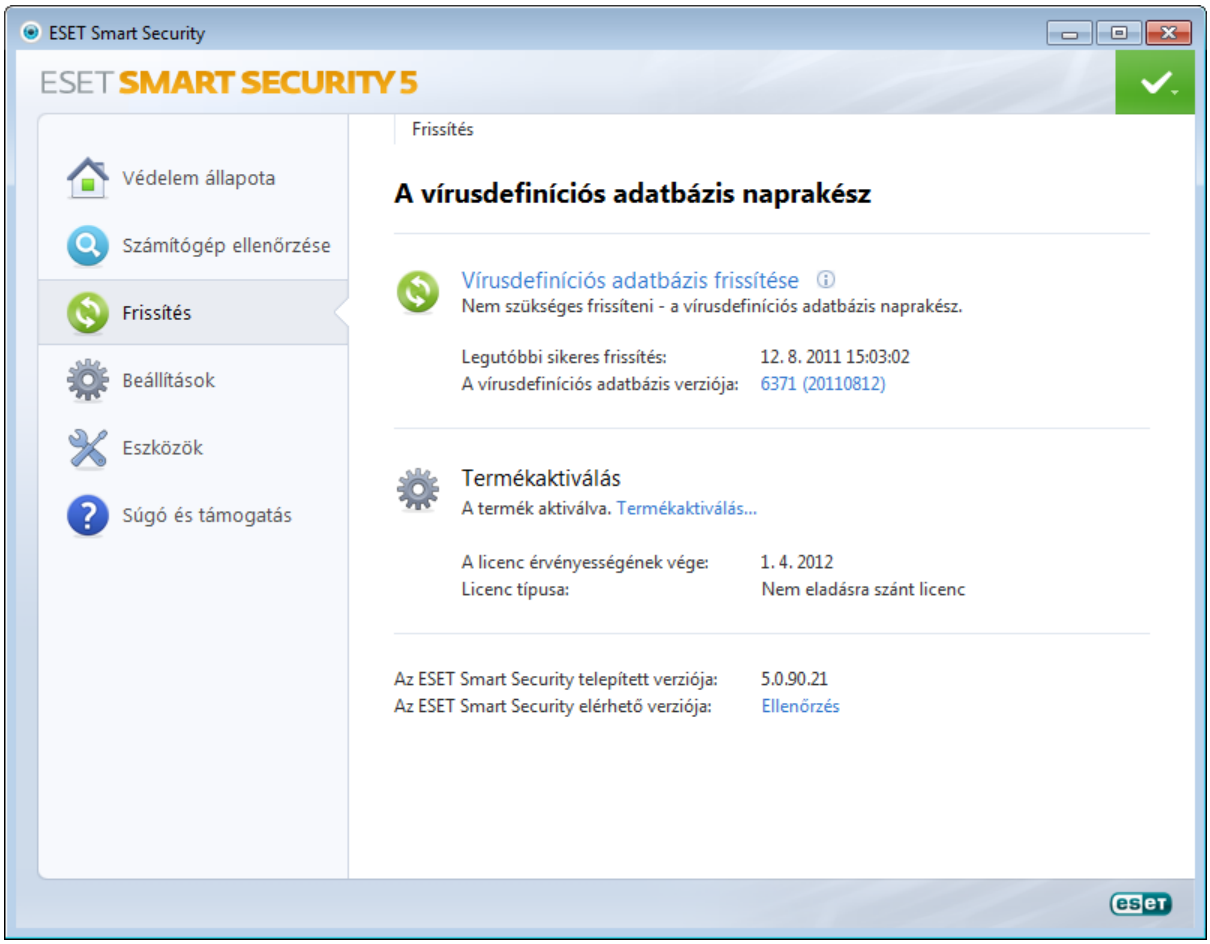
4.5 A program frissítése

Az ESET Smart Security rendszeres frissítésével biztosítható a leghatékonyabban a számítógép maximális védelme. A Frissítés modul két módon biztosítja, hogy a program mindig naprakész legyen: a vírusdefiníciós adatbázis és a rendszerösszetevők frissítésével.

A főmenü **Frissítés** lehetőségére kattintva megjelenítheti az aktuális frissítési állapotot, beleértve az utolsó sikeres frissítés dátumát és időpontját, valamint azt, hogy szükség van-e frissítésre. Az elsődleges ablakban látható a vírusdefiníciós adatbázis verziója is. Ez a verziószámjelzés egy hivatkozás az ESET weboldalára, ahol az adott frissítéssel hozzáadott vírusdefiníciók olvashatók.

Emellett itt található a frissítési folyamat kézi elindítására szolgáló – **A vírusdefiníciós adatbázis frissítése** – hivatkozás. A kártevők elleni maradéktalan védelem fontos összetevője a vírusdefiníciós adatbázis és a programösszetevők frissítése, ezért érdemes figyelmet fordítania a beállításukra és a működésükre. Ha a telepítés során nem adta meg a licenc részleteit, az ESET frissítési szervereihez való hozzáférés frissítésekor megadhatja a felhasználónevet és a jelszót.

Megjegyzés: A felhasználónevet és jelszót az ESET adja meg az ESET Smart Security megvásárlása után.



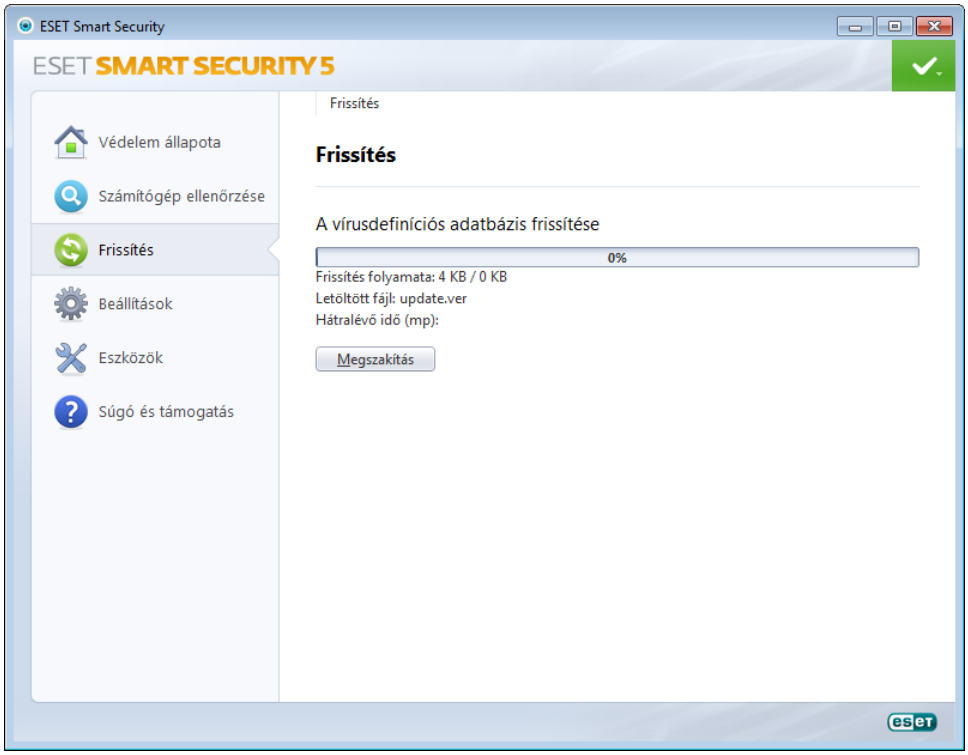
Legutóbbi sikeres frissítés – Itt látható a legutóbbi frissítés dátuma. Ennek közelmúltbeli dátumnak kell lennie, ugyanis ez jelzi, hogy a vírusdefiníciós adatbázis naprakész.

A vírusdefiníciós adatbázis verziója – A vírusdefiníciós adatbázis száma, amely egyben az ESET weboldalára mutató hivatkozásként is működik. Itt megtalálható az adott frissítésben szereplő összes vírusdefiníció listája. A verziószámra kattintva megtekintheti az adott frissítésbe foglalt definíciók listáját.

Kattintson az **Ellenőrzés** hivatkozásra az **ESET Smart Security** legújabb elérhető verziójának a kereséséhez.

A frissítési folyamat

A vírusdefiníciós adatbázis frissítése hivatkozásra kattintva megkezdődik a letöltési folyamat. Megjelenik a letöltési folyamatjelző sáv, illetve látható a letöltésből hátralévő idő. A frissítést a **Megszakítás** gombra kattintva megszakíthatja.

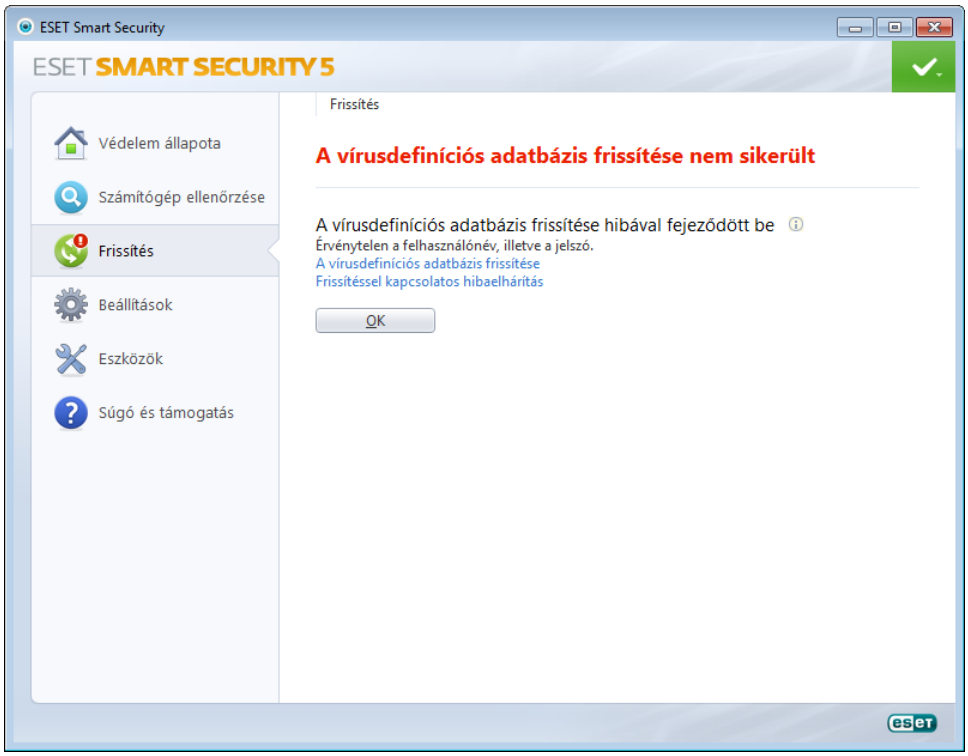


Fontos: Szokások körülmények között, a frissítések megfelelő letöltése esetén a **Nem szükséges frissíteni – a vírusdefiníciós adatbázis naprakész** üzenet jelenik meg a **Frissítés** ablakban. Ellenkező esetben ugyanis a program elavult, ami fokozza a fertőzés kockázatát. Ilyenkor a lehető leghamarabb frissítse a vírusdefiníciós adatbázist. Ellenkező esetben az alábbi üzenetek jelenhetnek meg:

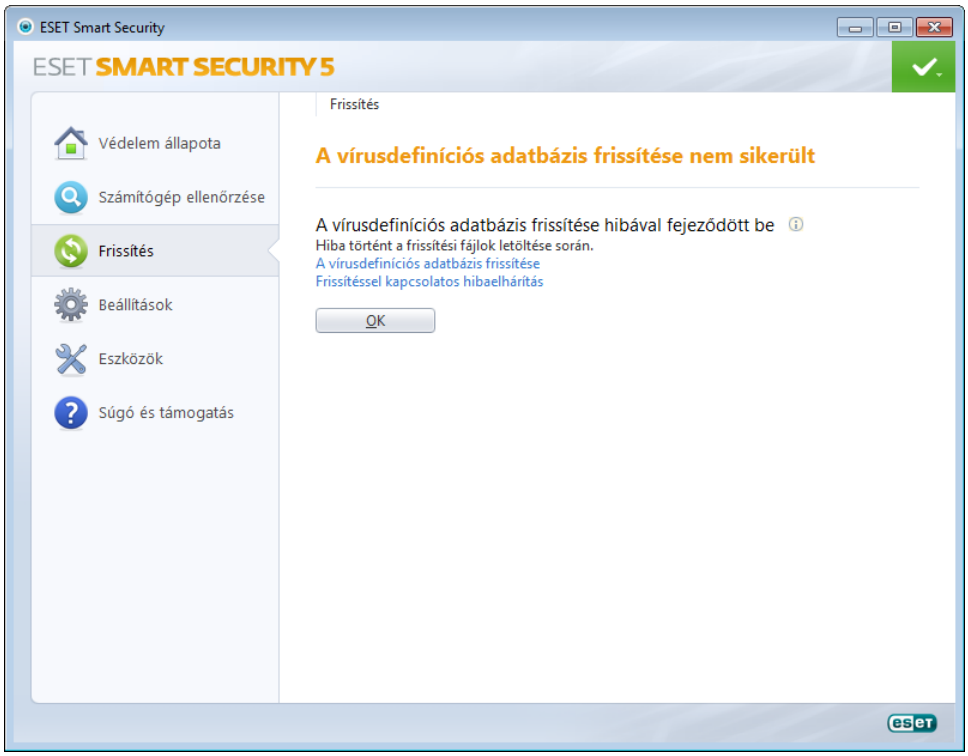
A vírusdefiníciós adatbázis elavult – Ez a hiba a vírusdefiníciós adatbázis frissítésére tett több sikertelen kísérletet követően jelenik meg. Javasolt ellenőrizni a frissítési beállításokat. Ennek a hibának a leggyakoribb oka a hitelesítő adatok téves megadása, illetve a csatlakozási beállítások helytelensége.

Az előző értesítés az alábbi két, sikertelen frissítésre vonatkozó üzenethez kapcsolódik:

A felhasználónév és a jelszó helytelenül van megadva a frissítési beállítások között. Azt javasoljuk, ellenőrizze a hitelesítési adatokat. A További beállítások ablak további frissítési lehetőségeket tartalmaz (megnyitásához kattintson a főmenü **Beállítások** ikonjára, majd a **További beállítások megnyitása** hivatkozásra, vagy nyomja le az F5 billentyűt). A további beállításokat tartalmazó listában kattintson a **Frissítés** > **Frissítés** lehetőségre.



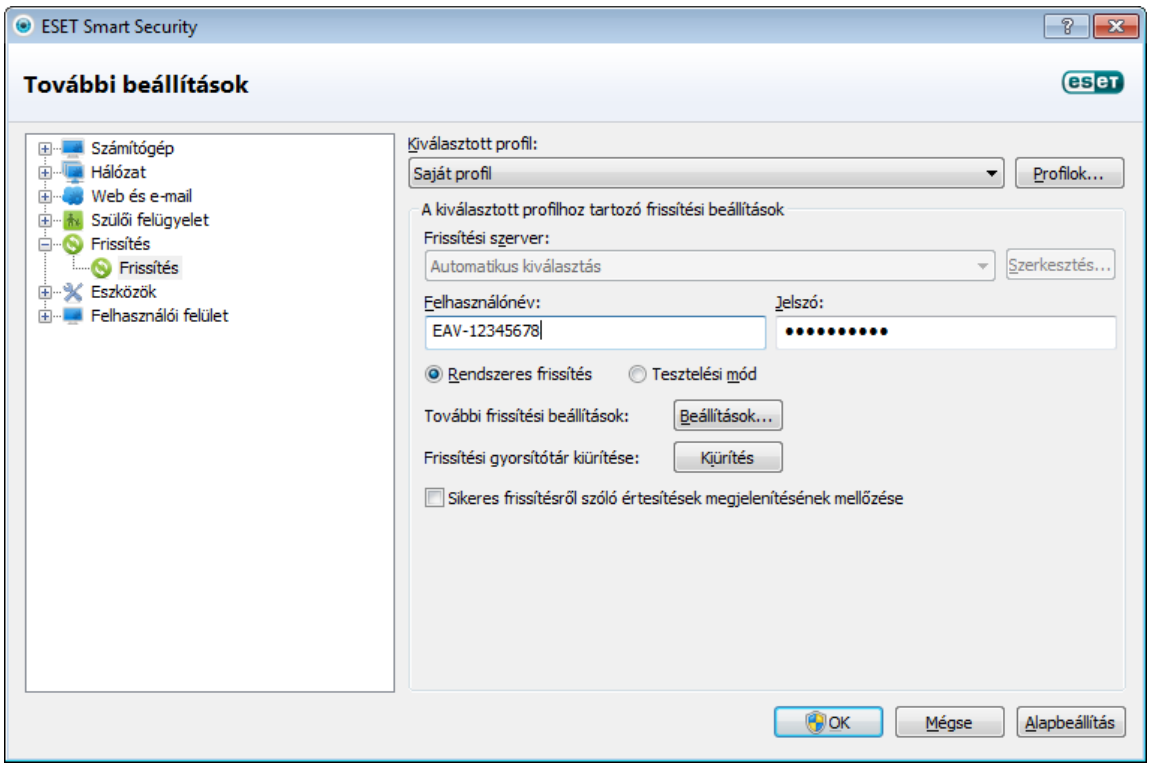
A vírusdefiníciós adatbázis frissítése nem sikerült – Elképzelhető, hogy a hibát a nem megfelelő internetes kapcsolatbeállítások okozzák. Ellenőrizze az internetkapcsolatot (ezt megteheti egy tetszőleges weboldal megnyitásával a böngészőben). Ha a webhely nem nyílik meg, valószínű, hogy nincs internetkapcsolat, vagy a számítógépen csatlakozási problémák léptek fel. Internetkapcsolati problémáit internetszolgáltatója felé jelezheti.



4.5.1 Frissítési beállítások

A frissítési beállításoknál adhatja meg a frissítés forrásának beállításait, például a frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat. A **Frissítési szerver** legördülő lista alapértelmezés szerinti **Automatikus kiválasztás** beállítása biztosítja, hogy a program – a lehető legkisebb hálózati forgalom mellett – automatikusan letöltse a frissítési fájlokat az ESET szerveréről. A frissítés beállításai a **További beállítások** fastruktúra (F5) **Frissítés** > **Frissítés** részében találhatók.

A program csak akkor tud frissíteni, ha minden paraméter pontosan be van állítva. Amennyiben tűzfalat használ, engedje ki a programot (ekrn.exe) a tűzfalon (HTTP-kommunikáció).



A **Kiválasztott profil** legördülő listában az aktuálisan használt frissítési profil látható. Új profil létrehozásához kattintson a **Profilok** gombra.

A rendelkezésre álló frissítési szerverek listája a **Frissítési szerver** legördülő listában található. A frissítési szerverek a frissítési fájlokat tartalmazó helyi vagy internetes szerverek. Amennyiben az ESET internetes szervereit kívánja használni, tartsa meg az alapértelmezett **Automatikus kiválasztás** beállítást. Új frissítési szerver hozzáadásához **A kiválasztott profilhoz tartozó frissítési beállítások** csoportban kattintson a **Szerkesztés**, majd a **Hozzáadás** gombra. Helyben létrehozott frissítési szerver alkalmazása esetén – ezt tükörnek is nevezik – a frissítési szervert a következőképpen kell beállítani:
http://számítógép_neve_vagy_IP_címe:2221.

A frissítési szerverekhez szükséges hitelesítés alapja a vásárlást követően létrehozott, és Önnek elküldött **Felhasználónév** és **Jelszó**. Helyi tükörszerver használata esetén a hitelesítés a szerver beállításaitól függ. Alapértelmezés szerint nincs szükség hitelesítésre, vagyis a **Felhasználónév** és a **Jelszó** mező üres.

A **Tesztelési mód** választógomb bejelölése esetén a frissítéskor a program letölti a bétamodulokat is, ami lehetővé teszi a felhasználónak a termék új szolgáltatásainak tesztelését. Az aktuális modulok listája a **Súgó és támogatás** > **Az ESET Smart Security névjegye** részben található. Kezdő felhasználóknak ajánlott megtartani a **Rendszeres frissítés** választógomb alapértelmezés szerinti bejelölését.

A frissítés további beállításait tartalmazó ablak megjelenítéséhez kattintson a **További frissítési beállítások** felirat mellett látható **Beállítások** gombra.

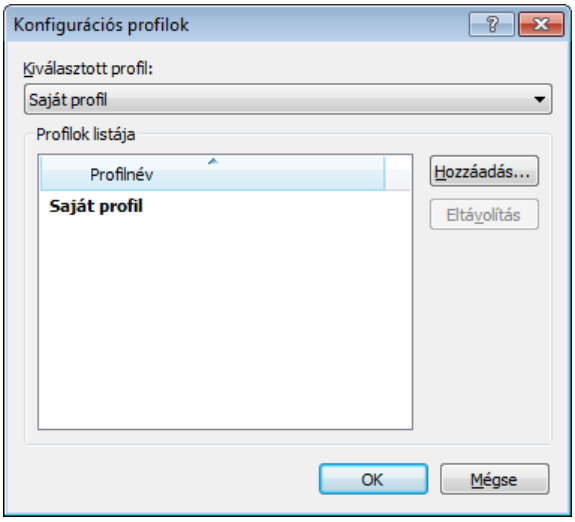
A frissítéssel kapcsolatos problémák esetén kattintson a **Kiürítés** gombra az ideiglenes frissítési fájlokat tartalmazó mappa kiürítéséhez.

Sikeres frissítésről szóló értesítések megjelenítésének mellőzése – A jelölőnégyzet bejelölésével kikapcsolja a képernyő jobb alsó sarkában, a tálcán megjelenő értesítéseket. A jelölőnégyzetet akkor célszerű bejelölni, ha egy alkalmazást teljes képernyős módban használ, vagy játékot futtat. Ne feledje, hogy a játékos üzemmód engedélyezésével minden értesítést kikapcsol.

4.5.1.1 Frissítési profilok

Frissítési profilok többféle frissítési konfigurációhoz és feladathoz létrehozhatók. A különféle frissítési profilok létrehozása különösen mobil felhasználók számára hasznos, akiknél az internetkapcsolat tulajdonságai gyakran változnak, és így létrehozhatnak egy alternatív profilt.

A **Kiválasztott profil** legördülő listában a jelenleg kiválasztott profil látható. Ez alapértelmezés szerint a **Saját profil** nevű profil. Új profil létrehozásához kattintson a **Profilok**, majd a **Hozzáadás** gombra, és írja be a profil nevét a **Profil neve** mezőbe. Új profil létrehozásakor átmásolhatja egy meglévő profil beállításait, ha kijelöli azt a **Beállítások másolása a következő profilból** legördülő listában.



A profilbeállítások párbeszédpaneljének frissítési szervereket tartalmazó legördülő listájában választhat egy frissítési szervert, de a párbeszédpanelen új szervert is megadhat. A jelenleg megadott frissítési szerverek a **Frissítési szerver** legördülő listában jelennek meg. Új frissítési szerver hozzáadásához **A kiválasztott profilhoz tartozó frissítési beállítások** csoportban kattintson a **Szerkesztés**, majd a **Hozzáadás** gombra.

4.5.1.2 További frissítési beállítások

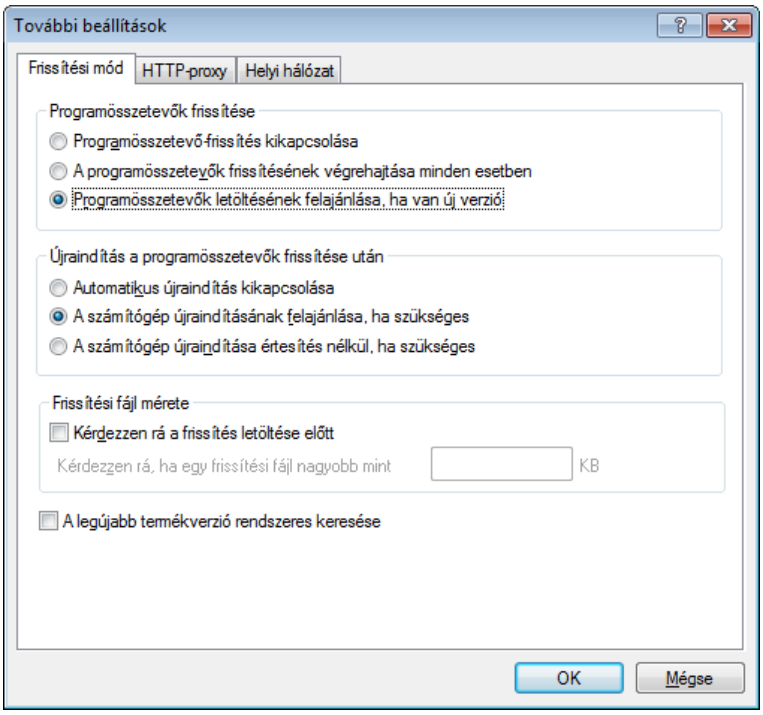
A további frissítési beállítások megjelenítéséhez kattintson a **Beállítások** gombra. A további frissítési beállítások a **frissítési mód**, a **HTTP-proxy** és a **helyi hálózat** konfigurálására szolgálnak.

4.5.1.2.1 Frissítési mód

A **Frissítési mód** lapon találhatók a programösszetevők frissítéséhez kapcsolódó beállítások. Megadható, hogy hogyan viselkedjen a program abban az esetben, ha valamelyik programösszetevőhöz frissítés érhető el.

A programösszetevő-frissítéssel új szolgáltatások válnak elérhetővé, vagy módosulnak a korábbi verziókban is rendelkezésre álló szolgáltatások. Automatikusan, felhasználói beavatkozás nélkül is végrehajtható, de a frissítésekről értesítés is kérhető. A programösszetevő-frissítés telepítése után a rendszer újraindítására lehet szükség. A **Programösszetevők frissítése** szakaszban három beállítás közül választhat:

- **Programösszetevő-frissítés kikapcsolása** - Soha nem kerül sor a programösszetevők frissítésére. Ezt a beállítást szervertelepítések esetén érdemes használni, hiszen a szerverek általában csak karbantartás esetén indíthatók újra.
- **A programösszetevők frissítésének végrehajtása minden esetben** - A rendszer automatikusan letölti és telepíti a programösszetevők frissítéseit. Ne felejtse el, hogy a számítógép újraindítására lehet szükség.
- **Programösszetevők letöltésének felajánlása, ha van új verzió** – Az alapértelmezett beállítás. A programösszetevők frissítésekor megjelenik egy párbeszédpanel, ahol megerősítheti vagy elutasíthatja a frissítést.



A programösszetevő-frissítéseket követően előfordulhat, hogy a modulok megfelelő működéséhez a számítógép újraindítása szükséges. Az **Újraindítás a programösszetevők frissítése után** részben a következő lehetőségek közül választhat:

- **Automatikus újraindítás kikapcsolása** – A számítógép újraindítása akkor sem történik meg, ha arra egyébként szükség lenne. Ez a beállítás nem ajánlott, mert előfordulhat, hogy a program a számítógép következő újraindításig nem működik megfelelően.
- **A számítógép újraindításának felajánlása, ha szükséges** – Ez az alapértelmezett beállítás. A programösszetevő-frissítés elvégzése után a rendszer egy párbeszédpanelen kéri a számítógép újraindítására.
- **A számítógép újraindítása értesítés nélkül, ha szükséges** – A programösszetevő-frissítés elvégzése után a rendszer újraindítja a számítógépet (ha szükséges).

Megjegyzés: A beállításokat az adott munkaállomástól függően kell kiválasztani. Érdemes figyelembe venni a munkaállomások és szerverek közötti különbségeket (súlyos károkat okozhat például, ha a frissítést követően automatikusan indítja újra a szervert).

A **Kérdezzen rá a frissítés letöltése előtt** választógomb bejelölése esetén értesítés jelenik meg az új frissítések kiadásakor.

Ha a frissítési fájl mérete a **Kérdezzen rá, ha egy frissítési fájl nagyobb mint** részben megadott értéknél nagyobb, a program értesítést jelenít meg.

A legújabb termékverzió rendszeres keresése beállítással engedélyezheti **A legújabb termékverzió rendszeres keresése** ütemezett feladat elvégzését (ezzel kapcsolatban a Feladatütemező című fejezet nyújt részletes tájékoztatást).

4.5.1.2.2 Proxyszerver

Az egyes frissítési profilokhoz tartozó proxyszerver-beállítások megnyitásához az F5 billentyűvel megnyitható További beállítások párbeszédpanel fájában kattintson a **Frissítés** ágra, majd a **További frissítési beállítások** felirat jobb oldalán található **Beállítások** gombra. Kattintson a **HTTP-proxy** fülre, és jelölje be az alábbi három választógomb egyikét:

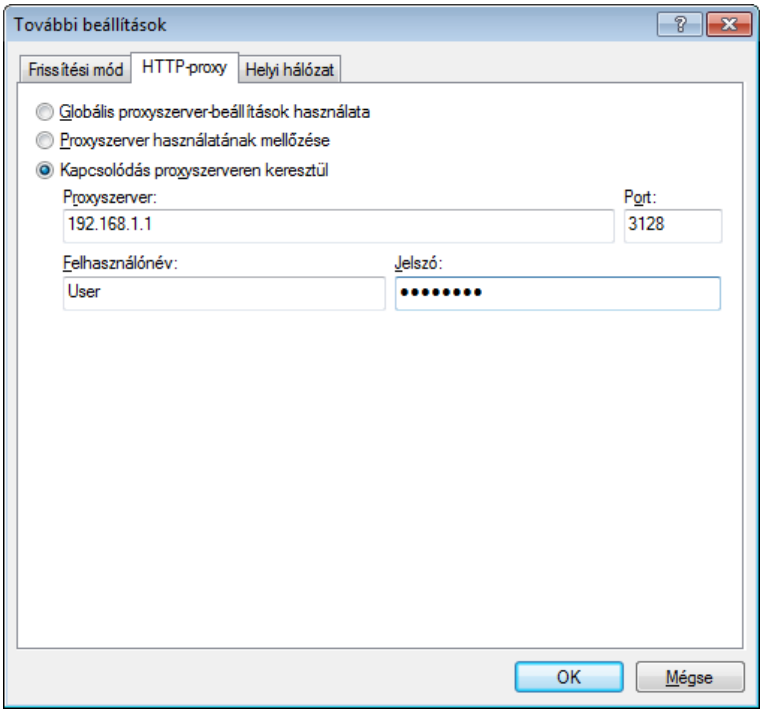
- **Globális proxyszerver-beállítások használata**
- **Proxyszerver használatának mellőzése**
- **Kapcsolódás proxyszerveren keresztül**

A **Globális proxybeállítások használata** választógomb bejelölése esetén a program a beállításfa **Eszközök** > **Proxyszerver** beállításcsoportjában korábban megadott beállításokat fogja figyelembe venni.

Ha az ESET Smart Security frissítéséhez nem használ proxyszervert, a **Proxyszerver használatának mellőzése** választógombot jelölje be.

A **Kapcsolódás proxyszerveren keresztül** választógombot kell bejelölnie az alábbi esetekben:

- Az ESET Smart Security frissítéséhez proxyszerver szükséges, de az eltér a globális beállítások között megadott proxyszervertől, melynek adatait az **Eszközök** > **Proxyszerver** lehetőséget választva tekintheti meg. Ebben az esetben még a következő beállításokat is meg kell adni: a **proxyszerver** címe és a kommunikációs **port** száma, valamint a **felhasználónév** és a **jelszó** – amennyiben a proxyszerver hitelesítést igényel.
- A proxyszerver beállításai a globális beállítások között nem szerepelnek, az ESET Smart Security azonban a frissítések beszerzése érdekében proxyszerverhez kapcsolódik.
- A számítógépe proxyszerveren keresztül csatlakozik az internetre. A beállításokat a program telepítés közben az Internet Explorer böngészőből veszi át, ám célszerű ellenőrizni, hogy azóta nem módosultak-e (például nem változott-e meg az internetszolgáltató), mert a program csak helyes beállításokkal tud csatlakozni a frissítési szerverekhez.



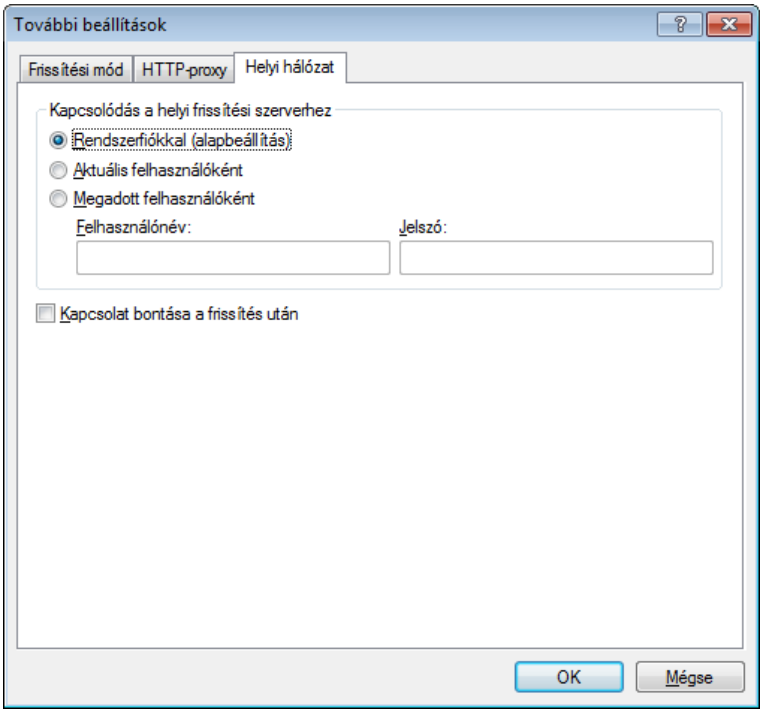
A proxyszerver alapértelmezett beállítása a **Globális proxybeállítások használata** lehetőség.

Megjegyzés: A hitelesítési adatok – például a **Felhasználónév** és **Jelszó** – megadására a proxyszerverhez való hozzáférés miatt van szükség. Csak akkor töltse ki ezeket a mezőket, ha a hozzáféréshez felhasználónév és jelszó szükséges. Ezek a mezők nem az ESET Smart Security licencében szereplő felhasználónév és jelszó megadására szolgálnak, és csak akkor szükséges kitölteni őket, ha az internet proxyszerveren keresztül történő eléréséhez felhasználónév és jelszó szükséges.

4.5.1.2.3 Csatlakozás a helyi frissítési szerverhez

Windows NT-alapú helyi frissítési szerverről történő frissítéskor alapértelmezés szerint minden hálózati kapcsolatot hitelesíteni kell. A legtöbb esetben a helyi rendszerfióknak nincs megfelelő hozzáférési joga a frissítési fájlok másolatát tartalmazó tükrözési mappához. Ebben az esetben írja be a felhasználónevet és a jelszót a frissítési beállításoknál, vagy adjon meg egy olyan fiókot, amellyel a program eléri a frissítési szervert (tükröt).

Ilyen fiók beállításához kattintson a **Helyi hálózat** fülre. A **Kapcsolódás a helyi frissítési szerverhez** szakaszban a **Rendszerfiókkal (alapbeállítás)**, az **Aktuális felhasználóként** és a **Megadott felhasználóként** választógombok közül választhat.



A **Rendszerfiókkal (alapbeállítás)** választógomb bejelölésekor a rendszerfiókot használhatja hitelesítésre. Ha a fő frissítési beállításoknál nem adta meg a hitelesítési adatokat, általában nem történik hitelesítés.

Ha azt szeretné, hogy a program az éppen bejelentkezett felhasználó fiókjával hitelesítse magát, jelölje be az **Aktuális felhasználóként** választógombot. E megoldás hátránya, hogy a program nem tud a frissítési szerverhez csatlakozni, ha nincs bejelentkezett felhasználó.

A **Megadott felhasználóként** beállítással egy adott felhasználói fiókot állíthat be a hitelesítéshez. Akkor alkalmazza ezt a módszert, ha a rendszerfiókkal történő kapcsolódás sikertelen volt. Ügyeljen arra, hogy a megadott felhasználó rendelkezzen olvasási joggal a frissítési fájlok mappájához a helyi szerveren. Ellenkező esetben a program nem tud kapcsolódni, és nem tudja letölteni a frissítéseket.

Figyelmeztetés: Ha az **Aktuális felhasználóként** vagy a **Megadott felhasználóként** választógomb van be jelölve, az identitásváltás hibát eredményezhet. Ezért célszerű a hálózati hitelesítési adatokat a fő frissítési beállításoknál megadni. Ebben a beállítási részben a hitelesítési adatokat a következőképpen kell beírni: *tartománynév\felhasználó* (munkacsoport esetében *munkacsoport\felhasználó*) és jelszó. Ha a helyi szerver HTTP-verziójáról frissít, nem szükséges hitelesítés.

Jelölje be a **Kapcsolat bontása a frissítés után** jelölőnégyzetet, ha azt szeretné, hogy a számítógép bontsa a kapcsolatot a helyi frissítési szerverrel (amennyiben a helyi frissítési szerver egy fájlszerverként is használt szerver, ne jelölje be a jelölőnégyzetet).

4.5.2 Frissítési feladatok létrehozása

A frissítések keresése és telepítése kézzel is elindítható, ha a fő ablakban a Frissítés fülre, majd a lapon **A vírusdefiníciós adatbázis frissítése** műveletre kattint.

A frissítések ütemezett feladatokként is futtathatók. Ha ütemezett feladatot szeretne beállítani, az **Eszközök** lapon válassza a **Feladatütemező** eszközt. Az ESET Smart Security programban alapértelmezés szerint az alábbi feladatok aktívak:

- **Rendszeres automatikus frissítés**
- **Automatikus frissítés a telefonos kapcsolat létrejötte után**
- **Automatikus frissítés a felhasználó bejelentkezése után**

Minden frissítési feladat módosítható az igényeinek megfelelően. Az alapértelmezett frissítési feladatok mellett a felhasználó által definiált konfigurációjú új feladatok is létrehozhatók. A frissítési feladatok létrehozásáról és beállításáról a Feladatütemező című fejezet nyújt részletes tájékoztatást.

4.6 Eszközök

Az **Eszközök** lapon található modulok segítik a program adminisztrációjának egyszerűsítését, és további lehetőségeket kínálnak a tapasztalt felhasználóknak.

A lapon az alábbi eszközök láthatók:

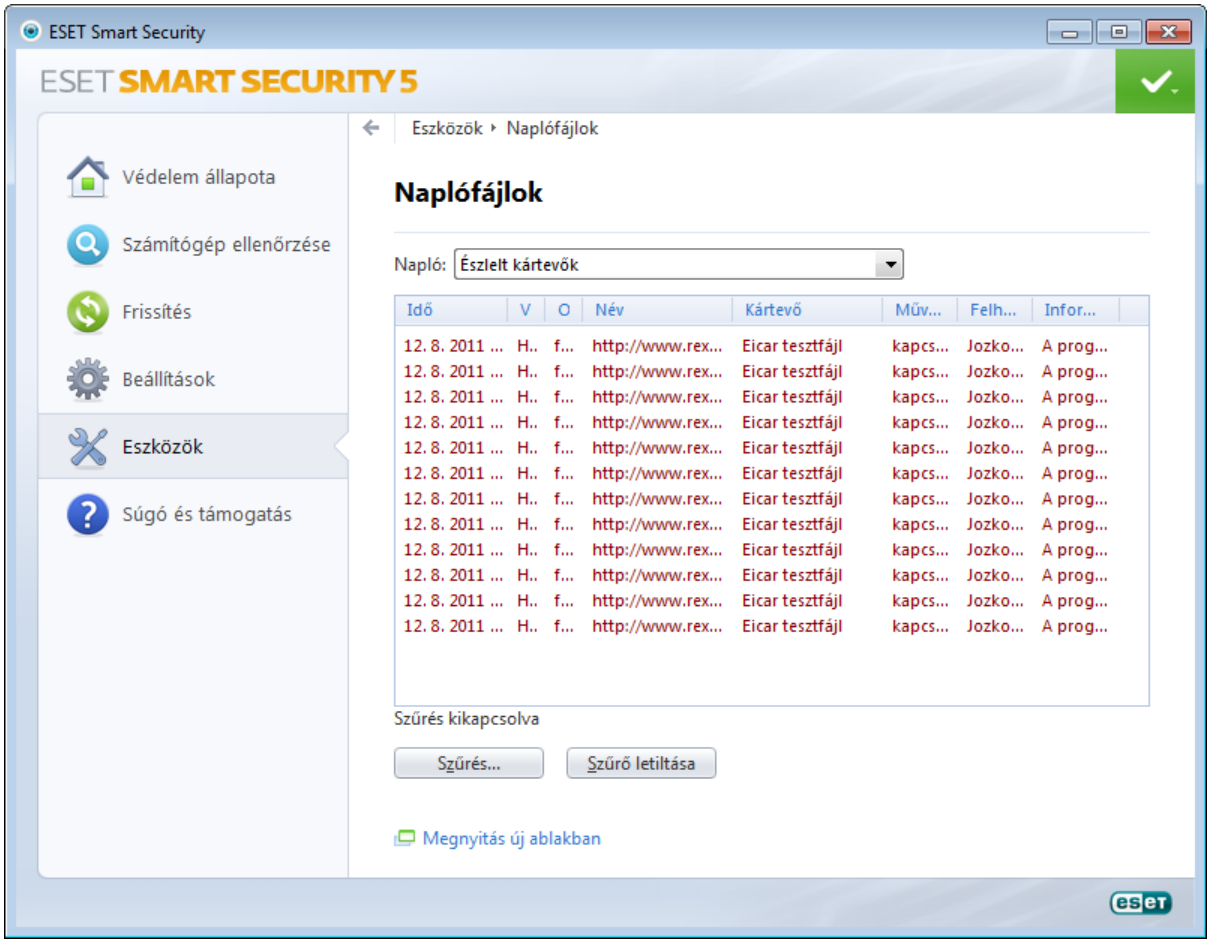
- Naplófájlok
- Védelem statisztikája
- Aktivitás
- Futó folyamatok
- Feladatütemező
- Karantén
- Hálózati kapcsolatok
- ESET SysInspector

Fájl elküldése elemzésre – A gyanús fájlok elküldése elemzésre az ESET víruslaborjaiba. A hivatkozásra kattintva egy párbeszédpanel jelenik meg, amelynek leírását a Fájlok elküldése elemzésre című szakaszban találja.

ESET SysRescue – Az ESET SysRescue létrehozási varázslójának indítása.

4.6.1 Naplófájlok

A Naplófájlok lap a fontos programeseményekről tájékoztatást, az észlelt veszélyekről áttekintést nyújt. A naplózás fontos szerepet tölt be a rendszerelemzésben, észlelésben és hibaelhárításban. A program a naplózást a háttérben aktívan, felhasználói beavatkozás nélkül végzi. Az információkat az aktuális naplórészletességi beállításoknak megfelelően rögzíti. A szöveges üzenetek és a naplófájlok közvetlenül az ESET Smart Security-programkörnyezetből is megtekinthetők, de ugyanitt nyílik lehetőség a naplófájlok archiválására is.



A naplófájlok a főmenü **Eszközök** lapjának **Naplófájlok** hivatkozására kattintva érhetők el. Jelölje ki a kívánt naplótípust az ablak tetején található **Napló** legördülő listában. A választható naplók az alábbiak:

- **Észlelt kártevők** – A kártevőnapló részletes információt szolgáltat az ESET Smart Security moduljai által észlelt fertőzésekről. Az információ tartalmazza az észlelés idejét, a fertőzés nevét és helyét, a végrehajtott műveletet és annak a felhasználónak a nevét, aki a fertőzés észlelésének idején be volt jelentkezve. A naplóbejegyzésre duplán kattintva külön ablakban megjelenik a részletes tartalom.
- **Események** – A program az ESET Smart Security által elvégzett összes műveletet rögzíti az eseménynaplókban. Az eseménynapló a programban történt eseményekre és hibákra vonatkozó információkat tartalmazza. Ezt a lehetőséget választva a rendszergazdák és a felhasználók megoldhatják az esetleges problémákat. Ezek az

információk gyakran hozzájárulnak a programban fellépő hibák megoldásához.

- **Számítógép-ellenőrzés** – Ezt a lehetőséget választva megtekintheti az összes korábbi kézi indítású és ütemezett ellenőrzés eredményét. Minden sor egy-egy számítógép-ellenőrzésnek felel meg. Az egyes bejegyzésekre duplán kattintva megjelennek az adott ellenőrzés részletes adatai.
- **Behatolásmegelőző rendszer** – A bejegyzésre megjelölt adott szabályok bejegyzéseit tartalmazza. A protokoll megjeleníti a műveletet meghívó alkalmazást, az eredményt (a szabály engedélyezett vagy letiltott volt-e) és a létrehozott szabály nevét.
- **Személyi tűzfal** – A tűzfalnapló megjeleníti a személyi tűzfal által észlelt összes távolról indított támadást, valamint a számítógép ellen indított támadások adatait. Az Esemény oszlopban láthatók az észlelt támadások, a Forrás oszlop további információkat szolgáltat a támadóról, a Protokoll oszlop pedig a támadáshoz használt protokollt ismerteti. A tűzfal naplójának elemzésével időben felderítheti a rendszer ellen végrehajtott behatolási kísérleteket, és megakadályozhatja a számítógéphez való jogosulatlan hozzáférést.
- **Levélszemétszűrő** – A levélszemétként megjelölt e-mail üzenetekhez tartozó bejegyzéseket tartalmazza.

A megjelenített információk mindegyik csoportból közvetlenül a vágólapra másolhatók (ehhez jelölje ki a kívánt bejegyzést, és kattintson a **Másolás** gombra, vagy nyomja le a Ctrl+C billentyűkombinációt). Több bejegyzés kijelöléséhez hosszan nyomja le a Ctrl vagy a Shift billentyűt.

Ha egy adott bejegyzésre kattint a jobb gombbal, megjelenítheti a helyi menüt, amelyben az alábbi parancsok találhatók:

- **Azonos típusú bejegyzések szűrése** – Ha aktiválja ezt a szűrőt, csak az azonos típusú bejegyzések jelennek meg (diagnosztika, figyelmeztetések stb.).
- **Szűrés/Keresés** – A beállításra kattintás után megjelenik a **Napló szűrése** ablak, ahol megadhatja a szűrési feltételeket.
- **Szűrő letiltása** – Törli a szűrőben megadott összes beállítást (a fentiek szerint).
- **Minden másolása** – Az ablakban lévő összes bejegyzésről másolja az információkat.
- **Törlés/Minden törlése** – Törli a kijelölt bejegyzés(eke)t vagy az összes megjelenített bejegyzést. A művelet végrehajtásához rendszergazdai jogosultságokra van szükség.
- **Exportálás** – Ezzel a lehetőséggel XML formátumban exportálhatja a bejegyzésekre vonatkozó információkat.
- **Napló görgetése** – Hagyja bejelölve ezt a parancsot, ha automatikusan szeretné görgetni a korábbi naplókat, és a **Naplófájlok** ablakban kívánja megnézni az aktív naplókat.

4.6.1.1 Naplókezelés

Az ESET Smart Security naplózási beállításai a program főablakában érhetők el. Kattintson a **Beállítások** > **További beállítások megnyitása** > **Eszközök** > **Naplófájlok** lehetőségre. A naplókkal kapcsolatos szakaszban szabályozható a naplók kezelése. A régebbi naplók automatikusan törlődnek, így nem foglalják a merevlemez-területet. A naplófájlokhoz az alábbi beállításokat adhatja meg:

Bejegyzés automatikus törlése – A jelölőnégyzet bejelölésekor a rendszer automatikusan törli a **Ha a bejegyzés X napnál régebbi** mezőben megadott számú napnál régebbi naplóbejegyzéseket.

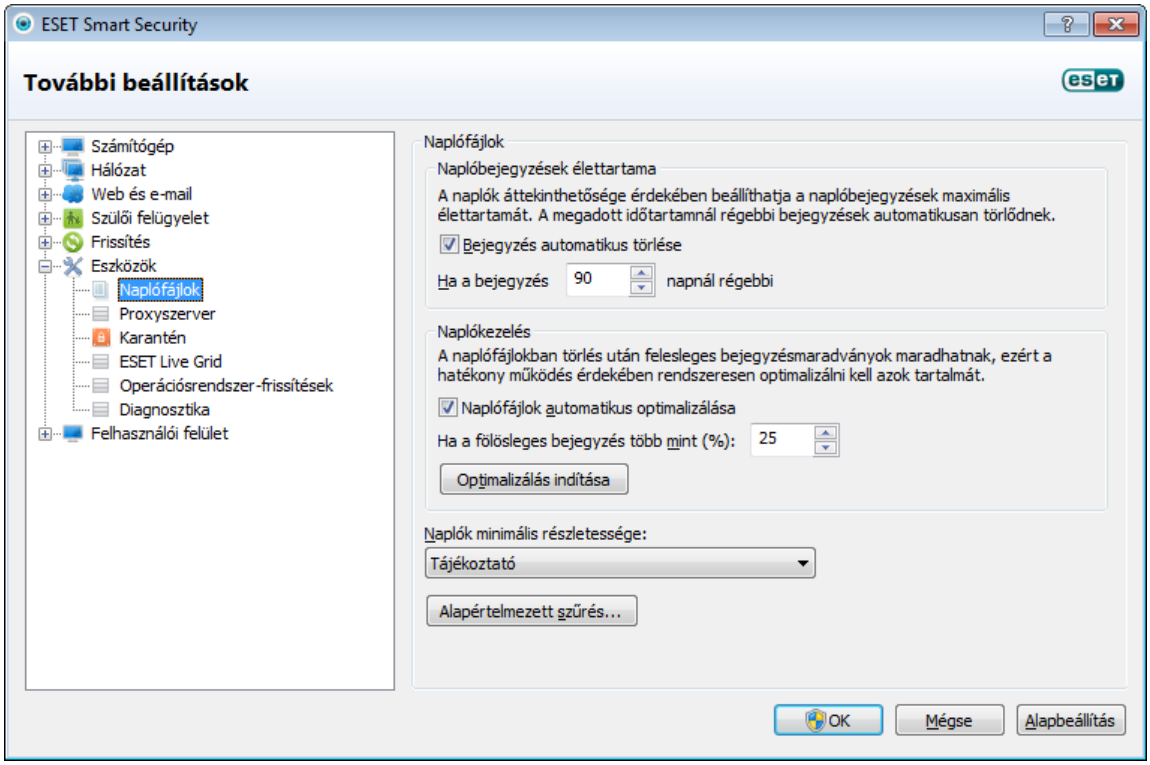
Naplófájlok automatikus optimalizálása – A jelölőnégyzet bejelölése esetén a naplófájlok töredezettségmentesítése automatikusan megtörténik, ha a százalékérték meghaladja a **Ha a fölösleges bejegyzés több mint (%)** mezőben megadott értéket.

Kattintson az **Optimalizálás indítása** gombra a naplófájlok töredezettségmentesítéséhez. A program a folyamat során az összes üres naplóbejegyzést eltávolítja, ami javítja a teljesítményt, és gyorsítja a naplók feldolgozását. A teljesítményjavulás különösen a nagyszámú bejegyzést tartalmazó naplófájloknál látványos.

Naplók minimális részletessége – Itt adhatja meg a naplózandó események minimális részletességi szintjét.

- **Diagnosztikai** – Ezt a lehetőséget választva a szoftver az alábbiak mellett az alkalmazás finomhangolásához szükséges információkat is bejegyzi a naplóba.
- **Tájékoztató** – Ezt a beállítást megadva a program a tájékoztató jellegű üzeneteket veszi fel a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett rekordokat).
- **Figyelmeztetések** – A program a kritikus figyelmeztetéseket és a figyelmeztető üzeneteket egyaránt megjeleníti.
- **Hibák** – Ezt a lehetőséget választva a program a *fájlletöltési* és a kritikus hibákat jegyzi be a naplóba.
- **Kritikus** – Ezt a lehetőséget választva a program csak a kritikus (például a vírusvédelem indításával, a személyi tűzfallal és egyebekkel kapcsolatos) hibákat naplózza.

Kattintson az **Alapértelmezett szűrés** gombra a Napló szűrése ablak megnyitásához. Jelölje be a naplókban megjelenítendő bejegyzéstípusokat, és kattintson az **OK** gombra.

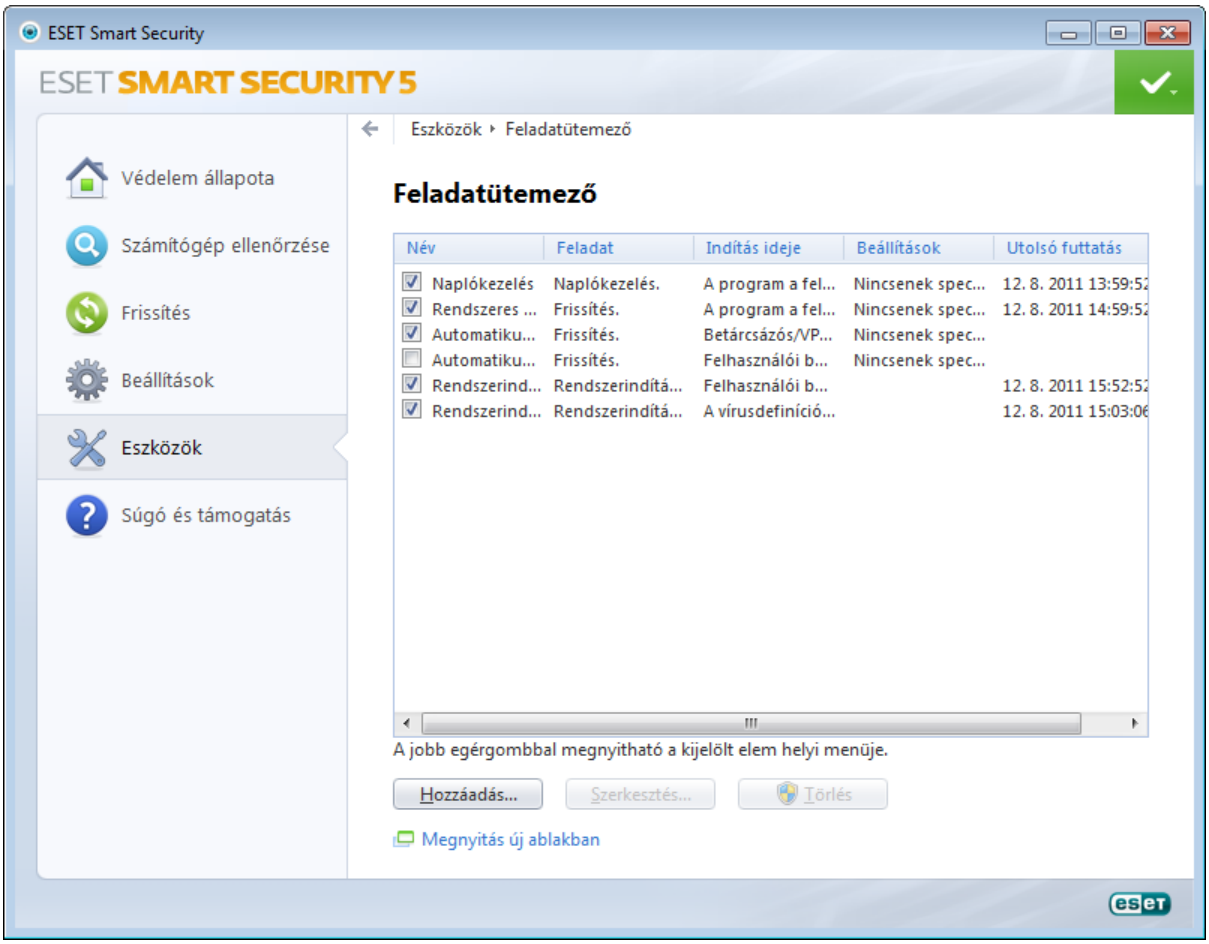


4.6.2 Feladatütemező

A Feladatütemező bizonyos feladatok (frissítés, számítógép ellenőrzése stb.) előre definiált beállításokkal történő indítását végzi.

A Feladatütemező az ESET Smart Security főmenüjéből érhető el az **Eszközök** lapon. A **Feladatütemező** valamennyi ütemezett feladat és beállított tulajdonságainak (például előre definiált dátum, időpont és ellenőrzési profil) összesített listáját tartalmazza.

A feladatütemező a következő feladatok időzített végrehajtására alkalmas: a vírusdefiníciós adatbázis frissítése, ellenőrzési feladatok, rendszerindításkor automatikusan futtatott fájlok ellenőrzése és naplókezelés. A Feladatütemező fő ablakából közvetlenül adhat hozzá vagy törölhet feladatokat. (Kattintson az ablak alján lévő **Hozzáadás** vagy **Törlés** gombra.) A Feladatütemező ablakban bárhol a jobb gombbal kattintva a következő műveleteket végezheti el: részletes adatok megjelenítése, a feladat azonnali végrehajtása, új feladat hozzáadása, meglévő feladat törlése. A feladatok előtt látható jelölőnégyzet bejelölésével, illetve a jelölések törlésével kapcsolhatja be és ki a feladatokat.



A **Feladatütemező** alapértelmezés szerint az alábbi ütemezett feladatokat jeleníti meg:

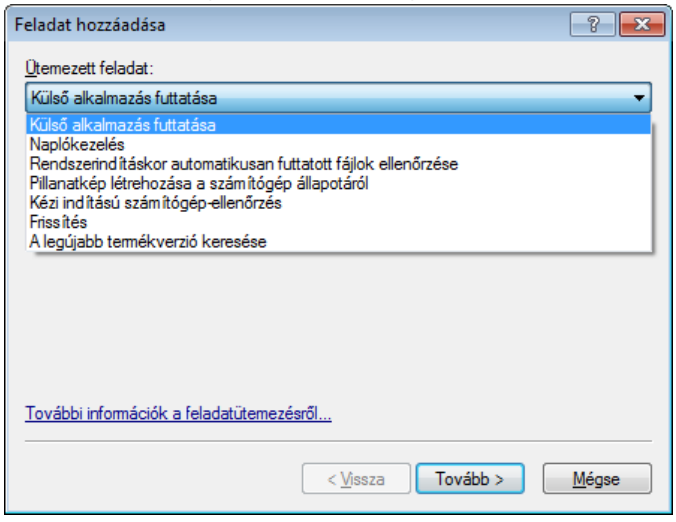
- **Naplókezelés**
- **Rendszeres automatikus frissítés**
- **Automatikus frissítés a telefonos kapcsolat létrejötte után**
- **Automatikus frissítés a felhasználó bejelentkezése után**
- **A legújabb termékverzió rendszeres keresése**
- **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** (a felhasználó bejelentkezése után)
- **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** (a vírusdefiníciós adatbázis sikeres frissítésekor)

A már meglévő (alapértelmezett és felhasználó által) ütemezett feladatok beállításainak módosításához kattintson a jobb gombbal a feladatra, és válassza a **Szerkesztés** parancsot, vagy jelölje ki a módosítandó feladatot, és kattintson a **Szerkesztés** gombra.

Új feladat hozzáadása

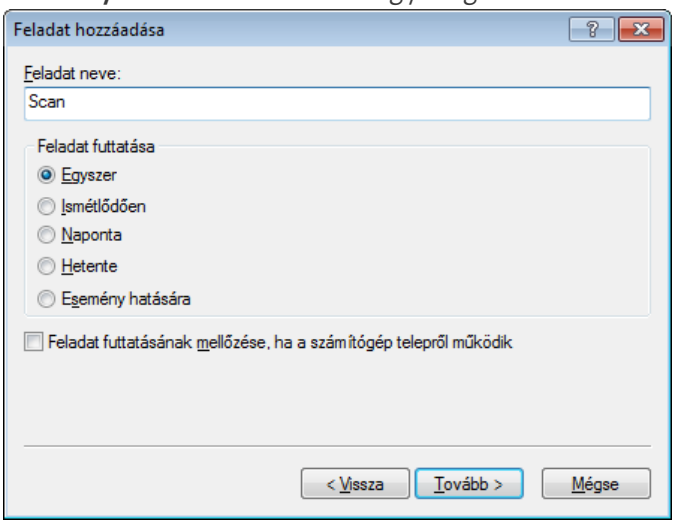
1. Kattintson az ablak alján található **Hozzáadás** gombra.

2. Jelölje ki a szükséges feladatot a legördülő listában.



3. Adja meg a feladat nevét, és válasszon egyet az időzítési lehetőségek közül:

   - **Egyszer** – A feladat csak egyszer, az előre meghatározott napon és időben lesz végrehajtva.
   - **Ismétlődően** – A feladat az órákban meghatározott időközönként lesz végrehajtva.
   - **Naponta** – A feladat minden nap a meghatározott időpontban fog futni.
   - **Hetente** – A feladat hetente egyszer vagy többször fog futni a kijelölt nap(ok)on és időpontban.
   - **Esemény hatására** – A feladat egy meghatározott esemény bekövetkezésekor lesz végrehajtva.



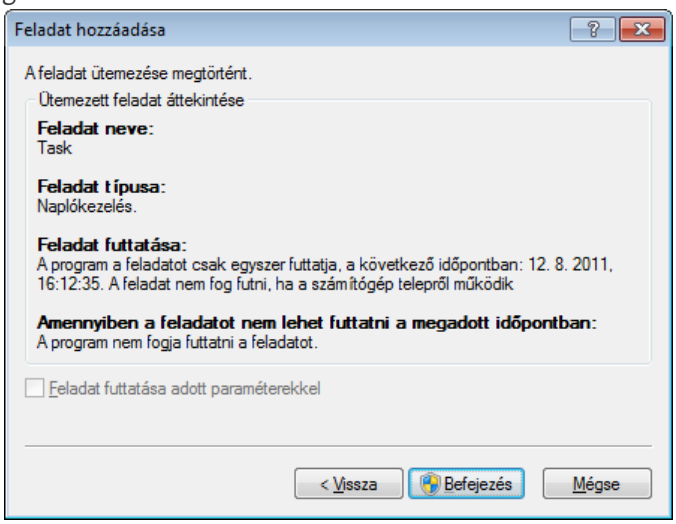
4. Az előző lépésben kiválasztott időzítési beállítástól függően az alábbi párbeszédpanelek egyike jelenik meg:

   - **Egyszer** – A feladat az előre meghatározott napon és időben lesz végrehajtva.
   - **Ismétlődően** – A feladat a meghatározott időközönként lesz végrehajtva.
   - **Naponta** – A feladat naponta ismétlődve, a megadott időpontban fut.
   - **Hetente** – A feladat a kijelölt napokon és időpontban fog futni.

5. Meghatározhatja, hogy mikor fusson a feladat, ha az előre meghatározott időben nem lehetett azt futtatni (például ki volt kapcsolva a számítógép). Választható lehetőségek:

   - Várjon a következő ütemezett időpontig
   - Hajtsa végre a feladatot az első adandó alkalommal
   - Azonnal hajtsa végre a feladatot, ha a legutóbbi végrehajtás óta a megadottnál hosszabb időtartam telt el

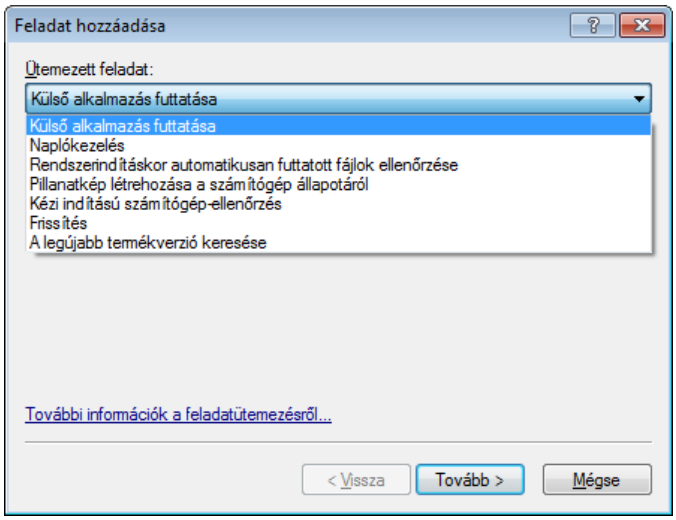
6. Az utolsó lépésben megtekintheti az ütemezni kívánt feladatot. A feladat alkalmazásához kattintson a **Befejezés** gombra.



4.6.2.1 Új feladatok létrehozása

Ha új feladatot szeretne létrehozni a Feladatütemezőben, kattintson a **Hozzáadás** gombra vagy a helyi menü **Hozzáadás** parancsára. Ötféle ütemezett feladat közül lehet választani:

- **Külső alkalmazás futtatása** – Ezen a lapon egy külső alkalmazás végrehajtásának ütemezése adható meg.
- **Naplókezelés** – A naplófájlokban törlés után felesleges bejegyzésmaradványok maradhatnak, ezért ez a feladat a hatékony működés érdekében optimalizálja azok tartalmát.
- **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** – A szoftver ellenőrzi azokat a fájlokat, amelyek futtatása rendszerindításkor vagy belépéskor engedélyezve van.
- **Pillanatkép létrehozása a számítógép állapotáról** – Az ESET SysInspector pillanatképének létrehozása a számítógépről; a rendszerösszetevőkre (például illesztőprogramokra, alkalmazásokra) vonatkozó részletes adatok összegyűjtése, és az egyes összetevők kockázati szintjének értékelése.
- **Számítógép ellenőrzése** – A számítógépe fájljainak és mappáinak ellenőrzése.
- **Frissítés** – Frissítési feladat ütemezése a vírusdefiníciós adatbázis és a rendszerösszetevők frissítésére.
- **A legújabb termékverzió keresése**



Mivel a **Frissítés** az egyik leggyakrabban használt ütemezett feladat, az alábbiakban megismerheti, hogy miként vehet fel újabb frissítési feladatokat.

Az **Ütemezett feladat** legördülő listában válassza a **Frissítés** beállítást. Kattintson a **Tovább** gombra, majd írja be a feladat nevét a **Feladat neve** mezőbe. Adja meg a feladat gyakoriságát. A választható lehetőségek az alábbiak: **Egyszer** , **Ismétlődően**, **Naponta**, **Hetente** és **Esemény hatására**. Telepről működő hordozható számítógép rendszererőforrásainak minimálisra csökkentéséhez jelölje be a **Feladat futtatásának mellőzése, ha a számítógép telepről működik** jelölőnégyzetet. A kiválasztott gyakoriságtól függően különböző frissítési paramétereket kell beállítani. Ezután meghatározhatja, hogy milyen műveletet hajtson végre a rendszer akkor, ha a feladat nem hajtható végre vagy nem fejezhető be az ütemezett időpontban. Az alábbi három lehetőség közül választhat:

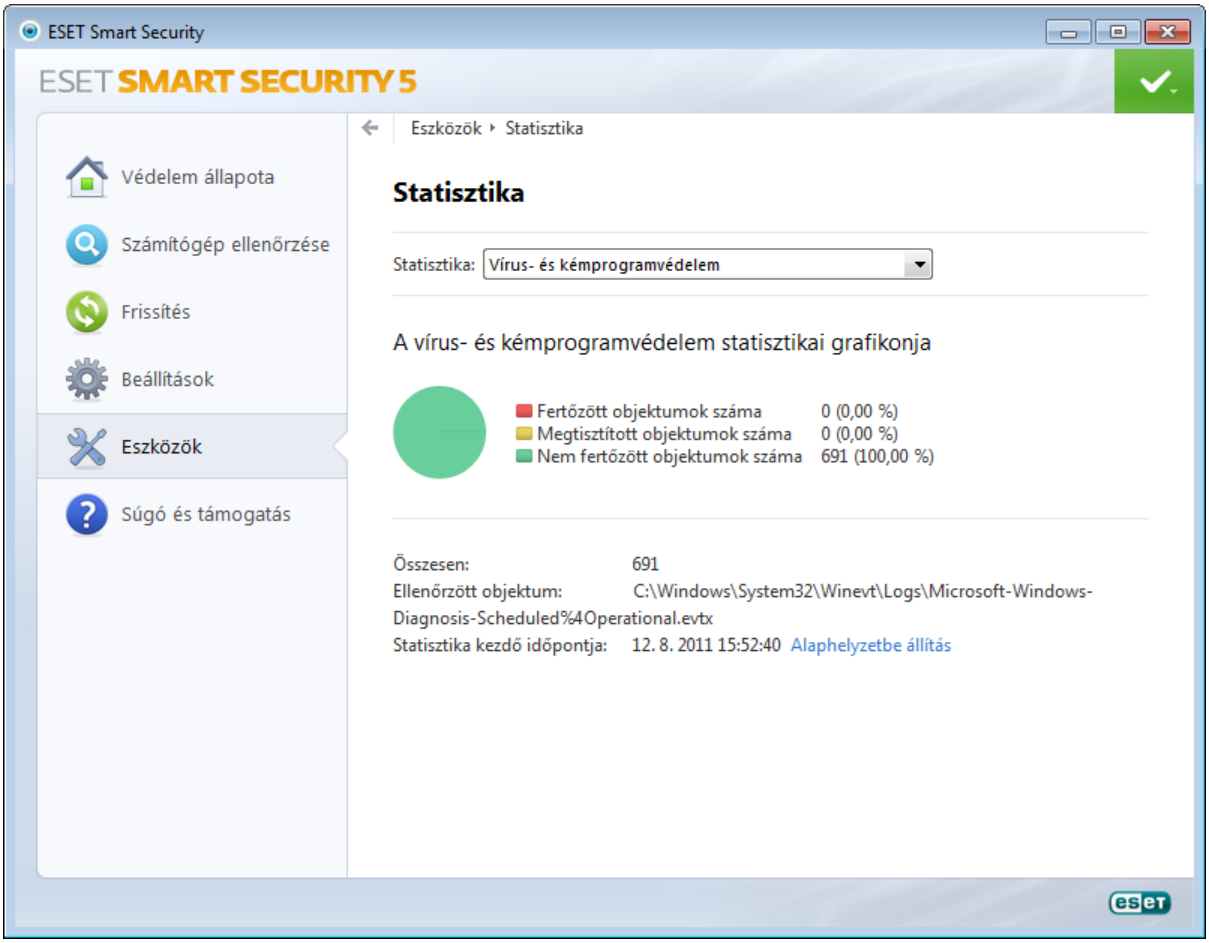
- **Várjon a következő ütemezett időpontig**
- **Hajtsa végre a feladatot az első adandó alkalommal**
- **Azonnal hajtsa végre a feladatot, ha a legutóbbi végrehajtás óta a megadottnál hosszabb időtartam telt el** (az időtartam az Időtartam görgetődobozban adható meg)

A következő lépésben a szoftver megjeleníti az aktuális ütemezett feladat teljes összegzését, és automatikusan bejelöli a **Feladat futtatása speciális paraméterekkel** jelölőnégyzetet. Kattintson a **Befejezés** gombra.

Megjelenik egy párbeszédpanel, amelyen kiválaszthatók az ütemezett feladathoz használandó profilok: megadható egy elsődleges és egy másodlagos profil – ez utóbbi akkor használható, ha a feladat nem hajtható végre az elsődleges profillal. Hagyja jóvá a művelet megkezdését a **Frissítési profilok** párbeszédpanel **OK** gombjára kattintva. A program felveszi az új ütemezett feladatot a jelenleg ütemezett feladatok listájára.

4.6.3 Védelem statisztikája

Ha meg szeretné tekinteni az ESET Smart Security védelmi moduljaival kapcsolatos statisztikai adatokat megjelenítő grafikont, az **Eszközök** lapon válassza a **Védelem statisztikája** lehetőséget. A **Statisztika** legördülő listában válassza ki a kívánt védelmi modult a hozzá tartozó grafikon és napló megtekintéséhez. Ha a jelmagyarázatban egy elem fölé viszi az egér mutatóját, a grafikonon csak az adott elem adatai jelennek meg.



A megtekinthető statisztikai grafikonok az alábbiak:

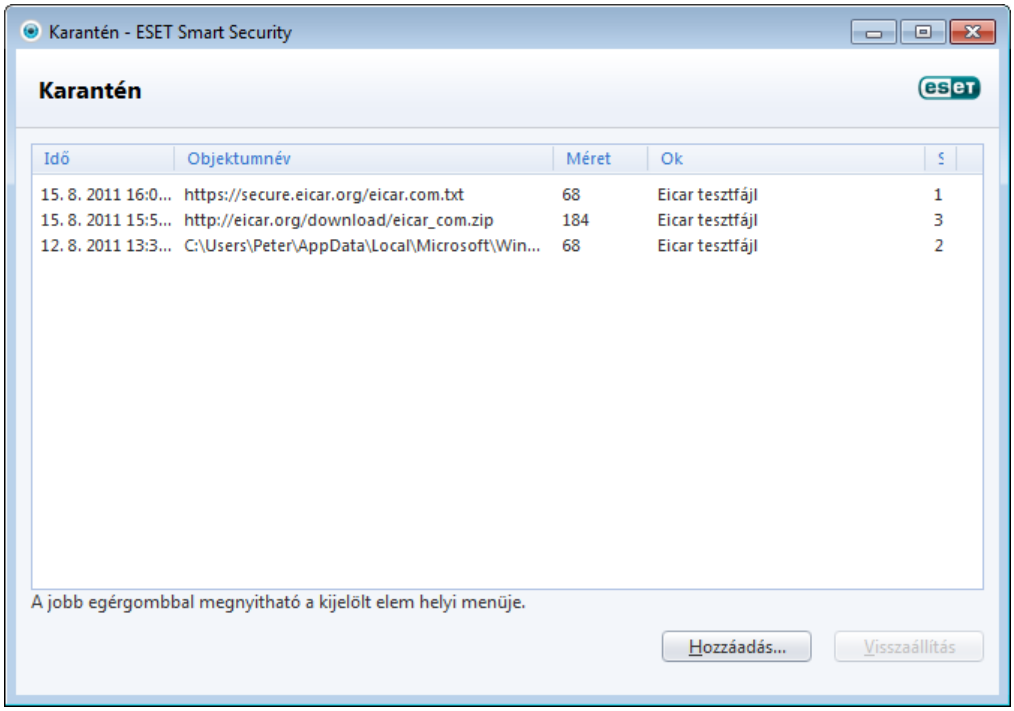
- **Vírus- és kémprogramvédelem** – A fertőzött és a megtisztított objektumok számát jeleníti meg.
- **Valós idejű fájlrendszervédelem** – Csak az olvasott és a fájlrendszerhez írt objektumokat jeleníti meg.
- **E-mail védelem** – Csak a levelezőprogramok által küldött vagy fogadott objektumokat jeleníti meg.
- **Webhozzáférés-védelem** – Csak a böngészők által letöltött objektumokat jeleníti meg.
- **E-mail védelem – levélszemétszűrés** – A levélszemétszűrő statisztikai előzményeit jeleníti meg a legutóbbi rendszerindításig visszamenőleg.

A statisztikai grafikon alatt látható az összes ellenőrzött objektum száma, a legutóbb ellenőrzött objektum és a statisztikai időbélyeg. Kattintson az **Alaphelyzetbe állítás** lehetőségre az összes statisztikai információ törléséhez.

4.6.4 Karantén

A karantén fő feladata a fertőzött fájlok biztonságos tárolása. A fájlokat akkor kell a karanténba helyezni, ha nem tisztíthatók meg, ha törlésük kockázattal jár vagy nem ajánlott, illetve ha az ESET Smart Security tévesen észlelte őket.

Bármilyen fájlt karanténba helyezhet. A szóban forgó fájlt akkor érdemes karanténba helyezni, ha viselkedése gyanús, a víruskereső azonban nem észleli. A karanténba helyezett fájlok elemzés céljából elküldhetők az ESET víruslaborjának.



A karanténmappában lévő fájlokat egy táblázat jeleníti meg, amelyben látható a karanténba helyezés dátuma és időpontja, a fertőzött fájl eredeti helyének elérési útja, a fájl bájtban megadott mérete, a karanténba helyezés oka (például a felhasználó vette fel az objektumot), és a fertőzések száma (például az, hogy egy több fertőzést is hordozó tömörített fájlról van-e szó).

4.6.4.1 Fájlok karanténba helyezése

Az ESET Smart Security automatikusan karanténba helyezi a törölt fájlokat (ha nem érvénytelenítette ezt a beállítást a riasztási ablakban). Szükség esetén bármely gyanús fájl karanténba helyezhető a **Karantén** gombra kattintással. Ebben az esetben a program nem távolítja el az eredeti fájlt az eredeti helyéről. A művelet a helyi menüből is végrehajtható: kattintson a jobb gombbal a **Karantén** ablakra, és válassza a **Karantén** parancsot.

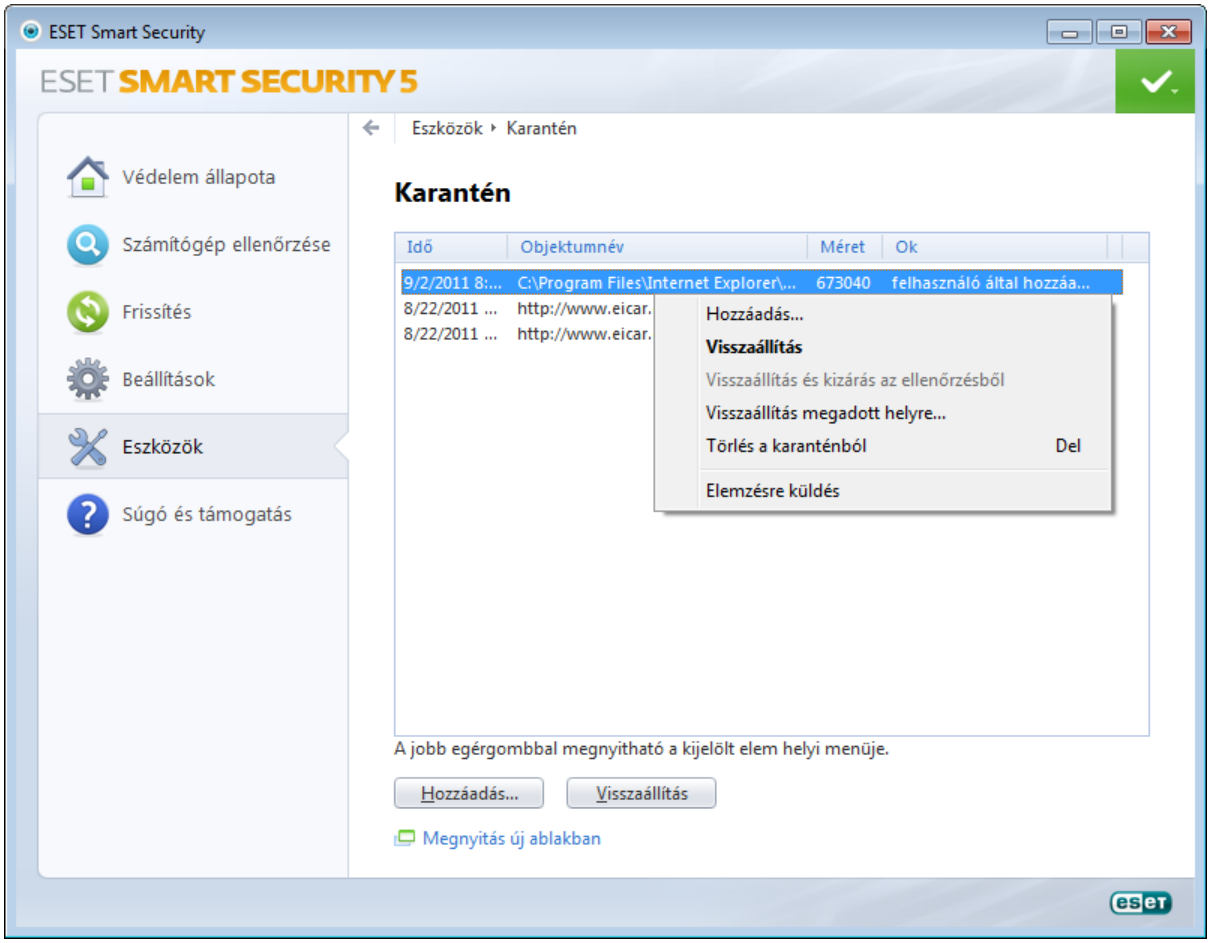
4.6.4.2 Visszaállítás a karanténból

A karanténba helyezett fájlok visszaállíthatók az eredeti helyükre. Erre a célra szolgál a karanténablakban lévő kérdéses fájlra a jobb gombbal kattintva megjelenő helyi menü **Visszaállítás** parancsa. A helyi menüben megtalálható a **Visszaállítás megadott helyre** parancs is, mellyel a törlés helyétől különböző mappába is visszaállíthatók a fájlok.

Megjegyzés: Ha a program tévesen helyezett karanténba egy fájlt, akkor visszaállítása után zárja ki azt az ellenőrzésből, és küldje el az ESET terméktámogatásának.

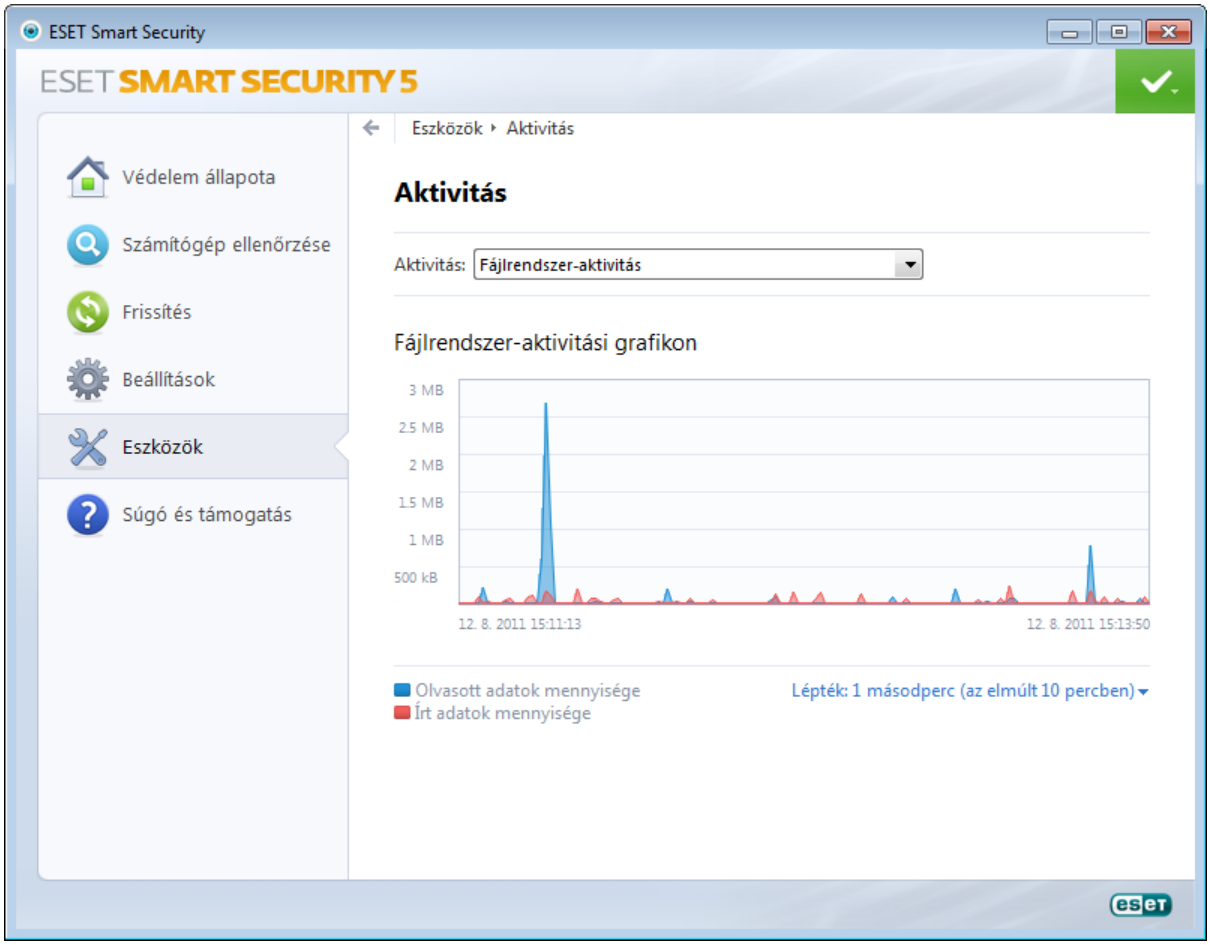
4.6.4.3 Fájl elküldése a karanténból

Ha karanténba helyezett egy, a program által nem észlelt gyanús fájlt, vagy ha egy adott fájlt a szoftver tévesen jelölt meg fertőzöttként (például a kód heurisztikus elemzése után), és ezért a karanténba helyezett, kérjük, küldje el a fájlt az ESET víruslaborjába. A karanténban lévő fájl elküldéséhez kattintson a jobb gombbal a fájlra, majd kattintson a helyi menü **Elemzésre küldés** parancsára.



4.6.5 Aktivitás

Az aktuális **fájlrendszer-aktivitás** grafikonos formában való megjelenítéséhez az **Eszközök** lapon válassza az **Aktivitás** lehetőséget. A grafikon alján egy idősor található, amely valós időben, a kiválasztott időköz alapján rögzíti a fájlrendszer-aktivitást. Az időköz változtatásához kattintson az ablak jobb alsó részén található **Lépték:** beállításra.



A választható lehetőségek az alábbiak:

- **Lépték: 1 másodperc (az elmúlt 10 percben)** – A grafikon másodpercenként frissül, az idősor pedig az elmúlt 10 percet fedi le.
- **Lépték: 1 perc (az elmúlt 24 órában)** – A grafikon percenként frissül, az idősor pedig az elmúlt 24 órát fedi le.
- **Lépték: 1 óra (az elmúlt hónapban)** – A grafikon óránként frissül, az idősor pedig az elmúlt hónapot fedi le.
- **Lépték: 1 óra (a kijelölt hónapban)** - – A grafikon óránként frissül, az idősor pedig a kijelölt hónapokat fedi le.

A **fájlrendszer-aktivitási grafikon** függőleges tengelye az olvasott (piros) és az írt adatokat (kék) jeleníti meg. Mindkét érték kilobájtban van megadva. Ha az egér mutatóját a grafikon alatti Olvasott adatok mennyisége vagy Írt adatok mennyisége felirat fölé viszi, a grafikon csak az adott aktivitástípushoz tartozó adatokat fogja megjeleníteni.

A **Hálózati aktivitás** grafikon az **Aktivitás** legördülő listában is elérhető. A **fájlrendszer-aktivitást** és a **hálózati aktivitást** megjelenítő grafikon megjelenése és beállításai attól eltekintve azonosak, hogy az utóbbi a fogadott adatok (piros) és az elküldött adatok (kék) mennyiségét jeleníti meg.

4.6.6 ESET SysInspector

Az ESET SysInspector egy alkalmazás, mely a számítógép részletes vizsgálatával adatokat gyűjt a rendszerösszetevőkről, például a telepített illesztőprogramokról és alkalmazásokról, a hálózati kapcsolatokról, a beállításjegyzék fontos bejegyzéseiről, valamint felméri ezek kockázati szintjét. Ez az információ segíthet a rendszer gyanús működését okozó esetleges szoftver- vagy hardver-inkompatibilitás és kártevőfertőzés felderítésében.

A SysInspector ablaka a létrehozott naplók alábbi adatait jeleníti meg:

- **Idő** – A napló létrehozásának időpontja.
- **Megjegyzés** – Egy rövid megjegyzés.
- **Felhasználó** – A naplót létrehozó felhasználó neve.
- **Állapot** - A napló létrehozásának állapota.

A választható műveletek az alábbiak:

- **Összehasonlítás** – Összehasonlít két meglévő naplót.
- **Létrehozás** – Új naplót hoz létre. Várja meg, amíg elkészül az ESET SysInspector naplója (az **Állapot** mezőben a Létrehozva felirat fog megjelenni).
- **Törlés** – Eltávolítja a kijelölt naplókat a listából.

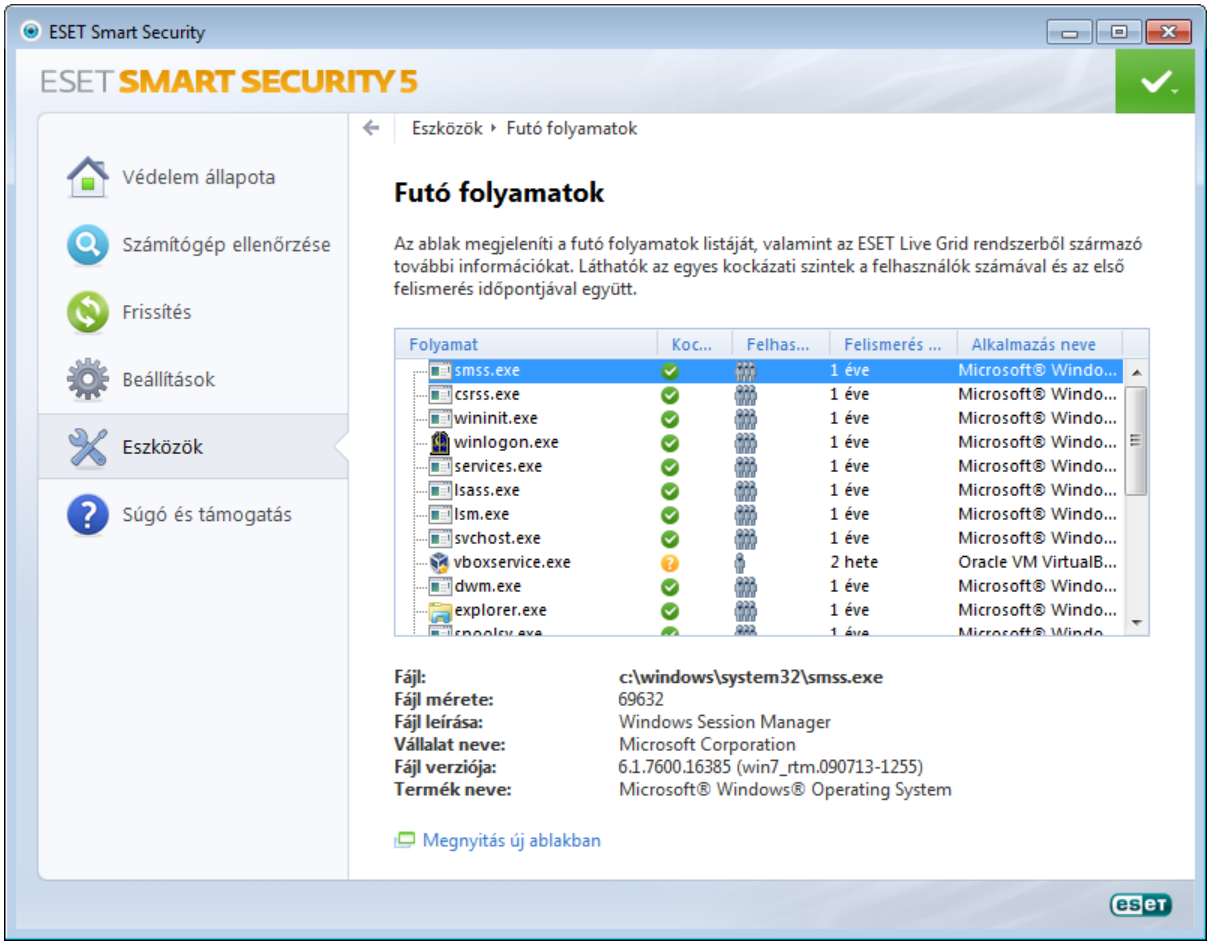
Ha a jobb gombbal a kijelölt naplók közül legalább egyre kattint, a helyi menüben az alábbi további parancsok láthatók:

- **Megjelenítés** – Megnyitja a kiválasztott naplót az ESET SysInspector alkalmazásban (ugyanezt az eredményt érheti el a naplóra duplán kattintva).
- **Minden törlése** – Törli az összes naplót.
- **Exportálás** – XML-fájlba exportálja a naplót (tömörített változatban is).

4.6.7 Futó folyamatok

A Felhőalapú megbízhatóság listában megtekintheti a futó programokat vagy folyamatokat. A megbízhatósági technológia révén az ESET azonnali és folyamatos tájékoztatást kap az új kártevőkről. Az ESET Smart Security által a futó folyamatokról szolgáltatott részletes adatok révén tudja az ESET Live Grid technológia védeni a felhasználókat.

Megjegyzés: Nem csak a futó programok és folyamatok megbízhatósága ellenőrizhető – bármilyen fájlt kijelölhet ellenőrzésre, csak kattintson rá, és válassza a helyi menü **További beállítások** > **Fájlok felhőalapú megbízhatósága** parancsát.



Folyamat – A számítógépen éppen futó program vagy folyamat neve. A számítógépen futó folyamatok a Windows Feladatkezelőben is megjeleníthetők. A Feladatkezelő megnyitásához kattintson a jobb gombbal a tálcán egy üres területre, majd válassza a Feladatkezelő parancsot, vagy nyomja le a Ctrl+Shift+Esc billentyűkombinációt.

Kockázat – A legtöbb esetben az ESET Smart Security az ESET Live Grid technológiát használva, heurisztikus szabályokkal kockázati szinteket rendel az objektumokhoz (fájlokhoz, folyamatokhoz, beállításkulcsokhoz stb.), ennek során megvizsgálva az egyes objektumok jellemzőit, majd súlyozva a kártékony tevékenységek előfordulásának lehetőségét. A heurisztikai szabályok alapján az objektumok kockázati szintje az „1: Elfogadható" (zöld) és a „9: Kockázatos" (vörös) közé eshet.

MEGJEGYZÉS: Az 1: Elfogadható kockázati szintű, zölddel jelölt ismert alkalmazások egészen biztosan nem fertőzöttek (engedélyezőlistán vannak), ezért a szűrésből kizártak, ami növeli a kézi indítású ellenőrzések és a valós idejű

fájlrendszervédelem sebességét.

Felhasználók – Egy adott alkalmazást használó felhasználók száma. Ezt az információt az ESET Live Grid technológia gyűjti.

Felismerve – Az az időtartam, amióta az ESET Live Grid technológia észlelte az alkalmazást.

MEGJEGYZÉS: A 9: Kockázatos kockázati szintű, pirossal jelölt alkalmazások sem feltétlenül kártevők; ezek rendszerint csak újabb alkalmazások. Ha kétségei vannak egy ilyen fájl biztonságosságát illetően, elemzésre elküldheti az ESET víruslaborjába. Ha a fájl ártalmas, bekerül a vírusdefiníciós adatbázis valamelyik későbbi frissítésébe.

Név – Egy programnak vagy folyamatnak adott név.

Megnyitás új ablakban – A futó folyamatok adatai egy új ablakban jelennek meg.

Ha az ablak alján egy alkalmazásra kattint, az alábbi információk jelennek meg róla:

- **Fájl** – Egy alkalmazás helye a számítógépen.
- **Fájlméret** – A fájl mérete kilobájtban (KB).
- **Fájlleírás** – A fájl jellemzői az operációs rendszer leírása alapján.
- **Vállalat neve** – A gyártó vagy az alkalmazásfolyamat neve.
- **Fájlverzió** – Az alkalmazás gyártójától származó információ.
- **Terméknév** – Az alkalmazás és/vagy a gyártó cég neve.

4.6.7.1 ESET Live Grid

Az ESET Live Grid, az ESET ThreatSense.Net rendszerének következő generációs változata a fejlett, megbízhatósági értékeléseken alapuló figyelmeztető rendszerével képes már korai fázisukban észlelni a terjedő kártevőket. A felhőben található kártevőadatok valós idejű letöltése révén az ESET víruslaborja folyamatosan frissen tudja tartani a védelmet, és állandó védelmi szintet képes nyújtani. A felhasználók a futó folyamatok és megnyitott fájlok megbízhatóságát közvetlenül a program felületén, illetve az ESET Live Grid rendszerből származó járulékos információkat is megjelenítő helyi menükben is megtekinthetik. Az alábbi két lehetőség közül választhat:

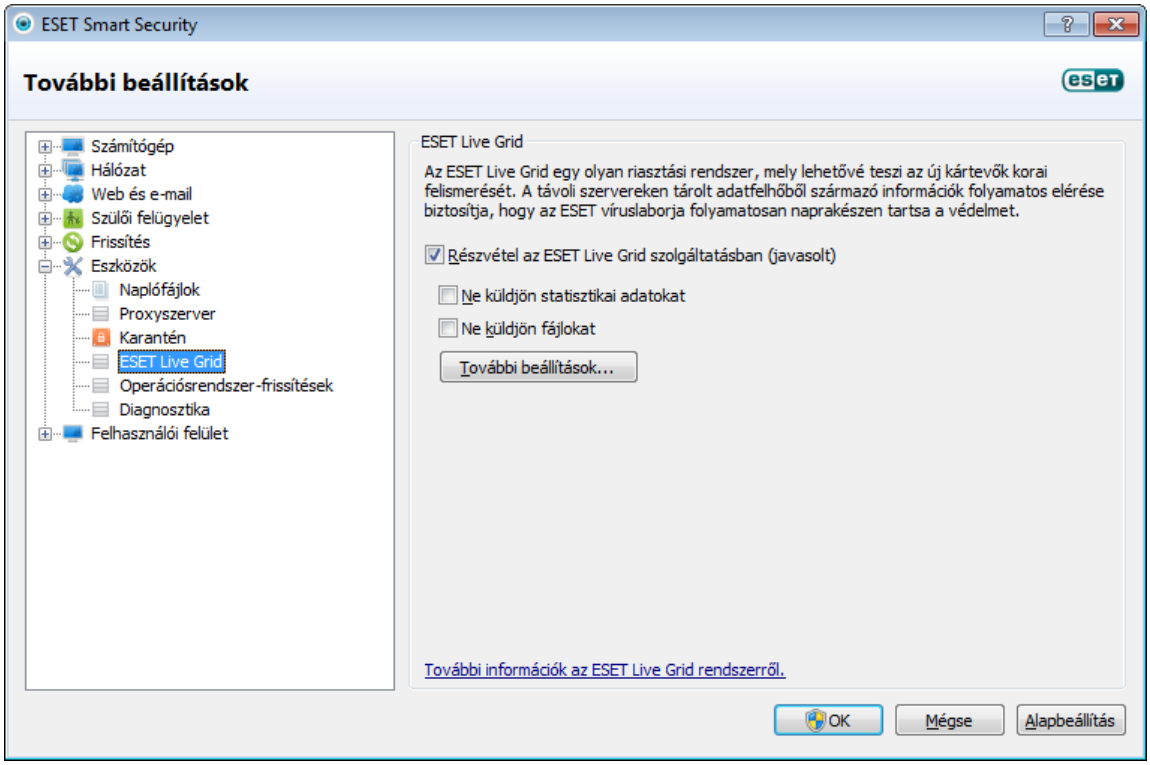
1. Eldöntheti, hogy engedélyezi-e az ESET Live Grid technológiát. Ez semmilyen funkcióvesztést nem okoz a szoftver működésében, így az továbbra is teljes körű védelmet biztosít.
2. Az ESET Live Grid beállítható az új kártevőkkel kapcsolatos adatok névtelen elküldésére. Az információk a kártevőket alkotó kódok helyét is tartalmazzák. A szoftver ezt a fájlt el tudja küldeni az ESET víruslaborjába további elemzés céljából. A kártevők tanulmányozásával az ESET javíthatja a kártevők észlelésének a hatékonyságát.

Az ESET Live Grid az újonnan felfedezett kártevőkkel kapcsolatos információkat gyűjt a számítógépről. Ez az információ tartalmazhatja a kártevőt magában foglaló fájl mintáját vagy másolatát, a fájl elérési útját és nevét, a dátumot és az időt, illetve azt a folyamatot, amelynek során a kártevő megjelent a számítógépen, valamint a számítógép operációs rendszerére vonatkozó adatokat.

Előfordulhat ugyan, hogy esetlegesen személyes, vagy a számítógépre jellemző információk (például egy elérési út részét képező felhasználónevek) is eljutnak az ESET víruslaborjába, azonban ezeket az információkat KIZÁRÓLAG az új kártevők elleni védelem mihamarabbi kiépítésére használjuk fel.

Az ESET Smart Security alapértelmezés szerint engedélyt kér a felhasználótól, mielőtt gyanús fájlokat küldene elemzésre az ESET víruslaborjába. A küldendő fájlok között néhány fájltípus – például a *.doc* és az *.xls* – sosem szerepel. Az elküldésből kitiltott fájltípusok listája testreszabható.

Az ESET Live Grid beállításai széles körű paraméterezési lehetőséget kínálnak a gyanús fájlokat és a névtelen statisztikai adatokat az ESET laborjába küldő ESET Live Grid engedélyezésére és letiltására. Az említett beállítások a További beállítások párbeszédpanel beállításfájának **Eszközök** > **ESET Live Grid** csomópontjában érhetők el.



Részvétel az ESET ESET Live Grid szolgáltatásban (javasolt) – A jelölőnégyzet bejelölésével engedélyezhető a gyanús fájlokat és a névtelen statisztikai adatokat az ESET laborjába küldő ESET Live Grid szolgáltatás.

Ne küldjön statisztikai adatokat – Ha nem szeretné, hogy az ESET Live Grid névtelenül adatokat küldjön számítógépéről, jelölje be ezt a jelölőnégyzetet. Ezek az információk az újonnan észlelt kártevőkre vonatkozó adatokat, például a kártevő nevét, az észlelés dátumát és időpontját, az ESET Smart Security verziószámát, valamint a számítógép operációs rendszerének verzióját és területi beállításait tartalmazhatják. A statisztikai adatokat a program általában naponta egy vagy két alkalommal küldi el az ESET szerverére.

Ne küldjön fájlokat – Ha bejelöli ezt a jelölőnégyzetet, az ESET Live Grid nem fogja elemzésre küldeni a kártevő jelenlétére utaló tartalommal rendelkező, vagy ilyen viselkedést mutató gyanús fájlokat az ESET laborjába.

További beállítások – Az ESET Live Grid további beállításait tartalmazó párbeszédpanel megnyitása.

Ha korábban engedélyezett volt az ESET Live Grid, a letiltás után előfordulhat, hogy maradtak még elküldendő adatcsomagok. Ezeket a program a letiltás ellenére is elküldi az ESET cégnek a következő alkalommal. A későbbiekben azonban már nem készülnek további adatcsomagok.

4.6.7.1.1 Gyanús fájlok

Az ESET Live Grid további beállításait tartalmazó párbeszédpanel **Fájlok** lapján állítható be a kártevők elküldésének módja az ESET víruslaborjába.

Ha gyanús fájlt talál, azt elküldheti elemzésre víruslaborjainknak. Ha a fájl ártalmas, bekerül a vírusdefiníciós adatbázis valamelyik későbbi frissítésébe.

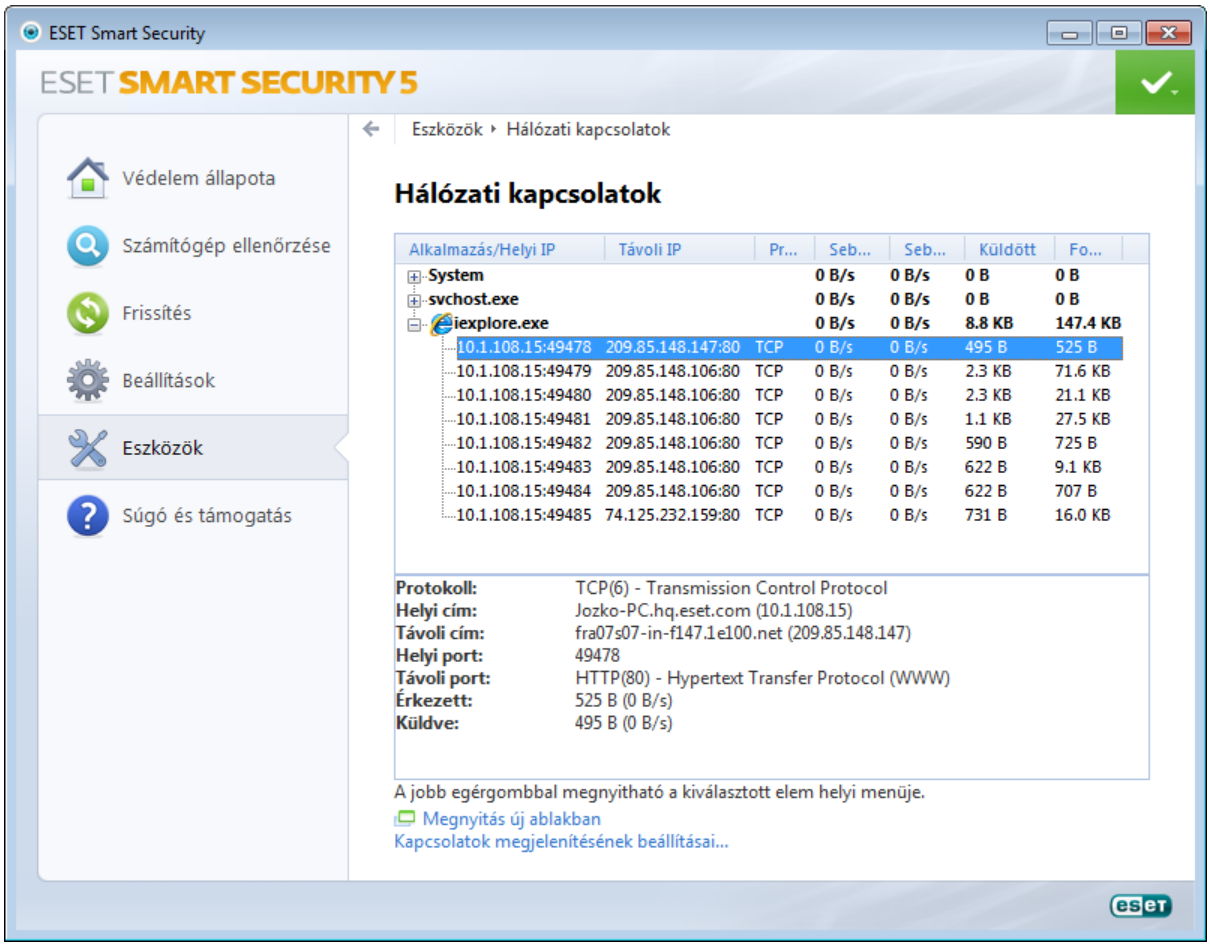
Fájlok kizárása – A fájlok kizárásával megadhatók azok a fájlok és mappák, melyek (vagy melyek tartalma) nem küldhető elemzésre. Az itt felsorolt fájlokat a program még abban az esetben sem küldi el az ESET víruslaborjába elemzésre, ha azok gyanús kódot tartalmaznak. Az olyan fájlokat érdemes kizárni, amelyek bizalmas információkat tartalmazhatnak (például a dokumentumok vagy a táblázatok). A leggyakoribb fájltípusok alapértelmezés szerint ki vannak zárva (Microsoft Office, OpenOffice). A kizárt fájlok listája szükség szerint bővíthető.

E-mail cím (nem kötelező) – E-mail címét a program a gyanús fájlokkal együtt elküldi az ESET víruslaborjába. Ne feledje, hogy az ESET munkatársai csak akkor keresik, ha a gyanús fájlokkal kapcsolatban további információra van szükség.

Naplózás engedélyezése – A jelölőnégyzet bejelölésével egy eseménynapló jön létre, mely rögzíteni fogja a fájlok és statisztikai adatok küldésének információit. Ezzel engedélyezi az eseménynapló használatát a fájlok és statisztikák küldésekor.

4.6.8 Hálózati kapcsolatok

A Hálózati kapcsolatok ablakban látható az aktív és a függőben lévő kapcsolatok listája. Ebben ellenőrizhető a kimenő kapcsolatot létesítő összes alkalmazás.



Az első sorban jelenik meg az alkalmazás neve és az adatátvitel sebessége. Az alkalmazás által létrehozott kapcsolatok (valamint további részletes adatok) megtekintéséhez kattintson a **+** jelre.

Alkalmazás/Helyi IP - Alkalmazásnév, helyi IP-címek és kommunikációs portok.

Távoli IP - Adott távoli számítógép IP-címe és portszáma.

Protokoll - A használt átviteli protokoll.

Sebesség felfelé/Sebesség lefelé - A kimenő és bejövő adatok aktuális sebessége.

Küldött/Fogadott - A kapcsolatban váltott adatok mennyisége.

Megnyitás új ablakban - Információk megjelenítése másik ablakban.

A **Kapcsolatok megjelenítésének beállításai** hivatkozás a hálózati kapcsolatok képernyőjén a speciális beállítások elérésére szolgál. A kapcsolatok megjelenítésének speciális beállításai az alábbiak.

Állomásnevek feloldása - A jelölőnégyzetet bejelölve a hálózatcímek minden lehetséges esetben tartományneves formátumban (DNS-névként) jelennek meg az IP-címes formátum helyett.

Csak a TCP-kapcsolatok megjelenítése - Ezt a jelölőnégyzetet bejelölve a listában csak a TCP-protokollkészletet használó kapcsolatok jelennek meg.

Figyelő módban lévő helyi portok megjelenítése - Ha bejelöli ezt a jelölőnégyzetet, a program azokat a nyitott porttal rendelkező, csatlakozásra váró kapcsolatokat is megjeleníti, amelyeken keresztül az adott pillanatban nem zajlik kommunikáció.

Számítógépen belüli kapcsolatok megjelenítése - A jelölőnégyzet bejelölése esetén a rendszer azokat a kapcsolatokat is megjeleníti, amelyekben a távoli oldal a helyi rendszer (a *localhost* tartománynévvel azonosított állomás).

Ha a jobb gombbal egy kapcsolatra kattint, többek között az alábbi parancsok jelennek meg:

Kommunikáció ideiglenes tiltása ezen a kapcsolaton - A létrejött kommunikáció megszakítása. Ez a parancs csak akkor jelenik meg, ha egy aktív kapcsolatra kattint.

Részletek megjelenítése - Ezzel a paranccsal megjeleníthetők a megadott kapcsolatra vonatkozó részletes információk.

Frissítési sebesség – Az aktív kapcsolatok frissítési gyakorisága.

Frissítés – Ezzel a paranccsal újból betöltheti a Hálózati kapcsolatok ablakot.

Az alábbi két beállítás csak akkor érhető el, ha nem egy aktív kapcsolatra, hanem egy alkalmazásra vagy egy folyamatra kattint:

Kommunikáció ideiglenes tiltása a folyamat számára – Elutasítja az adott alkalmazás aktuális kapcsolatait. Új kapcsolat létesítésekor a tűzfal előre meghatározott szabályt használ. A beállítások ismertetése a Szabályok és zónák című témakörben található.

Kommunikáció ideiglenes engedélyezése a folyamat számára – Engedélyezi az adott alkalmazás aktuális kapcsolatait. Új kapcsolat létesítésekor a tűzfal előre meghatározott szabályt használ. A beállítások ismertetése a Szabályok és zónák című témakörben található.

4.6.9 Fájlok elküldése elemzésre

Az **Eszközök** lapon található **Fájl elküldése elemzésre** hivatkozással megnyitható párbeszédpanel segítségével fájlokat küldhet elemzés céljából az ESET víruslaborjába. Ha gyanúsan viselkedő fájlt talál a számítógépen, elemzésre elküldheti az ESET víruslaborjába. Ha a fájl ártalmas, bekerül a vírusdefiníciós adatbázis valamelyik későbbi frissítésébe.

A fájlt e-mailben is elküldheti. Ha inkább ezt a megoldást választja, tömörítse a fájl(oka)t WinRAR vagy ZIP tömörítővel, lássa el a tömörített fájlt az „infected" jelszóval, majd küldje el a samples@eset.com címre. A levél tárgyában (lehetőség szerint angolul) ismertesse röviden és érthetően a problémát, a levélben pedig adjon meg minél több információt a fájlról (például a letöltés webhelyének a címét).

MEGJEGYZÉS: Mielőtt egy fájlt az ESET számára elküldene, ellenőrizze, hogy megfelel-e az alábbi feltételek valamelyikének: (i) a fájlt a program egyáltalán nem ismerte fel; (ii) a fájlt a program tévesen fertőzöttként ismerte fel. Válasz csak akkor érkezik, ha az elemzéshez további adatokra van szükség.

A fájl elküldésének oka – Jelölje ki az üzenethez leginkább illő leírást. A következő három lehetőség közül választhat: **Gyanús fájl**, **Téves riasztás** és **Egyéb**.

Fájl – A beküldeni kívánt fájl elérési útja.

E-mail cím – A megadott e-mail címet a program a gyanús fájlokkal együtt küldi el a víruslaborba. Ezen a címen az ESET kapcsolatba is léphet a felhasználóval, ha az elemzéshez további adatokra van szükség. Az e-mail cím megadása nem kötelező. Az ESET csak akkor válaszol, ha további információkra van szüksége. Mivel szerverei minden nap fájlok tízezreit fogadják, nem tud minden üzenetre válaszolni.

4.6.10 Operációsrendszer-frissítések

A Windows Update szolgáltatás fontos összetevő a felhasználók védelmében a kártevő szoftverek ellen, ezért alapvető fontosságú a Microsoft Windows-frissítések telepítése a kiadásukat követően a lehető leghamarabb. Az ESET Smart Security a megadott szintnek megfelelően értesítést küld a hiányzó frissítésekről. Az alábbi szintek állnak rendelkezésre:

- **Nincs értesítés** – A program nem ajánl fel letölthető rendszerfrissítést.
- **Választható frissítések** – A program az alacsony prioritásúként megjelölt és annál magasabb frissítéseket ajánlja fel letöltésre.
- **Javasolt frissítések** – A program az általánosként megjelölt és annál magasabb frissítéseket ajánlja fel letöltésre.
- **Fontos frissítések** – A program a fontosként megjelölt és annál magasabb frissítéseket ajánlja fel letöltésre.
- **Kritikus frissítések** – A program csak a kritikus frissítéseket ajánlja fel letöltésre.

A módosítások mentéséhez kattintson az **OK** gombra. Az Operációsrendszer-frissítések ablak azt követően jelenik meg, hogy a frissítési szerver ellenőrizte az állapotot. A módosítások mentését követően ennek megfelelően előfordulhat, hogy a rendszerfrissítésekre vonatkozó információk nem állnak azonnal rendelkezésre.

4.6.11 Diagnosztika

A diagnosztika az ESET folyamatainak (például *kernel (ekrn)*) alkalmazás-összeomlási képeit biztosítja. Ha egy alkalmazás összeomlik, a program egy képet hoz létre. Ez segíti a fejlesztőket az ESET Smart Security programmal kapcsolatos hibák keresésében, és a különféle problémák megoldásában. Két típusú kép létezik:

- **Teljes memóriakép** – A rendszermemória teljes tartalmát rögzíti, amikor egy alkalmazás váratlanul leáll. A teljes memóriakép a memóriakép összeállításakor futtatott folyamatok adatait tartalmazhatja.
- **Kis memóriakép** – A lehető legkevesebb információt rögzíti, amely segíthet megállapítani az alkalmazás váratlan összeomlásának okát. Az ilyen típusú memóriaképfájl akkor hasznos, amikor korlátozott mennyiségű hely áll rendelkezésre. Mivel azonban ilyenkor az információ mennyisége is korlátozott, a nem közvetlenül a probléma keletkezésekor futtatott szál által okozott hibák sem tárhatók fel biztosan az adott fájl elemzésével.
- A funkció kikapcsolásához válassza a **Memóriakép létrehozásának mellőzése** (alapértelmezett) lehetőséget.

Célkönyvtár – Az összeomlás során készült memóriaképet tároló könyvtár. Kattintson a **Mappa megnyitása** parancsra, ha a könyvtárat a *Windows Intéző* egy új ablakában szeretné megnyitni.

4.7 Felhasználói felület

A **Felhasználói felület** csoportban állíthatja be a program felhasználói felületének megjelenését és működését.

A Grafikus eszközzel módosíthatja a program vizuális megjelenését és az általa használt hatásokat.

A Riasztások és értesítések lapon módosíthatja az észlelt riasztások és a rendszerértesítések viselkedését. Mindezeket az igényeinek megfelelően testre is szabhatja.

A Rejtett értesítési ablakok szakaszban megtekinthetők a meg nem jelenített értesítések. Itt ellenőrizheti állapotukat, és további részleteket tudhat meg róluk, illetve el is távolíthatja őket az ablakból.

A szoftver maximális biztonsága érdekében a beállítások jogosulatlan módosítása ellen jelszó megadásával védekezhet. A jelszó a Hozzáférési beállítások beállításcsoportban adható meg.

Az egyes objektumokra a jobb gombbal kattintva helyi menü jelenik meg. Ezzel az eszközzel az ESET Smart Security vezérlőelemei a helyi menübe integrálhatók.

A Játékos üzemmód azon játékosok és más felhasználók számára hasznos, akik szeretnék, hogy tevékenységüket ne zavarják meg előugró ablakok, ütemezett feladatok, illetve processzor- és memóriaigényes összetevők.

4.7.1 Grafikus elemek

Az ESET Smart Security felhasználói felületének beállításai lehetővé teszik, hogy a felhasználó a saját igényei szerint alakítsa ki munkakörnyezetét. Ezek a beállítások az ESET Smart Security beállításfájának **Felhasználói felület** > **Grafikus** csomópontjában érhetők el.

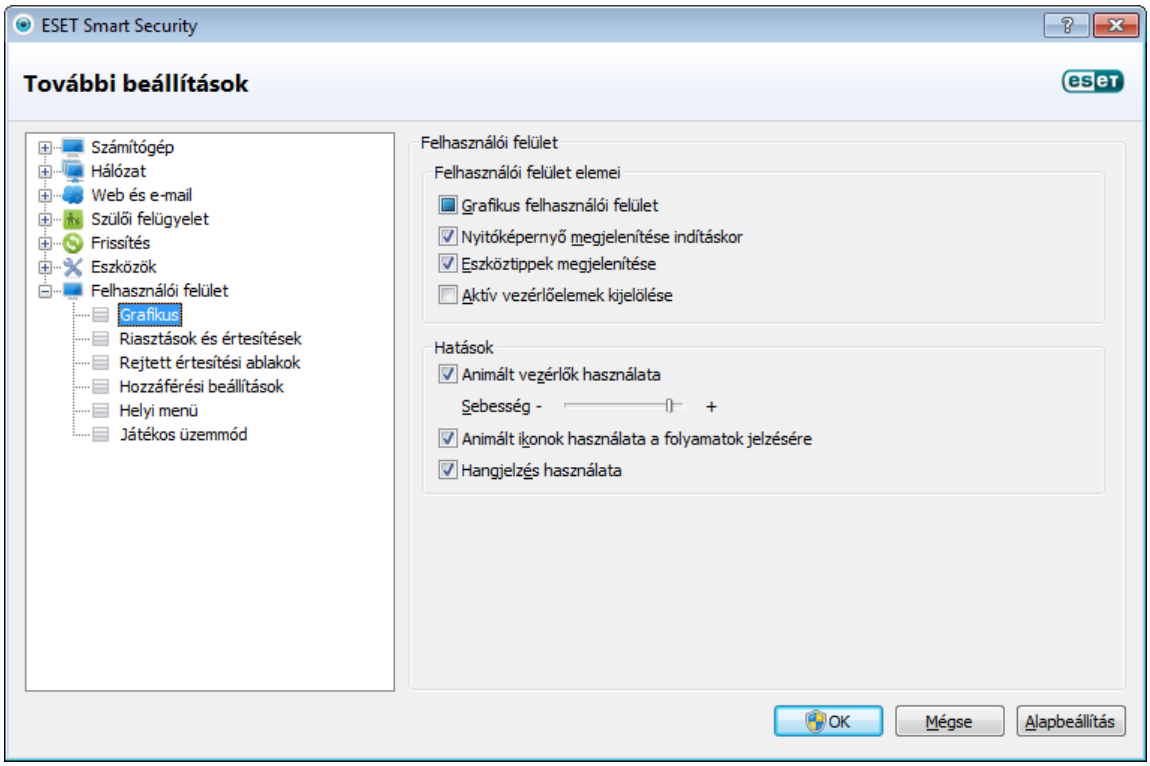
A **Felhasználói felület elemei** szakasz **Grafikus felhasználói felület** jelölőnégyzetének jelölését célszerű törölni, ha a grafikus elemek megjelenítése csökkenti a számítógép teljesítményét, vagy más problémákat okoz. A grafikus felhasználói felület kikapcsolása a látássérült felhasználóknak is javasolt, mivel az ütközhet a képernyőn megjelenített szöveg olvasására használt speciális alkalmazásokkal.

Az ESET Smart Security nyitóképernyőjének letiltásához törölje a **Nyitóképernyő megjelenítése indításkor** jelölőnégyzet jelölését.

Az **Eszköztippek megjelenítése** jelölőnégyzet bejelölése esetén egy rövid tájékoztatás jelenik meg a különböző eszközökről (parancsok, jelölőnégyzetek stb.), ha az egeret egy kis ideig fölöttük hagyja. Az **Aktív vezérlőelemek kijelölése** jelölőnégyzet bejelölése esetén a rendszer kiemeli az egérkurzor aktív területe alatt lévő elemeket. A kijelölt elem ezután egy egérkattintást követően aktívvá válik.

Az animációk sebességének csökkentéséhez vagy növeléséhez jelölje be az **Animált vezérlők használata** jelölőnégyzetet, és húzza balra vagy jobbra a **Sebesség** csúszkát.

Ha a különböző műveletek végrehajtásának menetéről animált ikonokon keresztül szeretne értesülni, jelölje be az **Animált ikonok használata a folyamatok jelzésére** jelölőnégyzetet. Ha a fontos eseményekről hangjelzést szeretne kérni, jelölje be a **Hangjelzés használata** jelölőnégyzetet.



4.7.2 Riasztások és értesítések

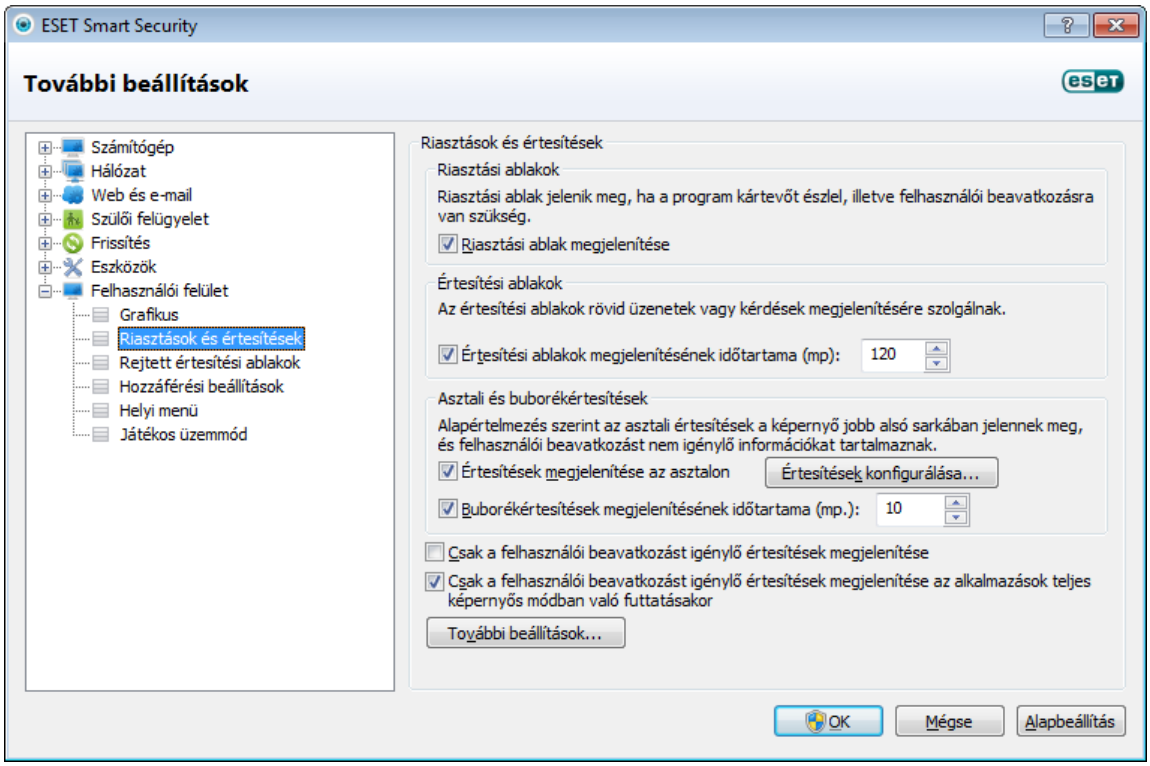
A **Felhasználói felület** szakasz **Riasztások és értesítések** csomópontjában beállítható a kártevőkkel kapcsolatos riasztások és a rendszerértesítések ESET Smart Security alkalmazásbeli viselkedési módja. Megadhatja a tálcán megjelenő értesítések megjelenítésének az időtartamát, valamint az átlátszóságuk mértékét is (csak a tálcán megjelenő értesítéseket támogató operációs rendszereken alkalmazható).

Az első jelölőnégyzet neve **Riasztási ablak megjelenítése**. Ha törli a négyzet jelölését, a szoftver egyetlen riasztást sem jelenít meg – mindez azonban csak az események szűk körére alkalmazható beállítás. A legtöbb felhasználó számára javasolt, hogy a jelölőnégyzetet hagyja bejelölve (alapértelmezett beállítás).

Az előugró ablakok adott időtartam utáni automatikus bezárásához jelölje be az **Értesítési ablakok megjelenítésének időtartama (mp)** jelölőnégyzetet. Ha a felhasználó nem zárja be az ablakokat, akkor ezt a megadott időtartam elteltével a program automatikusan megteszi.

Az asztali és buborékértesítések csupán a tájékoztatást szolgálják, és nem igénylik, illetve nem is teszik lehetővé a felhasználói beavatkozást, amikor a képernyő jobb alsó sarkában lévő értesítési területen megjelennek. Az asztali értesítések aktiválásához jelölje be az **Értesítések megjelenítése az asztalon** jelölőnégyzetet. A részletesebb beállítások – például az értesítések megjelenési időtartama és az ablakok átlátszósága – az **Értesítések konfigurálása** gombra kattintva adhatók meg. Az értesítések előnézetének a megtekintéséhez kattintson az **Előnézet** gombra.

A **Buborékértesítések megjelenítésének időtartama (mp.)** jelölőnégyzetet bejelölve megadhatja, hogy mennyi ideig legyenek láthatók az értesítések.



A **Csak a felhasználói beavatkozást igénylő értesítések megjelenítése** jelölőnégyzet bejelölésével kikapcsolhatja a választ nem igénylő riasztásokat és értesítéseket. A **Csak a felhasználói beavatkozást igénylő értesítések megjelenítése az alkalmazások teljes képernyős módban való futtatásakor** jelölőnégyzet bejelölése esetén egyetlen olyan értesítés sem fog megjelenni, mely nem kíván felhasználói reakciót.

A **További beállítások** gombra kattintva megnyithatja a további beállítások megadására szolgáló **Riasztások és értesítések** párbeszédpanelt

4.7.2.1 További beállítások

A megjelenítendő események minimális részletessége legördülő listában beállítható, hogy milyen súlyossági szinttől kezdve jelenjenek meg riasztások és értesítések.

- **Diagnosztikai** – Ezt a lehetőséget választva a szoftver az alábbiak mellett az alkalmazás finomhangolásához szükséges információkat is bejegyzi a naplóba.
- **Tájékoztató** – Ezt a beállítást megadva a program a tájékoztató jellegű üzeneteket veszi fel a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett rekordokat).
- **Figyelmeztetések** – A program a kritikus figyelmeztetéseket és a figyelmeztető üzeneteket egyaránt megjeleníti.
- **Hibák** – Ezt a lehetőséget választva a program a *fájlletöltési* és a kritikus hibákat jegyzi be a naplóba.
- **Kritikus** – Ezt a lehetőséget választva a program csak a kritikus (például a vírusvédelem indításával, a személyi tűzfallal és egyebekkel kapcsolatos) hibákat naplózza.

A párbeszédpanel másik beállításában azt adhatja meg, hogy többfelhasználós környezetben hol legyen az értesítések célhelye. A **Több felhasználó esetén az értesítések megjelenítése az alábbi felhasználó képernyőjén** mezőben adhatja meg, hogy a több felhasználó csatlakozását egy időben engedélyező rendszereken mely felhasználónak jelenjenek meg a rendszer- és egyéb értesítések. A mezőbe rendszerint a rendszer vagy a hálózat rendszergazdájának a címe kerül. Ez a lehetőség különösen hasznos terminálszerverek esetében, feltéve, hogy a rendszerrel kapcsolatos összes értesítést a rendszergazda kapja meg.

4.7.3 Rejtett értesítési ablakok

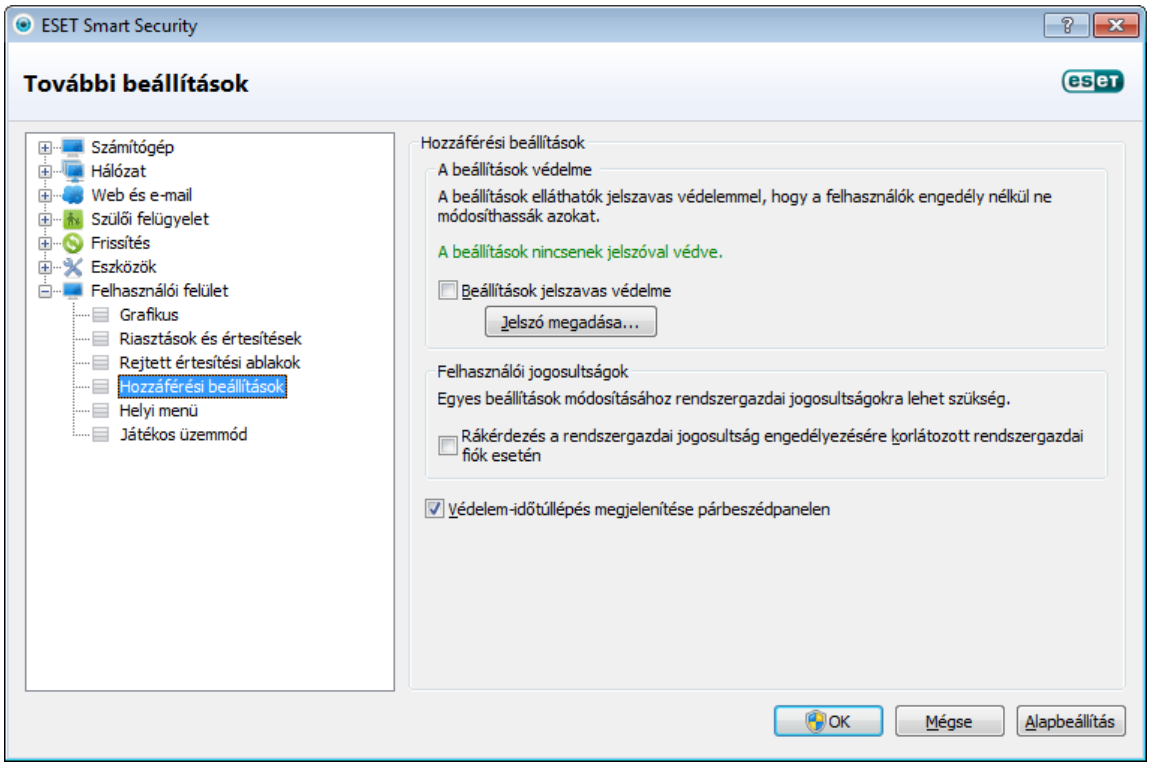
Ha bármely korábban megjelenített értesítési ablakban (riasztásban) bejelölte a **Ne kérdezzen rá újra** jelölőnégyzetet, az ablak meg fog jelenni a rejtett értesítési ablakok listájában. Azok a műveletek, amelyeket a program nem hajt végre automatikusan, a **Megerősítés** oszlopban jelennek meg.

Megjelenítés – A gombra kattintva az olyan aktuálisan nem látható értesítési ablakok előnézete jelenik meg, amelyekhez automatikusan végrehajtandó művelet van beállítva.

Eltávolítás – A gombbal a **rejtett értesítési ablakok** listájának elemei távolíthatók el. A listából eltávolított összes értesítési ablak meg fog jelenni újra.

4.7.4 Hozzáférési beállítások

A rendszer maximális biztonsága érdekében fontos, hogy az ESET Smart Security megfelelően legyen konfigurálva. A nem hozzáértő módosítások akár a lényeges adatok elvesztéséhez is vezethetnek. Ez a beállítási lehetőség a **Felhasználói felület** csoport **Hozzáférési beállítások** lapján található. A jogosulatlan módosítások elkerülése érdekében az ESET Smart Security beállításai jelszóval védhetők.



Beállítások jelszavas védelme – Zárolja, illetve feloldja a program beállítási paramétereit. A Jelszó beállítása ablak megnyitásához jelölje be a jelölőnégyzetet, illetve törölje a jelölését.

A beállítási paraméterek védelmére szolgáló jelszó megadásához vagy módosításához kattintson a **Jelszó megadása** gombra.

Rákérdezés a rendszergazdai jogosultság engedélyezésére korlátozott rendszergazdai fiók esetén – Jelölje be ezt a jelölőnégyzetet, ha az aktuális felhasználótól (ha nem rendelkezik rendszergazdai jogosultsággal) rendszergazdai felhasználónevet és jelszót szeretne kérni egyes rendszerparaméterek módosításakor (a Windows Vista rendszer UAC szolgáltatásához hasonlóan). A módosítások közé tartozik a védelmi modulok vagy a tűzfal kikapcsolása.

Védelem-időtúllépés megjelenítése párbeszédpanelen – A program rákérdez, hogy a jelölőnégyzet bejelölésekor kikapcsolta-e ideiglenesen a védelmet a programmenüben, vagy az **ESET Smart Security** program **Beállítások** szakaszában. **A vírusvédelem ideiglenes kikapcsolása** ablak **Időtartam** legördülő listája jeleníti meg azt az időtartamot, ameddig a védelem összes kijelölt eleme ki lesz kapcsolva.

4.7.5 Helyi menü

A helyi menü megjelenítéséhez kattintson a jobb gombbal a kijelölt objektumra. A menüben megtalálható az objektumon végrehajtható összes művelet.

Az ESET Smart Security vezérlőelemei a helyi menübe integrálhatók. A további beállítások **Felhasználói felület** és **Helyi menü** részében találhatók a funkció egyéb részletes beállítási lehetőségei.

Integrálás a helyi menübe – Az ESET Smart Security parancsainak beillesztése a helyi menükbe.

A **Menü típusa** legördülő listában az alábbi lehetőségek találhatók:

- **Teljes (első az ellenőrzés)** – Aktiválja a helyi menü összes parancsát; a főmenüben megjelenik az **Ellenőrzés az ESET Smart Security programmal** parancs.
- **Teljes (első a megtisztítás)** – Aktiválja a helyi menü összes parancsát; a főmenüben megjelenik a **Megtisztítás az ESET Smart Security programmal** parancs.
- **Csak ellenőrzés** – Csak az **Ellenőrzés az ESET Smart Security programmal** parancs jelenik meg a helyi menüben.
- **Csak megtisztítás** – Csak a **Megtisztítás az ESET Smart Security programmal** parancs jelenik meg a helyi menüben.

Megerősítések – További figyelmeztetést jelenít meg, ha a felhasználó a **Rákérdezés, ha a fájlok száma több mint** mezőben megadottnál több objektumon kísérli meg végrehajtani a helyi menüben található egyik műveletet. Alapértelmezés szerint 8 objektum van megadva.

4.7.6 Játékos üzemmód

A játékos üzemmód azoknak a játékosoknak hasznos, akiknek fontos a szoftverek megszakítás nélküli használata, és nem szeretnék, hogy előugró ablakok zavarják meg őket, illetve szeretnék minimalizálni a processzor terhelését. A játékos üzemmód prezentációs módként is használható – ilyenkor a bemutatók előadását nem zavarja meg a vírusvédelmi tevékenység. A funkció engedélyezésével letiltja az előugró ablakokat, valamint teljesen leállítja a feladatütemező tevékenységét. A rendszervédelem változatlanul működik a háttérben, felhasználói beavatkozást azonban nem igényel.

A játékos üzemmódot az ESET Smart Security fő ablakában, a **Beállítások** lap jobb oldalán, illetve a további beállításokat tartalmazó párbeszédpanelen lehet engedélyezni és letiltani. A további beállításokat tartalmazó párbeszédpanel megnyitásához kattintson a program fő ablakának alján elhelyezkedő **További beállítások megnyitása** műveletre. Ezután válassza a **Felhasználói felület** > **Játékos üzemmód** beállításcsoportot. Az üzemmód engedélyezéséhez jelölje be a **Játékos üzemmód engedélyezése** jelölőnégyzetet. A játékos üzemmód engedélyezése biztonsági kockázatot hordoz, ezért a védelmi állapot ikonja a tálcán sárgára vált, és egy figyelmeztetés jelenik meg rajta. A figyelmeztetés az ESET Smart Security fő ablakának **Védelem állapota** lapján is megjelenik, a sárga **A Játékos üzemmód engedélyezve van** üzenet kíséretében.

A **Játékos üzemmód engedélyezése automatikusan az alkalmazások teljes képernyős módban való futtatásakor** jelölőnégyzet bejelölése esetén a rendszer automatikusan játékos üzemmódba vált, amint elindít egy teljes képernyős alkalmazást. Az alkalmazás bezárásakor a rendszer kilép ebből az üzemmódból. A funkcióval a játékok, a teljes képernyős alkalmazások és a bemutatók indítása után automatikusan bekapcsolható a játékos üzemmód.

A **Játékos üzemmód letiltása automatikusan** jelölőnégyzet bejelölése esetén megadhatja, hogy mennyi idő után kapcsoljon ki az üzemmód (az alapértelmezett érték 1 perc). Ez akkor hasznos, ha a játékos módot csak egy adott ideig kívánja használni, és utána szeretné automatikusan letiltani.

Megjegyzés: Ha a személyi tűzfal interaktív módban van, és a játékos üzemmód engedélyezett, internetelérési problémák jelentkezhetnek. Ez akkor okozhat problémát, ha egy internetkapcsolatot igénylő játékot indít el. Normál esetben a rendszer megkérdezné, hogy mit tegyen ilyen esetben (ha nincsenek megadva kommunikációs szabályok és kivételek), de ebben az üzemmódban le van tiltva a felhasználóval folytatott kommunikáció. A probléma megoldásához hozzon létre egy kommunikációs szabályt minden olyan alkalmazáshoz, amelyik ütközhet ezzel a funkcióval, vagy állítson be más szűrési módot a személyi tűzfalban. Ne feledje továbbá, hogy a játékos üzemmódban a meglátogatott webhelyek és a futtatott alkalmazások biztonsági kockázatot hordozhatnak, illetve előfordulhat, hogy letiltódnak a webhelyek vagy alkalmazások, de erről semmiféle tájékoztatást vagy figyelmeztetést nem kap, mivel a felhasználóval folytatott kommunikáció le van tiltva.

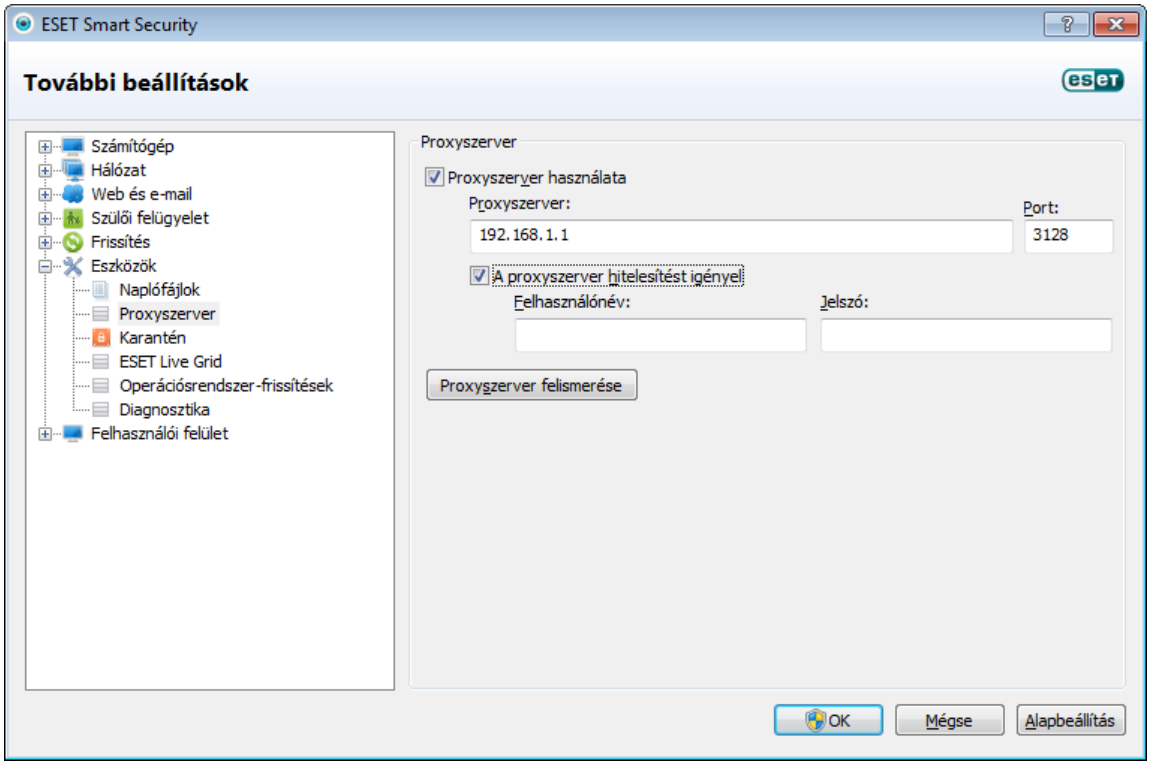
5. Útmutató Tapasztalt felhasználók részére

5.1 A proxyszerver beállításai

Nagyméretű helyi hálózatokon a számítógép és az internet közötti kapcsolatot egy proxyszerver közvetítheti. Ebben az esetben meg kell adnia az alábbi beállításokat, különben előfordulhat, hogy a program nem frissül automatikusan. Az ESET Smart Security programban a proxyszerver beállításai a További beállítások ablakon belül két különböző csoportban érhetők el.

A proxyszerver beállításai egyrészt a **További beállítások** párbeszédpanel beállításfájának **Eszközök** > **Proxyszerver** csomópontjában adhatók meg. A proxyszerver ezen a szinten való megadása az ESET Smart Security összes globális proxyszerver-beállítását meghatározza. Az itt található paramétereket fogja használja az internetkapcsolatot igénylő összes modul.

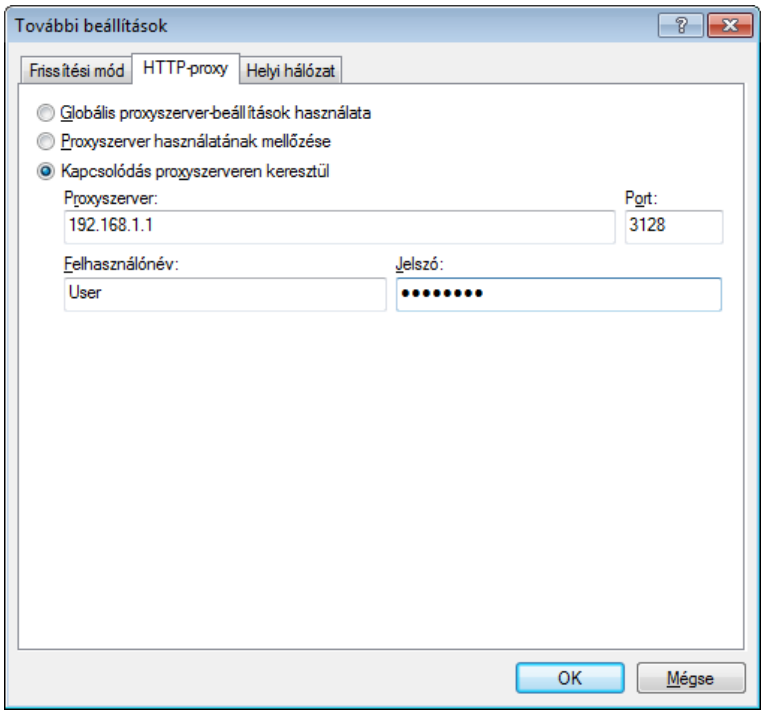
A proxyszerver ehhez a szinthez tartozó beállításainak megadásához jelölje be a **Proxyszerver használata** jelölőnégyzetet, majd írja be a proxyszerver címét a **Proxyszerver** mezőbe, a portszámot pedig a **Port** mezőbe.



Ha a proxyszerver hitelesítést igényel, jelölje be **A proxyszerver hitelesítést igényel** jelölőnégyzetet, és írjon be egy érvényes felhasználónév-jelszó párt a **Felhasználónév** és a **Jelszó** mezőbe. A **Proxyszerver felismerése** gombra kattintva a program automatikusan észleli és megadja a proxyszerver beállításait. Ekkor a program átmásolja az Internet Explorer alkalmazásban megadott paramétereket.

Megjegyzés: A funkció a hitelesítő adatokat (a felhasználónevet és a jelszót) nem tudja megállapítani, azokat kézzel kell megadni.

A proxyszerver-beállítások létrehozhatók a További frissítési beállítások lehetőségen belül is (a **További beállítások** fastruktúrában a **Frissítés** elem). Ez a beállítás adott frissítési profilra vonatkozik, és hordozható számítógépek esetén javasolt, mivel azok a vírusdefiníciós adatbázis frissítéseit gyakran különböző helyekről kapják. Erről a beállításról további információt a További frissítési beállítások című témakörben talál.



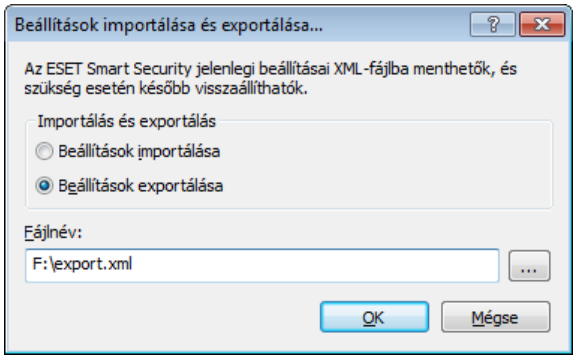
5.2 Beállítások importálása és exportálása

Az ESET Smart Security konfigurációinak importálására és beállítására a **Beállítások** lapon van lehetőség.

Az importálás és az exportálás egyaránt *.xml* típusú fájlokat használ. Az importálás és exportálás célja az ESET Smart Security aktuális konfigurációjának biztonsági mentése későbbi felhasználás céljára. Az exportálási funkció emellett arra is alkalmas, hogy az ESET Smart Security megfelelő konfigurációját a felhasználók egyszerűen beállíthassák más számítógépeken is az exportált XML-fájlok importálásával.

A konfigurációk importálása igen egyszerű: A főmenüben válassza a **Beállítások** > **Beállítások importálása és exportálása** lehetőséget, majd kattintson a **Beállítások importálása** parancsra. Írja be a konfigurációs fájl elérési útját, vagy a **Tallózás** gombra kattintva jelölje ki.

A konfiguráció exportálásának lépései nagyon hasonlóak: Válassza a főmenüben a **Beállítások** > **Beállítások importálása és exportálása** lehetőséget. Kattintson a **Beállítások exportálása** parancsra, és írja be a konfigurációs fájl nevét a **Fájlnév** mezőbe (például *export.xml*). A tallózási funkcióval kijelölheti a fájl tárolására szánt mappát.



5.3 Billentyűparancsok

Az ESET Smart Security alkalmazásban használható billentyűparancsok közé tartoznak az alábbiak:

Ctrl+G	a grafikus felhasználói felület letiltása a termékben
Ctrl+I	az ESET SysInspector lap megnyitása
Ctrl+L	a Naplófájlok lap megnyitása
Ctrl+S	a Feladatütemező lap megnyitása
Ctrl+Q	a Karantén lap megnyitása
Ctrl+U	a felhasználónév és a jelszó megadására szolgáló párbeszédpanel megnyitása

Az alábbi billentyűparancsok segítik a jobb navigálást az ESET biztonsági termékben:

F1	a súgólapok megnyitása
F5	a további beállításokat tartalmazó ablak megnyitása
Fel/Le	navigálás a termékben elemeken keresztül
Jobbra nyíl	– a További beállítások facsomópont kibontása
Balra nyíl	– a További beállítások facsomópont összecsukása
TAB	a kurzor mozgatása egy ablakban
Esc	az aktív párbeszédpanel bezárása

5.4 Parancssor

Az ESET Smart Security vírusvédelmi modulja a parancssor használatával is elindítható – akár manuálisan az „ecls" paranccsal, akár egy .bat kiterjesztésű kötegfájllal. Az ESET parancssoros ellenőrzőjének szintaxisa:

```
ecls [BEÁLLÍTÁSOK..] FÁJLOK..
```

A kézi indítású víruskereső indításakor az alábbi paraméterek és kapcsolók adhatók meg a parancssorban.

Beállítások

/base-dir=MAPPA	modulok betöltése a MAPPA mappából
/quar-dir=MAPPA	karantén MAPPA
/exclude=MASZK	a MASZK értékkel egyező fájlok kizárása az ellenőrzésből
/subdir	almappák ellenőrzése (alapértelmezés)
/no-subdir	almappák ellenőrzésének mellőzése
/max-subdir-level=SZINT	mappák maximális alszintje az ellenőrizendő mappákon belül
/symlink	szimbolikus hivatkozások követése (alapbeállítás)
/no-symlink	szimbolikus hivatkozások mellőzése
/ads	változó adatfolyamok (ADS) ellenőrzése (alapbeállítás)
/no-ads	változó adatfolyamok (ADS) ellenőrzésének mellőzése
/log-file=FÁJL	naplózás a FÁJL fájlba
/log-rewrite	kimeneti fájl felülírása (alapbeállítás: hozzáfűzés)
/log-console	naplózás a konzolba (alapbeállítás)
/no-log-console	a konzolba történő naplózás mellőzése
/log-all	nem fertőzött fájlok naplózása
/no-log-all	nem fertőzött fájlok naplózásának mellőzése (alapbeállítás)
/aind	aktivitásjelző megjelenítése
/auto	helyi lemezek ellenőrzése és automatikus megtisztítása

Víruskereső beállításai

/files	fájlok ellenőrzése (alapbeállítás)
/no-files	fájlok ellenőrzésének mellőzése
/memory	memória ellenőrzése
/boots	rendszerindítási szektorok ellenőrzése
/no-boots	rendszerindítási szektorok ellenőrzésének mellőzése (alapbeállítás)
/arch	tömörített fájlok ellenőrzése (alapbeállítás)
/no-arch	tömörített fájlok ellenőrzésének mellőzése
/max-obj-size=MÉRET	csak a MÉRET megabájtnál kisebb fájlok ellenőrzése (alapbeállítás 0 = korlátlan)
/max-arch-level=SZINT	tömörített fájlok maximális alszintje az ellenőrizendő tömörített fájlokon (többszörösen tömörített fájlokon) belül
/scan-timeout=KORLÁT	tömörített fájlok ellenőrzése legfeljebb KORLÁTOZOTT másodpercig

/max-arch-size=MÉRET	csak a MÉRET bájtnál kisebb fájlok ellenőrzése tömörített fájlok esetén (alapbeállítás: 0 = korlátlan)
/max-sfx-size=MÉRET	önkicsomagoló tömörített fájlokban csak a MÉRET megabájtnál kisebb fájlok ellenőrzése (alapbeállítás 0 = korlátlan)
/mail	e-mail fájlok ellenőrzése (alapbeállítás)
/no-mail	e-mail fájlok ellenőrzésének mellőzése
/mailbox	postaládák ellenőrzése (alapérték)
/no-mailbox	postaládák ellenőrzésének mellőzése
/sfx	önkicsomagoló tömörített fájlok ellenőrzése (alapbeállítás)
/no-sfx	önkicsomagoló tömörített fájlok ellenőrzésének tiltása
/rtp	futtatás közbeni tömörítők ellenőrzése (alapbeállítás)
/no-rtp	futtatás közbeni tömörítők ellenőrzésének mellőzése
/adware	reklámprogramok, kémprogramok és biztonsági kockázatot jelentő programok ellenőrzése (alapbeállítás)
/no-adware	reklámprogramok, kémprogramok és biztonsági kockázatot jelentő programok ellenőrzésének mellőzése
/unsafe	veszélyes alkalmazások keresése
/no-unsafe	veszélyes alkalmazások keresésének mellőzése (alapbeállítás)
/unwanted	kéretlen alkalmazások ellenőrzése
/no-unwanted	kéretlen alkalmazások ellenőrzésének mellőzése (alapbeállítás)
/pattern	vírusdefiníciók használata (alapbeállítás)
/no-pattern	vírusdefiníciók használatának mellőzése
/heur	alapheurisztika engedélyezése (alapbeállítás)
/no-heur	alapheurisztika letiltása
/adv-heur	kiterjesztett heurisztika engedélyezése (alapbeállítás)
/no-adv-heur	kiterjesztett heurisztika letiltása
/ext=KITERJESZTÉSEK	csak a kettősponttal elválasztott KITERJESZTÉSEK ellenőrzése
/ext-exclude=KITERJESZTÉSEK	a kettősponttal elválasztott KITERJESZTÉSEK kizárása az ellenőrzésből
/clean-mode=MÓD	megtisztítási MÓD használata a fertőzött objektumokhoz. A választható lehetőségek az alábbiak: none (nincs), standard (normál, alapbeállítás), strict (teljes), rigorous (alapos), delete (törlés)
/quarantine	a fertőzött fájlok karanténba másolása (a MŰVELET kiegészítése)
/no-quarantine	a fertőzött fájlok karanténba másolásának mellőzése

Általános beállítások

/help	súgó megjelenítése és kilépés
/version	verzióadatok megjelenítése és kilépés
/preserve-time	utolsó hozzáférés időbélyegének megőrzése

Kilépési kódok

0	a program nem talált kártevőt
1	a program kártevőt talált, és megtisztította az érintett objektumokat
10	néhány fertőzött fájl esetén nem sikerült a megtisztítás (előfordulhat, hogy kártevők)
50	a program kártevőt talált
100	hiba

Megjegyzés: A 100-nál nagyobb számmal jelölt kilépési kódok esetén az adott fájl nem volt ellenőrizve, ezért fertőzött lehet.

5.5 ESET SysInspector

5.5.1 Az ESET SysInspector ismertetése

Az ESET SysInspector alkalmazás alaposan átvizsgálja a számítógépét, és az összegyűjtött adatokat átfogó módon megjeleníti. A többek között a telepített illesztőprogramokra és alkalmazásokra, hálózati kapcsolatokra vagy fontos rendszer-beállítási bejegyzésekre vonatkozó információk segítségével megvizsgálhatja, hogy a rendszer gyanús működését a szoftver vagy a hardver inkompatibilitása, esetleg kártevőfertőzés okozza-e.

Az ESET SysInspector kétféleképpen érhető el: Az ESET Smart Security integrált verziójából vagy a különálló verzió (SysInspector.exe) ingyenes letöltésével az ESET weboldaláról. Az ESET SysInspector megnyitásához válassza az **Eszközök** > **ESET SysInspector** lehetőséget. Mindkét változat működése azonos, és megegyező programvezérlőket tartalmaznak. Az egyedüli különbség a kimenetek kezelésében van. A letöltött és integrált verziók mindegyike lehetővé teszi, hogy rendszerpillanatképeket exportáljon egy .xml fájlba, és lemezre mentse azokat. Az integrált verzióval a rendszer pillanatképeit közvetlenül az **Eszközök** lapról elérhető **ESET SysInspector** eszközben tárolhatja (részletes

tudnivalókért tanulmányozza a Az ESET SysInspector részét képező ESET Smart Security című témakört).

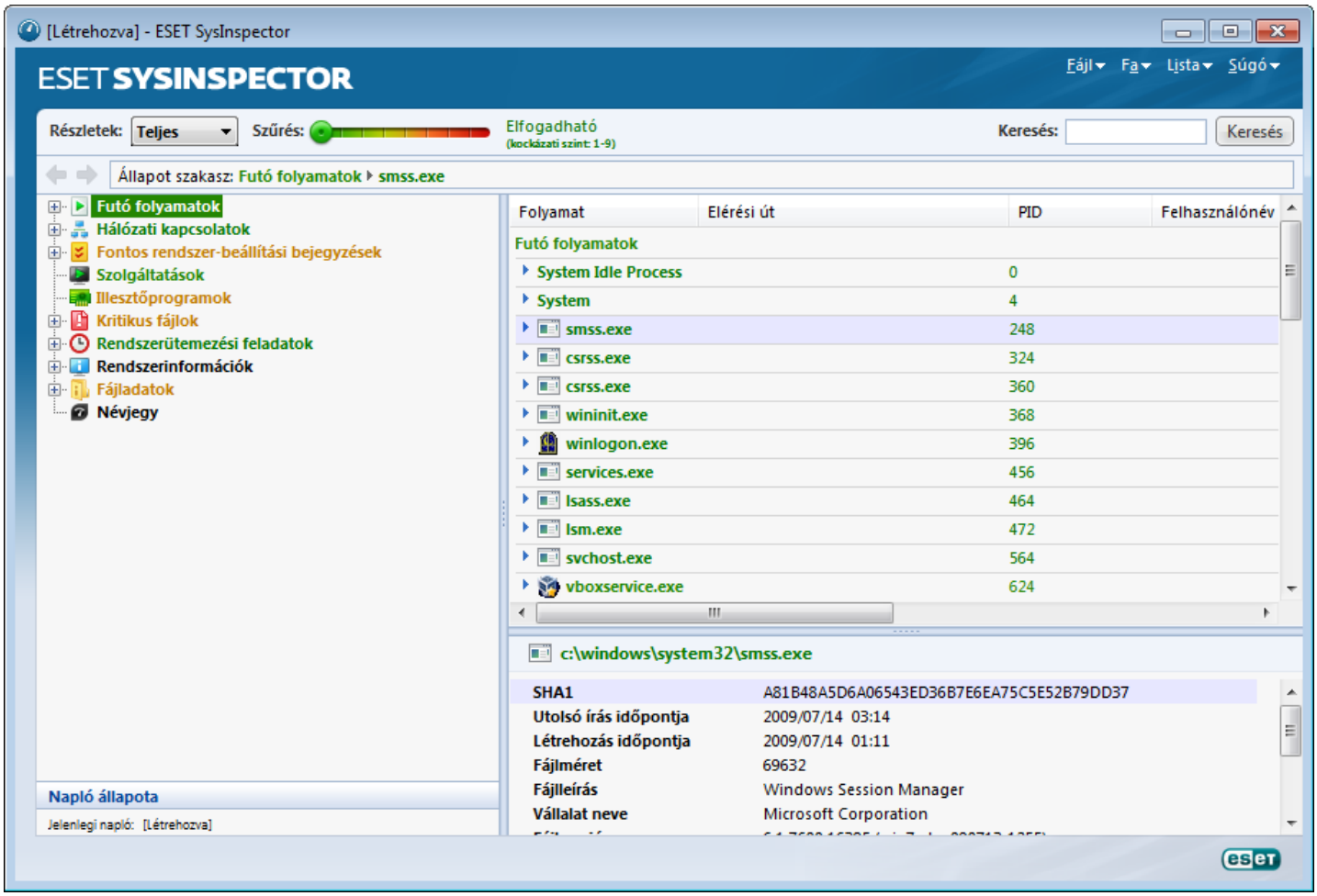
Hagyjon kis időt az ESET SysInspector számára a számítógép ellenőrzéséhez, amely 10 másodperctől pár percig terjedő időt vehet igénybe (ez a hardverkonfiguráció és a rendszeren telepített alkalmazásoktól függően változhat).

5.5.1.1 Az ESET SysInspector indítása

Az ESET SysInspector indításához egyszerűen futtassa az ESET weboldaláról letöltött *SysInspector.exe* programfájlt. Ha már telepítette az ESET valamelyik biztonsági termékét, az ESET SysInspector közvetlenül a Start menüből is futtatható, a **Programok** > **ESET** > **ESET Smart Security** parancsot választva. Várja meg, amíg az alkalmazás megvizsgálja a rendszert, ami a hardvertől és az összegyűjtendő adatoktól függően néhány percet igénybe vehet.

5.5.2 A felhasználói felület és az alkalmazás használata

Az egyszerűbb használat érdekében a főablak 4 szakaszból áll – a vezérlők találhatók a főablak tetején, a navigációs ablak a bal oldalon, az információs ablak jobb oldalon, középmagasságban, a részleteket tartalmazó ablak pedig a főablak jobb alsó részén. A napló állapotát megjelenítő szakasz tartalmazza a napló alapvető paramétereinek listáját (használt szűrő, a szűrő típusa, a napló egy összehasonlítás eredménye-e stb.).



5.5.2.1 Vezérlőelemek

Ez a szakasz tartalmazza az ESET SysInspector alkalmazásban rendelkezésre álló összes vezérlőelem ismertetését.

Fájl

A **Fájl** menüre kattintva későbbi vizsgálat céljából mentheti az aktuális rendszerállapotot, illetve megnyithat egy korábban mentett naplót. Javasoljuk, hogy közzétételi célokból hozzon létre egy **küldésre alkalmas** naplót. Ebben a formában a naplóból hiányoznak a bizalmas adatok (aktuális felhasználónév, számítógép neve, tartomány neve, aktuális felhasználó jogosultságai, környezeti változók stb.).

Megjegyzés: Az ESET SysInspector korábbi jelentéseit megnyithatja, ha egyszerűen a fő ablakba húzza azokat.

Fa

Lehetővé teszi az összes csomópont kibontását vagy összecsukását, és a kijelölt szakaszok exportálását az eltávolító szkriptbe.

Lista

A programon belüli egyszerű navigálásra szolgáló funkciókat, valamint számos egyéb műveletet tartalmaz (többek között az információk online keresését).

Súgó

Az alkalmazásra és funkcióira vonatkozó információkat tartalmaz.

Részletek

A beállítás a fő ablak egyéb szakaszaiban megjelenített információkat határozza meg, ezáltal egyszerűsíti a program használatát. „Alap" módban hozzáférhet a rendszerben fellépő általános problémák megoldásának kereséséhez használt információkhoz. „Közepes" módban a program megjeleníti a kevésbé használt részleteket, míg a „Teljes" módban az ESET SysInspector megjeleníti a nagyon specifikus problémák megoldásához szükséges összes információt.

Elemek szűrése

Az elemek szűrése a rendszerben lévő gyanús fájlok vagy rendszer-beállítási bejegyzések kereséséhez használható. A csúszka húzásával az elemeket a kockázati szintjük szerint szűrheti. Ha a csúszkát teljesen balra húzza (1. kockázati szint), a program az összes elemet megjeleníti. A csúszka jobbra húzásával a program kiszűri az aktuális szintnél kevésbé kockázatos összes elemet, és csak a megjelenített szinttel megegyező vagy annál magasabb kockázati szintű (gyanúsabb) elemeket jeleníti meg. Ha a csúszkát a jobb oldali szélső helyzetbe állítja, a program csak az ismert káros elemeket jeleníti meg.

A 6–9 értékkel rendelkező elemek biztonsági kockázatot jelenthetnek. Ha az ESET SysInspector ilyen elemeket talált, és nem használja az ESET biztonsági megoldásait, ajánlott ellenőriznie rendszerét az ESET Online Scanner eszközzel. Az ESET Online Scanner ingyenes szolgáltatás.

Megjegyzés: Az egyes elemek kockázati szintje gyorsan meghatározható, ha összehasonlítja az elem színét a kockázati szint csúszkájának színével.

Keresés

Ez a szolgáltatás használható adott elemek gyors kereséséhez a név vagy a név egy része alapján. A keresési eredmények a leírásokat megjelenítő ablakban láthatók.

Visszalépés

A Balra vagy Jobbra nyílbillentyűre kattintva lépkedhet a leírásokat megjelenítő ablakban látható információkra. Ezek helyett használhatja a Backspace és a Szóköz billentyűt is.

Állapot szakasz

Megjeleníti az aktuális csomópontot a navigációs ablakban.

Fontos: A vörössel kiemelt elemek ismeretlenek, ezért jelöli a program potenciálisan veszélyesnek azokat. Ha egy elem vörös, az nem jelenti automatikusan azt, hogy a fájl törölhető. Törlés előtt győződjön meg arról, hogy a fájlok valóban veszélyesek, illetve nem szükségesek.

5.5.2.2 Keresés az ESET SysInspector alkalmazásban

Az ESET SysInspector néhány alapvető szakaszra (csomópontra) osztja a különböző típusú információkat. Az egyes csomópontok alcsomópontokra bontásával további részleteket jeleníthet meg. Ha egy csomópontot ki szeretne bontani vagy össze kíván csukni, kattintson duplán a csomópont nevére vagy a név mellett látható ⊞ vagy ⊟ jelre. Ha a navigációs ablakban tallózással kiválaszt egy-egy csomópontot vagy alcsomópontot, az arra vonatkozó adatok megjelennek a leírásokat tartalmazó ablakban. Ha ebben az ablakban tallóz az elemek között, további adatok jelenhetnek meg a részleteket megjelenítő ablakban.

Az alábbiakban a fő csomópontok navigációs ablakban látható leírásai, valamint a leírásokat és a részleteket tartalmazó ablakban szereplő kapcsolódó információk találhatók.

Futó folyamatok

Ez a csomópont a napló létrehozásának időpontjában futó alkalmazásokra és folyamatokra vonatkozó információkat tartalmaz. Az egyes folyamatokra vonatkozóan a leírásokat megjelenítő ablak további részleteket tartalmaz (például a folyamat által használt dinamikusan csatolt függvénytárak vagy helyük a rendszerben, az alkalmazások gyártójának neve, a fájl kockázati szintje stb.).

A részleteket megjelenítő ablak a leírásokat tartalmazó ablakban kijelölt elemek további adatait (például a fájl méretét vagy kivonatát) jeleníti meg.

Megjegyzés: Az operációs rendszerek számos fontos, éjjel-nappal futó kernelösszetevőből állnak, és alapvető funkciókat biztosítanak a többi felhasználói alkalmazás számára. Bizonyos esetekben az ilyen folyamatok \??\ kezdetű elérési úttal jelennek meg az ESET SysInspector alkalmazásban. Ezek a jelek a folyamatok indítás előtti optimalizálását biztosítják; biztonságosak a rendszer számára.

Hálózati kapcsolatok

A leírásokat tartalmazó ablak a navigációs ablakban kijelölt (TCP vagy UDP) protokollt használó hálózaton keresztül kommunikáló folyamatok és alkalmazások listáját tartalmazza azzal a távoli címmel együtt, amelyhez az alkalmazás kapcsolódik. Ellenőrizheti a DNS-szerverek IP-címeit is.

A részleteket megjelenítő ablak a leírásokat tartalmazó ablakban kijelölt elemek további adatait (például a fájl méretét vagy kivonatát) jeleníti meg.

Fontos rendszer-beállítási bejegyzések

Ebben a csomópontban látható a kijelölt, gyakran a rendszerrel kapcsolatos különböző hibákra (például az indítási programok vagy a böngésző segédobjektumainak megadására stb.) vonatkozó rendszer-beállítási bejegyzések listája.

A leírásokat megjelenítő ablakban megtalálható, hogy mely fájlok kapcsolódnak az adott rendszer-beállítási bejegyzésekhez. További adatokat találhat a részleteket megjelenítő ablakban.

Szolgáltatások

A leírásokat megjelenítő ablak tartalmazza a Windows-szolgáltatásként regisztrált fájlok listáját. A részleteket megjelenítő ablakban ellenőrizheti a szolgáltatás indításának beállított módját, valamint a fájl adatait.

Illesztőprogramok

A rendszerben telepített illesztőprogramok listája.

Kritikus fájlok

A leírásokat tartalmazó ablakban látható a Microsoft Windows operációs rendszerrel kapcsolatos kritikus fájlok tartalma.

Rendszerinformációk

A hardverrel és a szoftverrel, valamint a beállított környezeti változókkal és a felhasználói jogokkal kapcsolatos részletes információkat jeleníti meg.

Fájladatok

A Program Files mappában található fontos rendszerfájlok és fájlok listája. A fájlokkal kapcsolatos további információk a leírásokat és a részleteket megjelenítő ablakokban találhatók.

Névjegy

Az ESET SysInspector alkalmazással kapcsolatos információk.

5.5.2.3 Összehasonlítás

Az Összehasonlítás szolgáltatás lehetővé teszi a felhasználónak, hogy összehasonlítson két meglévő naplót. A szolgáltatás megjeleníti azokat az elemeket, amelyek egyik naplóban sem gyakoriak. Akkor érdemes használni, ha nyomon szeretné követni a változásokat a rendszerben – felismerheti például a kártékony kódok tevékenységét.

Elindítását követően az alkalmazás létrehoz egy új naplót, amely új ablakban jelenik meg. Ha egy naplót fájlba szeretne menteni, keresse meg a **Fájl** menü **Napló mentése** parancsát. A naplófájlokat később megnyithatja és megtekintheti. Meglévő napló a **Fájl** menü **Napló megnyitása** parancsával nyitható meg. A program főablakában az ESET SysInspector egyszerre mindig egy naplót jelenít meg.

A naplók összehasonlításának előnye, hogy összevethet egy jelenleg aktív naplót egy fájlba mentett korábbival. A naplók összehasonlításához mutasson a **Fájl** menü **Naplók összehasonlítása** pontjára, majd válassza a **Fájl kijelölése** parancsot. A program összehasonlítja a kijelölt naplót a fő programablakokban lévő aktív naplóval. Az összehasonlítási napló csak a két napló közötti különbségeket jeleníti meg.

Megjegyzés: Két naplófájl összehasonlítása esetén válassza a **Fájl** menü **Napló mentése** parancsát, és mentse a fájlt ZIP-fájlként. Ekkor a program mindkét fájlt menti. Ha később megnyit egy ilyen fájlt, a program automatikusan összehasonlítja a benne található naplókat.

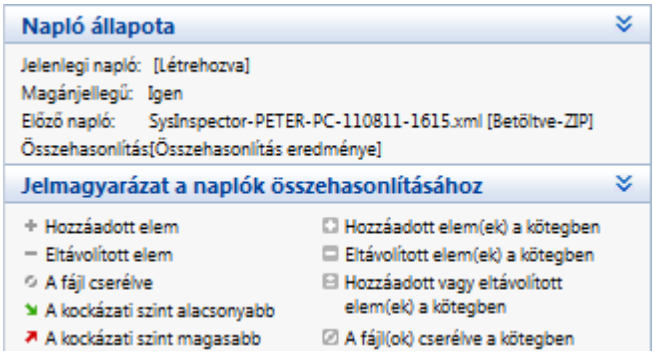
A megjelenített elemek mellett az ESET SysInspector feltünteti az összehasonlított naplók közötti különbségeket azonosító jeleket.

– jel azonosítja azokat az elemeket, amelyek csak az aktív naplóban találhatók meg, és nem szerepeltek a megnyitott összehasonlítási naplóban. + jel azonosítja azokat az elemeket, amelyeket csak a megnyitott napló tartalmazott, az aktív naplóból hiányoznak.

Az elemek mellett látható jelek magyarázata:

- + új érték, nem szerepel az előző naplóban
- a fastruktúra rész új értékeket tartalmaz
- – eltávolított érték, csak a korábbi naplóban szerepel
- a fastruktúra rész eltávolított értékeket tartalmaz
- érték/fájl megváltozott
- a fastruktúra rész módosított értékeket/fájlokat tartalmaz
- a kockázati szint csökkent, vagy az előző naplóban magasabb volt
- a kockázati szint nőtt, vagy az előző naplóban alacsonyabb volt

A bal alsó sarokban látható magyarázó rész ismerteti az összes szimbólumot, és megjeleníti az összehasonlított naplók nevét.



Minden összehasonlító napló egy fájlba menthető, és később megnyitható.

Példa

Hozzon létre és mentsen egy naplót, amelyben a rendszerre vonatkozó eredeti információkat rögzíti egy előző.xml nevű fájlba. A rendszeren végzett módosításokat követően nyissa meg az ESET SysInspector eszközt, és engedélyezze egy új napló létrehozását. Mentse azt egy *jelenlegi.xml* nevű fájlba.

A két napló közötti változások nyomon követéséhez válassza a **Fájl** menü **Naplók összehasonlítása** parancsát. A program létrehozza a naplók közötti különbségeket megjelenítő összehasonlító naplót.

Ugyanaz az eredmény érhető el az alábbi parancssori kapcsoló használata esetén:

SysIsnpector.exe jelenlegi.xml korabbi.xml

5.5.3 Parancssori paraméterek

Az ESET SysInspector támogatja a jelentések parancssorból történő létrehozását az alábbi paraméterek használatával:

/gen	napló létrehozása közvetlenül a parancssorból a grafikus felhasználói felület futtatása nélkül
/privacy	napló létrehozása a bizalmas adatok kihagyásával
/zip	a létrejövő napló tárolása közvetlenül a merevlemezen egy tömörített fájlban
/silent	a napló-létrehozási folyamatjelző sáv megjelenítésének letiltása
/help, /?	a parancssori paraméterekre vonatkozó információk megjelenítése

Példák

Adott napló betöltése közvetlenül a böngészőbe: *SysInspector.exe "c:\kliensnaplo.xml"*
Napló létrehozása egy aktuális helyen: *SysInspector.exe /gen*
Napló létrehozása adott mappában: *SysInspector.exe /gen="c:\mappa\"*
Napló létrehozása adott fájlba/helyen: *SysInspector.exe /gen="c:\mappa\ujnaplom.xml"*
Napló létrehozása a bizalmas adatok kihagyásával közvetlenül egy tömörített fájlba: *SysInspector.exe /gen="c:\ujnaplom.zip" /privacy /zip*
Két napló összehasonlítása: *SysInspector.exe "jelenlegi.xml" "eredeti.xml"*

Megjegyzés: Ha a fájl vagy mappa neve szóközt tartalmaz, idézőjelek közé kell tenni.

5.5.4 Eltávolító szkript

A szolgáltatási szkriptekkel a felhasználók az ESET SysInspector alkalmazásban könnyen eltávolíthatják a nemkívánatos objektumokat a rendszerből.

A szolgáltatási szkript lehetővé teszi, hogy a felhasználó teljes egészében vagy részlegesen exportálja az ESET SysInspector naplóját. Az exportálás után megjelölheti a törlendő kéretlen objektumokat. Ezután a megjelölt objektumok törlése céljából futtathatja a módosított naplót.

Az eltávolító szkriptet a rendszerhibák diagnosztizálásában gyakorlattal rendelkező tapasztalt felhasználók használhatják. A nem megalapozott módosítások az operációs rendszer sérüléséhez vezethetnek.

Példa

Ha azt gyanítja, hogy a számítógépet megfertőzte egy vírus, amelyet a vírusirtó program nem ismer fel, kövesse az alábbi részletes utasításokat:

- Futtassa az ESET SysInspector alkalmazást egy új rendszer-pillanatkép létrehozásához.
- Jelölje be az első elemet a csoport bal oldalán (a fastruktúrában), nyomja le a Ctrl billentyűt, majd az összes elem megjelöléséhez jelölje ki az utolsó elemet.
- Kattintson a jobb gombbal a kijelölt objektumokra, és a helyi menüben válassza a **Kijelölt szakaszok exportálása az eltávolító szkriptbe** parancsot.
- A program egy új naplóba exportálja a kijelölt objektumokat.
- Ez a teljes folyamat legfontosabb lépése: nyissa meg az új naplót, és módosítsa a - attribútumot a + jelre az eltávolítandó összes objektum esetén. Ellenőrizze, hogy nem jelölte-e meg az operációs rendszer fontos fájljainak és objektumainak valamelyikét.
- Nyissa meg az ESET SysInspector alkalmazást, kattintson a **Fájl** > **Eltávolító szkript futtatása** parancsra, és írja be a szkript elérési útját.
- Kattintson az **OK** gombra a szkript futtatásához.

5.5.4.1 Eltávolító szkript létrehozása

Ha létre szeretne hozni egy szkriptet, az ESET SysInspector fő ablakában kattintson a jobb gombbal a menü fastruktúrájának bármely elemére (a bal oldali panelen). A helyi menüben válassza a **Minden szakasz exportálása az eltávolító szkriptbe** vagy a **Kijelölt szakaszok exportálása az eltávolító szkriptbe** parancsot.

Megjegyzés: Két napló összehasonlítása közben nem lehet az eltávolító szkriptet exportálni.

5.5.4.2 Az eltávolító szkript struktúrája

A szkript fejlécének első sorában láthatók a motor verziójára (ev), a grafikus felhasználói felület verziójára (gv) és a napló verziójára (lv) vonatkozó információk. Ezek az adatok használhatók a szkriptet létrehozó és a végrehajtás során az eltéréseket megakadályozó .xml fájl lehetséges módosításainak a nyomon követéséhez. A szkript ezen részét nem célszerű módosítani.

A fájl többi része olyan szakaszokból áll, amelyekben szerkeszthetők az elemek (jelölje meg a szkript által feldolgozandókat). A feldolgozáshoz az egyes elemek előtt található „-" karakter „+" karakterré változtatásával jelölheti meg az elemeket. A szkriptben üres sor választja el egymástól a szakaszokat. Minden szakaszhoz tartozik egy szám és egy cím.

01) Running processes

Ez a szakasz a rendszerben futó összes folyamat listáját tartalmazza. Az egyes folyamatok azonosítására szolgál az UNC-útvonal és azt követően a CRC16 kivonatkód csillag jelek (*) között.

Példa:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Ebben a példában egy folyamat, a module32.exe a kiválasztott („+" karakterrel megjelölt); a folyamat a szkript végrehajtásakor fejeződik be.

02) Loaded modules

Ez a szakasz tartalmazza az aktuálisan használt rendszermodulokat.

Példa:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Ebben a példában a khbekhb.dll modul van megjelölve egy „+" karakterrel. Amikor a szkript fut, felismeri az adott modult használó folyamatokat, és befejezi azokat.

03) TCP connections

Ebben a szakaszban találhatók a meglévő TCP-kapcsolatokra vonatkozó adatok.

Példa:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Amikor a szkript fut, megkeresi a szoftvercsatorna tulajdonosát a megjelölt TCP-kapcsolatokban, bezárja a szoftvercsatornát, és így rendszererőforrásokat szabadít fel.

04) UDP endpoints

Ez a szakasz a meglévő UDP-végpontokról tartalmaz információkat.

Példa:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Amikor a szkript fut, elszigeteli a szoftvercsatorna tulajdonosát a megjelölt UDP-végpontoknál, és leállítja a szoftvercsatornát.

05) DNS server entries

Ez a szakasz az aktuális DNS-szerver konfigurációjáról tartalmaz információkat.

Példa:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

A szkript futtatásakor a szoftver eltávolítja a megjelölt DNS-szerverbejegyzéseket.

06) Important registry entries

Ez a szakasz a beállításjegyzék (rendszerleíró adatbázis) fontos bejegyzéseiről tartalmaz információkat.

Példa:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

A szkript végrehajtásakor a szoftver törli, O bájt értékre csökkenti, illetve az alapértékekre visszaállítja a megjelölt elemeket. Az egyes bejegyzésekhez alkalmazandó művelet az adott beállításjegyzékben szereplő bejegyzés kategóriájától és kulcsértékétől függ.

07) Services

Ez a szakasz jeleníti meg a rendszerben regisztrált szolgáltatásokat.

Példa:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

A szkript végrehajtásakor a szoftver leállítja és eltávolítja a megjelölt szolgáltatásokat és az azoktól függő szolgáltatásokat.

08) Drivers

Ez a szakasz a telepített illesztőprogramokat sorolja fel.

Példa:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

A szkript végrehajtásakor a szoftver megszünteti a kijelölt illesztőprogramok regisztrálását, és eltávolítja az illesztőprogramokat.

09) Critical files

A szakasz az operációs rendszer alapvető fontosságú fájljainak adatait tartalmazza.

Példa:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

A szoftver törli a kijelölt elemeket vagy visszaállítja azok eredeti értékeit.

5.5.4.3 Eltávolító szkriptek végrehajtása

Jelölje meg az összes kívánt elemet, majd mentse és zárja be a szkriptet. Futtassa a szerkesztett szkriptet az ESET SysInspector fő ablakából. a Fájl menü **Eltávolító szkript futtatása** parancsával. Amikor megnyit egy szkriptet, a program a következő üzenetet küldi: **Biztosan futtatja a(z) "%Scriptname%" eltávolító szkriptet?** A kiválasztás megerősítését követően egy másik figyelmeztetés jelenhet meg arról, hogy a futtatni kívánt eltávolító szkript nincs aláírva. Kattintson a **Futtatás** gombra a szkript futtatásához.

A szkript sikeres végrehajtásáról egy párbeszédpanelen kap megerősítést.

Ha a szkript csak részlegesen hajtható végre, a következő üzenetet tartalmazó párbeszédpanel jelenik meg: **Az eltávolító szkript futtatása részlegesen sikerült. Megtekinti a hibajelentést?** Kattintson az **Igen** gombra, ha meg szeretne tekinteni egy olyan összetett hibajelentést, amely a végre nem hajtott műveleteket tartalmazza.

Ha a szkript nem ismerhető fel, a következő üzenet jelenik meg: **A kijelölt eltávolító szkript nincs aláírva. Aláíratlan és ismeretlen szkriptek futtatásával komoly veszélynek teszi ki a számítógép adatait. Biztosan futtatja a szkriptet, és végrehajtja a műveleteket?** Ezt okozhatják a szkriptben lévő eltérések (sérült fejléc vagy szakaszcím, szakaszok közül hiányzó üres sor stb.). Újranyithatja a szkriptfájlt, és a szkripten belül javíthatja a hibákat, illetve létrehozhat egy új eltávolító szkriptet.

5.5.5 Billentyűparancsok

Az ESET SysInspector alkalmazásban használható billentyűparancsok közé tartoznak az alábbiak:

Fájl

Ctrl+O	meglévő napló megnyitása
Ctrl+S	létrehozott naplók mentése

Létrehozás

Ctrl+G	általános rendszerállapot-ellenőrzés
Ctrl+H	rendszerellenőrzés végrehajtása, amely során a program naplózhatja a bizalmas információkat

Elemek szűrése

1, O	elfogadható, az 1–9. kockázati szintű elemek jelennek meg
2	elfogadható, a 2–9. kockázati szintű elemek jelennek meg
3	elfogadható, a 3–9. kockázati szintű elemek jelennek meg
4, U	ismeretlen, a 4–9. kockázati szintű elemek jelennek meg
5	ismeretlen, az 5–9. kockázati szintű elemek jelennek meg
6	ismeretlen, a 6–9. kockázati szintű elemek jelennek meg
7, B	kockázatos, a 7–9. kockázati szintű elemek jelennek meg
8	kockázatos, a 8–9. kockázati szintű elemek jelennek meg
9	kockázatos, a 9. kockázati szintű elemek jelennek meg
-	kockázati szint csökkentése
+	kockázati szint növelése
Ctrl+9	szűrési mód, azonos vagy magasabb szint
Ctrl+O	szűrési mód, csak azonos szint

Nézet

Ctrl+5	megtekintés gyártó szerint, összes gyártó
Ctrl+6	megtekintés gyártó szerint, csak Microsoft
Ctrl+7	megtekintés gyártó szerint, összes többi gyártó
Ctrl+3	megjelenítés teljes részletességgel
Ctrl+2	megjelenítés közepes részletességgel
Ctrl+1	alapmegjelenítés
Backspace	navigálás vissza egy lépéssel
Szóköz	navigálás előre egy lépéssel
Ctrl+W	fa kibontása
Ctrl+Q	fa összecsukása

Egyéb billentyűparancsok

Ctrl+T	a keresési eredményekben való kijelölést követően az elem eredeti helyére ugrás
Ctrl+P	elem alapinformációinak megjelenítése
Ctrl+A	elemre vonatkozó összes információ megjelenítése
Ctrl+C	az aktuális elem fastruktúrájának másolása
Ctrl+X	elemek másolása
Ctrl+B	a kijelölt elemre vonatkozó információk keresése az interneten
Ctrl+L	a kijelölt fájlt tartalmazó mappa megnyitása
Ctrl+R	a megfelelő bejegyzés megnyitása a beállításszerkesztőben
Ctrl+Z	elérési út másolása fájlba (ha az elem egy fájlra vonatkozik)
Ctrl+F	a keresési mező megjelenítése
Ctrl+D	keresési eredmények bezárása
Ctrl+E	eltávolító szkript futtatása

Összehasonlítás

Ctrl+Alt+O	eredeti/összehasonlítási napló megnyitása
Ctrl+Alt+R	összehasonlítás visszavonása
Ctrl+Alt+1	összes elem megjelenítése
Ctrl+Alt+2	csak a hozzáadott elemek megjelenítése, a napló csak az aktuális naplóban lévő elemeket jeleníti meg
Ctrl+Alt+3	csak az eltávolított elemek megjelenítése, a napló az előző naplóban lévő elemeket jeleníti meg
Ctrl+Alt+4	csak a cserélt elemek megjelenítése (fájlokat beleértve)
Ctrl+Alt+5	csak a naplók közötti különbségek megjelenítése
Ctrl+Alt+C	összehasonlítás megjelenítése
Ctrl+Alt+N	jelenlegi napló megjelenítése
Ctrl+Alt+P	előző napló megnyitása

Egyéb

F1	súgó megnyitása
Alt+F4	program bezárása
Alt+Shift+F4	program bezárása automatikusan
Ctrl+I	napló statisztikája

5.5.6 Rendszerkövetelmények

Az ESET SysInspector zavartalan működéséhez a rendszernek meg kell felelnie az alábbi hardver- és szoftverkövetelményeknek:

Windows 2000, Windows XP vagy Windows 2003 operációs rendszer esetén

400 MHz 32 bites (x86) / 64 bites (x64)
128 MB RAM rendszermemória
10 MB szabad lemezterület
Super VGA (800 × 600 képpont felbontással)

Windows 7, Windows Vista, Windows 2008 operációs rendszer esetén

1 GHz 32 bites (x86) / 64 bites (x64)
512 MB RAM rendszermemória
10 MB szabad lemezterület
Super VGA (800 × 600 képpont felbontással)

5.5.7 Gyakori kérdések

Szükséges az ESET SysInspector futtatásához rendszergazdai jogosultság?

Az ESET SysInspector futtatásához nincs szükség rendszergazdai jogosultságra, az összegyűjtött információk némelyike azonban csak rendszergazdai fiókból érhető el. Ha szokásos vagy korlátozott jogosultsággal bíró felhasználóként futtatja az eszközt, kevesebb információhoz jut az operációs rendszer környezetével kapcsolatosan.

Létrehoz az ESET SysInspector egy naplófájlt?

Az ESET SysInspector létrehoz egy naplófájlt a számítógép konfigurációjáról. A naplófájl mentéséhez a főmenüben válassza a **Fájl** > **Napló mentése** parancsot. A program XML formátumban menti a naplókat. Alapértelmezés szerint a program a *%USERPROFILE%\Dokumentumok* mappába menti a fájlokat a következő fájlelnevezési szabályok szerint: SysInpsector-%COMPUTERNAME%-ÉÉHHNN-ÓÓPP.XML. A mentés előtt a naplófájl helyét és nevét tetszés szerint módosíthatja.

Hogyan tekinthetem meg az ESET SysInspector naplófájlját?

Az ESET SysInspector által létrehozott naplófájl megtekintéséhez futtassa a programot, és a főmenüben válassza a **Fájl** menü **Napló megtekintése** parancsát. Emellett az ESET SysInspector alkalmazásba is húzhatja a naplófájlokat. Ha gyakran kell ellenőriznie az ESET SysInspector naplófájljait, javasoljuk, hogy az asztalon hozzon létre egy, a SYSINSPECTOR.EXE fájlra mutató parancsikont, majd ezt követően az alkalmazásba húzhatja, és megtekintheti a fájlokat. Biztonsági okokból a Windows Vista/Windows 7 letilthatja a különböző biztonsági engedélyekkel rendelkező ablakok közötti húzást.

Elérhető a naplófájl formátumának specifikációja és egy szoftverfejlesztői készlet (SDK)?

A program még fejlesztés alatt áll, ezért jelenleg sem a naplófájl formátumának specifikációja, sem SDK nem érhető el. A program kiadását követően a vásárlói visszajelzések és igények alapján várható, hogy elérhetővé tesszük ezeket.

Hogyan méri fel az ESET SysInspector az adott objektumok kockázatát?

A legtöbb esetben az ESET SysInspector heurisztikai szabályok használatával kockázati szinteket rendel az objektumokhoz (fájlokhoz, folyamatokhoz, beállításkulcsokhoz stb.), melyek megvizsgálják az egyes objektumok jellemzőit, majd mérlegelik a kártevő tevékenység előfordulásának lehetőségét. A heurisztikai szabályok alapján az objektumok kockázati szintje az 1: Elfogadható (zöld) és a 9: Kockázatos (vörös) közé eshet. A bal oldali navigációs ablakban a szakaszok színezése az ott található objektum legmagasabb kockázati szintje alapján történik.

A „6: ismeretlen" (vörös) kockázati szint azt jelenti, hogy az objektum veszélyes?

Az ESET SysInspector értékelése nem bizonyítja, hogy egy objektum veszélyes – ezt egy biztonsági szakértőnek kell eldöntenie. Az ESET SysInspector gyors értékelést biztosít, így a biztonsági szakértők megállapíthatják, hogy a rendszerben lévő mely objektumokat kell tovább vizsgálniuk szokatlan működést keresve.

Hogyan kapcsolódik az ESET SysInspector az internethez?

Számos alkalmazáshoz hasonlóan az ESET SysInspector aláírása is digitális aláírású „tanúsítvánnyal" bizonyítja, hogy a szoftvert az ESET cég adta ki, és nem volt módosítva. A tanúsítvány hitelesítéséhez az operációs rendszer felveszi a kapcsolatot egy hitelesítésszolgáltatóval a szoftver kibocsátójának azonosítása céljából. Ez a normál eljárás a Microsoft

Windows rendszerben futó összes digitálisan aláírt program esetén.

Mi az Anti-Stealth technológia?

Az Anti-Stealth technológia a rootkitek hatékony felismerésére szolgál.

Ha a rendszert megtámadja egy rootkitként viselkedő kártékony kód, a felhasználó ki van téve annak a kockázatnak, hogy az adatai megsérülnek, vagy ellopják azokat. A rootkitek felismerése szinte lehetetlen az ellenük védelmet nyújtó speciális eszköz nélkül.

Mi az oka, hogy a fájlok néha „Signed by MS" (MS által aláírva) jelzéssel rendelkeznek, ugyanakkor eltérő a „vállalatnév" bejegyzésük?

Amikor az ESET SysInspector megkísérli egy végrehajtható fájl digitális aláírásának azonosítását, először megkeresi, hogy a fájlban található-e beágyazott digitális aláírás. Ez az oka, hogy érvényesítéskor a fájlon belül azonosítást használ a program. Másrészt, ha a fájl nem tartalmaz digitális aláírást, az ESI elkezdi megkeresni a feldolgozott végrehajtható fájl információit tartalmazó CAT-fájlt (biztonsági katalógus – *%systemroot%\system32\catroot* mappa). Ha megtalálja a kapcsolódó CAT-fájlt, annak digitális aláírását fogja alkalmazni a végrehajtható fájl érvényesítési folyamatában.

Ez az oka, hogy egyes fájlok „Signed by MS" megjelölésűek, „vállalatnév" bejegyzésük azonban eltér.

Példa:

A Windows 2000 tartalmazza a HyperTerminal alkalmazást. Helye: *C:\Program Files\Windows NT*. A fő alkalmazás végrehajtható fájlja nem digitálisan aláírt, az ESET SysInspector azonban a Microsoft által aláírt fájlként jelöli meg. Ennek oka a *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* elérési útban a *C:\Program Files\Windows NT\hypertrm.exe* fájlra (a HyperTerminal alkalmazás fő fájljára) mutató hivatkozás, és az *sp4.cat* a Microsoft által aláírt fájl.

5.5.8 Az ESET Smart Security részét képező ESET SysInspector

Az ESET SysInspector szakasz megnyitásához az ESET Smart Security **Eszközök** lapján kattintson az **ESET SysInspector** gombra. Az ESET SysInspector ablak kezelési rendszere hasonló a számítógép-ellenőrzési naplók vagy az ütemezett feladatok esetén megismert rendszerhez. A rendszer pillanatképeivel végzett minden művelet – létrehozás, megtekintés, összehasonlítás, eltávolítás és exportálás – egy vagy két kattintással elérhető.

Az ESET SysInspector ablak a létrehozott pillanatképekre vonatkozó alapinformációkat tartalmazza, többek között a létrehozás idejét, egy rövid megjegyzést, a pillanatképet készítő felhasználó nevét, valamint a pillanatkép állapotát.

A pillanatképek **összehasonlításához**, **létrehozásához** vagy **törléséhez** az ESET SysInspector ablakban a pillanatképek listája alatt található gombok használhatók. Ezek a műveletek a helyi menüből is elérhetők. A rendszer kijelölt pillanatképe a helyi menü **Nézet** parancsával tekinthető meg. Ha a kijelölt pillanatképet fájlba szeretné exportálni, kattintson a jobb gombbal a fájlra, majd válassza az **Exportálás** parancsot.

Az elérhető parancsok részletes leírása:

- **Összehasonlítás** – Lehetővé teszi két meglévő napló összehasonlítását. Akkor érdemes használni, ha össze szeretné hasonlítani a jelenlegi és az előző naplót. A beállítás érvénybe lépéséhez jelöljön ki két összehasonlítandó pillanatképet.
- **Hozzáadás** – Új rekordot hoz létre. Ezt megelőzően egy rövid megjegyzést kell hozzáfűzni a bejegyzéshez. A pillanatkép létrehozási folyamatának (az aktuálisan létrehozott pillanatképből) százalékos értékben megadott haladása az **Állapot** oszlopban látható. Minden létrehozott pillanatképet a **Létrehozva** állapot jelöl.
- **Eltávolítás** – Eltávolítja a listából a bejegyzéseket.
- **Exportálás** – XML-fájlba menti a kijelölt bejegyzést (tömörített változatban is).

5.6 ESET SysRescue

Az ESET SysRescue egy segédprogram, amely lehetővé teszi az ESET Smart Security szoftvert tartalmazó rendszerindító lemez létrehozását. Az ESET SysRescue fő előnye abban rejlik, hogy az ESET Smart Security az operációs rendszertől függetlenül fut, így közvetlen hozzáféréssel rendelkezik a lemezhez és a teljes fájlrendszerhez. Ennek köszönhetően eltávolíthatók az általában (például az operációs rendszer futásakor) nem törölhető fertőzések.

5.6.1 Minimális követelmények

Az ESET SysRescue a Windows Vista-alapú Microsoft Windows előtelepítési környezet (Windows PE) 2.x verziójával működik. A Windows PE az ingyenes Windows automatikus telepítési csomag (Windows AIK) részét képezi, ezért az ESET SysRescue helyreállító CD létrehozása előtt telepíteni kell a Windows AIK csomagot (http://go.eset.eu/AIK). A Windows PE 32 bites verzió támogatása következtében 32 bites ESET Smart Security telepítési csomag szükséges az ESET SysRescue helyreállító CD létrehozásához a 64 bites rendszereken. Az ESET SysRescue a Windows AIK 1.1-es és újabb verzióit támogatja. Az ESET SysRescue az ESET Smart Security 4.0-s és újabb verzióinak részét képezi.

Támogatott operációs rendszerek

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 a KB926044. számú cikkel
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 a KB926044. számú cikkel
- Windows XP Service Pack 3

5.6.2 Helyreállító CD készítése

Az ESET SysRescue indításához kattintson a **Start** > **Programok** > **ESET** > **ESET Smart Security** > **ESET SysRescue** parancsra.

A varázsló először ellenőrzi, hogy megtalálható-e a Windows AIK és a rendszerindító adathordozó létrehozásához megfelelő eszköz. Ha a *Windows AIK* nincs telepítve a számítógépen (vagy hibás, esetleg nem megfelelő a telepítése), a varázsló felajánlja a telepítés lehetőségét, vagy megadja a Windows AIK mappájának elérési útját (http://go.eset.eu/AIK).

A következő lépésben jelölje ki az ESET SysRescue helyeként szolgáló adathordozót.

5.6.3 A cél kiválasztása

Az ESET SysRescue CD, DVD és USB-meghajtó mellett ISO-fájlba is menthető. Az ISO-lemezképet később CD-re vagy DVD-re írhatja, illetve más módon is használhatja (olyan virtuális környezetben, mint például a VmWare vagy a Virtualbox).

Az USB céladathordozóként való kijelölése esetén előfordulhat, hogy egyes számítógépeken nem működik a rendszerindítás. A BIOS néhány verziójánál probléma léphet fel a BIOS és a rendszertöltés-vezérlő kommunikációjával (például a Windows Vista rendszeren). Ebben az esetben a rendszerindításkor az alábbi hibaüzenetek jelennek meg:

```
fájl: \boot\bcd
állapot: 0xc000000e
információ: Hiba történt a rendszerindítási konfigurációs adatok olvasásakor.
```

A hiba esetén javasoljuk, hogy USB-adathordozó helyett használjon CD-t.

5.6.4 Beállítások

Az ESET SysRescue CD létrehozásának megkezdése előtt a telepítési varázsló a létrehozási paramétereket az ESET SysRescue varázsló utolsó lépésében jeleníti meg. Ezek a **Módosítás** gombra kattintva változtathatók meg. A beállítások az alábbiak:

- Mappák
- ESET vírusirtó
- További lehetőségek
- Internetes protokoll
- Rendszerindító USB-eszköz (ha célként USB-eszköz van kijelölve)
- Írás (ha célként CD vagy DVD van kijelölve)

A **Létrehozás** gomb akkor inaktív, ha nincs MSI telepítési csomag megadva vagy ESET biztonsági szoftver telepítve a számítógépen. Telepítési csomag kijelöléséhez kattintson a **Módosítás** gombra, és lépjen az **ESET vírusirtó** lapra. Ha nem ad meg felhasználónevet és jelszót (**Módosítás** > **ESET vírusirtó**), a **Létrehozás** gomb inaktív marad.

5.6.4.1 Mappák

Ideiglenes mappa – A helyreállító CD ESET SysRescue alkalmazással történő létrehozásakor szükséges fájlok munkamappája.

ISO-mappa – a létrehozás befejezését követően a létrejövő ISO-fájl mentéséhez használt mappa

A lapon lévő listában látható az összes helyi és társított hálózati meghajtó a rendelkezésre álló szabad területtel együtt. Ha egyes mappák kevés szabad lemezterülettel rendelkező meghajtón találhatók, javasoljuk, hogy jelöljön ki egy több szabad hellyel rendelkező másik meghajtót. Ellenkező esetben előfordulhat, hogy a kevés szabad lemezterület miatt a létrehozás idő előtt befejeződik.

Külső alkalmazások – Olyan további programok megadását teszi lehetővé, amelyeket az ESET SysRescue adathordozóról történő rendszerindítás után kíván futtatni vagy telepíteni.

Külső alkalmazások belefoglalása – Külső programok hozzáadását teszi lehetővé a készítendő ESET SysRescue CD-hez.

Kijelölt mappa – Ez az ESET SysRescue-lemezre másolandó programokat tartalmazó mappa.

5.6.4.2 ESET vírusirtó

Az ESET SysRescue CD létrehozásához az ESET-fájlok két forrásból kerülhetnek a fordítóprogramba.

ESS/EAV-mappa – Az a mappa, ahová az ESET programot telepítette a számítógépen.

MSI-fájl – Az MSI telepítőcsomag.

Ezután frissítheti a nup-fájlok helyét. Alapértelmezés szerint általában az **ESS/EAV-mappa/MSI-fájl** beállítást célszerű megadni. Egyes esetekben egyéni **frissítési mappa** is választható, például a vírusdefiníciós adatbázis régebbi vagy újabb verziójának használatakor.

Felhasználónév és jelszó az alábbi két forrásból választható:

Telepített ESS/EAV – Az aktuálisan telepített ESET Smart Security szoftverből másolt felhasználónév és jelszó.

Felhasználó által megadott – A megfelelő mezőkben megadott felhasználónév és jelszó.

Megjegyzés: Az ESET SysRescue CD-n található ESET Smart Security frissítése az interneten keresztül vagy az ESET SysRescue CD-t futtató számítógépen telepített ESET Security mappájából történhet.

5.6.4.3 További beállítások

A **További lehetőségek** lapon optimalizálhatja az ESET SysRescue CD-t a számítógép memóriájának a méretéhez. Jelölje be az **576 MB vagy nagyobb** választógombot a CD tartalmának a műveleti memóriába (RAM) történő írásához. Ha a **kisebb mint 576 MB** választógombot jelöli be, a program a helyreállító CD-ről fog futni.

Külső illesztőprogramok – Itt adhat meg illesztőprogramokat az adott hardverhez (általában hálózati adapterhez). Bár a Windows előtelepítési környezet a hardverek széles skáláját támogató Windows Vista SP1 rendszeren alapul, a rendszer néha nem ismeri fel a hardvert. Ekkor kézzel kell felvenni az illesztőprogramot. Az illesztőprogram két módon vehető fel az ESET SysRescue alkalmazással végzett CD-létrehozáshoz: kézzel (a **Hozzáadás** gombbal) és automatikusan (az **Aut. keresés** gombbal). A kézi felvétel esetén ki kell jelölnie a megfelelő .inf fájl elérési útját (megfelelő *.sys fájlnak is lennie kell a mappában). Automatikus felvétel esetén az illesztőprogram keresése automatikusan történik az adott számítógép operációs rendszerében. Az automatikus felvételt csak abban az esetben javasoljuk, ha az ESET SysRescue alkalmazást olyan számítógépen használja, amelynek hálózati adaptere megegyezik az ESET SysRescue CD létrehozásához használt számítógép hálózati adapterével. A CD létrehozásakor az ESET SysRescue felveszi az illesztőprogramot, így a felhasználónak nem kell később keresnie azt.

5.6.4.4 Internetes protokoll

Ezen a részen az alapvető hálózati információknak és az előre definiált kapcsolatoknak az ESET SysRescue szoftver szerint történő beállítását végezheti el.

Válassza az **Automatikus magán IP-cím** lehetőséget az IP-cím DHCP-szerverről történő automatikus beszerzéséhez.

Alternatívaként ez a hálózati kapcsolat kézzel megadott (azaz statikus) IP-címet is használhat. Válassza az **Egyéni** lehetőséget a megfelelő IP-beállítások megadásához. Ha ezt a lehetőséget választja, meg kell adnia egy **IP-címet** és egy **Alhálózati maszkot** a helyi hálózat és a nagy sebességű internetkapcsolat számára. Írja be az **Előnyben részesített DNS-szerver** és az **Alternatív DNS-szerver** mezőbe az elsődleges és a másodlagos DNS-szerver címét.

5.6.4.5 Rendszerindító USB-eszköz

Ha céladathordozóként USB-eszközt adott meg, a rendelkezésre álló USB-adathordozók közül (ha több is van) a **Rendszerindító USB-eszköz** lapon jelölhet ki egyet.

Az **Eszköz** kiválasztásával adja meg a megfelelő cél helyét, ahová az ESET SysRescue szoftvert telepíteni fogja.

Figyelmeztetés: A kijelölt USB-eszköz formázása az ESET SysRescue adatainak létrehozása során történik meg. Az eszközön lévő összes adat törlődik.

Ha a **Gyorsformázás** lehetőséget választja, a formázás a partícióban lévő összes adatot eltávolítja, de nem vizsgálja a lemez rossz szektorait. Akkor használja ezt a lehetőséget, ha az USB-eszköz előzőleg formázva volt, és bizonyosan nem sérült.

5.6.4.6 Írás

Ha CD-t vagy DVD-t jelölt ki céladathordozóként, további írási paramétereket adhat meg az **Írás** lapon.

ISO-fájl törlése – Jelölje be ezt a jelölőnégyzetet, ha az ESET SysRescue CD létrehozása után törölni szeretné az ISO-fájlokat.

Törlés engedélyezve – A jelölőnégyzet bejelölésével kiválaszthatja a gyors és a teljes törlést.

Lemezíró eszköz – Jelölje ki az íráshoz használandó meghajtót.

Figyelmeztetés: Ez az alapértelmezett beállítás. Újraírható CD/DVD használata esetén a rajta lévő összes adat törlődik.

Az Adathordozó csoportban találhatók a CD/DVD-meghajtóban lévő adathordozóra vonatkozó információk.

Írási sebesség – Jelölje ki a kívánt sebességet a legördülő listában. Az írási sebesség kiválasztásakor figyelembe kell venni a lemezíró eszköz jellemzőit és a használt CD/DVD típusát.

5.6.5 Az ESET SysRescue használata

A helyreállító CD/DVD/USB akkor használható, ha a számítógépet az ESET SysRescue rendszerindító adathordozóról indítja. A rendszerindítási prioritás a BIOS-ban módosítható. A rendszerindítási menüt a számítógép indításakor is megjelenítheti, általában (az alaplap/BIOS verziójától függően) az F9–F12 billentyűk egyikének lenyomásával.

Miután a számítógép elindult a rendszerindító adathordozóról, az ESET Smart Security is elindul. Mivel az ESET SysRescue csak adott esetekben használatos, a **Számítógép ellenőrzése**, a **Frissítés** és a **Beállítások** egyes csoportjai kivételével az ESET Smart Security általános verziójában található néhány védelmi modulra és szolgáltatásra nincs szükség. Az ESET SysRescue legfontosabb szolgáltatása a vírusdefiníciós adatbázis frissítése. Javasoljuk, hogy a számítógép ellenőrzése előtt frissítse a programot.

5.6.5.1 Az ESET SysRescue alkalmazása

Tételezzük fel, hogy a számítógépet megfertőzte egy vírus, amely a végrehajtható (.exe) fájlokat módosítja. Az ESET Smart Security minden fertőzött fájlt képes megtisztítani az *explorer.exe* kivételével, amely még csökkentett módban sem tisztítható meg.

Ennek oka, hogy az alapvető Windows-folyamatok egyikeként az *explorer.exe* csökkentett módban is elindul. Az ESET Smart Security semmilyen műveletet nem tud végrehajtani a fájlon, ezért az fertőzött marad.

Ilyen esetben az ESET SysRescue segítségével megoldhatja a problémát. Az ESET SysRescue nem igényli az operációs rendszer egyetlen összetevőjét sem, ezért képes a lemezen lévő bármely fájl feldolgozására (megtisztítására, törlésére).

6. Szószedet

6.1 Kártevők típusai

A kártevő egy olyan szoftver, amely a felhasználó tudta nélkül megpróbál bejutni a rendszerbe, és felhasználja azt saját maga továbbterjesztésére, miközben egyéb kártékony tevékenységet is végez.

6.1.1 Vírusok

A számítógépes vírus olyan fertőzés, amely fájlokat rongál meg a számítógépen. A vírusok a biológiai vírusokról kapták a nevüket, mert hozzájuk hasonló technikákkal terjednek egyik számítógépről a másikra.

Elsősorban végrehajtható fájlokat és dokumentumokat támadnak meg. Úgy replikálódnak, hogy „törzsüket" hozzáfűzik a célfájl végéhez. A vírusok működése dióhéjban a következő: a fertőzött fájl végrehajtása után a vírus (még az eredeti alkalmazás előtt) aktiválódik, és elvégzi meghatározott feladatát. Az eredeti alkalmazás csak ezt követően indul el. A vírus csak akkor képes megfertőzni a számítógépet, ha a felhasználó (véletlenül vagy szándékosan) futtatja vagy megnyitja a kártékony programot.

A számítógépes vírusok céljukat és súlyosságukat tekintve igen változatosak. Némelyikük rendkívül veszélyes, mert képes szándékosan fájlokat törölni a merevlemezről. Ugyanakkor vannak vírusok, amelyek nem okoznak valódi károkat, és egyetlen céljuk, hogy bosszantsák a felhasználót, vagy fitogtassák szerzőjük műszaki jártasságát.

Fontos megjegyezni, hogy a vírusok (a trójaiakkal vagy a kémprogramokkal összehasonlítva) egyre inkább a ritkaság kategóriájába tartoznak, mert anyagilag nem jelentenek vonzerőt a kártékony szoftverek szerzőinek. Magát a „vírus" kifejezést az összes fertőzés megjelölésére is szokták – gyakran tévesen – alkalmazni. Használatát azonban fokozatosan egy új, pontosabb elnevezés, a „kártevő" (angolul malware – malicious software, vagyis kártékony szoftver) kezdi kiszorítani.

Ha a számítógépet vírus fertőzi meg, a fájlokat vissza kell állítani eredeti állapotukba, azaz egy vírusvédelmi programmal meg kell tisztítani őket.

Jól ismert vírusok például a következők: OneHalf, Tenga és Yankee Doodle. Jól ismert rootkitek például a következők: AFX, Settec, FU és Vanquish.

6.1.2 Férgek

A számítógépes féreg olyan kártékony kódot tartalmazó program, amely hálózatba kötött számítógépeket támad meg, és a hálózaton önmagától terjed. A vírus és a féreg között az az alapvető különbség, hogy a férgek önállóan képesek replikálódni és terjedni – ehhez nincs szükségük gazdafájlokra (vagy rendszertöltő szektorokra). A férgek a névjegylista e-mail címein keresztül terjednek, illetve a hálózati alkalmazások biztonsági réseit használják ki.

A férgek tehát sokkal életképesebbek, mint a vírusok. Az internet széles körű hozzáférhetősége miatt kibocsátásuk után már néhány órán – esetenként néhány percen – belül a világon bárhol felbukkanhatnak. Az önálló és gyors replikációra való képességük más kártevő szoftvereknél lényegesen veszélyesebbé teszi őket.

A rendszerben aktiválódott féreg számos kellemetlenséget okozhat: fájlokat törölhet, ronthatja a rendszer teljesítményét, sőt akár kikapcsolhat egyes programokat. A férgek természetéből adódóan alkalmasak más típusú kártékony kódok szállítására.

Ha a számítógép féreggel fertőződik meg, ajánlatos törölni a fertőzött fájlokat, mivel azok nagy valószínűséggel kártékony kódot tartalmaznak.

Jól ismert férgek például a következők:: Lovsan/Blaster, Stration/Warezov, Bagle és Netsky.

6.1.3 Trójaiak

Előzményeiket tekintve a számítógépes trójaiak olyan kártékony kódok, amelyek hasznos programként tüntetik fel magukat, és csalárd módon ráveszik a felhasználót a futtatásukra. Fontos azonban megjegyezni, hogy ez a régebbi trójaiakra volt igaz, az újabbaknak már nincs szükségük álcázásra. Kizárólagos céljuk, hogy a lehető legegyszerűbben bejussanak a rendszerbe, és kifejtsék kártékony tevékenységüket. A „trójai" olyan gyűjtőfogalommá vált, amely a más kategóriákba nem sorolható kártékony szoftvereket jelöli.

Tág fogalomról lévén szó, gyakran különböző alkategóriákra osztják.

- **Letöltő** – Olyan kártékony program, amely képes más fertőző kódokat letölteni az internetről.
- **Vírushordozó** – Olyan trójai faló, amelynek rendeltetése, hogy más típusú kártevő szoftvereket telepítsen a fertőzött számítógépekre.
- **Hátsó kapu** – Olyan alkalmazás, amely távoli támadókkal kommunikál, lehetővé téve számukra a rendszerbe való behatolást és irányításának átvételét.
- **Billentyűzetfigyelő** – Olyan program, amely rögzíti, hogy a felhasználó milyen billentyűket üt le, és elküldi ezt az információt a távoli támadóknak.
- **Tárcsázó** – Emelt díjas telefonszámok tárcsázására tervezett program. Szinte lehetetlen észrevenni, amikor egy ilyen program új kapcsolatot létesít. A tárcsázók csak faxmodemek révén tudnak kárt okozni, ezek azonban már egyre ritkábbak.

A trójaiak általában .exe kiterjesztésű alkalmazások. Ha a számítógép valamelyik fájljáról kiderül, hogy trójai faló, ajánlatos törölni, mivel nagy valószínűséggel kártevő kódot tartalmaz.

Jól ismert trójaiak például a következők:: NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 Rootkitek

A rootkitek olyan kártékony programok, amelyek a támadónak hozzáférést biztosítanak a rendszerhez, miközben jelenlétüket elrejtik. Miután bejutnak a rendszerbe (általában annak biztonsági rését kihasználva), a rootkitek az operációs rendszer funkcióinak használatával igyekeznek észrevétlenek maradni a vírusvédelmi szoftverek előtt: folyamatokat, fájlokat és Windows-beállításértékeket (rendszerleíró adatbázisbeli adatokat) rejtenek el. Emiatt a szokványos vizsgálati technikákkal szinte lehetetlen felderíteni őket.

Kétféle felismerési szinten kerülhető el a rootkitek okozta fertőzés:

1. Az első szint az, amikor ezek a szoftverek megpróbálnak bejutni a rendszerbe. Még nincsenek jelen, ezért inaktívak. A legtöbb vírusvédelmi rendszer ezen a szinten képes a rootkitek elhárítására (feltéve, hogy egyáltalán fertőzöttként felismerik az ilyen fájlokat).
2. A második szint az, amikor a szokványos ellenőrzés elől elrejtőznek. Az ESET Smart Security felhasználói élvezhetik az aktív rootkitek észlelésére és elhárítására képes Anti-Stealth technológia előnyeit.

6.1.5 Reklámprogramok

A reklámprogramok a hirdetések terjesztésére szolgáló szoftverek. Ebbe a kategóriába a reklámanyagokat megjelenítő programok tartoznak. A reklámprogramok gyakran automatikusan megnyitnak egy reklámot tartalmazó előugró ablakot a böngészőben, vagy módosítják a kezdőlapot. Gyakran szabadszoftverekkel („freeware" programokkal) vannak egybecsomagolva, mert ezek fejlesztői így próbálják meg csökkenteni az (általában hasznos) alkalmazásaik költségeit.

A reklámprogram önmagában nem veszélyes, de a hirdetések zavarhatják a felhasználókat. A veszélyt az jelenti, hogy az ilyen programok (a kémprogramokhoz hasonlóan) nyomkövetést is végezhetnek.

Ha freeware szoftver használata mellett dönt, szenteljen különleges figyelmet a telepítőprogramnak. A legtöbb telepítő valószínűleg értesítést küld a reklámprogramok telepítéséről. Gyakran lehetőség van a szoftver reklámprogram nélküli telepítésére.

Egyes szoftverek nem telepíthetők reklámprogram nélkül, vagy csak korlátozottan használhatók. Ez azt jelenti, hogy a reklámprogram gyakran „legálisan" férhet hozzá a rendszerhez, mert a felhasználó erre engedélyt adott neki. Részesítse azonban előnyben a biztonságot, hiszen jobb félni, mint megijedni. Ha a számítógépen található valamelyik fájlról kiderül, hogy reklámprogram, ajánlatos törölni, mivel nagy valószínűséggel kártékony kódot tartalmaz.

6.1.6 Kémprogramok

Ebbe a kategóriába tartozik az összes olyan alkalmazás, amely magánjellegű információkat továbbít a felhasználó tudta vagy hozzájárulása nélkül. A kémprogramok nyomkövető funkciókat használva különféle statisztikai adatokat küldhetnek, például a meglátogatott webhelyek listáját, a felhasználó névjegyalbumában lévő e-mail címeket vagy a leütött billentyűk listáját.

A kémprogramok szerzői azt állítják, hogy ezek az eljárások a felhasználók igényeinek és érdeklődési körének feltérképezésére, így hatékonyabban célzott reklámok létrehozására szolgálnak. A probléma azonban az, hogy nincs világos határvonal a hasznos és a kártékony alkalmazások között, és senki sem lehet biztos abban, hogy az összegyűjtött információkkal nem élnek-e vissza. A kémprogramokkal megszerzett adatok lehetnek biztonsági kódok, PIN kódok, bankszámlaszámok és így tovább. A kémprogramokat szerzőik gyakran ingyenes programverziókkal csomagolják egybe, hogy jövedelemre tegyenek szert, vagy szoftverük megvásárlására csábítsanak. Gyakran előfordul, hogy egy program a telepítéskor tájékoztatja a felhasználót a kémprogram jelenlétéről, amivel arra igyekszik rávenni őt, hogy frissítsen a szoftver kémprogrammentes verziójára.

Az egyenrangú (P2P) hálózatok kliensalkalmazásai például olyan ingyenes („freeware") termékek, amelyekről köztudott, hogy kémprogrammal egybecsomagolva jelennek meg. A Spyfalcon vagy a Spy Sheriff (és sok más) szoftver külön alkategóriába tartozik – ezek kémprogramvédelmi alkalmazásoknak tüntetik fel magukat, ám valójában maguk is kémprogramok.

Ha a számítógép valamelyik fájljáról kiderül, hogy kémprogram, ajánlatos törölni, mivel nagy valószínűséggel kártékony kódot tartalmaz.

6.1.7 Veszélyes alkalmazások

Számtalan törvényesen használható alkalmazás létezik a hálózati számítógépek adminisztrációjának egyszerűsítése céljából. Nem megfelelő kezekben azonban kártékony célokra használhatók. Az ESET Smart Security az ilyen kártevők felismerésére szolgál.

A „veszélyes alkalmazások" csoportjába a kereskedelemben kapható, törvényes szoftverek tartoznak, többek között a távoli hozzáférést biztosító eszközök, a jelszófeltörő alkalmazások, valamint a billentyűzetfigyelők (a felhasználó minden billentyűleütését rögzítő programok).

Ha észreveszi, hogy egy veszélyes alkalmazás van jelen a számítógépen és fut (de nem Ön telepítette), kérjen tanácsot a hálózati rendszergazdától, vagy távolítsa el az alkalmazást.

6.1.8 Kéretlen alkalmazások

A **kéretlen alkalmazások** nem feltétlenül kártevők, de hátrányosan befolyásolhatják a számítógép teljesítményét. Ezek az alkalmazások általában engedélyt kérnek a telepítésükhöz. Miután a számítógépre kerülnek, a rendszer a telepítésük előtti állapotához képest eltérően kezd viselkedni. A lényegesebb változások az alábbiak:

- Korábban nem látott új ablakok nyílnak meg (előugró ablakok, hirdetések).
- Rejtett alkalmazások aktiválódnak és futnak.
- Megnő a rendszererőforrások terhelése.
- Módosulnak a keresési eredmények.
- Az alkalmazások távoli szerverekkel kommunikálnak.

6.2 Távolról kezdeményezett támadások típusai

Sok olyan speciális eljárás létezik, amely lehetővé teszi a támadóknak, hogy távoli rendszerek biztonságát megsértsék. Ezek különböző kategóriákba sorolhatók.

6.2.1 Szolgáltatásmegtagadási támadások (DoS, DDoS)

A *szolgáltatásmegtagadás* olyan támadás, amely megkísérli a számítógépet vagy a hálózatot elérhetetlenné tenni a felhasználók számára. Előfordulhat, hogy az érintett felhasználók közötti kommunikáció megszakad, és később sem működik normálisan. A szolgáltatásmegtagadási támadásnak kitett számítógépeket általában újra kell indítani, mert egyébként nem működnek megfelelően.

A támadás célpontja a legtöbb esetben egy webszerver, a célja pedig, hogy bizonyos időre elérhetetlenné tegye azt a felhasználóknak.

6.2.2 DNS-mérgezés

A DNS (tartománynévszerver) mérgezésével a hackerek becsaphatják a számítógép által használt DNS-szervert, hogy az általuk küldött hamis adatokat szabályszerűnek és hitelesnek fogadja el. A hamis adatok egy ideig a gyorsítótárban találhatók, lehetővé téve, hogy a támadók átírják például a DNS-szerver IP-címek formájában küldött válaszait. Ennek következményeként a webhelyekhez hozzáférni kívánó felhasználók az eredeti tartalom helyett vírusokat és férgeket fognak letölteni.

6.2.3 Féregtámadások

A számítógépes féreg olyan kártékony kódot tartalmazó program, amely hálózatba kötött számítógépeket támad meg, és a hálózaton önmagától terjed. A hálózati férgek különböző alkalmazások biztonsági réseit aknázzák ki. Az internet elterjedtsége miatt kibocsátásuk után már néhány órán – esetenként néhány percen – belül a világon bárhol felbukkanhatnak.

A legtöbb féregtámadás (például a Sasser vagy az SqlSlammer) kivédhető a tűzfal alapértelmezett biztonsági beállításainak alkalmazásával, vagy a nem védett, illetve nem használt portok letiltásával. Szintén fontos az operációs rendszer frissítése a legújabb biztonsági javítócsomagok letöltésével és telepítésével.

6.2.4 Portfigyelés

A portfigyeléssel megállapítható, hogy mely portok nyitottak egy hálózatba kötött számítógépen. A portfigyelő olyan szoftver, amelyet ilyen portok felderítésére terveztek.

A számítógép portjai a kimenő és a bejövő adatokat kezelő virtuális pontok, így biztonsági szempontból kulcsfontosságúak. Nagyméretű hálózatokon a portfigyelők által gyűjtött információk segítséget nyújthatnak a lehetséges biztonsági rések felderítéséhez. A portfigyelők ilyen célú használata törvényes.

A portfigyelést azonban a biztonság megsértésével kísérletező hackerek is alkalmazzák. Első lépésként adatcsomagokat küldenek mindegyik portra. A visszaérkező válaszok típusától függően megállapíthatják, hogy mely portok vannak használatban. Maga a figyelés nem okoz károkat, de jó tudni, hogy az ilyesfajta tevékenység felfedheti az esetleges biztonsági réseket, és lehetővé teheti, hogy a támadók átvegyék az irányítást a távoli számítógépek felett.

A hálózati rendszergazdáknak tanácsos a használaton kívüli portokat letiltani, a használatban lévőket pedig védeni a jogosulatlan hozzáférés ellen.

6.2.5 TCP-deszinkronizáció

A TCP-deszinkronizáció a TCP-eltérítéses támadásokban alkalmazott eljárás. Egy folyamat váltja ki, amelyben a bejövő adatcsomagok sorozatszáma eltér a várttól. A váratlan sorozatszámú csomagokat a rendszer elveti (vagy pufferbe menti, ha az aktuális kommunikációs ablakban találhatók).

A deszinkronizációban mindkét kommunikációs végpont elveti a fogadott csomagokat. Ezen a ponton a távoli támadók behatolhatnak a rendszerbe, és helyes sorozatszámú csomagokat juttathatnak be. A támadók befolyásolhatják vagy akár módosíthatják is a kommunikációt.

A TCP-eltérítéses támadások célja, hogy megszakítsák a szerver és a kliens, illetve az egyenrangú társgépek kommunikációját. Sok támadás elkerülhető azzal, ha minden TCP-szegmensen hitelesítést alkalmaznak. Szintén tanácsos a hálózati eszközöket az ajánlott konfigurációval használni.

6.2.6 SMB-továbbítás

Az SMBRelay és az SMBRelay2 olyan speciális programok, amelyek képesek távoli számítógépek megtámadására. Ehhez a Server Message Block fájlmegosztási protokollt használják, amely réteg a NetBIOS felett helyezkedik el. A helyi hálózaton keresztül mappát vagy könyvtárt megosztó felhasználók nagy valószínűséggel ezt a fájlmegosztási protokollt használják.

A helyi hálózaton zajló kommunikációban jelszókivonatok is továbbítódnak oda-vissza.

Az SMBRelay egy kapcsolatot fogad a 139-es és a 445-ös UDP-porton, továbbítja a kliens és a szerver között váltott csomagokat, és módosítja azokat. A csatlakozás és a hitelesítés után a kliens kapcsolata megszakad. Az SMBRelay egy új virtuális IP-címet hoz létre. Az új cím a „net use \\192.168.1.1" paranccsal érhető el, majd a Windows bármely hálózati szolgáltatásával használható. Az SMBRelay az egyeztetés és a hitelesítés kivételével továbbítja az SMB protokollon folytatott kommunikációt. A távoli támadók mindaddig használhatják az IP-címet, amíg a a kliensszámítógéppel fennáll a kapcsolat.

Az SMBRelay2 ugyanazon az elven működik, mint az SMBRelay, csak IP-címek helyett NetBIOS-neveket használ. Mindkét program képes a betolakodó illetéktelen személyek általi támadások kivitelezésére. Ez azt jelenti, hogy távoli támadók észrevétlenül elolvashatják és módosíthatják azokat az üzeneteket, amelyeket két kommunikációs végpont között váltanak, illetve üzeneteket szúrhatnak be a kommunikációs folyamatba. Az ilyen jellegű támadásoknak kitett számítógépek gyakran lefagyhatnak, vagy váratlanul újraindulhatnak.

A támadások elkerülése érdekében azt javasoljuk, hogy alkalmazzon hitelesítő jelszavakat vagy kulcsokat.

6.2.7 ICMP protokollon alapuló támadások

Az ICMP (Internet Control Message Protocol) egy elterjedt és széles körben alkalmazott internetes protokoll. Legfőképpen hálózati számítógépek használják különféle hibaüzenetek küldésére.

Távoli támadók megkísérlik kihasználni az ICMP protokoll sebezhetőségét. Az ICMP protokoll a hitelesítést nem igénylő egyirányú kommunikációhoz használható. Hibáit kihasználva úgynevezett szolgáltatásmegtagadási (DoS, Denial of Service) támadás idézhető elő. Elképzelhető olyan támadás is, amely jogosulatlan személyeknek biztosíthat hozzáférést a számítógép bejövő és kimenő adatcsomagjaihoz.

Az ICMP-alapú támadások tipikus példái a pingelárasztás, az ICMP_ECHO-elárasztás és a smurf-támadások. Az ICMP-alapú támadásnak kitett gépek (főleg az interneten kommunikáló alkalmazások) lényegesen lassabban működnek, és az internetkapcsolat létrehozásakor különböző hibákat érzékelnek.

6.3 E-mail

Az e-mail (elektronikus levél) egy számos előnyt kínáló modern kommunikációs forma. A rugalmas, gyors és közvetlen e-mail kulcsszerepet játszott az internet 1990-es évek eleji elterjedésében.

A nagyfokú anonimitás miatt azonban az e-mail (és általában az internet) levélszemétküldésre és hasonló illegális tevékenységekre is lehetőséget nyújt. A levélszemét magába foglalja a kéretlen reklámleveleket, a megtévesztő üzeneteket és a kártékony szoftverek, kártevők terjesztését. Az ezzel járó kényelmetlenséget és veszélyt növeli, hogy a levélszemét küldése minimális költséggel jár, és készítőiknek számos eszköz rendelkezésükre áll ahhoz, hogy új e-mail címeket szerezzenek. Emellett a levélszemét mennyisége és változatossága is megnehezíti a kordában tartását. Minél hosszabb ideig használja e-mail címét, annál nagyobb a valószínűsége, hogy az bekerül egy levélszemétküldő adatbázisába. Néhány tipp a megelőzéshez:

- Lehetőség szerint ne tegye közzé e-mail címét az interneten.
- Címét csak megbízható embereknek adja át.
- A bonyolult címek kitalálására kevesebb az esély, ezért lehetőség szerint ne használjon egyszerű e-mail címeket (aliasokat).
- Ne válaszoljon a már a postafiókjába került levélszemétre.
- Az internetes űrlapok kitöltésekor legyen elővigyázatos, különösen az „Igen, szeretnék tájékoztatást kapni" jellegű válaszokkal.
- Használjon külön e-mail címeket – egyet például a munkához, másikat a barátokkal történő kapcsolattartáshoz stb.
- Időnként módosítsa az e-mail címét.
- Használjon levélszemétszűrő alkalmazást.

6.3.1 Reklámok

Az internetes reklám a hirdetési módszerek egyik leggyorsabban fejlődő változata. Marketingszempontból ennek a módszernek a legjelentősebb előnyei a költségtakarékosság, a célközönség közvetlen elérése és a hatékonyság. Ezenkívül az üzenetek szinte azonnal célba érnek. Számos cég e-mailes marketingeszközöket használ a meglévő és a leendő ügyfelekkel való kapcsolattartáshoz.

Ez a hirdetési mód törvényes, mert a felhasználó bizonyos termékek esetében kíváncsi lehet kereskedelmi információkra is. Számos cég azonban kéretlen kereskedelmi üzeneteket küld. Ebben az esetben az e-mail reklám levélszemétnek minősül.

A kéretlen üzenetek száma napjainkra jelentős problémává vált, és nincs jele annak, hogy ez a szám csökkenne. A kéretlen e-mailek szerzői gyakran szabályszerű üzenetnek álcázzák a levélszemetet.

6.3.2 Megtévesztő üzenetek

A téves információkat hordozó megtévesztő üzenetek (angolul: hoax) az interneten terjednek. A megtévesztő üzenetek általában e-mailben és kommunikációs eszközökön (például ICQ és Skype) keresztül terjednek. Az üzenet tartalma gyakorta vicc vagy városi legenda.

A megtévesztő üzenetek félelmet, bizonytalanságot és kétséget próbálnak kelteni a címzettekben, elhitetve velük, hogy egy felderíthetetlen vírus fájlokat töröl és jelszavakat olvas be, illetve más káros tevékenységet folytat a rendszerben.

Egyes megtévesztő üzenetek arra kérik a címzetteket, hogy továbbítsák az üzeneteket ismerőseiknek, és így életben tartják az adott megtévesztő üzenetet. Vannak mobiltelefonos témájú, segélykérő, külföldről pénzt ajánló stb. témájú üzenetek is. A készítő célját a legtöbbször nem lehet megállapítani.

Ha egy üzenet arra szólítja fel, hogy minden ismerősének továbbítsa, az jó eséllyel lehet megtévesztő üzenet. Az interneten számos webhely képes ellenőrizni, hogy egy e-mail szabályszerű-e. Továbbküldés előtt keressen rá az interneten a megtévesztésgyanús üzenetekre.

6.3.3 Adathalászat

Az adathalászat kifejezés olyan bűnözői tevékenységet határoz meg, amely manipulációs technikákat alkalmaz (vagyis a felhasználót bizalmas információk kiszolgáltatására veszi rá). Célja bizalmas adatok, például bankszámlaszámok vagy PIN kódok megszerzése.

Hozzáférésre általában úgy tesznek szert, hogy megbízható személyek vagy cégek (például pénzintézetek, biztosítási társaságok) nevében e-mailt küldenek a célszemélynek. Az esetleg az eredeti forrásból származó grafikus vagy tartalmi elemeket tartalmazó e-mail külsőre eredetinek tűnhet. Benne különféle ürügyekkel (adategyeztetés, pénzügyi műveletek) arra kérhetik a felhasználót, hogy adjon meg bizonyos személyes adatokat, például bankkártyaszámot vagy felhasználónevet és jelszót. Az ily módon megadott adatokat azután könnyűszerrel ellophatják, és visszaélhetnek velük.

A bankok, biztosítási társaságok és más törvényesen működő cégek sohasem kérnek felhasználóneveket és jelszavakat kéretlen levelekben.

6.3.4 Levélszemét felismerése

A kéretlen e-mailek azonosításában segítségére lehet néhány ismérv. Ha egy üzenet megfelel az alábbi feltételek némelyikének, akkor az valószínűleg levélszemét.

- A feladó címe nem szerepel az Ön címjegyzékében.
- Az üzenet nagyobb pénzösszeget ígér, de előzetesen egy kisebb összeget kér.
- Az üzenet különféle indokokra (adategyeztetés, pénzügyi műveletek) hivatkozva személyes adatok (bankszámlaszám, felhasználónév, jelszó stb.) megadását kéri.
- Az üzenetet idegen nyelven írták.
- Olyan termék megvásárlására szólít fel, amely iránt Ön nem érdeklődik. Ha mégis vásárolni szeretne, ellenőrizze, hogy az üzenet feladója megbízható forgalmazó-e. Ehhez forduljon az eredeti termék gyártójához.
- Egyes szavakat hibás írásmóddal tartalmaz a levélszemétszűrő megtévesztése érdekében. Ilyen például a „vaigra” a „viagra” helyett stb.

6.3.4.1 Szabályok

A vírusvédelmi alkalmazások és levelezőprogramok szövegkörnyezetében a szabályok a levelezés működésének szabályozására szolgáló eszközök. Két logikai részből állnak:

1. Feltétel (például egy adott címről érkező üzenet)
2. Művelet (például az üzenet törlése vagy megadott mappába helyezése)

A szabályok száma és párosítási lehetőségei vírusvédelmi alkalmazásonként eltérőek. Ezek a szabályok jelentik a levélszemét (kéretlen levelek) elleni védővonalat. Tipikus példák:

- 1. Feltétel: A beérkező e-mail olyan szavakat tartalmaz, amelyek gyakran fordulnak elő kéretlen levelekben
  2. Művelet: Az üzenet törlése
- 1. Feltétel: A beérkező e-mail .exe kiterjesztésű mellékletet tartalmaz
  2. Művelet: A melléklet törlése, és a levél kézbesítése a postaládába
- 1. Feltétel: A beérkező üzenet attól a cégtől érkezik, ahol dolgozik
  2. Művelet: Az üzenet áthelyezése a „Munka" mappába

Javasolt az ilyen szabályok vegyes alkalmazása, mert ezzel megkönnyítheti a levelek kezelését, és hatékonyabban szűrheti ki a levélszemetet.

6.3.4.2 Bayes-féle szűrő

A Bayes-féle eljáráson alapuló levélszemétszűrés az e-mailek szűrésének hatékony, szinte minden levélszemétszűrő program által használt módja. A Bayes-féle szűrő felhasználónként használható, és igen nagy pontossággal képes azonosítani a kéretlen e-maileket.

A szűrő a következő elv szerint működik: Az első fázis a tanítási folyamat. A felhasználó kellő számú üzenetet megjelöl szabályszerűként, illetve levélszemétként (általában mindkettőből 200-at). A szűrő elemzi a kategóriákat és megtanulja, hogy a levélszemét gyakran tartalmazza például a „rolex" vagy a „viagra" szót, míg a szabályszerű üzenetek például a családtagoktól vagy a felhasználó címjegyzékében szereplő címről származnak. Megfelelő számú üzenet feldolgozását követően a Bayes-féle szűrő képes egy bizonyos „levélszemétindexet" rendelni az üzenetekhez, és meghatározni, hogy az adott üzenet levélszemétnek minősül-e.

A Bayes-féle szűrő legfőbb előnye a rugalmasság. Ha például a felhasználó biológus, a biológiára és a kapcsolódó tudományágakra vonatkozó bejövő e-mailek általában alacsonyabb valószínűségi indexet kapnak. Ha egy üzenet olyan szót tartalmaz, amely általában kéretlen levéllé minősítené, de a felhasználó címjegyzékében szereplő egyik személytől származik, a program szabályszerűként jelöli meg, mert a címjegyzékben szereplő feladókra alacsonyabb valószínűségi index vonatkozik.

6.3.4.3 Engedélyezőlista

Általánosságban az engedélyezőlista olyan elemek vagy személyek listája, amelyek vagy akik elfogadottak, illetve hozzáférési engedélyt kaptak. Az „e-mail engedélyezőlista" kifejezés olyan partnerek listáját jelenti, akiktől a felhasználó üzeneteket fogad. Az ilyen listák e-mail címekben, tartománynevekben vagy IP-címekben keresett kulcsszavakon alapulnak.

Ha az engedélyezőlista „kivételek" módban működik, a többi címről, tartományból vagy IP-címről érkező üzeneteket a program nem fogadja. Ha azonban ha a lista nem kizáró jellegű, a program az ilyen üzeneteket nem törli, hanem más módon szűri.

Az engedélyezőlista a tiltólista alapelvének fordítottjára épül. Karbantartása viszonylag egyszerű, sokkal inkább, mint a tiltólistáké. A levélszemét hatékonyabb szűrése érdekében azt javasoljuk, hogy engedélyező- és tiltólistát egyaránt használjon.

6.3.4.4 Tiltólista

A tiltólista általános értelemben a nem elfogadott vagy tiltott elemek és személyek felsorolása. A virtuális világban ez egy olyan technika, amely a listán nem szereplő összes felhasználótól származó üzenet fogadását engedélyezi.

A tiltólistának két típusa van. A felhasználók által a levélszemétszűrő alkalmazásukban létrehozott és a speciális szervezetek által létrehozott professzionális, rendszeresen frissített, az interneten megtalálható tiltólisták.

A hatékony levélszemétszűréshez elengedhetetlen a tiltólisták használata, a listák kezelése azonban a minden nap megjelenő új letiltandó elemek miatt bonyolult. A levélszemét hatékonyabb szűrése érdekében azt javasoljuk, hogy engedélyező- és tiltólistát egyaránt használjon.

6.3.4.5 Szerveroldali ellenőrzés

A szerveroldali ellenőrzés olyan technika, amellyel a fogadott üzenetek száma és a felhasználók reakciója alapján azonosítható a tömegesen küldött levélszemét. Minden üzenet (a tartalmától függően) egyedi digitális „lenyomatot" hagy a szerveren. Az egyedi azonosítószám semmit nem árul el az e-mail tartalmáról. Két azonos üzenet azonos lenyomatot hagy, de két különböző üzenet lenyomata eltérő.

Ha a felhasználó egy üzenetet levélszemétként jelöl meg, a program elküldi az üzenet lenyomatát a szervernek. Ha a szerver több azonos lenyomatot kap (egy bizonyos levélszemétre vonatkozóan), adatbázisba menti őket. A bejövő üzenetek ellenőrzésekor a program a lenyomatukat elküldi a szervernek. A szerver azt az információt küldi vissza, hogy mely lenyomatok felelnek meg a felhasználók által már levélszemétként megjelölt üzenetnek.