ESET Smart Security

telepítési útmutató

A telepítési útmutatóból megismerheti a szoftver újdonságait, és segítséget kap a telepítéshez. Az egyes funkciókat részletesen a szoftverhez tartozó kézikönyvből ismerheti meg, melyet a www.eset.hu/letoltes oldalon talál.

A telepítési útmutató tartalma

1. ESET Smart Security

Az ESET Smart Security egy megbízható, integrált és gyors biztonsági programcsomag, melynek vírus- és kémprogramvédelme az ESET NOD32 Antiviruson alapszik.
Az AV-Comparatives víruslaboratórium által több alkalommal az Év Antivírusának választott ESET NOD32 Antivirus tartja a nemzetközileg elismert Virus Bulletin tesztek VB100% rekordját, és számos más független elismeréssel is rendelkezik.

Az ESET Smart Security ezenkívül tartalmazza az ESET saját fejlesztésű tűzfalát és levélszemétszűrőjét, melyek a NOD32 vírus- és kémprogramvédelemmel szorosan együttműködve intelligens védelmi rendszert alkotnak.

Az ESET Smart Security a hagyományos védelem mellett mesterséges intelligencián alapuló proaktív felismerő algoritmusokat is tartalmaz, így a holnap károkozói ellen is felkészült biztonsági megoldást nyújt. Ezzel a megközelítéssel az ESET új szintre emelte a proaktív védelmet, és biztosítja, hogy az ESET Smart Security felhasználói az olyan legújabb fenyegetések ellen is védve legyenek, melyek ellenszerét még senki sem készítette el a világon.

Az ESET Smart Security segítségével a különböző biztonsági modulok egyazon kezelőfelületről érhetőek el. A program moduljai együttműködnek, és adatokat adnak át egymásnak - a biztonsági programcsomag így igen alacsony erőforrásigény mellett biztosít maximális védelmet.

1.1 Újdonságok

Az ESET Smart Security biztonsági programcsomag három modulból áll, melyek különböző feladatokat látnak el. Az alábbiakban olvashat a modulok funkcióiról és beállítási lehetőségeiről.

■ Vírus- és kémprogramvédelem

Az ESET Smart Security vírus-és kémprogramvédelme a díjnyertes ESET NOD32 Antivirus védelmi rendszeréből ismert ThreatSense® technológián alapszik, mely a szoftver korábbi verzióiban már bizonyította megbízhatóságát. Az ESET Smart Security 4-es változatába a ThreatSense® keresőmotor továbbfejlesztett és optimalizált változata került beépítésre, mely tökéletesen együttműködik az ESET Smart Security többi moduljával.

Szolgáltatás	Leírás
Továbbfejlesztett tisztítás	A vírusvédelmi rendszer intelligens módon, felhasználói beavatkozás nélkül megtisztítja a legtöbb fertőzött fájlt, és csak azokban az esetekben kéri a felhasználó beavatkozását, amikor az automatikus tisztítás nem lehetséges.
Ellenőrzés a háttérben	A számítógép ellenőrzése a háttérben lefuttatható, és nem csökkenti a rendszer teljesítményét.
Kisebb frissítési fájlok	A frissítési fájlok mérete kisebb, mint a NOD32 3-as verziójában. A frissítési fájlok sérülés elleni védelme is javult.
Védelem a népszerű levelezőprogramoknak	A beérkező üzenetek ellenőrzése már nem csak a Microsoft Outlook és Outlook Express, hanem a következő népszerű levelezőprogramokban is lehetséges: Windows Mail, Windows Live Mail és Mozilla Thunderbird.
Önvédelem	A beépített önvédelmi technológia segítségével a szoftver felismeri, ha egy kártevő ki akarja kapcsolni valamelyik védelmi modult, és megakadályozza az ilyen kísérleteket.
Figyelmeztetés az operációs rendszer frissítésére	Az ESET Smart Security figyelmeztet az operációs rendszer frissítéseinek hiányára, mivel a frissítések telepítése nélkül nem biztosított a maximális védelem.
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.
Helyreállító CD	Az ESET SysRescue segítségével a felhasználók létrehozhatnak egy, az ESET Smart Security szoftvert tartalmazó és az operációs rendszertől függetlenül is futtatható rendszerindító CD/DVD/USB adathordozót. Az adathordozó segítségével megtisztíthatja a rendszert a nehezen eltávolítható fertőzésektől.
ESET SysInspector	A számítógépen futó folyamatokról információt nyújtó ESET SysInspector alkalmazás közvetlenül az ESET Smart Security szoftverbe van integrálva. Ha segítségre van szüksége a szoftver használata során, és a szoftver kezelőfelületén **Súgó és támogatás > Kapcsolatfelvétel** lehetőség segítségével lép kapcsolatba a terméktámogatási szolgáltatással, a számítógépről az ESET SysInspector alkalmazással készített állapot-pillanatképet is csatolhat.
Szülői felügyelet	Az ESET Smart Security lehetőséget biztosít arra, hogy korlátozza az Interneten elérhető tartalmakat. A korlátozást a beépített http-szűrő végzi, tiltó és engedélyező listák segítségével. A funkció beállításáról részletesen a 21. oldalon, illetve részletesen http://www.eset.hu/szuloifelugyelet weboldalon olvashat.
Játékos üzemmód	Teljes képernyős módban használt alkalmazások esetén (például prezentációk, videók, számítógépes játékok) célszerű, ha a szoftver nem zavarja a felhasználót felugró tájékoztató üzenetekkel. Amikor a program teljes képernyős felhasználást érzékel, csak azokat a figyelmeztetéseket jeleníti meg, amelyek felhasználói beavatkozást igényelnek.
Külső adathordozók tiltása	Az ESET Smart Security segítségével ellenőrizhetővé válik a külső adathordozók használata. A program lehetőséget ad a külső adathordozók letiltására, így elkerülhető az ismeretlen adathordozókról történő fájlmásolás és futtatás. Vállalati rendszerek esetében a külső adathordozókhoz történő hozzáférés a távadminisztrációt bonyolító ESET Remote Administrator szoftver segítségével is szabályozható.

Személyi tűzfal

A személyi tűzfal figyeli a védett számítógép és a hálózat más számítógépei közötti teljes adatforgalmat.

Az ESET Smart Security személyi tűzfal modulja az alábbi funkciókat tartalmazza:

Szolgáltatás	Leírás
A hálózati kommunikáció alacsony rétegben való ellenőrzése	A hálózati kommunikációnak az adatkapcsolati rétegben való ellenőrzése lehetővé teszi, hogy a személyi tűzfal modul olyan típusú támadásokat is észleljen, amelyek egyébként felderítetlenek maradnának.
IPv6-támogatás	A személyi tűzfal modul megjeleníti az IPv6 típusú címeket, és lehetővé teszi, hogy a felhasználó szabályokat állítson fel hozzájuk.
Alkalmazások figyelése	A program figyeli az alkalmazásokban bekövetkező változásokat, hogy elejét vegye a fertőzéseknek. Az aláírással rendelkező alkalmazások fájljainak módosítása engedélyezhető.
http és pop3 protokollal integrált fájlellenőrzés	A http és a pop3 protokollon érkező fájlokat már azok érkezésekor ellenőrzi a program. A felhasználók így az internet böngészése és e-mailek letöltése közben is biztonságban vannak.
IDS (Behatolás-érzékelő rendszer)	A program képes felismerni a hálózati kommunikáció jellegét és a különféle hálózati támadásokat, és képes automatikusan kivédeni ezeket.
Interaktív, automatikus és házirend alapú üzemmód	A felhasználó választhat, hogy a tűzfal műveleteit a program automatikusan hajtsa-e végre, vagy lehetővé tegye a szabályok interaktív definiálását. A házirend alapú üzemmódban a kommunikáció kezelése a felhasználó vagy a hálózati rendszergazda által előre megadott szabályok szerint történik.
Tanuló üzemmód	A tanuló üzemmód segítségével saját magunk „taníthatjuk” a tűzfalat az új kapcsolatok kezelésére. Amennyiben egy rövid ideig ezt az üzemmódot használjuk, minden használt folyamat automatikusan engedélyezésre kerül egy listán, majd a felhasználók/rendszergazdák a szabályok szerkesztésével létrehozhatják a megfelelően szigorú, de az alkalmazások használatát lehetővé tévő tűzfal-szabályrendszert.
A beépített Windows tűzfal kiváltása	A program feleslegessé teszi a Windows beépített tűzfalát, és együttműködik a Windows Biztonsági központtal, így a felhasználó mindig világos képet kaphat a biztonság állapotáról. Telepítésekor az ESET Smart Security alapértelmezés szerint kikapcsolja a Windows tűzfalat.

■ Levélszemétszűrő

Az ESET Smart Security levélszemétszűrő modulja kiszűri a kéretlen e-maileket, ezáltal fokozza az elektronikus kommunikáció biztonságát és kényelmét.

Szolgáltatás	Leírás
A beérkező levelek pontozása	A program az összes beérkező üzenetet 0-tól (jó levél) 100-ig (levélszemét) terjedő pontozással minősíti, és ez alapján a levélszemétmappába, vagy más, a felhasználó által létrehozott egyéni mappába helyezi át a leveleket.
Optimalizált levélszemétszűrés	Az ESET Smart Security 4 levélszemétszűrő modulja alacsony rendszerterhelés mellett képes kiemelkedő teljesítményt nyújtani. Az integrált szűrő úgy szűri ki a kéretlen leveleket, hogy közben a rendszerre kifejtett hatása minimális marad.
Különböző ellenőrzési eljárások támogatása	- Bayes-féle elemzés. - Szabály alapú ellenőrzés. - Globális ujjlenyomat-adatbázis ellenőrzése.
Teljes együttműködés a levelezőprogramokkal	A levélszemétszűrés már nem csak a Microsoft Outlook, az Outlook Express és a Windows Live Mail levelező-programokban használható, de a Mozilla Thunderbird programok is teljes támogatást élveznek.
Kézi üzenetminősítés-tanítás	Az egyes e-mailek manuálisan is megjelölhetők levélszemét-ként, illetve jó levélként. A rendszer ilyen módon történő tanításával növelhető a levélszemétszűrő hatékonysága.
Kibővített e-mail kiszolgáló támogatás	A POP3 mellett a program az IMAP protokollban történő vírusellenőrzést is támogatja.

1.2 Rendszerkövetelmények

Az ESET Smart Security és az ESET Smart Security Business Edition használatához az alábbi szoftverkörnyezet és hardverkiépítés használata javasolt:

Windows 2000, XP	400 MHz 32-bit (x86) / 64-bit (x64) 128 MB RAM rendszermemória 130 MB szabad lemezterület Super VGA (800 x 600) monitorfelbontás
Windows Vista	1 GHz 32-bit (x86) / 64-bit (x64) 512 MB RAM rendszermemória 130 MB szabad lemezterület Super VGA (800x600) monitorfelbontás

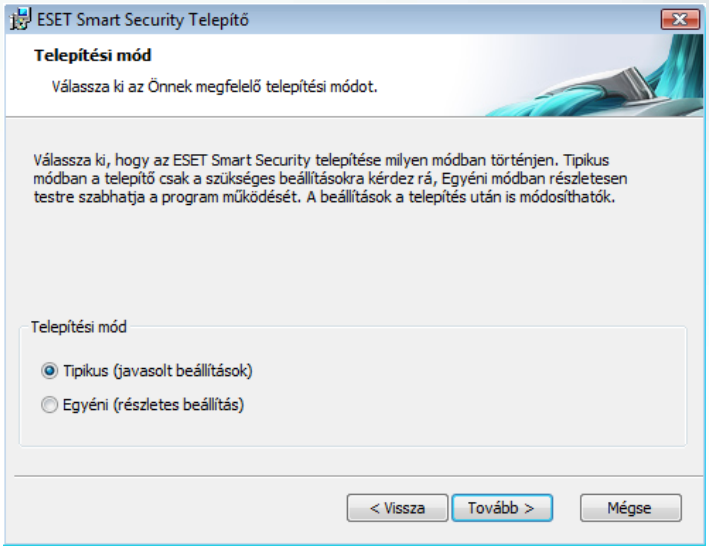
2. Telepítés

A program megvásárlása után az ESET Smart Security telepítőcsomagja letölthető az ESET magyarországi weboldaláról (www.eset.hu/letoltes). A telepítőcsomag neve a programváltozat rövidítéséből, a platform típusából és a program nyelvéből áll össze. Például az ess_nt32_hun.msi névben a tagok a következőket jelentik:
ess = Eset Smart Security
nt32 = Windows NT/XP/2000/2003/Vista 32 bites operációs rendszerhez
hun= Magyar nyelvű

A telepítőcsomag elindítása után a Telepítő Varázsló végigvezeti a telepítés folyamatán.

Először a két elérhető telepítési mód közül kell kiválasztania a megfelelőt:

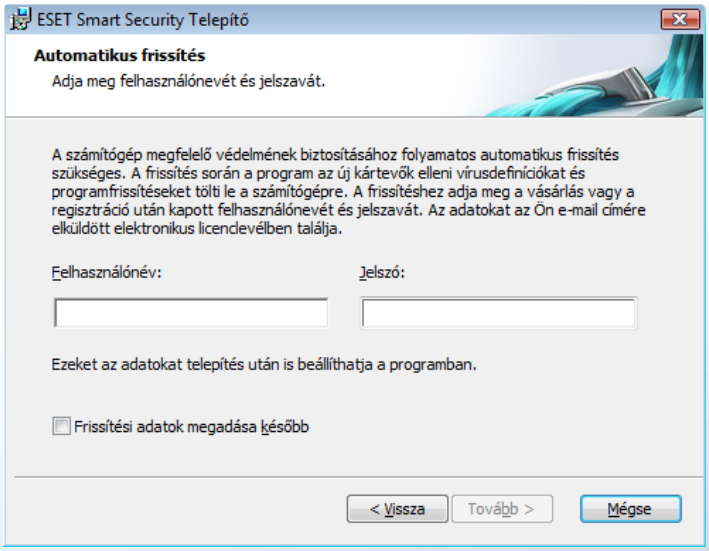
1. Tipikus (javasolt beállítások)
2. Egyéni (részletes beállítás)



2.1 Tipikus telepítési mód

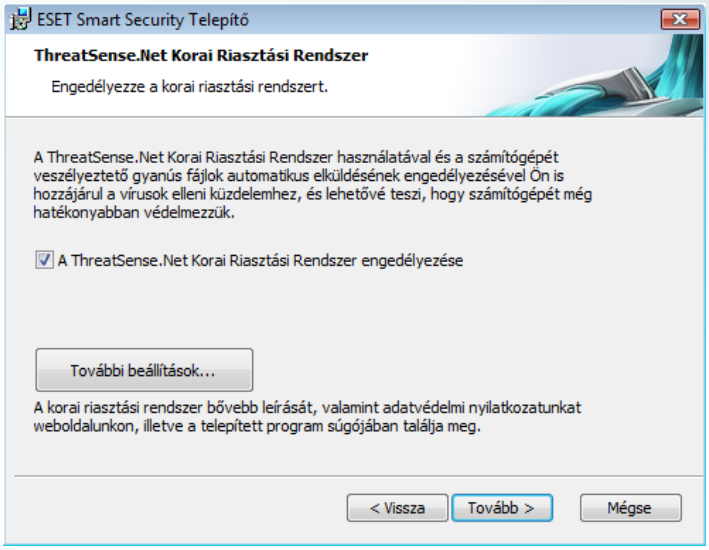
A Tipikus telepítési mód azon felhasználók számára ajánlott, akik nem szeretnék megváltoztatni az ESET Smart Security javasolt beállításait. A Tipikus telepítési mód során azon alapbeállítások kerülnek alkalmazásra, melyek biztosítják a számítógép maximális védelmét, így válassza ezt a telepítési módot, amennyiben nem kíván a részletes konfigurációval foglalkozni.

A Tipikus telepítés során az első fontos lépés, hogy megadjuk a programnak azt a felhasználónevet és jelszót, melynek segítségével letöltheti az automatikus frissítéseket. Az automatikus frissítések letöltése elengedhetetlen a számítógép folyamatos védelmének biztosításához.



A megfelelő mezőkbe gépelje be azt a felhasználónevet és jelszót, melyet a program megvásárlása vagy regisztrációja után kapott. Ha a telepítés időpontjában nem rendelkezik felhasználónévvel és jelszóval, válassza a **Frissítési adatok megadása később** opciót. A felhasználónevet és jelszót később bármikor megadhatja a feltelepített program kezelőfelületén keresztül.

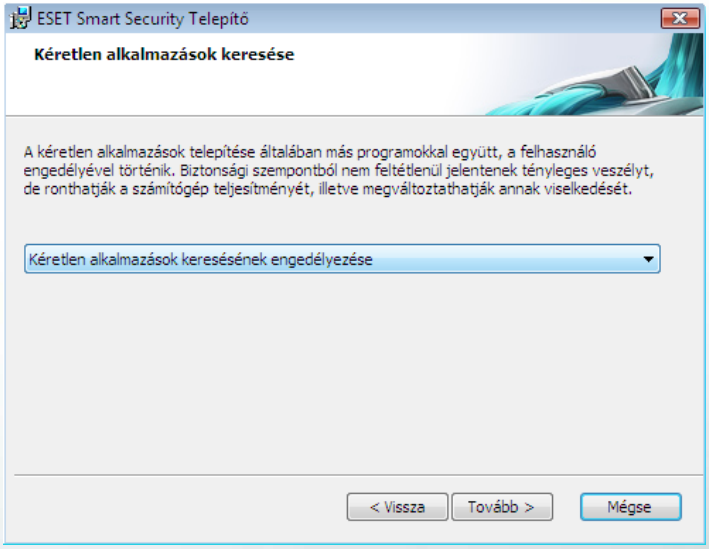
A következő lépés a ThreatSense.Net Korai Riasztási Rendszer engedélyezése. A ThreatSense.Net Korai Riasztási Rendszer segítségével a számítógépét veszélyeztető gyanús fájlokat elküldheti az ESET víruslaboratóriumának, ahol szakértők elemzik őket, majd elkészítik az új vírusok ellenszerét, és frissítik az ESET termékeinek vírusdefiníciós adatbázisát. A ThreatSense.Net Korai Riasztási Rendszer használatával, és a számítógépét veszélyeztető gyanús fájlok automatikus elküldésének engedélyezésével Ön is hozzájárul a vírusok elleni küzdelemhez, és lehetővé teszi, hogy a számítógépét még hatékonyabban védelmezhessük.



Alapértelmezés szerint a ThreatSense.Net Korai Riasztási Rendszer használata engedélyezve van. Amennyiben módosítani szeretné a rendszer beállításait, kattintson a **További beállítások** gombra.

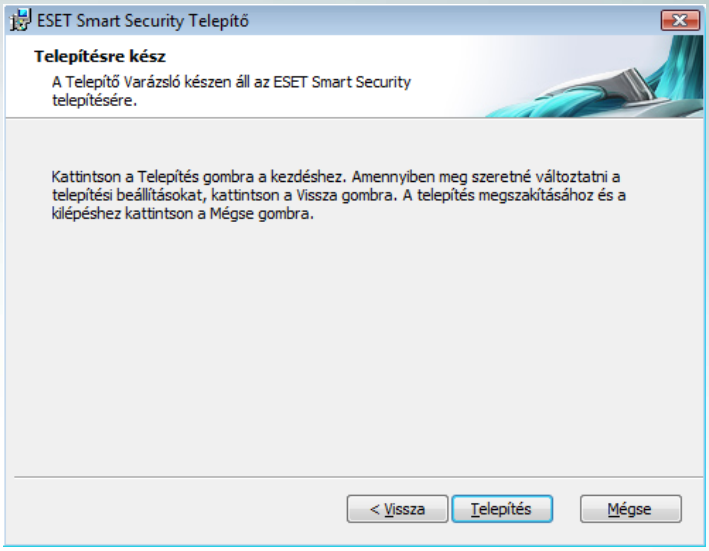
A telepítés következő lépése a kéretlen alkalmazások keresésének engedélyezése. A kéretlen alkalmazások olyan programok, melyek biztonsági szempontból nem feltétlenül jelentenek tényleges veszélyt, de ronthatják a számítógép teljesítményét, illetve megváltoztathatják annak viselkedését.

A kéretlen alkalmazások sokszor más programokkal együtt kerülnek telepítésre úgy, hogy a felhasználó a telepítés során nem veszi észre, hogy a használni kívánt alkalmazás mellett más szoftver is a számítógépére kerül.



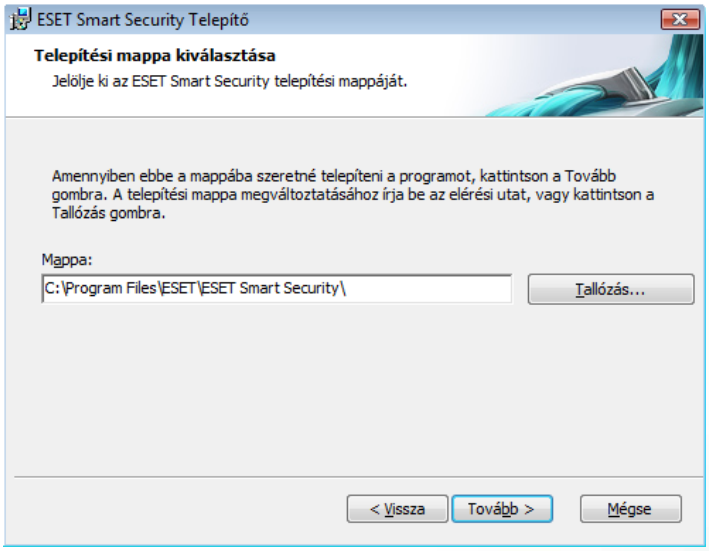
Válassza ki a kéretlen alkalmazások keresésének engedélyezését (javasolt), így engedélyezheti, hogy az ESET Smart Security meggátolhassa a kéretlen alkalmazások feltelepülését.

A Tipikus telepítés utolsó lépése a Telepítés jóváhagyása, mely a **Telepítés** gomb megnyomásával történik.



2.2 Egyéni telepítési mód

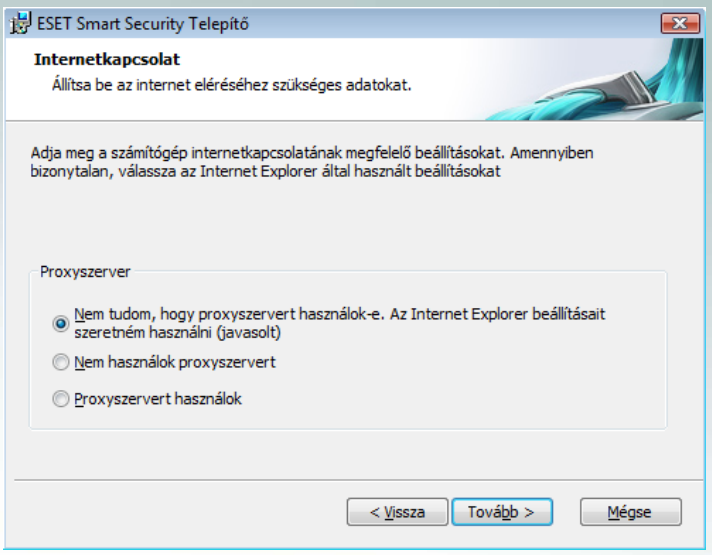
Az Egyéni telepítési mód azon felhasználók számára javasolt, akik tapasztalattal rendelkeznek a programok beállításainak finomhangolása területén, és módosítani kívánják az ESET Smart Security hozzáértő felhasználók számára kínált beállításait.



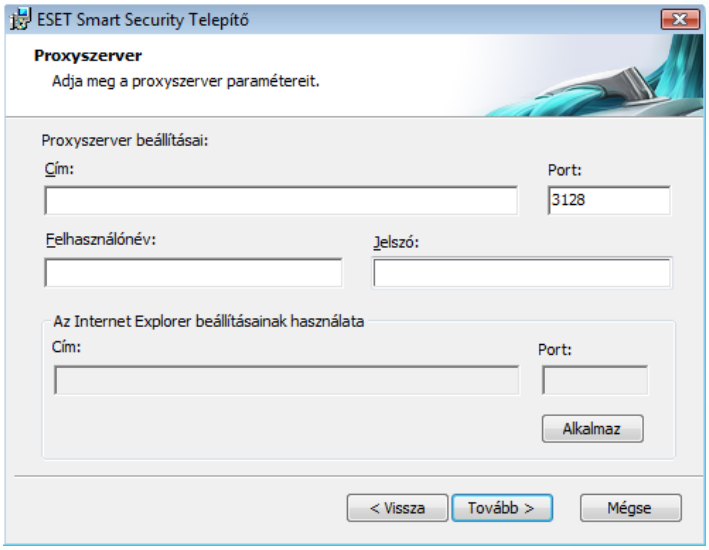
Az Egyéni telepítés során az első lépés annak kiválasztása, hogy az ESET Smart Security programcsomagot a merevlemez mely területére kívánjuk telepíteni. Alapértelmezés szerint a program a C:\Program Files\ESET\ESET Smart Security\ mappába kerül telepítésre. Amennyiben meg szeretné változtatni a telepítés helyét (nem javasolt), kattintson a **Tallózás** gombra.

A következő lépésben adja meg felhasználónevét és jelszavát. Ez a lépés megegyezik a Tipikus telepítés hasonló lépésével (8. oldal).

Miután megadta felhasználónevét és jelszavát, kattintson a **Tovább** gombra, és konfigurálja, hogy milyen internetkapcsolatot kíván használni. (Amennyiben a telepítés során azt az opciót jelölte be, hogy a frissítési adatokat később adja meg, a következő két lépés – a proxyszerver beállítása, valamint az automatikus frissítések letöltésének konfigurálása – nem jelenik meg. Ezeket a beállítási lehetőségeket később is megadhatja a feltelepített program kezelőfelületén keresztül.)



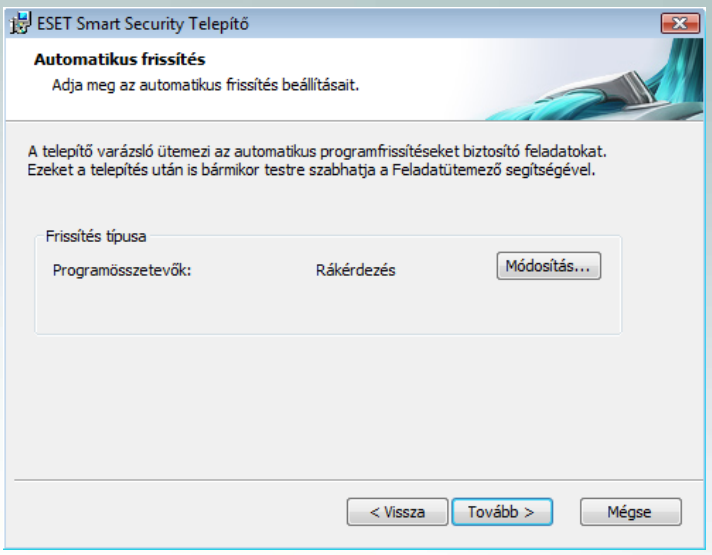
Amennyiben proxyszervert használ, azt megfelelően konfigurálnia kell a vírusdefiníciós adatbázis frissítéseinek eléréséhez. Amennyiben nem biztos abban, hogy proxyszervert használ, válassza ki a **Nem tudom, hogy proxyszervert használok-e. Az Internet Explorer beállításait szeretném használni. (javasolt)** beállítást, majd kattintson a **Tovább** gombra. Ha nem használ proxyszervert, válassza ki az ennek megfelelő beállítást.



A proxyszerver beállításához válassza ki a **Proxyszervert használok** beállítást, majd kattintson a **Tovább** gombra. A Cím mezőben adja meg a proxyszerver nevét vagy IP-címét. A Port mezőben adja meg azt a portot, melyen a proxyszerver fogadja a beérkező kommunikációt (alapértelmezés szerint a 3128-as port).

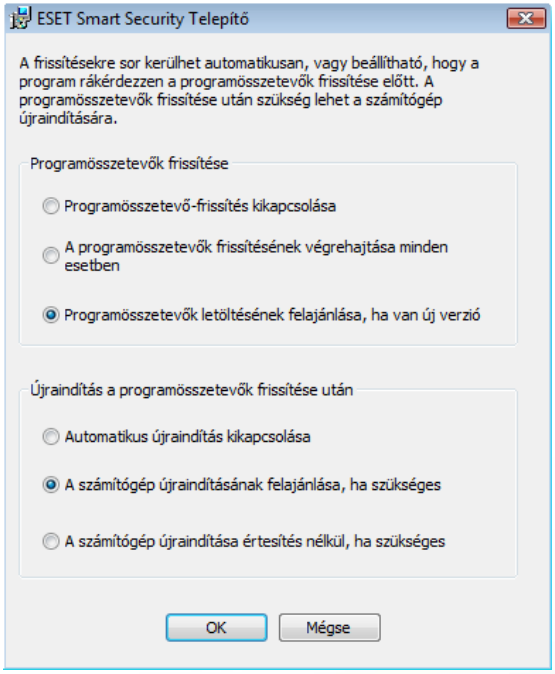
Abban az esetben, ha a proxyszerver használatához felhasználónév és jelszó szükséges, a megfelelő mezőkbe gépelje be ezeket.

A proxyszerver beállításai az Internet Explorer programból is kimásolhatók. Ehhez nyomja meg az **Alkalmaz** gombot. Ha befejezte a proxyszerver konfigurálását, kattintson a **Tovább** gombra.



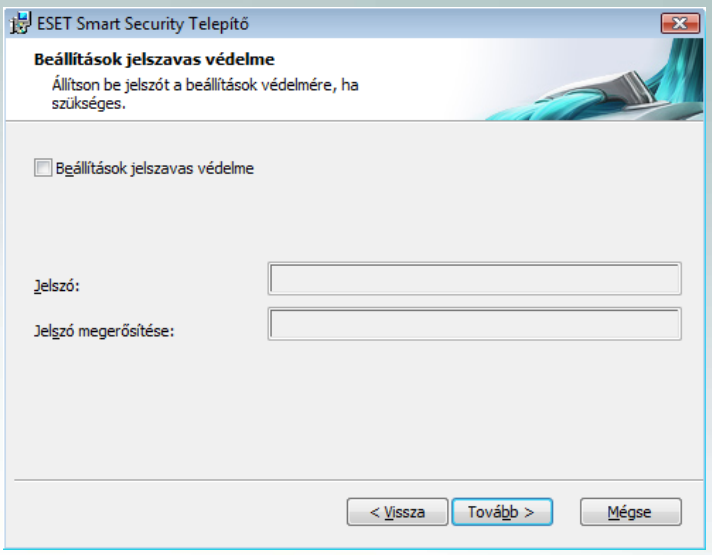
A következő lépésben megadhatja az automatikus frissítés beállításait. Kattintson a **Módosítás** gombra, ha be szeretné állítani, hogy a programösszetevők frissítését a program hogyan hajtsa végre.

Ha nem szeretné, hogy az ESET Smart Security programösszetevői frissítésre kerüljenek, válassza a **Programösszetevő-frissítés kikapcsolása** opciót. Ha szeretné, hogy a programösszetevők automatikusan frissítésre kerüljenek, válassza a **Programösszetevők frissítésének végrehajtása minden esetben** opciót. Amennyiben szeretné, hogy a programösszetevők frissítésére a program mindig rákérdezzen, válassza az alapértelmezett **Programösszetevők letöltésének felajánlása, ha van új verzió** opciót.



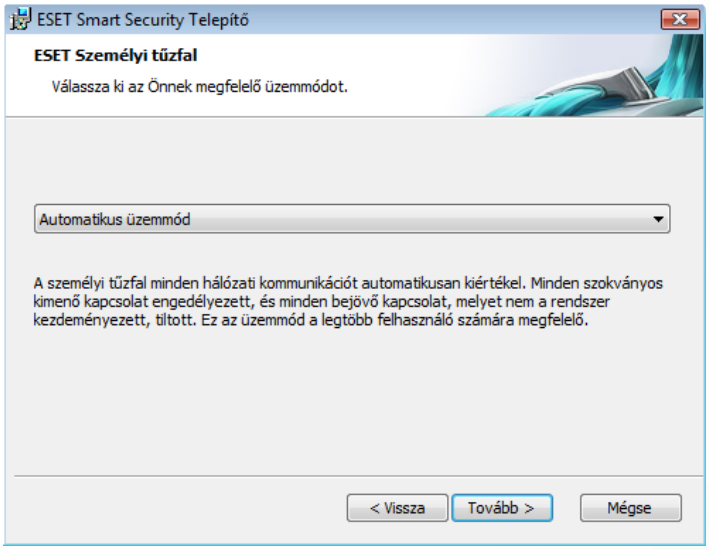
Ez után válassza ki, hogy a programösszetevők frissítése után a számítógép automatikusan újraindításra kerüljön-e. A javasolt beállítás **A számítógép újraindítása értesítés nélkül, ha szükséges**.

A következő lépésben jelszóval védheti le a program beállításait. Amennyiben azt szeretné, hogy a program letelepítésére vagy a beállítások módosítására a későbbiekben csakis egy jelszó megadása után kerülhessen sor, jelölje ki a **Beállítások jelszavas védelme** opciót, és adjon meg egy jelszót, majd a jelszó ismételt begépelésével erősítse azt meg. Ez után kattintson a **Tovább** gombra.



A ThreatSense.Net Korai Riasztási Rendszer beállításainak konfigurálása és a Kéretlen alkalmazások keresésének beállítása megegyezik a Tipikus telepítési mód ismertetése során leírtakkal (lásd 8. oldal).

Az Egyéni telepítés következő lépéseként az ESS Személyi tűzfal üzemmódját választhatja ki. Négy üzemmód érhető el:
- Automatikus üzemmód
- Interaktív üzemmód
- Házirend alapú üzemmód
- Tanuló üzemmód



Az Automatikus üzemmód javasolt a legtöbb felhasználó számára. Ebben az üzemmódban előre meghatározott szabályok alapján kerül elemzésre az adatforgalom. Minden szokványos kimenő kommunikáció engedélyezett, és minden kéretlen bejövő kommunikáció tiltásra kerül.

Az Interaktív üzemmód hozzáértő felhasználók számára javasolt. A kommunikáció ebben az esetben a felhasználó által meghatározott szabályok alapján kerül engedélyezésre vagy tiltásra. Amennyiben egy alkalmazás által kezdeményezett kommunikáció engedélyezésére vagy tiltására még nem létezik szabály, a program értesítése alapján a felhasználónak kell döntenie az engedélyezésről vagy a tiltásról.

A Házirend alapú üzemmódban a Személyi tűzfal a rendszergazda által előre meghatározott engedélyek és tiltások alapján engedélyezi vagy blokkolja a kommunikációt. Amennyiben egy adott alkalmazás által kezdeményezett kommunikációt a rendszergazda nem engedélyezett, és így nincs az adott kommunikációról rendelkező szabály, a kommunikációt a Személyi tűzfal automatikusan, a felhasználó értesítése nélkül blokkolja. Azt javasoljuk, hogy kizárólag akkor válassza ezt a beállítást, ha Ön rendszergazda, és szándékában áll a hálózati kommunikációra vonatkozó részletes szabályzat létrehozása.

Az ESET Smart Security 4-es verziójába beépítésre került az ún. Tanuló üzemmód is. Ennek segítségével saját magunk „taníthatjuk" a tűzfalat az új kapcsolatok kezelésére. Amennyiben egy rövid ideig ezt az üzemmódot használjuk, minden használt folyamat automatikusan engedélyezésre kerül egy listán, majd a felhasználók/rendszergazdák a szabályok szerkesztésével létrehozhatják a megfelelően szigorú, de az alkalmazások használatát lehetővé tévő tűzfalszabályokat. A Tanuló üzemmód használatát szintén rendszergazdák, vagy haladó informatikai ismerettel rendelkező felhasználóink számára ajánljuk.

Az utolsó lépésben a program engedélyt kér a telepítés befejezéséhez.
A telepítéshez kattintson a **Telepítés** gombra.

A telepítés közben a program érzékeli a hálózati beállításokat, és feltesz egy kérdést a tűzfal védelmi módjára vonatkozóan.

Vezeték nélküli hálózat esetén a **Szigorú védelem** kiválasztása ajánlott.
Ebben a módban nem látható a számítógép a hálózat többi tagja számára.

Otthoni vagy irodai hálózat esetén, abban az esetben, ha szeretné biztosítani, hogy megosztott mappái és nyomtatói elérhetőek legyenek a többi számítógépről, válassza a **Megosztás engedélyezése** opciót.

A védelmi mód a későbbiekben is megváltoztatható. Amennyiben a számítógép több hálózatnak is a része, mindegyik hálózathoz külön védelmi mód választható ki.

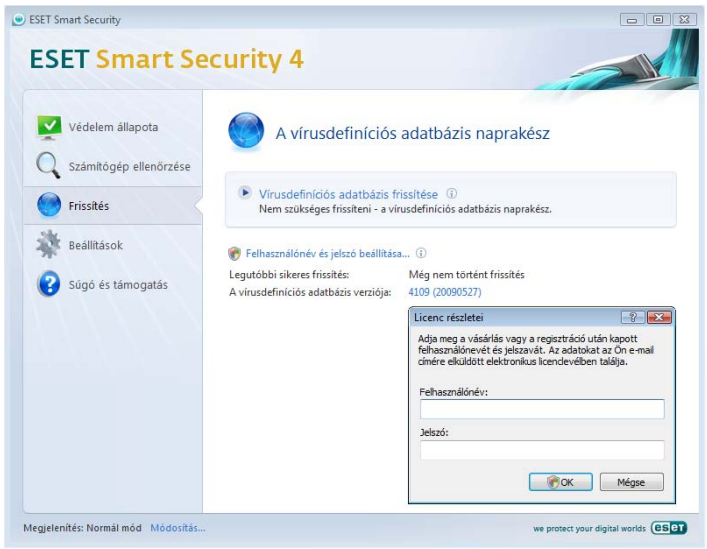
2.3 Az eredeti beállítások visszaállítása

Amennyiben a későbbiek során újratelepíti az ESET Smart Security programot, alapértelmezés szerint a **Jelenlegi beállítások használata** van kijelölve. Amennyiben az újratelepítés során nem szeretne változtatni a program beállításain, hagyja kijelölve ezt a beállítást. Amennyiben szeretne változtatni a program beállításain, vegye ki a jelölőpipát a **Jelenlegi beállítások használata** opció mellől, és adja meg, hogy Tipikus vagy Egyéni módban kívánja telepíteni a programot, majd kattintson a **Tovább** gombra.

2.4 Felhasználónév és jelszó megadása

A program megfelelő működéséhez fontos, hogy az automatikus frissítések engedélyezve legyenek. Az automatikus frissítések letöltése csak akkor lehetséges, ha a **Frissítés** menüpontban található **Felhasználónév és jelszó beállítása** opciónál érvényes felhasználónév és jelszó van megadva.

Ha a telepítés során a Frissítési adatok beállításánál nem adott meg érvényes felhasználónevet és jelszót, ezt a program kezelőfelületén keresztül is megteheti. A Windows operációs rendszer Start menüjén keresztül, vagy a jobb alsó sarokban, a tálcán látható ESET Smart Security ikon segítségével indítsa el a feltelepített program Vezérlőközpontját, és a program kezelőfelületén kattintson a **Frissítés** menüpontban található **Felhasználónév és jelszó beállítása** opcióra. A felugró **Licenc részletei** ablakban adja meg a vásárlás vagy a regisztráció után kapott felhasználónevét és jelszavát. Ezeket az adatokat a vásárlás vagy a regisztráció során megadott e-mail címére elküldött elektronikus licenclevélben találja.

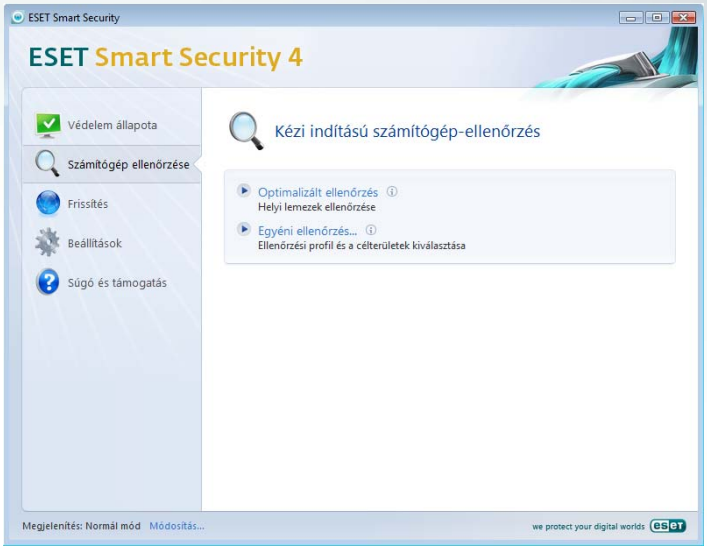


2.5 Kézi indítású számítógép-ellenőrzés

Az ESET Smart Security telepítése után javasolt egy kézi indítású számítógép-ellenőrzés lefuttatása, melynek során a program megvizsgálja, hogy a számítógépen található-e károkozó (vírus, trójai, kémprogram stb.).

A kézi indítású számítógép-ellenőrzés gyors elindításához válassza a **Számítógép ellenőrzése** menüpontot a program kezelőfelületén, majd válassza az **Optimalizált ellenőrzés** opciót.

Az ESET Smart Security 4 minden egyes kézi indítású ellenőrzés után megjeleníti az ellenőrzés legfontosabb adatait tartalmazó naplófájl linkjét, így a felhasználó könnyedén nyomon követheti a számítógépét érintő változásokat.



3. Rövid használati útmutató

Ez a fejezet röviden áttekinti az ESET Smart Security funkcióit és alapbeállításait.

3.1 A kezelőfelület bemutatása – Megjelenítési módok

Az ESET Smart Security kezelőfelülete két fő területre van osztva. A bal oldali oszlop a felhasználóbarát főmenühöz biztosít hozzáférést. A jobb oldali területen a bal oldali menüpontokhoz tartozó tartalmak jelennek meg aszerint, hogy a bal oldali főmenüben melyik menüpont került kiválasztásra.

Az alábbiakban a főmenü menüpontjainak funkcióit ismerheti meg:

Védelem állapota – Ez a menüpont információt nyújt az ESET Smart Security által biztosított védelem állapotáról. Amennyiben a megjelenítési módok közül a Hozzáértő mód kerül kiválasztásra, az egyes modulok által biztosított védelem szintje és állapota részletesen is megtekinthető. Statisztikák kérhetők le többek között a valós idejű fájlrendszervédelem és a levélszemétszűrő működéséről, valamint a fel-és letöltések és a lemezműveletek alakulásáról is.

Számítógép ellenőrzése – Ez a menüpont lehetőséget nyújt a Kézi indítású számítógép-ellenőrzés konfigurálására és végrehajtására.

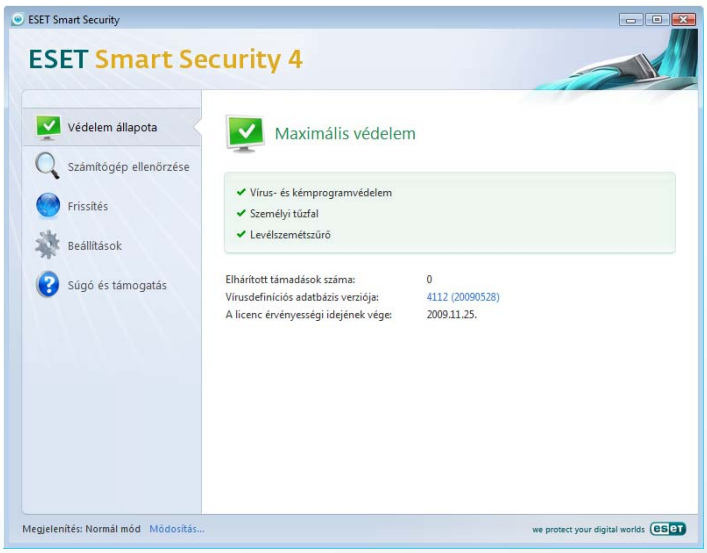
Frissítés – A frissítés, illetve a felhasználónév és jelszó beállításához válassza ezt a menüpontot.

Beállítások – Válassza ezt a menüpontot a számítógép védelmi szintjének konfigurálásához. Amennyiben a megjelenítési módok közül a Hozzáértő mód került kiválasztásra, a Beállítások menüpont alatt megjelennek az egyes modulok – a Vírus- és kémprogramvédelem, a Személyi tűzfal, valamint a Levélszemétszűrő – beállítási lehetőségei.

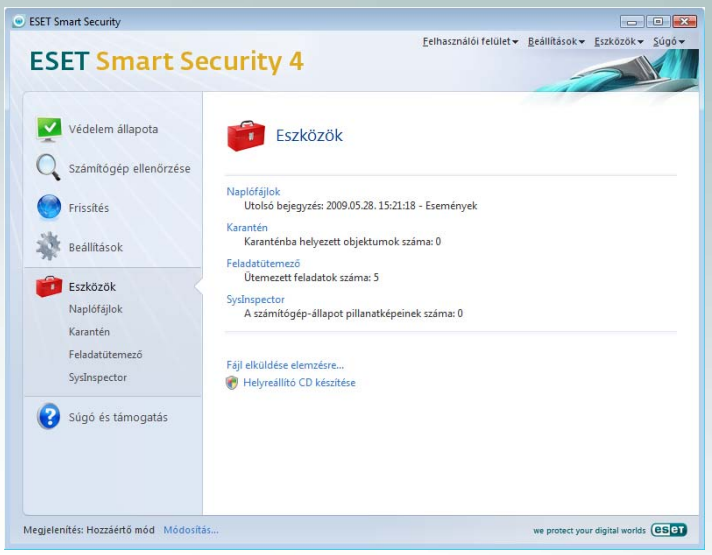
Eszközök – Ez a menüpont kizárólag a Hozzáértő megjelenítési mód kiválasztása esetén jelenik meg, és a Naplófájlokhoz, a Karanténhoz, valamint a Feladatütemezőhöz biztosít hozzáférést. A Hozzáértő beállításokat a CTRL-M billentyűk együttes lenyomásával, vagy pedig a főmenü alatt található **Módosítás** hivatkozás segítségével hívhatjuk elő.

Súgó és támogatás – E menüpont segítségével elérheti a Súgót, a Gyakori kérdések megoldásait, illetve más támogatási funkciókat. Szintén ebben a menüpontban találja a kapcsolatfelvételi lehetőségeket, melyek segítségével közvetlenül elérheti terméktámogatásunkat.

Megjelenítés – Az ESET Smart Security kezelőfelülete két megjelenítési módot tesz lehetővé, a Normál és a Hozzáértő módot. A két megjelenítési mód közötti váltás a főmenü alatt található **Módosítás** hivatkozás segítségével, vagy a CTRL-M billentyűk együttes lenyomásával lehetséges.



A Normál megjelenítési mód a legtöbb felhasználó számára megfelelő, és hozzáférést biztosít a leggyakrabban használt funkciókhoz. A Normál megjelenítési módban a hozzáértő felhasználók számára nyújtott beállítási lehetőségek nem jelennek meg.

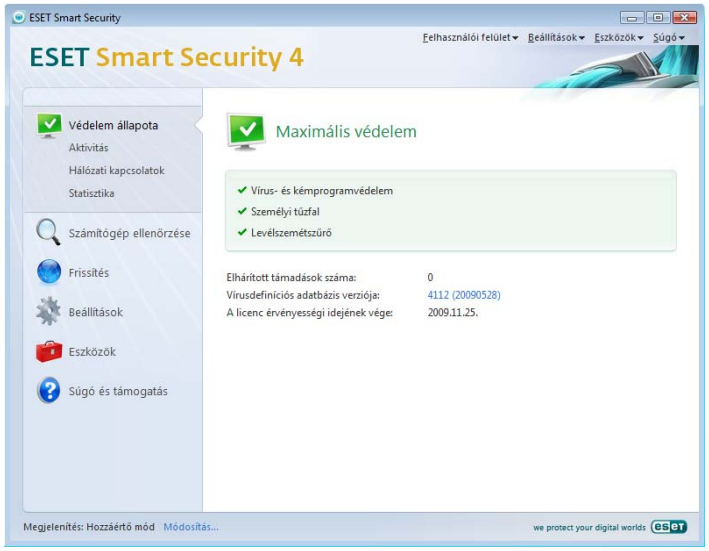


Amennyiben a megjelenítést átváltja Hozzáértő megjelenítési módra, a Főmenüben megjelenik az **Eszközök** menüpont, mely hozzáférést nyújt a Naplófájlokhoz, a Karanténhoz, a Feladatütemezőhöz, a SysInspectorhoz, valamint innen indítható a helyreállító CD elkészítése is.

Megjegyzés: a felhasználói útmutató további részei kizárólag a Hozzáértő megjelenítési módban elérhető funkciókat mutatják be.

3.1.1 A védelem állapotának ellenőrzése

A védelem állapotának megtekintéséhez kattintson a főmenüben a **Védelem állapota** menüpontra.



Amennyiben az egyes modulok működése engedélyezett, és a modulok megfelelően működnek, a modulok neve mellett zöld pipa található. Ellenkező esetben az egyes modulok mellett egy piros felkiáltójel vagy narancssárga figyelmeztető jel jelenik meg, és a jobb oldali terület tetején további információt talál a modul működéséről. A letiltott modulok működésének engedélyezéséhez, vagy a modulok által biztosított védelem beállításainak megváltoztatásához kattintson a főmenü **Beállítások** menüpontjára, és válassza ki a megfelelő modult.

Ezenkívül az ESET Smart Security program jelzi a védelmi állapot szintjét a Windows értesítési területén (a tálca jobb alsó sarkában, az óra mellett) is. Az egyes védelmi állapotokat a következő három szín jelöli:

Zöld (ajánlott) – A vírusvédelem megfelelően működik, a számítógép védett a kártevőkkel szemben. Ez az állapot azt jelenti, hogy minden védelmi modul be van kapcsolva, és a vírusdefiníciós adatbázis is naprakész.

Sárga – A valós idejű fájlrendszervédelem be van kapcsolva, de a maximális szintű védelem nem biztosított. A sárga ikon akkor jelenik meg, ha az alábbi események valamelyike következik be:
- Ki van kapcsolva, vagy nem működik megfelelően a dokumentumvédelem, a webhozzáférés-védelem vagy az e-mailvédelem.
- Az operációs rendszer nem naprakész.

Vörös – Le van tiltva a valós idejű fájlrendszervédelem, vagy ki van kapcsolva a személyi tűzfal. Mivel a különböző védelmi moduloknak a működése elengedhetetlen a rendszer biztonságának megteremtéséhez, ajánlott azonnal visszakapcsolni az inaktív modult.

3.1.2 Mit tegyünk, ha a program nem működik megfelelően?

Amennyiben az ESET Smart Security bármilyen problémát érzékel az egyes modulok működésében, azt a **Védelem állapota** menü alatt jelzi. A program ugyanakkor ezen a helyen megoldást is kínál a problémára.

Amennyiben egy probléma nem oldható meg a megjelenített megoldási lehetőségek segítségével, kattintson a **Súgó és támogatás** menüpontra, hogy további segítséget kapjon. Amennyiben sem a súgóban, sem a Gyakori kérdések megoldásai listájában nem talál megoldást a problémára, kattintson a kapcsolatfelvételi lehetőségek egyikére, hogy kapcsolatba lépjen munkatársainkkal. Ennek módjairól a dokumentum végén talál pontos útmutatást.

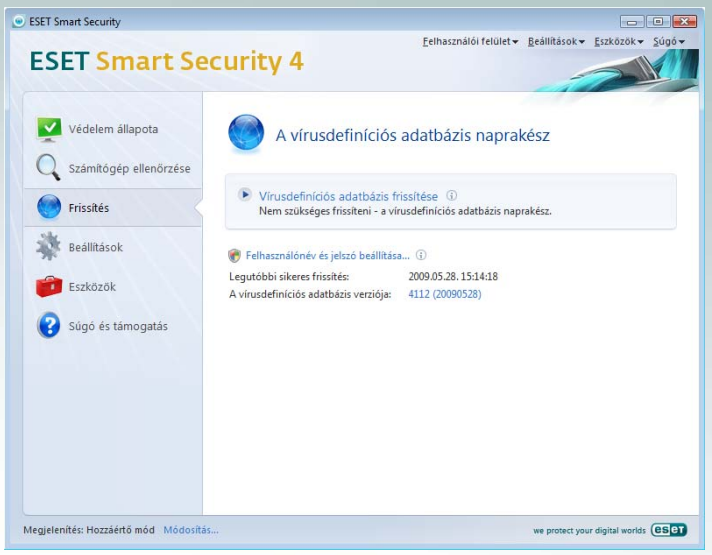
3.2 Frissítés beállításai

A vírusdefiníciós adatbázis és a programösszetevők frissítése fontos ahhoz, hogy az ESET Smart Security a megfelelő védelmet tudja biztosítani. Kérjük, fordítson kiemelt figyelmet arra, hogy ezeket a beállításokat megfelelően konfigurálja.

Amennyiben a programot azonnal szeretné frissíteni, kattintson a főmenü **Frissítés** menüpontjára, majd válassza a **Vírusdefiníciós adatbázis frissítése** opciót. A program megvizsgálja, hogy elérhető-e frissítés, és amennyiben igen, letölti azt.

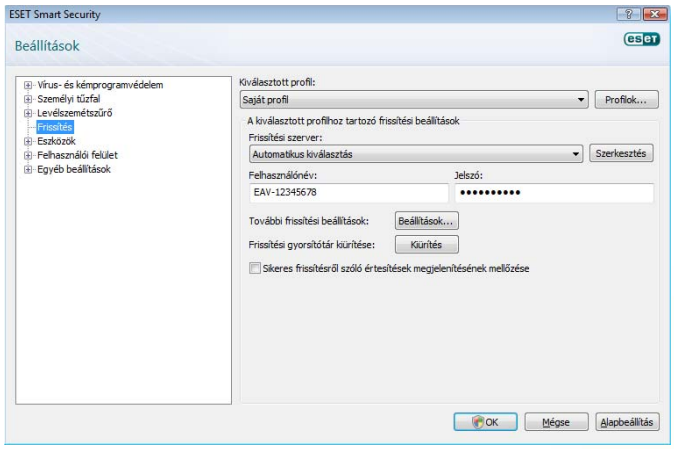
Ha a telepítés során nem adott meg felhasználónevet és jelszót a frissítések letöltéséhez, a program ezen a ponton kéri a felhasználónevet és jelszót. Ezeket a vásárlás vagy a regisztráció során megadott e-mail címére küldött elektronikus licenclevélben találja.

Amennyiben a frissítés során hibaüzenetet kap, ellenőrizze, hogy a felhasználónév és jelszó beállítása megfelelő-e. Ehhez kattintson a **Felhasználónév és jelszó beállítása** opcióra, és adjon meg érvényes felhasználónevet és jelszót. Vigyázzon a kisbetűk és a nagybetűk használatára, és ellenőrizze, hogy a Caps Lock billentyű nincs-e véletlenül használatban.



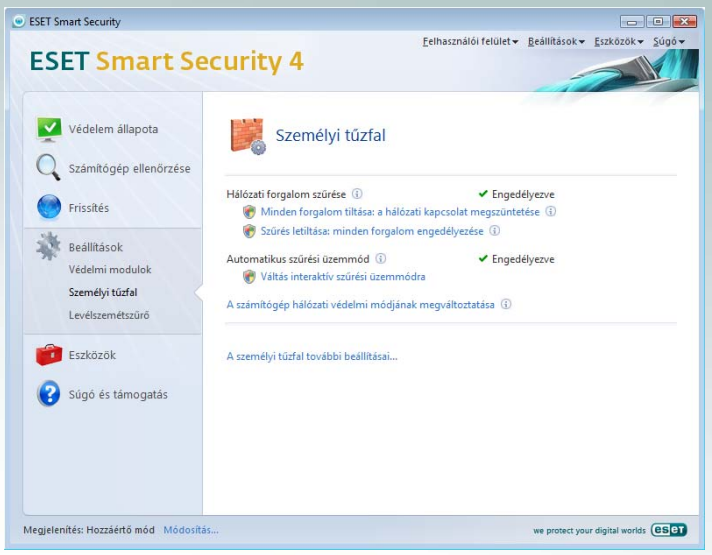
A frissítés további hozzáértő beállításainak eléréséhez nyomja meg az F5 billentyűt, vagy amennyiben **Hozzáértő módban** használja a programot, válassza ki a **Beállítások** menü **További beállítások** elemét. A felbukkanó ablak bal oldali menüfájában válassza ki a **Frissítés** menüpontot. A jobb oldalon megjelenő területen megtalálja a **Frissítési szerver** legördülő menüjét, melynek javasolt értéke az Automatikus kiválasztás.

A hozzáértő beállítási paraméterek megváltoztatásához kattintson a **További frissítési beállítások** felirat mellett lévő **Beállítások** gombra. A felbukkanó ablakban megadhatja a frissítés módját, a http proxyszerver beállításait, valamint konfigurálhatja a helyi hálózaton található tükrözött vírusadatbázis elérésének útvonalát (az ESET Smart Security Business Edition esetében).

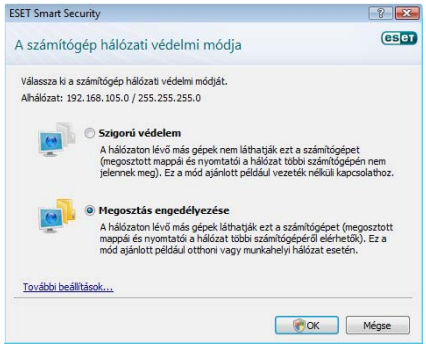


3.3 Megbízható zóna beállítása

A Megbízható zóna beállítása fontos lépés a számítógép hálózati védelmének konfigurálásában. **A Számítógép hálózati védelmi módjának megváltoztatása** során a **Megosztás engedélyezésével** lehetővé teheti, hogy más felhasználók a hálózaton keresztül kapcsolódhassanak a számítógéphez. Ennek engedélyezéséhez kattintson a **Beállítások** menüpontra, majd válassza a **Számítógép hálózati védelmi módjának megváltoztatása** opciót.
A felugró ablakban kiválaszthatja, hogy az adott hálózatban milyen védelmi módot kíván beállítani. Amennyiben nem kíván fájlokat vagy mappákat megosztani, és nem szeretné, hogy a hálózat más felhasználói is láthassák számítógépét, válassza a Szigorú védelmet.



A Megbízható zóna beállítására vonatkozó figyelmeztetés automatikusan felugrik az ESET Smart Security telepítése után, illetve minden alkalommal, amikor a számítógép új hálózathoz csatlakozik, ezért a Megbízható zóna fentiekben leírt manuális meghatározására a legtöbb esetben nincs szükség. Ehelyett, amikor új hálózathoz csatlakozik, és a Megbízható zóna beállítására vonatkozó párbeszédablak felugrik, válassza ki, hogy az adott hálózatban milyen védelmi szintet kíván alkalmazni.

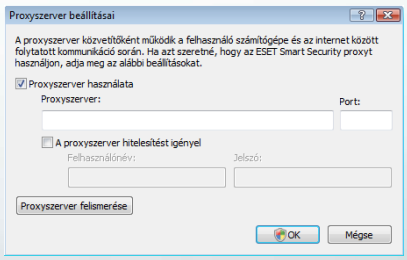


Figyelmeztetés! Amennyiben egy megbízhatatlan hálózatban a **Megosztás engedélyezése** mellett dönt, lehetséges, hogy ezzel biztonsági problémát okoz, és a számítógépet veszélynek teszi ki.

Megjegyzés: Az alapértelmezés szerint a megbízható zónában található más felhasználók hozzáférnek a számítógépen lévő megosztott fájlokhoz és nyomtatókhoz, engedélyezett a bejövő RPC (Remote Procedure Calls) kommunikáció, valamint elérhető a távoli asztal megosztása funkció.

3.4 Proxyszerver beállítása

Amennyiben a számítógép proxyszerveren keresztül kapcsolódik az internethez, az ESET Smart Security megfelelő paraméterezésével be kell állítania a proxyszerver elérését. Ehhez először hívja elő a Hozzáértő beállításokat az F5 gomb segítségével. A proxyszerver beállításainak eléréséhez kattintson duplán a bal oldali menüfában az **Egyéb beállítások** menüpontra, majd válassza ki a **Proxyszerver** menüpontot. A jobb oldali beállítási területen jelölje ki a **Proxyszerver használata** opciót, és adja meg a proxyszerver nevét vagy IP-címét, valamint azt a portot, melyen a proxyszerver a hálózati kommunikációt fogadja (alapértelmezés szerint ez a 3128-as port). Amennyiben a proxyszerver hitelesítést igényel, adja meg a megfelelő **Felhasználónevet** és **Jelszót**.

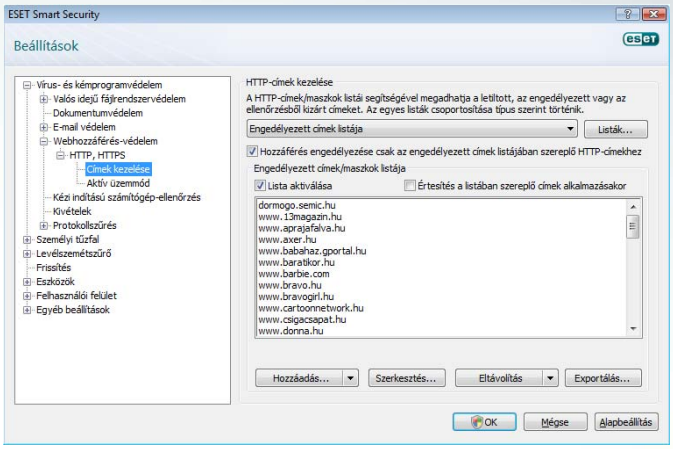


Amennyiben nem ismeri a proxyszerver címét, nyomja meg a **Proxyszerver felismerése** gombot, melynek hatására az ESET Smart Security megpróbálja automatikusan detektálni a szerver címét.

Megjegyzés: A megfelelő proxyszerver beállítások különbözhetnek az egyes frissítési profilok esetében. Ilyenkor az egyes profilokra vonatkozó beállításokat a Hozzáértő beállítások előhívása (F5) után a **Frissítés** beállításainak módosításával hozhatja létre.

3.5 Szülői felügyelet

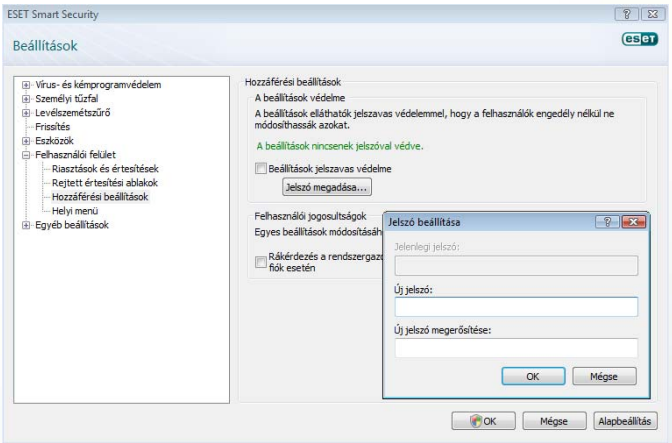
Az ESET Smart Security lehetőséget biztosít arra, hogy korlátozza az interneten elérhető tartalmakat. A korlátozást a beépített http-szűrő végzi, tiltó és engedélyező listák segítségével.



Honlapunkról letölthető a legnépszerűbb, gyermekeknek szánt internetes weboldalak listája. Amennyiben ezt a listát beállítja engedélyezettnek, kiválasztja a **Hozzáférés engedélyezése csak az engedélyezett címek listájában szereplő http-címekhez** opciót, biztos lehet benne, hogy gyermeke csak neki szánt weboldalakhoz fér hozzá internetezés közben.
A részletes beállításokat és a legfrissebb listát megtalálja a www.eset.hu/szuloifelugyelet oldalon.

3.6 A beállítások jelszavas védelme

Az ESET Smart Security megfelelő beállítása nagyon fontos a hálózatok megfelelő védelmének biztosításához. A beállítások jogosulatlan módosítása veszélyeztetheti a számítógép biztonságát. Az ESET Smart Security beállításainak jelszavas védelméhez hívja elő a Hozzáértő beállításokat az F5 gomb megnyomásával, majd a bal oldali menüfában válassza ki a **Felhasználói felület** menüpontban lévő **Hozzáférési beállítások** almenüt, és a jobb oldali területen jelölje ki a **Beállítások jelszavas védelme** opciót. A felugró párbeszédablakban adja meg a kívánt jelszót, majd ismételt begépeléssel erősítse meg, és kattintson az **OK** gombra. Ezután kizárólag a megadott jelszó segítségével módosíthatja az ESET Smart Security beállításait, illetve telepítheti le a programot.



4. Segítség

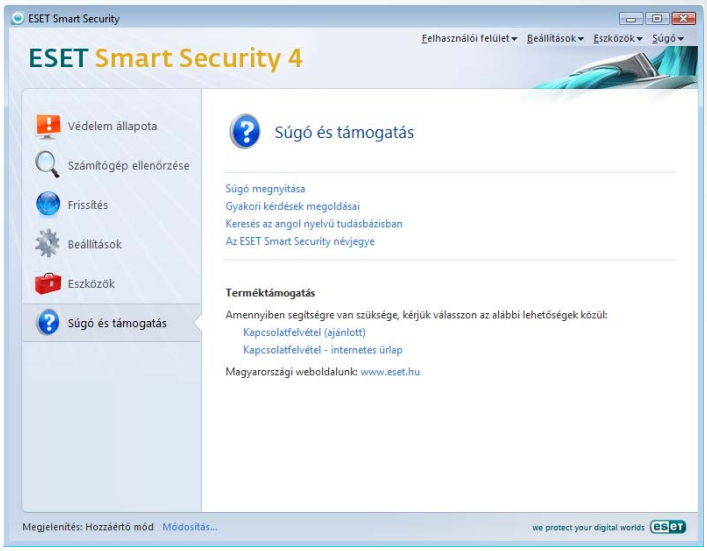
Az ESET ügyfélszolgálati szakemberei készséggel állnak rendelkezésére az esetleges problémák megoldásában.

4.1 A problémamegoldáshoz elérhető anyagok

A leggyakoribb kérdésekre adott válaszokat megtalálhatja az alábbi weboldalakon:
http://www.eset.hu/segitseg/gyik
http://www.eset.eu/support/faq (angol nyelven)

A különböző problémákra kínált megoldásokat, útmutatást és tippeket az alábbi címeken elérhető angol és magyar nyelvű Tudástárban találja:
http://www.eset.hu/segitseg/tudastar
http://kb.eset.eu (angol nyelven)

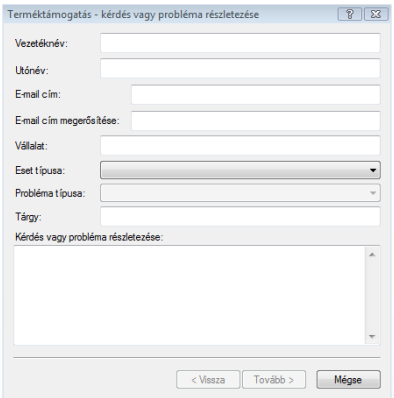
Ezek a források elérhetők a program **Súgó és támogatás** menüjéből is.



4.2 Terméktámogatási kérelem küldése

A programba integrált támogatáskérő űrlap segítségével kapcsolatba léphet az ESET ügyfélszolgálati részlegével. A **Súgó és támogatás** menüpontban válassza a **Kapcsolatfelvétel** lehetőséget.

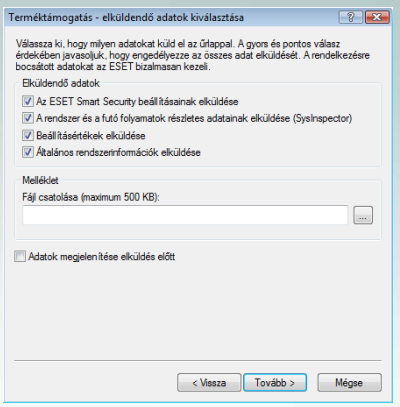
Kattintásra megjelenik az űrlapot tartalmazó ablak, amelyben kapcsolattartási adatait, a probléma típusát és leírását kell megadnia. A hatékony segítségnyújtás érdekében kérjük, igyekezzen minél pontosabban körülírni a problémát.



A **Probléma típusa** mezőben adja meg a kérdéses probléma tömör leírását, majd a **Kérdés vagy probléma részletezése** mezőben ismertesse részletesen.

A következő lépéshez kattintson a **Tovább** gombra.

A probléma leírásán túl a program támogatja a probléma forrásának feltárását segítő további hasznos információk elküldését is. Ajánlott az összes adat elküldését engedélyezni.



Ha elküldés előtt ellenőrizni szeretné az adatokat, jelölje be az **Adatok megjelenítése elküldés előtt** jelölőnégyzetet.

A rendszerinformációk elküldésén túl a kérdés vagy probléma szempontjából releváns fájlt is csatolhat az űrlaphoz.

A következő lépéshez kattintson a **Tovább** gombra.

A szükséges adatok megadását követően a **Befejezés** gombra kattintva elküldheti a kérelmet a terméktámogatási részlegnek.

4.3 Egyéb elérhetőségeink

Amennyiben a fentiek segítségével nem talál választ kérdésére, illetve nem sikerül megoldania problémáját, keresse terméktámogató szakembereinket a következő elérhetőségek egyikén:

e-mail: support@sicontact.hu

telefon: (1) 346 7048
Hétfőtől csütörtökig: 9:00 - 16:00
Pénteken: 9:00 - 13:00