

# ESET Smart Security

telepítési útmutató



we protect your digital worlds

# 1. ESET Smart Security

Az ESET Smart Security egy megbízható, integrált és gyors biztonsági programcsomag, melynek vírus- és kémprogramvédelme az ESET NOD32 Antivíruson alapszik. Az AV-Comparatives víruslaboratórium által több alkalommal az Év Antivírusának választott ESET NOD32 Antivírus tartja a nemzetközileg elismert Vírus 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 károkozóit 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 ugyanakkor egy valóban integrált biztonsági programcsomag, mely nem csupán a különböző biztonsági programok egyazon kezelőfelület segítségével történő elérésének lehetőségét nyújtja. Az ESET Smart Security különböző moduljai együttműködnek, és adatokat adnak át egymásnak. A biztonsági programcsomag így igen alacsony erőforrásigény mellett biztosít maximális védelmet.

## 1.1 Újdonságok

Az ESET szakértőinek kitartó munkáját demonstrálja az ESET Smart Security teljesen új architektúrája, melynek köszönhetően a program nem terheli le a számítógépeket.

Az ESET Smart Security biztonsági programcsomag modulokból 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 az ESET NOD32 Antivírus rendszerben is használt ThreatSense® technológián alapszik. A programba 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 2.7-es verziójában. A frissítési fájlok sérülés elleni védelme is javult.
Védelem a népszerű levelezőprogramoknak	A beérkező üzenetek mostantól nemcsak a Microsoft Outlook, hanem az Outlook Express és a Windows Mail programokban is ellenőrizhetők.
Egyéb fejlesztések	Közvetlen hozzáférés a rendszerfájlokhoz a nagyobb sebesség és teljesítmény érdekében. A fertőzött fájlokhoz való hozzáférés tiltása. Együttműködés a Windows Biztonsági Központtal és Windows Vista operációs rendszerrel.

## ■ 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 fejlett 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 felderíthetetlenek 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 fájlellenőrzés egybeépült a HTTP és a POP3 alkalmazás-protokollal. A felhasználók így az internet böngészése és e-mailek letöltése közben is biztonságban vannak.
IDS	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 hajtja-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.
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 kéréslen 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.
Különböző ellenőrzési eljárások támogatása	- Bayes-féle elemzés. - Szabály alapú ellenőrzés. - Globális ujjlenyomat-adatbázis ellenőrzése.
Együttműködés a levelezőprogramokkal	A levélszemétszűrés a Microsoft Outlook, az Outlook Express és a Windows Mail levelezőprogramokban használható.
Kézi üzenetminősítés	Az egyes e-mailek manuálisan is megjelölhetők levélszemétként, illetve jó levélként.

## 1.2 Rendszerkövetelmények

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

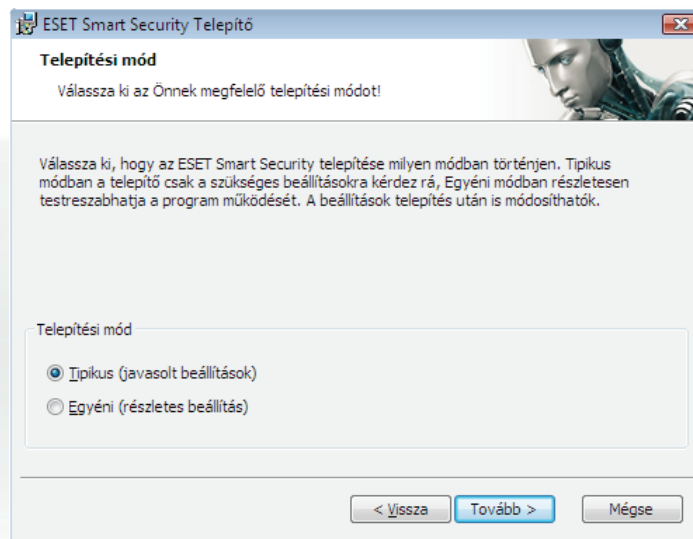
Windows 2000, XP	400 MHz 32-bit /64-bit (x86 /x64) • 128 MB RAM rendszermemória 35 MB szabad lemezterület • SVGA (800x600) monitorfelbontás
Windows Vista	1 GHz 32-bit /64-bit (x86 /x64) • 512 MB RAM rendszermemória 35 MB szabad lemezterület • SVGA (800x600) monitorfelbontás

## 2. Telepítés

Az ESET Smart Security telepítőcsomagja letölthető az ESET magyarországi weboldaláról (<http://www.eset.hu/letoltes>). A telepítőcsomag elindítása után a Telepítő Varázsló végigvezeti a telepítés folyamatán.

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

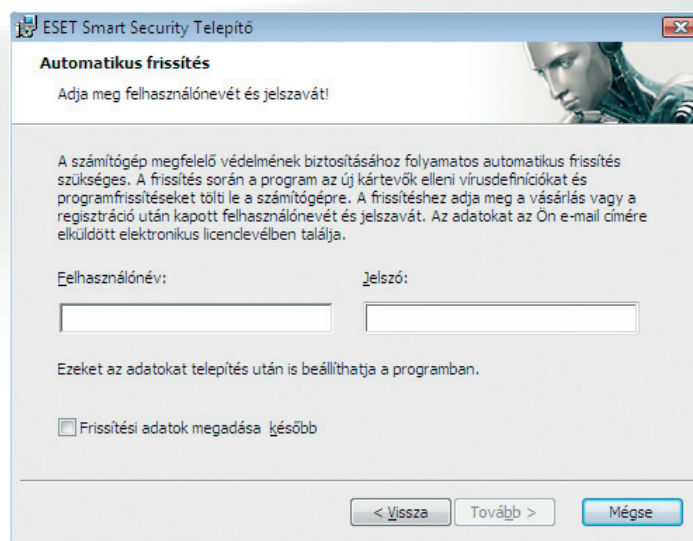
1. Tipikus (javasolt beállítások)
2. Egyéni (részletes beállítás)



### 2.1 Tipikus telepítési mód

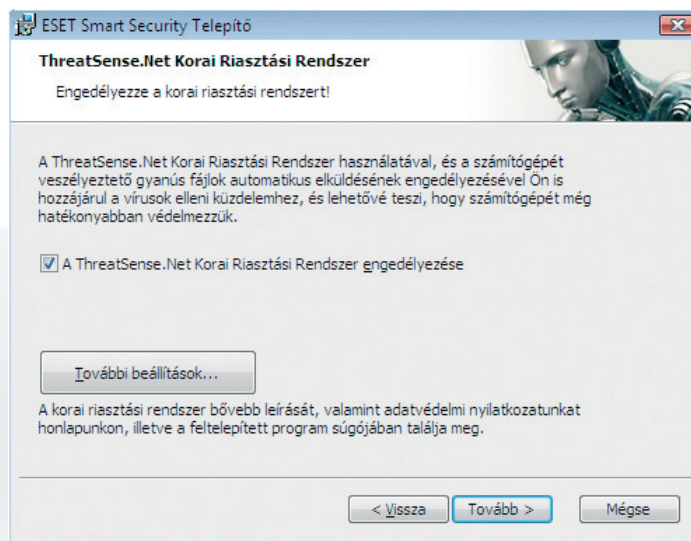
A Tipikus telepítési mód azon felhasználók számára ajánlott, akik nem szeretnék megváltoztatni az ESET Smart Security javasolt beállításait. A Tipikus telepítési mód során azon alapbeállítások kerülnek alkalmazásra, melyek biztosítják a számítógép maximális védelmét.

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

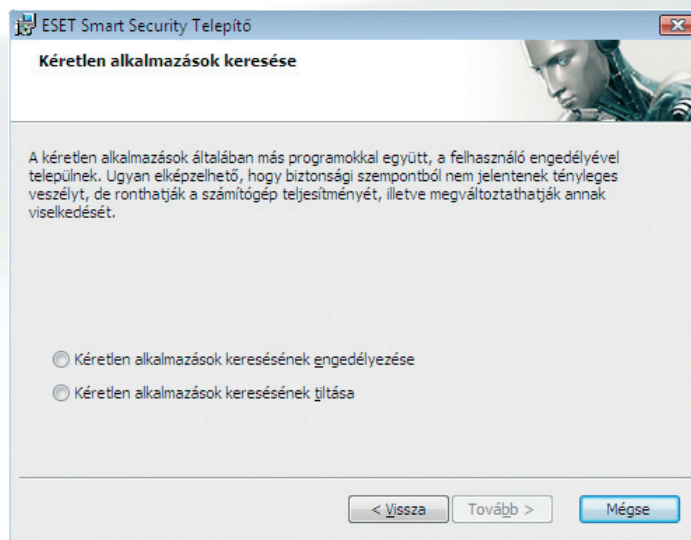
A következő lépés a ThreatSense.Net Korai Riasztási Rendszer engedélyezése. A korai riasztási rendszer segítségével a számítógépet veszélyeztető gyanús fájlokat elküldheti az ESET víruslaboratóriumának, ahol szakértők elemzik őket, majd elkészítik az új vírusok ellenszerét, és frissítik az ESET termékeinek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



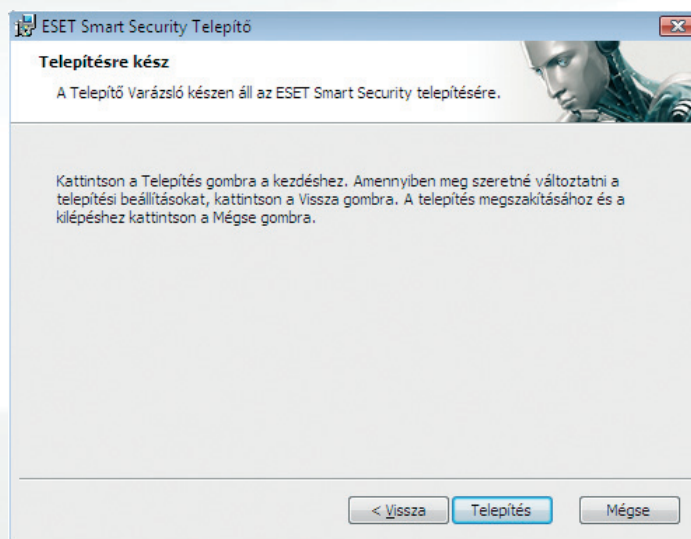
Alapértelmezés szerint a ThreatSense.Net Korai Riasztási Rendszer használata engedélyezve van. Amennyiben módosítani szeretné a rendszer beállításait, kattintson a **További beállítások** gombra.

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).



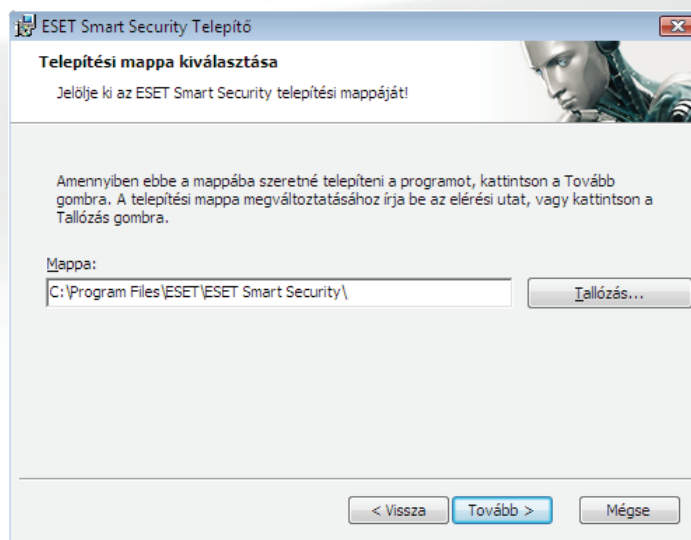
A Tipikus telepítés utolsó lépése a Telepítés jóváhagyása, mely a **Telepítés** gomb megnyomásával történik.

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

## 2.2 Egyéni telepítési mód

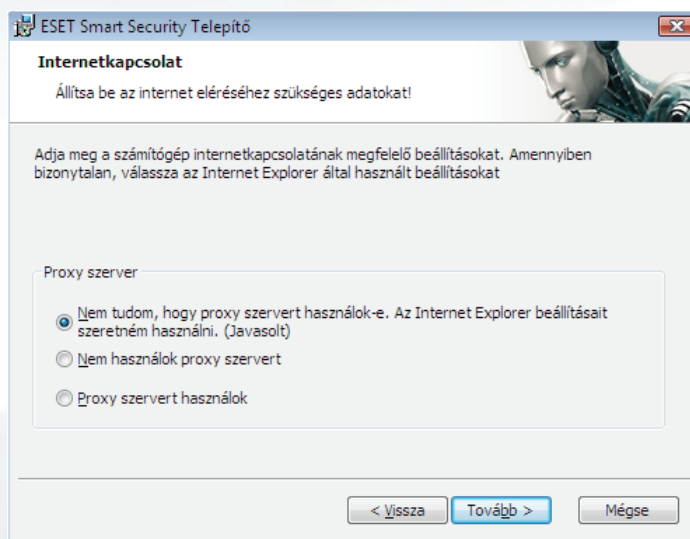
Az Egyéni telepítési mód azon felhasználók számára javasolt, akik tapasztalattal rendelkeznek a programok beállításainak finomhangolása területén, és módosítani kívánják az ESET Smart Security hozzáértő felhasználók számára kínált beállításait.

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 (4. oldal).

Miután beállította felhasználónevét és jelszavát, kattintson a **Tovább** gombra, és adja meg az internetkapcsolatának megfelelő beállításokat. (Amennyiben a telepítés során azt az opciót jelölte be, hogy a frissítési adatokat később adja meg, a következő két lépés – a proxy szerver beállítása, valamint az automatikus frissítések letöltésének konfigurálása – nem jelenik meg. Ezeket később is beállíthatja a feltelepített programban.)



**ESET Smart Security Telepítő**

**Internetkapcsolat**  
Állítsa be az internet eléréséhez szükséges adatokat!

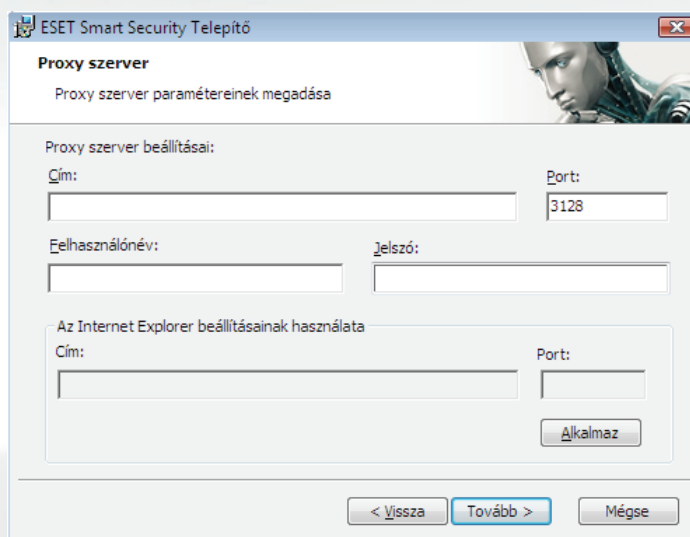
Adja meg a számítógép internetkapcsolatának megfelelő beállításokat. Amennyiben bizonytalan, válassza az Internet Explorer által használt beállításokat

Proxy szerver

Nem tudom, hogy proxy szerveret használok-e. Az Internet Explorer beállításait szeretném használni. (Javasolt)  
 Nem használok proxy szerveret  
 Proxy szerveret használok

< Vissza   **Tovább >**   Mégse

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



**ESET Smart Security Telepítő**

**Proxy szerver**  
Proxy szerver paramétereinek megadása

Proxy szerver beállításai:

Cím:  Port:

Felhasználónév:  Jelszó:

Az Internet Explorer beállításainak használata

Cím:  Port:

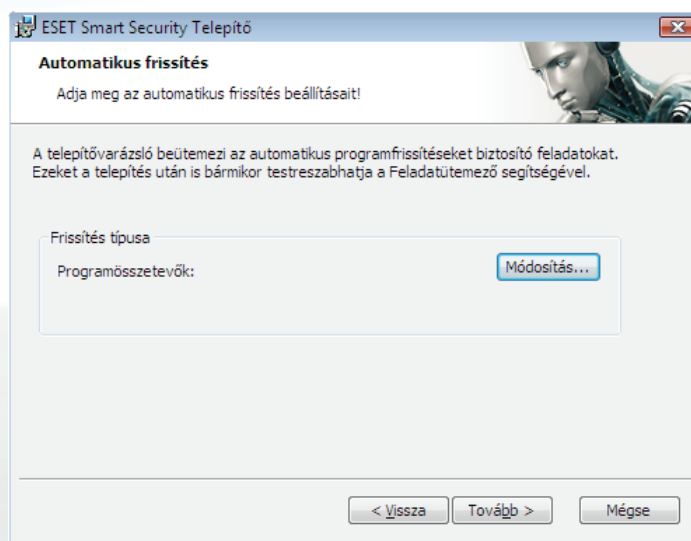
< Vissza   **Tovább >**   Mégse

A proxy szerver beállításához válassza ki a **Proxy szerveret használok** beállítást, majd kattintson a **Tovább** gombra. A Cím mezőben adja meg a proxy szerver URL vagy IP-címét. A Port mezőben állítsa be a proxy szerver portját (alapértelmezés szerint a 3128-as port).

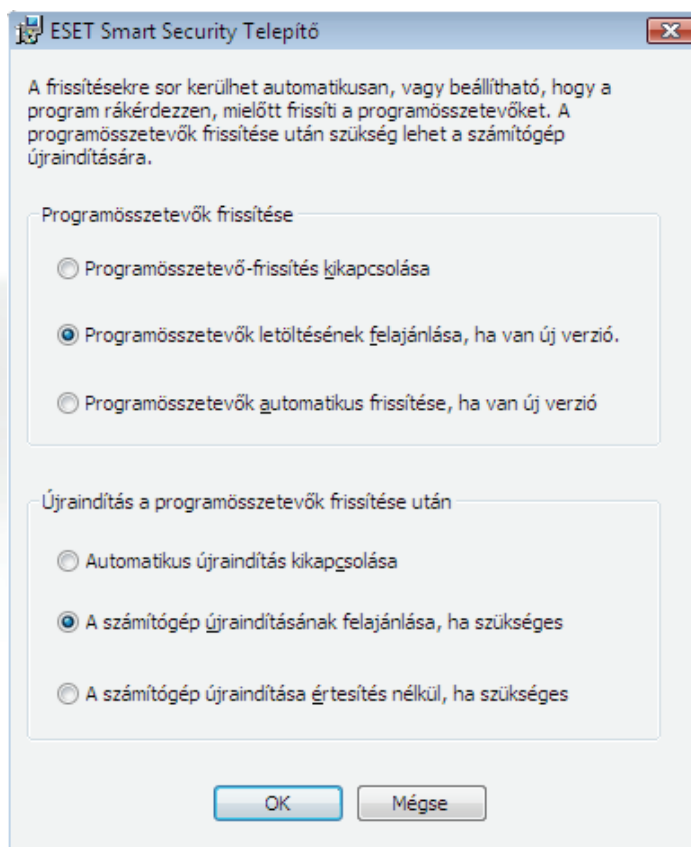
Abban az esetben, ha a proxy szerver használatához felhasználónév és jelszó szükséges, a megfelelő mezőkbe gépelje be ezeket.

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

A következő lépésben beállíthatja a programfrissítések működését. Kattintson a **Módosítás** gombra, ha be szeretné állítani, hogy a programösszetevők frissítését a program hogyan hajtsa végre.



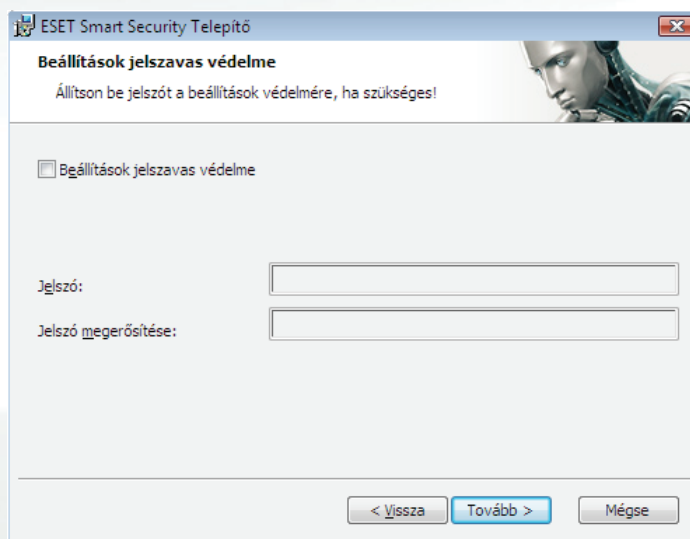
Ha nem szeretné, hogy az ESET Smart Security programösszetevői frissítésre kerüljenek, válassza a **Programösszetevő-frissítés kikapcsolása** opciót (nem javasolt). Ha szeretné, hogy a programösszetevők automatikusan frissítésre kerüljenek, válassza a **Programösszetevők automatikus frissítése, ha van új verzió** 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 beállításait a későbbiekben csak egy jelszó megadása után lehessen módosítani, jelölje ki a **Beállítások jelszavas védelme** opciót, és adjon meg egy jelszót, majd a jelszó ismételt begépelésével erősítse azt meg. Ezt követően kattintson a **Tovább** gombra.

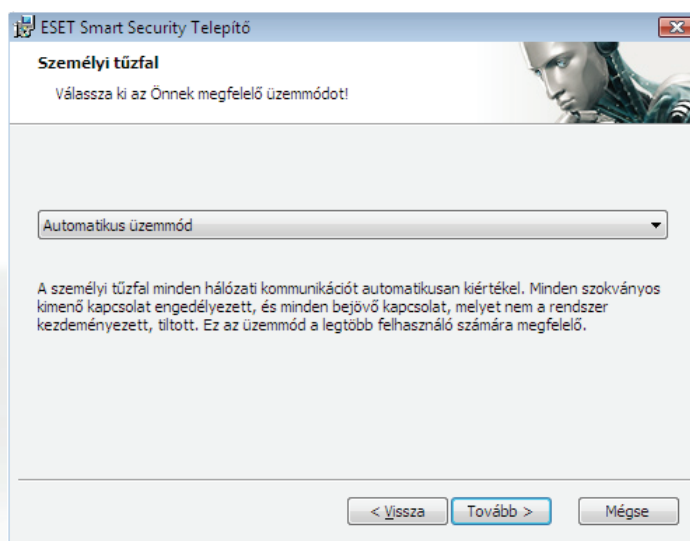




A ThreatSense.Net Korai Riasztási Rendszer beállításainak konfigurálása és a Kéretlen alkalmazások keresésének beállítása megegyezik a Tipikus telepítési mód ismertetése során leírtakkal (lásd 5. oldal).

Az Egyéni telepítés következő lépéseként az ESS Személyi tűzfal üzemmódját választhatja ki. A tűzfal három üzemmódban használható:

- **Automatikus üzemmód**
- **Interaktív üzemmód**
- **Házirend alapú üzemmód**



Az Automatikus üzemmód javasolt a legtöbb felhasználó számára. Ebben az üzemmódban előre meghatározott szabályok alapján kerül elemzésre az adatforgalom. Minden sztenderd 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. Ez a beállítás kizárólag hálózati rendszergazdák számára ajánlott.

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

### 2.3 Az eredeti beállítások visszaállítása

Amennyiben a későbbiek során újratelepíti az ESET Smart Security programot, a Telepítő Varázslóban 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.

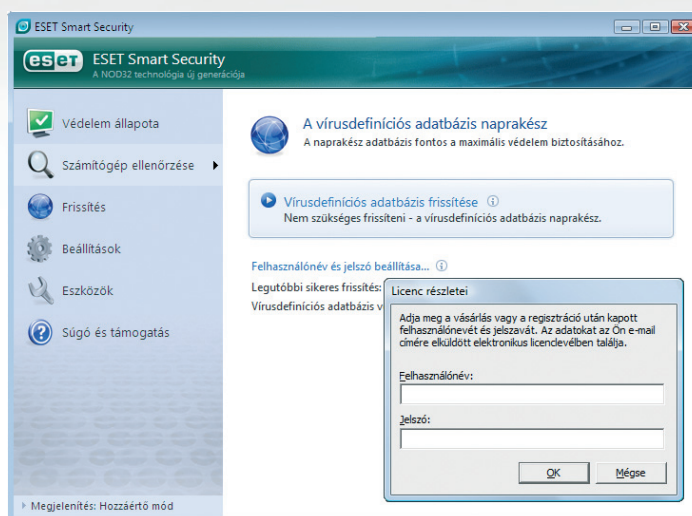


Figyelem, ez a képernyő különböző programváltozatok esetén eltérő lehet!

### 2.4 Felhasználónév és jelszó megadása

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

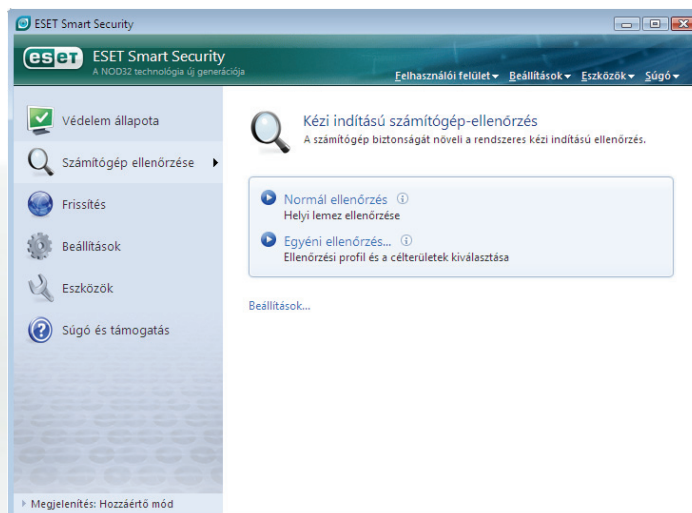
Ha a telepítés során a Frissítési adatok beállításánál nem adott meg érvényes felhasználónevet és jelszót, ezt a program kezelőfelületén keresztül is megteheti. A Windows operációs rendszer Start menüjén keresztül, vagy a jobb alsó sarokban, a tálcán látható ESET Smart Security ikon segítségével nyissa meg a feltelepített program főablakát, és kattintson a **Frissítés** menüpontban található **Felhasználónév és jelszó beállítása** opcióra. A felugró **Licenc részletei** ablakban adja meg a vásárlás vagy a regisztráció után kapott felhasználónevet 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 a **Normál ellenőrzés** opciót.



### 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 tartalmazza a főmenüt. A jobb oldali területen a bal oldali menüpontokhoz tartozó tartalmak jelennek meg aszerint, hogy melyik menüpont került kiválasztásra.

A alábbiakban a menüpontok tartalmát 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.

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

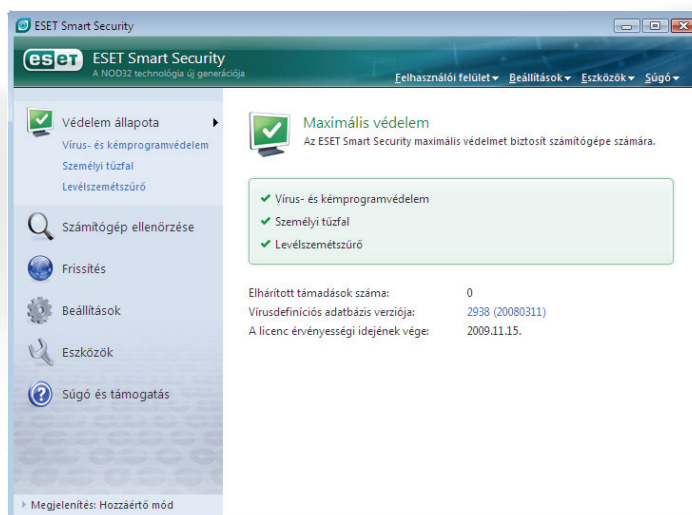
**Frissítés** – A frissítés, valamint a felhasználónév és jelszó beállításainak megtekintéséhez válassza ezt a menüpontot.

**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.

**Súgó és támogatás** – E menüpont segítségével elérheti a Súgót, a Gyakori Kérdések Ismertetőjét, illetve más támogatási funkciókat. Szintén ebben a menüpontban található 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 **Megjelenítés** nyomógomb segítségével 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.

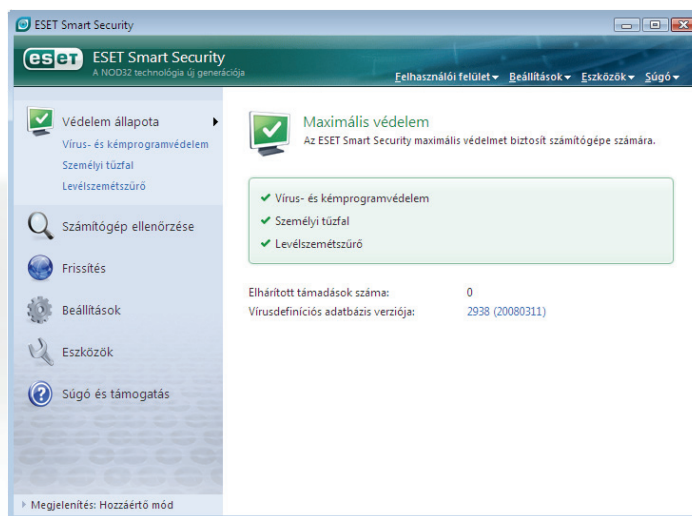


Amennyiben a megjelenítést átváltja Hozzáértő megjelenítési módra, a Főmenüben megjelenik az **Eszközök** menüpont, mely hozzáférést nyújt a Naplófájlokhoz, a Karanténhoz, valamint a Feladatütemezőhöz.

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

### 3.1.1 A védelem állapotának ellenőrzése

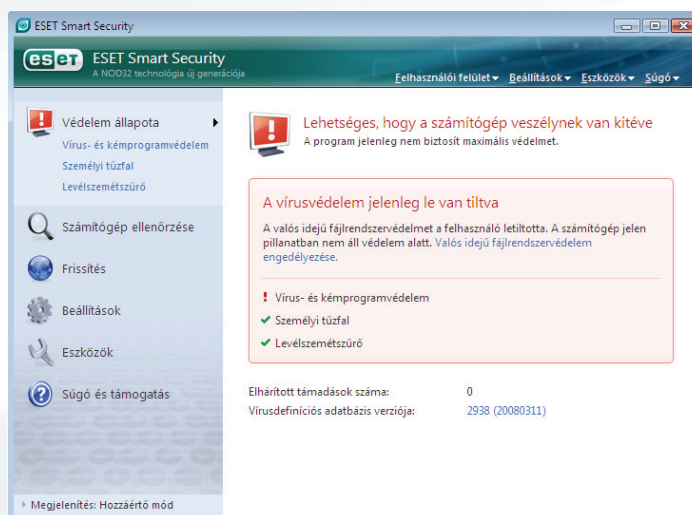
A védelem állapotának megtekintéséhez kattintson a főmenüben a **Védelem állapota** menüpontra. Ekkor a jobb oldalon a védelem állapotát összefoglaló információ jelenik meg, a bal oldalon pedig három menüpont: **Vírus- és kémprogramvédelem**, **Személyi tűzfal**, **Levélzemszűrő**. Válassza ki e menüpontok közül a megfelelőt, hogy az egyes modulok által biztosított védelem állapotáról részletes információt kapjon.



Amennyiben a modulok megfelelően működnek, a nevük 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.

### 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, és megoldást is kínál a problémára.



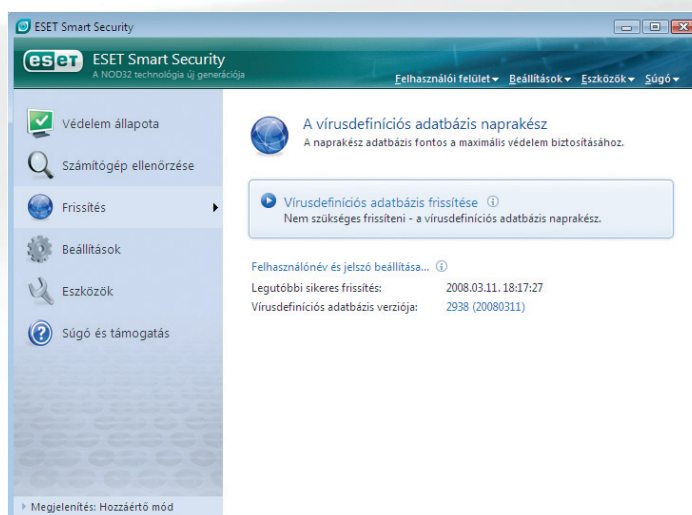
Amennyiben egy probléma nem oldható meg a megjelenített megoldási lehetőségek segítségével, további segítségért kattintson a **Súgó és támogatás** menüpontra. Amennyiben sem a súgóban, sem a gyakran ismételt kérdések listájában nem talál megoldást a problémára, vegye fel a kapcsolatot munkatársainkkal a **Kapcsolatfelvétel...** hivatkozás segítségével. Az Ön által megadott információk alapján szakértőink segítenek a probléma elhárításában.

### 3.2 Frissítés beállításai

A vírusdefiníciós adatbázis és a programösszetevők frissítése fontos ahhoz, hogy az ESET Smart Security naprakész védelmet tudjon 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.

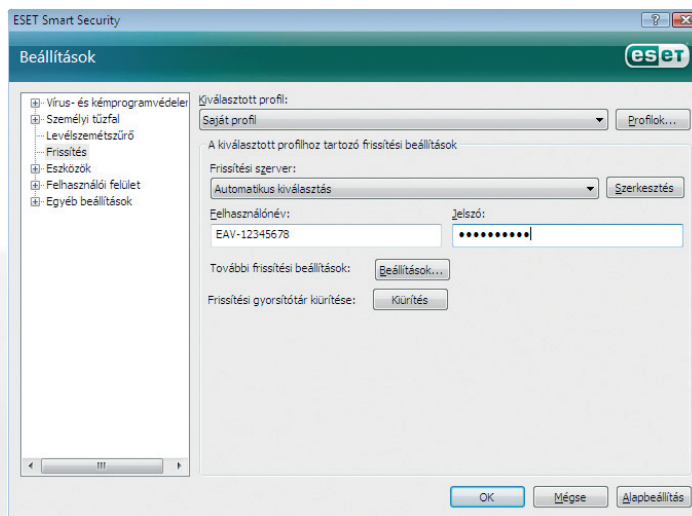
Ha a telepítés során nem adott meg felhasználónevet és jelszót a frissítések letöltéséhez, a program ezen a ponton kéri azokat. A felhasználónevet és a jelszót a vásárlás vagy a regisztráció során megadott e-mail címére küldött elektronikus licenclevélben találja.



Amennyiben a frissítés során hibüzenetet 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 beállításainak eléréséhez nyomja meg az F5 billentyűt, majd a felbukkanó ablak bal oldali menüfájában válassza ki a **Frissítés** menüpontot. A jobb oldalon megjelenő területen megtalálja a **Frissítési szerver** beállítását, melynek javasolt beállítása az Automatikus kiválasztás.

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

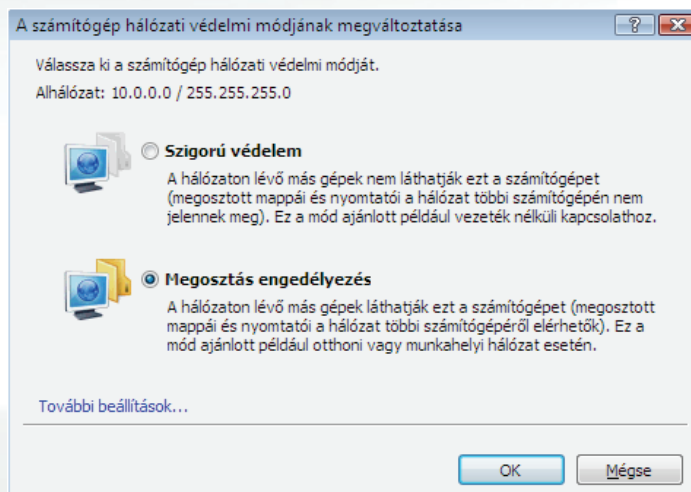


### 3.3 Megbízható zóna beállítása

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 az adott hálózatra vonatkozó védelmi módot.



A Megbízható zóna beállítására vonatkozó figyelmeztetés automatikusan felugrik az ESET Smart Security telepítése után, illetve minden alkalommal, amikor a számítógép új hálózathoz csatlakozik. Ilyenkor válassza ki, hogy az adott hálózatban milyen védelmi szintet kíván alkalmazni.

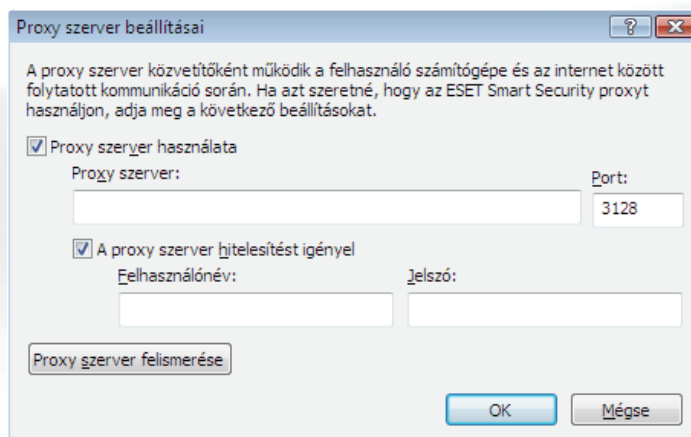


**Figyelmeztetés!** Amennyiben egy megbízhatatlan hálózatban a **Megosztás engedélyezése** mellett dönt, lehetséges, hogy ezzel biztonsági problémát okoz, és a számítógépet veszélynek teszi ki.

**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 Proxy szerver beállítása

Amennyiben a számítógép proxy szerveren keresztül kapcsolódik az internethez, ezt be kell állítani az ESET Smart Security programban. A beállításhoz hívja elő a Hozzáértő beállításokat az F5 gomb segítségével, majd kattintson duplán a bal oldali menüfában az **Egyéb beállítások** menüpontra, és válassza ki a **Proxy szerver** menüpontot. A jobb oldali beállítási területen jelölje ki a **Proxy szerver használata** opciót, és adja meg a proxy szerver URL vagy IP-címét, valamint a proxy szerver portját (alapértelmezés szerint ez a 3128-as port). Amennyiben a proxy szerver hitelesítést igényel, adja meg a megfelelő felhasználónevet és jelszót.



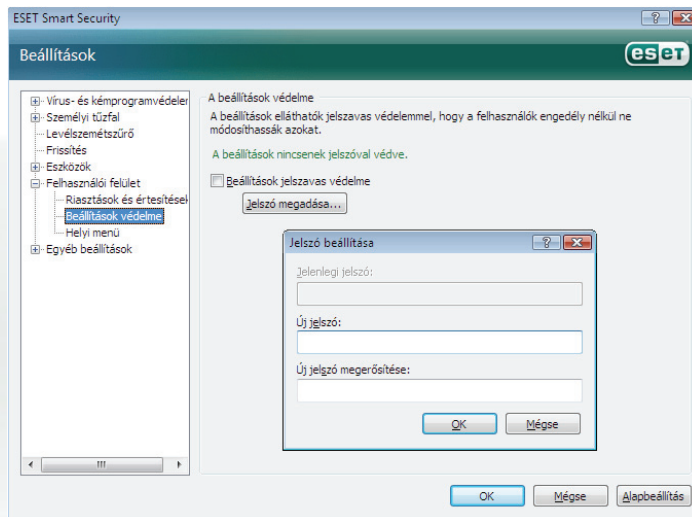
Amennyiben nem ismeri a proxy szerver címét, nyomja meg a **Proxy szerver felismerése** gombot, melynek hatására az ESET Smart Security megpróbálja automatikusan elvégezni a beállításokat.

**Megjegyzés:** A proxy szerver 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 A beállítások jelszavas védelme

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 **Beállítások védelme** 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.



### 4. További információk

Amennyiben kérdése merül fel az ESET Smart Security telepítésével vagy használatával kapcsolatban, tekintse meg a honlapon olvasható útmutatókat ([www.eset.hu/segitseg/utmutatok](http://www.eset.hu/segitseg/utmutatok)) és a gyakran ismételt kérdéseket ([www.eset.hu/segitseg/gyik](http://www.eset.hu/segitseg/gyik)).

További kérdéseivel forduljon bizalommal az ESET magyarországi képviselőjét ellátó Sicontact Kft. munkatársaihoz az alábbi e-mail címen vagy telefonszámon:

e-mail: [support@sicontact.hu](mailto:support@sicontact.hu)

telefon: **(1) 346 7054**  
Hétfőtől csütörtökig: 9:00 - 16:00  
Pénteken: 9:00 - 13:00