ESET Internet Security

Felhasználói útmutató

Ide kattintva megjelenítheti a dokumentum verzióját

Digital Security
Progress. Protected.

Copyright ©2023 – ESET, spol. s r.o.

Az ESET Internet Security terméket az ESET, spol. s r.o. fejlesztette ki

További információkért látogasson el a https://www.eset.com oldalra.

Minden jog fenntartva. A szerző írásos engedélye nélkül a jelen dokumentáció egyetlen része sem reprodukálható, nem tárolható adatlekérő rendszerben, illetve nem továbbítható semmilyen formában és semmilyen módon, legyen az elektronikus, mechanikus, fénymásolási, rögzítési, szkennelési vagy más mód.

Az ESET, spol. s r.o. fenntartja magának a jogot, hogy az ismertetett alkalmazásszoftvert előzetes értesítés nélkül megváltoztassa.

Műszaki terméktámogatás: https://support.eset.com

REV. 2023.03.19.

1 ESET Internet Security 1
1.1 Újdonságok 2
1.2 Melyik termékkel rendelkezem? 3
1.3 Rendszerkövetelmények 4
1.3 Az Ön által használt Windows 7 elavult 4
1.3 A Microsoft már nem támogatja a Windows 7 rendszert 5
1.3 A Windows Vista már nem támogatott 5
1.4 Megelőzés 6
1.5 Súgótémakörök 7
2 Telepítés 8
2.1 Online telepítő 8
2.2 Offline telepítés 10
2.3 Licenc aktiválása 11
2.3 A licenckulcs megadása az aktiválás során 12
2.3 A ESET HOME-fiók használata 13
2.3 Aktiválás próba üzemmódban 14
2.3 Ingyenes ESET-licenckulcs 14
2.3 Az aktiválás nem sikerült – gyakori forgatókönyvek 15
2.3 Az aktiválás nem sikerült túlhasznált licenc miatt 15
2.3 A licenc frissítése 16
2.3 A termék frissítése 17
2.3 A licenc visszaléptetése 18
2.3 A termék visszaléptetése 18
2.4 Telepítési hibaelhárító 19
2.5 Első ellenőrzés a telepítés után 19
2.6 Frissítés egy újabb verzióra 20
2.6 Régi termék automatikus frissítése 21
2.7 ESET-termék ajánlása ismerősnek 21
2.7 ESET Internet Security lesz telepítve 22
2.7 Váltson másik terméktípusra 22
2.7 Regisztráció 22
2.7 Aktiválási folyamat 22
2.7 Az aktiválás sikerült 22
3 Útmutató kezdő felhasználók számára 23
3.1 Csatlakozzon a ESET HOME szolgáltatáshoz 23
3.1 Bejelentkezés a ESET HOME szolgáltatásba 24
3.1 Nem sikerült a bejelentkezés – gyakori hibák 25
3.1 Eszköz hozzáadása a ESET HOME szolgáltatásban 26
3.2 A program főablaka 26
3.3 Frissítések 29
3.4 További biztonsági ESET-eszközök telepítése 30
3.5 Hálózati védelem konfigurálása 30
3.6 Engedélyezés Lopásvédelem 32
3.7 Szülői felügyeleti eszközök 32
4 Az ESET Internet Security használata 33
4.1 A számítógép védelme 35
4.1 Keresőmotor 36
4.1 A keresőmotor további beállításai 41
4.1 A program fertőzést észlelt 41
4.1 Valós idejű fájlrendszervédelem 43

4.1 Megtisztítási szintek 45
4.1 Mikor érdemes módosítani a valós idejű védelem beállításain? 46
4.1 A valós idejű védelem ellenőrzése 46
4.1 Teendők, ha a valós idejű védelem nem működik 46
4.1 Folyamatkivételek 47
4.1 Folyamatkivételek felvétele vagy szerkesztése 48
4.1 Felhőalapú védelem 48
4.1 Kivételszűrő a Felhőalapú védelemhez 51
4.1 Számítógép ellenőrzése 51
4.1 Egyéni ellenőrzés indítása 54
4.1 Az ellenőrzés folyamata 55
4.1 Számítógép-ellenőrzés naplója 57
4.1 Kártevő-ellenőrzések 59
4.1 Üresjárat idején történő ellenőrzés 59
4.1 Ellenőrzési profilok 60
4.1 Ellenőrizendő célterületek 61
4.1 Eszközfelügyelet 61
4.1 Eszközfelügyeleti szabályok szerkesztője 62
4.1 Észlelt eszközök 63
4.1 Eszközcsoportok 64
4.1 Eszközfelügyeleti szabályok hozzáadása 65
4.1 Webkamera-védelem 67
4.1 Webkamera-védelem szabályszerkesztője 68
4.1 Behatolásmegelőző rendszer (HIPS) 68
4.1 A Behatolásmegelőző rendszer interaktív ablaka 71
4.1 Lehetséges zsarolóprogram-viselkedés észlelve 72
4.1 Behatolásmegelőző rendszer szabályainak kezelése 73
4.1 Behatolásmegelőző rendszer szabálybeállításai 74
4.1 Alkalmazás vagy beállításkulcs elérési útjának hozzáadása a HIPS-hez 77
4.1 A Behatolásmegelőző rendszer haladó beállításai 77
4.1 Az illesztőprogramok mindig betölthetők 78
4.1 Játékos üzemmód 78
4.1 Rendszerindításkor futtatott ellenőrzés 79
4.1 Rendszerindításkor automatikusan futtatott fájlok ellenőrzése 79
4.1 Dokumentumvédelem 80
4.1 Kivételek 80
4.1 Teljesítménybeli kivételek 81
4.1 Teljesítménybeli kivételek felvétele vagy szerkesztése 82
4.1 Útvonalkivétel formátuma 84
4.1 Észlelési kivételek 85
4.1 Észlelési kivétel felvétele vagy szerkesztése 86
4.1 Varázsló létrehozása észlelési kivételekhez 87
4.1 HIPS-kivételek 88
4.1 ThreatSense paraméterek 88
4.1 Ellenőrzésből kizárt fájlkiterjesztések 92
4.1 További ThreatSense-paraméterek 92
4.2 Internetes védelem 93
4.2 Protokollszűrés 95
4.2 Kizárt alkalmazások 95
4.2 Kizárt IP-címek 96
4.2 IPv4-cím hozzáadása 97

4.2 IPv6-cím hozzáadása 97
4.2 SSL/TLS 97
4.2 Tanúsítványok 99
4.2 Titkosított hálózati forgalom 99
4.2 Ismert tanúsítványok listája 100
4.2 SSL/TLS szűrésű alkalmazások listája 101
4.2 E-mail védelem 101
4.2 Integrálás a levelezőprogramokkal 102
4.2 Microsoft Outlook-eszköztár 102
4.2 Outlook Express- és Windows Mail-eszköztár 103
4.2 Megerősítés 104
4.2 Üzenetek újraellenőrzése 104
4.2 Levelezési protokollok 104
4.2 POP3/POP3S-szűrő 105
4.2 E-mail-címkék 106
4.2 Levélszemétszűrő 107
4.2 Címfeldolgozási eredmény 108
4.2 Levélszemét-címlisták 108
4.2 Címlisták 109
4.2 Cím felvétele vagy módosítása 111
4.2 Webhozzáférés-védelem 111
4.2 A webhozzáférés-védelem haladó beállításai 114
4.2 Webprotokollok 114
4.2 URL-címek kezelése 115
4.2 URL-címlista 116
4.2 Új URL-címlista létrehozása 117
4.2 URL-maszk hozzáadása 118
4.2 Adathalászat elleni védelem 118
4.3 Hálózati védelem 120
4.3 Hálózatvédelem speciális beállítása 121
4.3 Ismert hálózatok 123
4.3 Ismert hálózatok szerkesztése 123
4.3 Hálózati hitelesítés – Szerverkonfiguráció 126
4.3 Zónák konfigurálása 127
4.3 Tűzfalzónák 127
4.3 Tűzfal 128
4.3 Tűzfalprofilok 130
4.3 Párbeszédablak – Tűzfalprofilok szerkesztése 130
4.3 Hálózati adapterekhez rendelt profilok 131
4.3 Szabályok beállítása és használata 131
4.3 Tűzfalszabályok listája 132
4.3 Tűzfalszabályok hozzáadása vagy szerkesztése 133
4.3 Tűzfalszabály – Helyi 135
4.3 Tűzfalszabályok – Távoli 136
4.3 Alkalmazások módosításának felismerése 137
4.3 Az ellenőrzésből kizárt alkalmazások listája 138
4.3 Tanuló mód beállításai 138
4.3 Hálózati támadások elleni védelem (IDS) 139
4.3 Brute-force támadás elleni védelem 140
4.3 Szabályok 140
4.3 IDS-szabályok 142

4.3 Lehetséges kártevő letiltva 145
4.3 Hálózati védelem hibájának elhárítása 145
4.3 Engedélyezett szolgáltatások és további beállítások 145
4.3 Csatlakoztatott hálózatok 148
4.3 Hálózati adapterek 149
4.3 IP-címek ideiglenes tiltólistája 149
4.3 Hálózatvédelmi napló 150
4.3 Kapcsolat létesítése – észlelés 151
4.3 Az ESET Tűzfallal kapcsolatos problémák megoldása 153
4.3 Hibaelhárítási varázsló 153
4.3 Naplózás és szabályok vagy kivételek létrehozása naplóból 153
4.3 Új szabály létrehozása naplóból 154
4.3 Kivételek létrehozása a személyi tűzfal értesítéseiből 154
4.3 A hálózati védelem speciális naplózása 154
4.3 Protokollszűrési problémák megoldása 154
4.3 A program új hálózatot észlelt 156
4.3 Alkalmazásmódosulás 157
4.3 Bejövő megbízható kommunikáció 157
4.3 Kimenő megbízható kommunikáció 158
4.3 Bejövő kommunikáció 160
4.3 Kimenő kommunikáció 161
4.3 Kapcsolatok megjelenítésének beállításai 162
4.4 Biztonsági eszközök 162
4.4 Netbank- és tranzakcióvédelem 163
4.4 Netbank- és tranzakcióvédelem speciális beállítása 164
4.4 Védett webhelyek 165
4.4 Böngészőn belüli értesítés 165
4.4 Szülői felügyelet 166
4.4 Webhelykivételek 168
4.4 Felhasználói fiókok 170
4.4 Kategóriák 170
4.4 A felhasználói fiókok használata 171
4.4 Kivétel másolása felhasználótól 173
4.4 Kategóriák másolása fiókból 173
4.4 A szülői felügyelet engedélyezése 173
4.4 Lopásvédelem 174
4.4 Jelentkezzen be az ESET HOME-fiókjába. 175
4.4 Készüléknév beállítása 176
4.4 Lopásvédelem engedélyezve/letiltva 177
4.4 Az új eszköz hozzáadása nem sikerült 177
4.5 A program frissítése 177
4.5 Frissítési beállítások 180
4.5 Frissítési fájlok visszaállítása 182
4.5 Visszaállítási időintervallum 184
4.5 Termékfrissítések 184
4.5 Kapcsolati beállítások 184
4.5 Frissítési feladatok létrehozása 185
4.5 Párbeszédablak – Újraindítás szükséges 186
4.6 Eszközök 186
4.6 Hálózatfelügyelet 187
4.6 Hálózati eszköz a Hálózatfelügyeletben 189

4.6 Értesítések | Hálózatfelügyelet ... 192
4.6 Az ESET Internet Security eszközei ... 192
4.6 Naplófájlok ... 194
4.6 Napló szűrése ... 196
4.6 Naplózási konfiguráció ... 197
4.6 Futó folyamatok ... 198
4.6 Biztonsági jelentés ... 200
4.6 Hálózati kapcsolatok ... 202
4.6 Hálózati aktivitás ... 203
4.6 ESET SysInspector ... 204
4.6 Feladatütemező ... 205
4.6 Ütemezett ellenőrzés beállításai ... 208
4.6 Ütemezett feladat áttekintése ... 209
4.6 Feladat részletei ... 209
4.6 Feladat időzítése ... 209
4.6 Feladat időzítése – Egyszer ... 210
4.6 Feladat időzítése – Naponta ... 210
4.6 Feladat időzítése – Hetente ... 210
4.6 Feladat időzítése – Esemény hatására ... 210
4.6 Kihagyott feladat ... 211
4.6 Feladat részletei – Frissítés ... 211
4.6 Feladat részletei – Alkalmazás futtatása ... 211
4.6 Rendszertisztító ... 212
4.6 ESET SysRescue Live ... 213
4.6 Karantén ... 214
4.6 Proxyszerver ... 216
4.6 Minta kiválasztása elemzésre ... 217
4.6 Minta kiválasztása elemzésre – Gyanús fájl ... 218
4.6 Minta kiválasztása elemzésre – Gyanús webhely ... 218
4.6 Minta kiválasztása elemzésre – Tévesen jelentett fájl ... 219
4.6 Minta kiválasztása elemzésre – Tévesen jelentett webhely ... 219
4.6 Minta kiválasztása elemzésre – Egyéb ... 220
4.6 Microsoft Windows® frissítés ... 220
4.6 Párbeszédablak – Rendszerfrissítések ... 220
4.6 Frissítési információk ... 220
4.7 Felhasználói felület ... 221
4.7 Felhasználói felület elemei ... 221
4.7 Hozzáférési beállítások ... 222
4.7 Jelszó a További beállításokhoz ... 223
4.7 A rendszer tálcaikonja ... 223
4.7 Képernyőolvasók támogatása ... 225
4.7 Súgó és támogatás ... 225
4.7 Az ESET Internet Security névjegye ... 226
4.7 ESET Hírek ... 226
4.7 Rendszer-konfigurációs adatok küldése ... 227
4.7 Műszaki terméktámogatás ... 228
4.8 Értesítések ... 228
4.8 Párbeszédablak – Alkalmazásállapotok ... 229
4.8 Asztali értesítések ... 229
4.8 Asztali értesítések listája ... 231
4.8 Interaktív riasztások ... 232

4.8 Megerősítési üzenetek ... 234
4.8 Cserélhető adathordozók ... 235
4.8 Továbbítás ... 236
4.9 Adatvédelmi beállítások ... 238
4.10 Profilok ... 239
4.11 Billentyűparancsok ... 240
4.12 Diagnosztika ... 241
4.12 Műszaki terméktámogatás ... 243
4.12 Beállítások importálása és exportálása ... 243
4.12 Az összes beállítás visszaállítása ezen a részen ... 244
4.12 Visszaállítás az alapbeállításokra ... 244
4.12 Hiba a konfiguráció mentésekor ... 244
4.13 Parancssori víruskereső ... 244
4.14 ESET CMD ... 247
4.15 Üresjárat idején történő ellenőrzés ... 248
5 Gyakori kérdések ... 249
5.1 Az ESET Internet Security frissítése ... 250
5.2 Vírus eltávolítása a számítógépről ... 250
5.3 Kommunikáció engedélyezése adott alkalmazás számára ... 250
5.4 Szülői felügyelet engedélyezése egy fiókhoz ... 251
5.5 Új feladat létrehozása a feladatütemezőben ... 252
5.6 Heti számítógép-ellenőrzés ütemezése ... 253
5.7 A következő hiba elhárítása: „A Netbank- és tranzakcióvédelem átirányítása nem sikerült a kért weboldalra” ... 254
5.8 A További beállítások feloldása ... 256
5.9 Hogyan hárítható el a termékdeaktiválási probléma a ESET HOME portálról? ... 257
5.9 A termék inaktiválva, az eszköz leválasztva ... 257
5.9 A licenc nincs aktiválva ... 257
6 Felhasználói élmény javítását célzó program ... 258
7 Végfelhasználói licencszerződés ... 259
8 Adatvédelmi szabályzat ... 270

ESET Internet Security

ESET Internet Security – ez egy újszerű megoldást jelentő integrált biztonsági programcsomag. Az ESET LiveGrid® keresőmotor legújabb, a Tűzfal és a Levélszemétszűrő modullal kombinált 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 Internet Security egy teljes körű biztonsági termék, amely minimális rendszerterhelés mellett kínál maximális védelmet. Korszerű technológiánk a mesterséges intelligencián alapuló elemző algoritmusok segítségével képes kivédeni a vírusok, kémprogramok, trójaiak, férgek, kéretlen reklámprogramok, rootkitek és más károkozók támadását anélkül, hogy visszafogná a rendszer teljesítményét vagy zavarná a számítógép működését.

Szolgáltatások és előnyök

Újratervezett felhasználói felület	Ennek a verziónak a felhasználói felülete újra lett tervezve, és egyszerűsödött a használhatósági tesztek eredménye alapján. A felhasználói felület szövegei és értesítései alapos ellenőrzésen estek át, és a felület már a jobbról balra író nyelveket (például héber és arab) is támogatja. Az online súgó az ESET Internet Security termék része lett, és dinamikusan frissített támogatási tartalommal áll rendelkezésre.
Vírus- és kémprogramvédelem	Proaktív módon felismeri az ismert és a még ismeretlen vírusokat, férgeket, trójaiakat, rootkiteket, és megtisztítja az érintett fájlokat. A kiterjesztett heurisztikai észlelés korábban soha nem látott kártevőket észlel, így védelmet nyújt az ismeretlen fenyegetésekkel szemben, és még azt megelőzően semlegesíti azokat, hogy bármilyen kárt okozhatnának. A webhozzáférés-védelem és az adathalászat elleni védelem figyeli a böngészők és a távoli szerverek közötti kommunikációt (az SSL-t is beleértve). Az e-mail védelem a POP3(S) és az IMAP(S) protokollon keresztül folytatott e-mailes kommunikáció felügyeletét biztosítja.
Rendszeres frissítések	A keresőmotor (korábbi nevén „vírusdefiníciós adatbázis”) és a programmodulok rendszeres frissítésével biztosítható a legjobban a számítógép legmagasabb fokú védelme.
ESET LiveGrid® (Felhőalapú megbízhatóság)	A futó folyamatok és fájlok megbízhatóságát közvetlenül az ESET Internet Security alkalmazásból ellenőrizheti.
Eszközfelügyelet	Automatikusan ellenőrzi az összes USB flash meghajtót, memóriakártyát, CD-t és DVD-t. Letiltja a cserélhető adathordozókat az adathordozó típusa, a gyártó, a méret és más attribútumok alapján.
Behatolásmegelőző rendszer	Részletesen testre szabhatja a rendszer működését, szabályokat adhat meg a rendszer beállításjegyzékére, az aktív folyamatokra és programokra vonatkozóan, és pontosíthatja a biztonsági állapotát.
Játékos üzemmód	Elhalasztja a felugró ablakok megjelenését, a frissítéseket és minden egyéb, a rendszert igénybe vevő tevékenységet, hogy a rendszererőforrásokat a játékokhoz vagy más teljes képernyős tevékenységekhez őrizze meg.

Az ESET Internet Security szolgáltatásai

Netbank- és tranzakcióvédelem	A Netbank- és tranzakcióvédelem biztonságos böngészőt nyújt az online banki tranzakciók vagy online fizetőfelületek használatakor, hogy minden online tranzakció megbízható és biztonságos környezetben történjen.

Hálózati definíciók támogatása	A hálózati definíciók lehetővé teszik a felhasználók eszközeitől érkező vagy azokra irányuló kártékony forgalom (például botok és exploitcsomagok) gyors azonosítását és tiltását. Ez a funkció a Botnet elleni védelem bővítésének tekinthető.
Intelligens tűzfal	Megakadályozza, hogy jogosulatlan felhasználók hozzáférjenek számítógépéhez, és megszerezzék személyes adatait.
ESET Levélszemétszűrő	A levélszemét a teljes levelezés mintegy 50 százalékát teszi ki. A levélszemétszűrés megoldást nyújt erre a problémára.
Lopásvédelem	Az Lopásvédelem növeli a felhasználó biztonságát a számítógép elvesztése vagy ellopása esetén. Miután a felhasználók telepítik az ESET Internet Security alkalmazást és az Lopásvédelem szolgáltatást, eszközük megjelenik a webes felület listájában. A webes felületen a felhasználók kezelhetik az Lopásvédelem konfigurációját, és beállíthatják a lopásvédelmi funkciókat az eszközükön.
Szülői felügyelet	A különféle webhely-kategóriák letiltásával biztosítja családja védelmét az esetlegesen nem kívánt webes tartalmak ellen.

Az ESET Internet Security szolgáltatásainak működéséhez aktív licencre van szükség. Javasoljuk, hogy az ESET Internet Security licencének a lejárata előtt néhány héttel újítsa meg a licencét.

Újdonságok

Újdonságok az ESET Internet Security 15-es verziójában

Továbbfejlesztett Hálózatfelügyelet (korábban Összekapcsolt otthon)

Segít megvédeni a hálózatot és az IoT-eszközöket, és megjeleníti a routerhez csatlakoztatott eszközöket. Nézze meg, hogyan ellenőrizheti az Ön által használt hálózatokat, és hogy milyen eszközök csatlakoznak.

ESET HOME (korábban myESET)

Átláthatóbb és részletesebb felügyeleti lehetőségeket nyújt a csatlakoztatott eszközök biztonságát illetően. Védelmet telepíthet új eszközökre, hozzáadhat és megoszthat licenceket, valamint a mobilalkalmazás vagy a webportál révén fontos értesítéseket kaphat. További információkért tekintse meg a ESET HOME online súgóját.

Továbbfejlesztett Behatolásmegelőző rendszer (HIPS)

Ellenőrzi azokat a memóriaterületeket is, amelyek csak kifinomultabb kártevőinjektálási technikákkal módosíthatók. Fejlesztéseinknek köszönhetően ezek a támadási eljárások is észlelhetővé válnak.

Az ESET Internet Security új funkcióival kapcsolatos képekről és további információkról Az ESET otthoni termékek legújabb verziójának újdonságai című témakörben olvashat.

> Az **újdonságokról szóló értesítések** letiltásához kattintson a **További beállítások** > **Értesítések** > **Asztali értesítések** elemre. Kattintson az **Asztali értesítések** szöveg melletti **Szerkesztés** gombra, és törölje a jelet az **Újdonságokról szóló értesítések megjelenítése** jelölőnégyzetből. Az értesítésekkel kapcsolatos további információkért tekintse meg az Értesítések szakaszt.

Melyik termékkel rendelkezem?

Az ESET számos biztonsági réteget nyújt az új termékekben, a hatékony és gyors vírusvédelmi megoldástól kezdve a minimális rendszerterhelés mellett mindenre kiterjedő biztonsági megoldásig:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Ha meg szeretné állapítani, hogy Önnél melyik termék van telepítve, nyissa meg a fő programablakot, és tekintse meg a termék nevét az ablak tetején (lásd az erről szóló tudásbáziscikket).

Az alábbi táblázat felsorolja az egyes termékekben rendelkezésre álló funkciókat.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Keresőmotor	✔	✔	✔
Speciális gépi tanulás	✔	✔	✔
Exploit blokkoló	✔	✔	✔
Szkript-alapú támadások elleni védelem	✔	✔	✔
Adathalászat elleni védelem	✔	✔	✔
Webhozzáférés-védelem	✔	✔	✔
Behatolásmegelőző rendszer (Zsarolóprogram elleni védelem is)	✔	✔	✔
Levélszemétszűrő		✔	✔
Tűzfal		✔	✔
Hálózatfelügyelet		✔	✔
Webkamera-védelem		✔	✔
Hálózati támadások elleni védelem		✔	✔
Botnet elleni védelem		✔	✔
Netbank- és tranzakcióvédelem		✔	✔
Szülői felügyelet		✔	✔
Lopásvédelem		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Előfordulhat, hogy a fenti termékek némelyike nem érhető el az Ön nyelvén/régiójában.

Rendszerkövetelmények

A rendszernek az alábbi hardver- és szoftverkövetelményeknek kell megfelelnie az ESET Internet Security optimális működéséhez:

Támogatott processzorok

Intel vagy AMD processzor, 32 bites (x86) SSE2 utasításkészlettel vagy 64 bites (x64), 1 GHz-es vagy nagyobb ARM64 alapú processzor, 1 GHz vagy magasabb

Támogatott operációs rendszerek*

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1 és a legújabb Windows-frissítések
Microsoft® Windows® Home Server 2011 64-bit

Törekedjen arra, hogy az operációs rendszer mindig naprakész legyen.

Az Lopásvédelem nem támogatja a Microsoft Windows Home Server szoftvert.

Egyéb

Internetkapcsolat szükséges az aktiváláshoz és ahhoz, hogy az ESET Internet Security frissítései megfelelően működjenek.

Ha két víruskereső program fut egyszerre egy adott eszközön, akkor ez elkerülhetetlenül ütközéseket okoz a rendszererőforrások között, például lelassítja a rendszert, és működésképtelenné válhat.

*Az ESET nem tud védelmet nyújtani nem támogatott operációs rendszerekhez 2021 februárja óta.

Az Ön által használt Windows 7 elavult

Hiba

Az operációs rendszer elavult verzióját futtatja. A védelem további biztosításához törekedjen arra, hogy az operációs rendszer mindig naprakész legyen.

Megoldás

Az ESET Internet Security telepítve van a következő rendszeren: {GET_OSNAME} {GET_BITNESS}.

Győződjön meg arról, hogy telepítette a Windows 7 SP1 rendszert és a legújabb Windows-frissítéseket (legalább a KB4474419 és a KB4490628 számú frissítést).

Ha nincs beállítva, hogy a Windows 7 automatikusan frissüljön, kattintson a **Start menü** > **Vezérlőpult** > **Rendszer és biztonság** > **Windows Update** > **Frissítések keresése** elemre, majd kattintson a **Frissítések telepítése** gombra.

Tekintse meg a következő cikket is: A Microsoft már nem támogatja a Windows 7 rendszert.

A Microsoft már nem támogatja a Windows 7 rendszert

Hiba

A Microsoft 2020. január 14. óta nem támogatja a Windows 7-et. Mivel jár ez?

Ha a támogatás megszűnése után is használja a Windows 7-et, a számítógép továbbra is működni fog, de sebezhetőbbé válhat a biztonsági kockázatokkal és a vírusokkal szemben. A számítógép a továbbiakban nem kapja meg a Windows-frissítéseket (beleértve a biztonsági frissítéseket is).

Megoldás

Windows 7-ről frissít Windows 10-re? Frissítse az ESET-terméket is.

A frissítési folyamat viszonylag egyszerű, és sok esetben a fájlok elvesztése nélkül is megteheti. A Windows 10-re való frissítés előtt:

1. Ellenőrizze/frissítse az ESET-terméket
2. Fontos adatok biztonsági mentése
3. Olvassa el a Microsoft Frissítés Windows 10-re: GYIK című cikkét, és frissítse a Windows operációs rendszert

Új számítógépet vagy eszközt szerez be? Vigye át rá az ESET-terméket.

Ha új számítógépet vagy eszközt fog vásárolni, vagy már megtette, tekintse meg, hogyan vihető át a meglévő ESET-termék az új eszközre.

Tekintse meg a következőt is: Megszűnt a Windows 7 támogatása.

A Windows Vista már nem támogatott

Hiba

A Windows Vista technikai korlátai miatt az ESET Internet Security nem tud védelmet nyújtani **2021 februárja** után. Az ESET-termék ezután nem lesz **működőképes**. Emiatt a rendszer sebezhetővé válhat a fertőzésekkel szemben.

A Microsoft 2017. április 11. óta nem támogatja a Windows Vistát. Mivel jár ez?

Ha a támogatás megszűnése után is használja a Windows Vista, a számítógép továbbra is működni fog, de sebezhetőbbé válhat a biztonsági kockázatokkal és a vírusokkal szemben. A számítógép a továbbiakban nem kapja meg a Windows-frissítéseket (beleértve a biztonsági frissítéseket is).

Megoldás

Windows Vistáról Windows 10-re szeretne frissíteni? Szerezzen be egy új számítógépet vagy eszközt, és vigye át rá az ESET-terméket.

A Windows 10-re való frissítés előtt:

1. Fontos adatok biztonsági mentése
2. Olvassa el a Microsoft Frissítés Windows 10-re: GYIK című cikkét, és frissítse a Windows operációs rendszert
3. Telepítse vagy vigye át a meglévő ESET-terméket az új eszközre.

> Tekintse meg a következőt is: Megszűnt a Windows Vista támogatása.

Megelőzés

Számítógép használata, és különösen internetes böngészés közben folyton tartsa szem előtt, hogy a világon egyetlen vírusvédelmi szoftver sem képes teljesen megszüntetni azt a kockázatot, hogy a számítógépben kárt okozhatnak a kártevők és a távolról kezdeményezett támadások. A legmagasabb szintű védelem és kényelem érdekében fontos, hogy megfelelően használja a vírusvédelmi megoldást, és kövesse a különféle hasznos szabályokat:

Rendszeres frissítés

A ESET LiveGrid® 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 növeljék a védelmi szintet a felhasználók számára. A frissítések maximális hatékonyságának biztosításához a frissítéseket megfelelően kell beállítani a rendszeren. A frissítések beállításának módjáról a Frissítési beállítások című fejezetben olvashat bővebben.

Biztonsági javítócsomagok letöltése

A kártékony szoftverek szerzői előszeretettel használják ki a rendszer különféle biztonsági réseit, hogy megkönnyítsék kódjaik terjesztését. 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. A Microsoft Windows és a böngészők, például az Internet Explorer két példa, amelyek esetében rendszeresen adnak ki biztonsági frissítéseket.

Fontos adatok biztonsági mentése

A kártevők készítői általában nem foglalkoznak a felhasználók igényeivel, és az ilyen programok tevékenysége gyakran az operációs rendszer tönkretételével és a fontos adatok szándékos elvesztésével 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

Az ismert és ismeretlen vírusok, férgek, trójaiak és rootkitek észlelését a Valós idejű fájlrendszervédelem modul végzi. Ez azt jelenti, hogy valahányszor elér vagy megnyit egy fájlt, a modul abban kártevőket keres. Javasoljuk azonban, hogy havonta egyszer végezzen teljes számítógép-ellenőrzést, mert a kártevők változhatnak, és a keresőmotor naponta frissül.

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 időt és erőfeszítést. Hasznos tanácsok:

- 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.

Súgótémakörök

Üdvözli az ESET Internet Security felhasználói útmutatója! A súgóbeli információk segítenek a termék megismerésében és a számítógép biztonságosabbá tételében.

Első lépések

Javasoljuk, hogy az ESET Internet Security használata előtt ismerkedjen meg azokkal a különféle fertőzéstípusokkal és távoli támadásokkal, amelyekkel találkozhat a számítógép használata közben.

Az ESET Internet Security új funkcióit felsoroló listát is összeállítottuk, valamint egy útmutatót is biztosítunk az alapvető beállítások konfigurálásához.

Az ESET Internet Security súgótémaköreinek használata

A súgótémakörök fejezetekből és alfejezetekből állnak. Az **F1** billentyűt lenyomva megtekintheti az éppen aktív ablakkal kapcsolatos információkat.

A súgóban kulcsszavakkal és tetszőleges keresőkifejezésekkel is kereshet. A két módszer között az a különbség, hogy a kulcsszavak logikailag olyan súgótémakörökhöz is kapcsolódhatnak, melyek szövegében nem szerepel az adott kulcsszó. A szabadszavas keresés esetén azok a témakörök jelennek meg, melyek szövege tartalmazza a keresett szót vagy szavakat.

A konzisztencia érdekében és a félreértések elkerülése végett a jelen útmutatóban használt terminológia az ESET Internet Security paraméternevein alapul. A különös jelentőséggel bíró témakörök kiemelésére emellett egy egységes szimbólumkészletet is használunk.

A megjegyzések rövid észrevételek. Bár kihagyhatja, a megjegyzések értékes információkat nyújtanak, amilyenek például az adott funkciók vagy egy kapcsolódó témakörre mutató hivatkozás.

Azt javasoluk, hogy ne hagyja ki ezt a lépést. Általában nem kritikus fontosságú, de jelentős információkról van szó.

Ezek az információk különleges figyelmet és elővigyázatosságot igényelnek. A figyelmeztetések kifejezetten arra szolgálnak, hogy figyelembevételükkel elkerülhesse a potenciálisan kárt okozó hibákat. Olvassa el, és értelmezze az ilyen figyelmeztetéseket, mivel rendkívül érzékeny rendszerbeállításokra vagy egyéb, kockázattal járó körülményekre hívják fel a figyelmét.

Ezek használatot bemutató esetek vagy gyakorlati példák, amelyek bizonyos funkciók vagy szolgáltatások használatának a megismerését segítik.

Konvenció	Jelentés
Félkövér formázás	A felhasználói felület elemeinek (például mezők és gombok) neve.
Dőlt formázás	Az Ön által megadandó információk helyőrzője. A fájlnév vagy az elérési út például azt jelenti, hogy Önnek meg kell adnia a tényleges elérési utat vagy fájlnevet.
`Courier New`	Kódminták vagy parancsok
Hivatkozás	Gyors és egyszerű hozzáférést nyújt az útmutatón belül hivatkozott témakörre vagy külső webhelyre. A hivatkozások kék színűek, és előfordulhat, hogy alá vannak húzva.
%ProgramFiles%	A Windows rendszerben telepített programokat tároló Windows rendszerbeli könyvtár.

A súgótartalom elsődleges forrása az **online súgó**. Az online súgó legújabb verziója automatikusan megjelenik, ha aktív az internetkapcsolat.

Telepítés

Az ESET Internet Security terméket számos módon telepítheti a számítógépre. A telepítési módszerek az országtól és a terjesztés módjától függően eltérhetnek:

- Online telepítő – Letölthető az ESET webhelyéről vagy CD/DVD-lemezről. A telepítőcsomag minden nyelvhez használható (válassza ki a kívánt nyelvet). Az online telepítő egy kis fájl, az ESET Internet Security telepítéséhez szükséges további fájlok automatikusan letöltődnek.

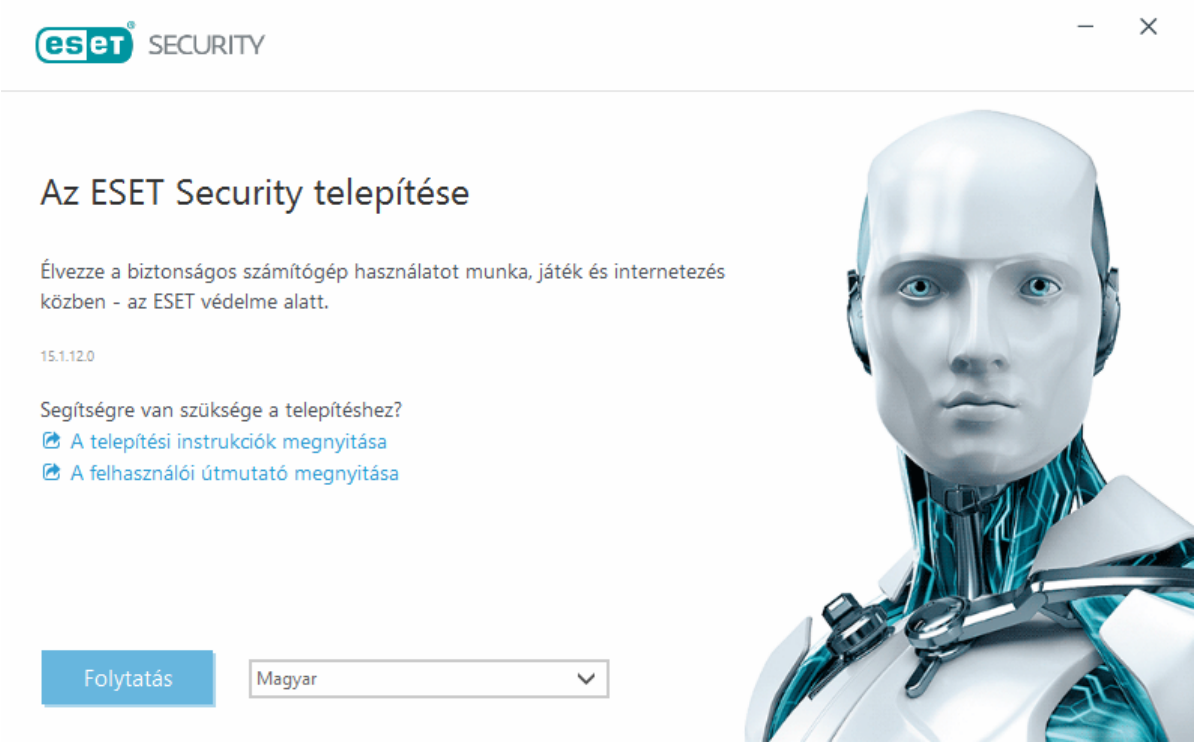
- Offline telepítés – Az online telepítőfájlnál nagyobb .exe fájlt használ, és nem igényel internetkapcsolatot vagy további fájlokat a telepítés elvégzéséhez.

Az ESET Internet Security telepítése előtt 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. Az általános vírusvédelmi szoftverek eltávolítására szolgáló eszközök listáját tudásbáziscikkünk tartalmazza (angolul és néhány más nyelven).

Online telepítő

Miután letöltötte az Live Installer telepítőcsomag, kattintson duplán a telepítőfájlra, és kövesse a Telepítővarázsló ablakában megjelenő utasításokat.

Ehhez a telepítési típushoz aktív internetkapcsolatra van szükség.



1. Válassza ki a megfelelő nyelvet a legördülő menüből, majd kattintson a **Folytatás** gombra.

Ha újabb verziót telepít egy korábbi verzióra jelszóval védett beállításokkal, írja be a jelszavát. A beállítások jelszavát az Hozzáférési beállítások lapon konfigurálhatja.

2. Válassza ki a következő funkciók beállításait, olvassa el a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot, majd a **Folytatás** vagy **Az összes engedélyezése és folytatás** gombra kattintva engedélyezze az összes funkciót:

- ESET LiveGrid® visszajelzési rendszer
- Kéretlen alkalmazások
- Felhasználói élmény javítását célzó program

A **Folytatás** vagy **Az összes engedélyezése és folytatás** gombra kattintva elfogadja a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot.

3. A ESET HOME segítségével történő eszközaktiváláshoz, -kezeléshez és az eszköz biztonságának megtekintéséhez csatlakoztassa eszközét a ESET HOME-fiókhoz. A **Bejelentkezés kihagyása** gombra kattintva a ESET HOME portálhoz való csatlakozás nélkül folytathatja. Később csatlakoztathatja eszközét a ESET HOME-fiókjához.

4. Ha a ESET HOME szolgáltatáshoz való csatlakozás nélkül lép tovább, válasszon egy aktiválási lehetőséget. Ha újabb verziót telepít egy korábbi verzióra, akkor a rendszer automatikusan beírja a licenckulcsot.

5. A Telepítővarázsló határozza meg, hogy melyik ESET-termék van telepítve a licenc alapján. A legtöbb biztonsági funkcióval rendelkező verzió van mindig előre kiválasztva. Kattintson a **Termék váltása** elemre, ha az ESET-termék egy másik verzióját szeretné telepíteni. Kattintson a **Folytatás** gombra a telepítési folyamat

elindításához. Ez néhány percet igénybe vehet.

Ha a múltban eltávolított ESET-termékekből vannak még maradványok (fájlok vagy mappák), akkor a rendszer megkéri, hogy engedélyezze az eltávolításukat. Kattintson a **Telepítés** gombra a folytatáshoz.

6. Kattintson a **Kész** gombra a Telepítővarázslóból való kilépéshez.

Telepítési hibaelhárító.

A termék telepítése és aktiválása után megkezdődik a modulok letöltése. Megkezdődik a védelem inicializálása, és előfordulhat, hogy néhány funkció nem működik teljes mértékben a letöltés befejeződéséig.

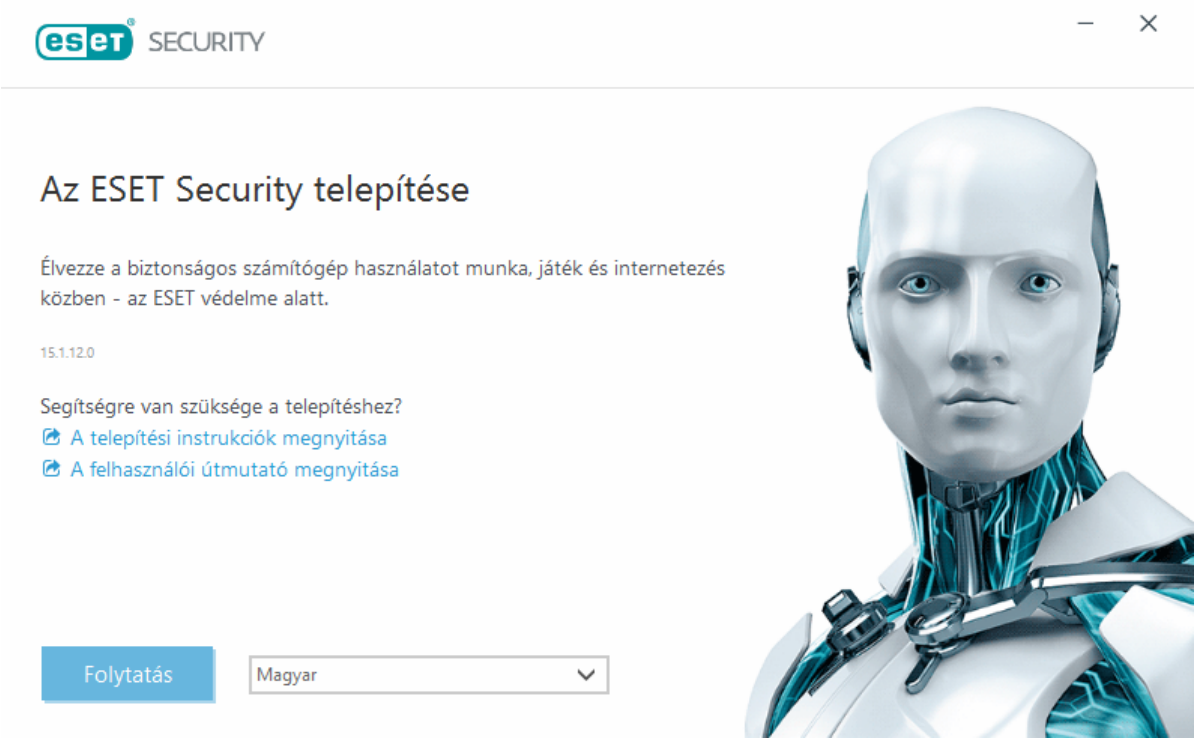
Offline telepítés

Töltse le és telepítse az ESET Windows otthoni terméket a lenti offline telepítő (.exe) segítségével. Válassza ki az ESET otthoni termék letölteni kívánt verzióját (32 bites, 64 bites vagy ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
64 bites letöltés 32 bites letöltés ARM letöltés	64 bites letöltés 32 bites letöltés ARM letöltés	64 bites letöltés 32 bites letöltés ARM letöltés

Ha aktív internetkapcsolata van, telepítse az ESET-terméket egy online telepítő segítségével.

Az offline telepítő (.exe) elindítása után a Telepítővarázsló végigvezeti Önt a telepítési folyamaton.



1. Válassza ki a megfelelő nyelvet a legördülő menüből, majd kattintson a **Folytatás** gombra.

Ha újabb verziót telepít egy korábbi verzióra jelszóval védett beállításokkal, írja be a jelszavát. A beállítások jelszavát az Hozzáférési beállítások lapon konfigurálhatja.

2. Válassza ki a következő funkciók beállításait, olvassa el a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot, majd a **Folytatás** vagy **Az összes engedélyezése és folytatás** gombra kattintva engedélyezze az összes funkciót:

- ESET LiveGrid® visszajelzési rendszer
- Kéretlen alkalmazások
- Felhasználói élmény javítását célzó program

> A **Folytatás** vagy **Az összes engedélyezése és folytatás** gombra kattintva elfogadja a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot.

3. Kattintson a **Bejelentkezés kihagyása** gombra. Ha rendelkezik internetkapcsolattal, csatlakoztathatja eszközét a ESET HOME-fiókjához.

4. Kattintson az **Aktiválás kihagyása** gombra. Az ESET Internet Security szolgáltatást aktiválni kell a telepítés után, hogy teljesen működőképes legyen. A termék aktiválásához aktív internetkapcsolat szükséges.

5. A Telepítővarázsló megmutatja, hogy melyik ESET-termék lesz telepítve a letöltött offline telepítő alapján. Kattintson a **Folytatás** gombra a telepítési folyamat elindításához. Ez néhány percet igénybe vehet.

> Ha a múltban eltávolított ESET-termékekből vannak még maradványok (fájlok vagy mappák), akkor a rendszer megkéri, hogy engedélyezze az eltávolításukat. Kattintson a **Telepítés** gombra a folytatáshoz.

6. Kattintson a **Kész** gombra a Telepítővarázslóból való kilépéshez.

Telepítési hibaelhárító.

Licenc aktiválása

A termék számos módon aktiválható. Az aktiválási ablakban elérhető adott aktiválási lehetőség függ az országtól, valamint attól, hogy a telepítőfájl milyen formában érhető el (CD/DVD, ESET weboldala stb.).

- Ha kiskereskedelmi forgalomban kapható dobozos változatot vásárolt, vagy egy e-mailt kapott a licenc adataival, aktiválja a terméket a **Licenckulcs megadása** elemre kattintva. A licenckulcs a termék dobozában, online vásárlás esetén a kapott e-mailben található. A sikeres aktiváláshoz pontosan kell megadni a licenckulcsot. Licenckulcs – A licenctulajdonos azonosítására és a licenc aktiválására szolgáló egyedi, XXXX-XXXX-XXXX-XXXX-XXXX vagy XXXX-XXXXXXXX formátumú karakterlánc.

- Miután kiválasztotta A ESET HOME-fiók használata lehetőséget, felszólítást kap a ESET HOME fiókba való bejelentkezésre.

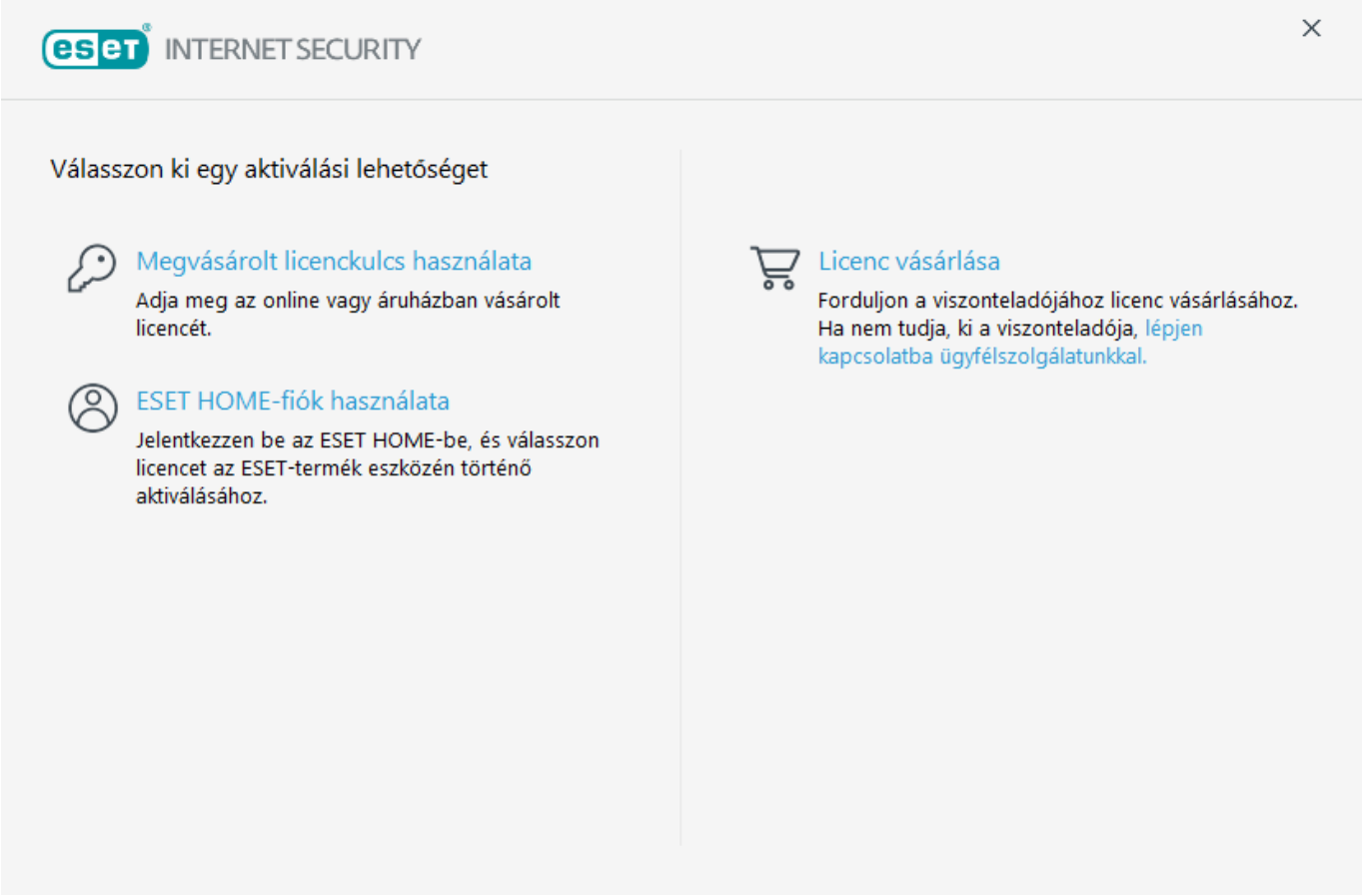
- Ha vásárlás előtt ki szeretné próbálni az ESET Internet Security programot, jelölje be az Ingyenes próbaverzió választógombot. Az ESET Internet Security korlátozott idejű használatát lehetővé tévő aktiváláshoz adja meg e-mail címét és tartózkodási helyének országát. A próbaverzióhoz tartozó licencet e-mailben küldjük el Önnek. Minden kliens csak egyszer aktiválhatja a próbaverzió licencét.

- Ha még nincs licence, és szeretne vásárolni egyet, kattintson a **Licenc vásárlása gombra**. A program ekkor átirányítja az ESET helyi forgalmazójának a weboldalára. Az ESET Windows otthoni termékekhez használható teljes licencek nem ingyenesek.

A terméklicenc bármikor módosítható. Ehhez kattintson a **Súgó és támogatás** > **Licenc módosítása** elemre a fő programablakban. Ekkor megjelenik az ESET terméktámogatásának megadandó, a licenc azonosítására szolgáló nyilvános licencazonosító.

Ha van régebbi ESET-termékek aktiválásához használt felhasználóneve és jelszava, és nem tudja, hogyan kell aktiválni az ESET Internet Security terméket, konvertálja régi hitelesítő adatait licenckulcsra.

Nem sikerült a termékaktiválás?



A licenckulcs megadása az aktiválás során

Az automatikus frissítések fontosak a biztonság szempontjából. Az ESET Internet Security csak akkor kapja meg a frissítéseket, ha aktiválva lett.

A **Licenckulcs** megadásakor fontos, hogy pontosan írja be azt:

- A licenckulcs a licenctulajdonos azonosítására és a licenc aktiválására szolgáló egyedi, XXXX-XXXX-XXXX-XXXX-XXXX formátumú karakterlánc.

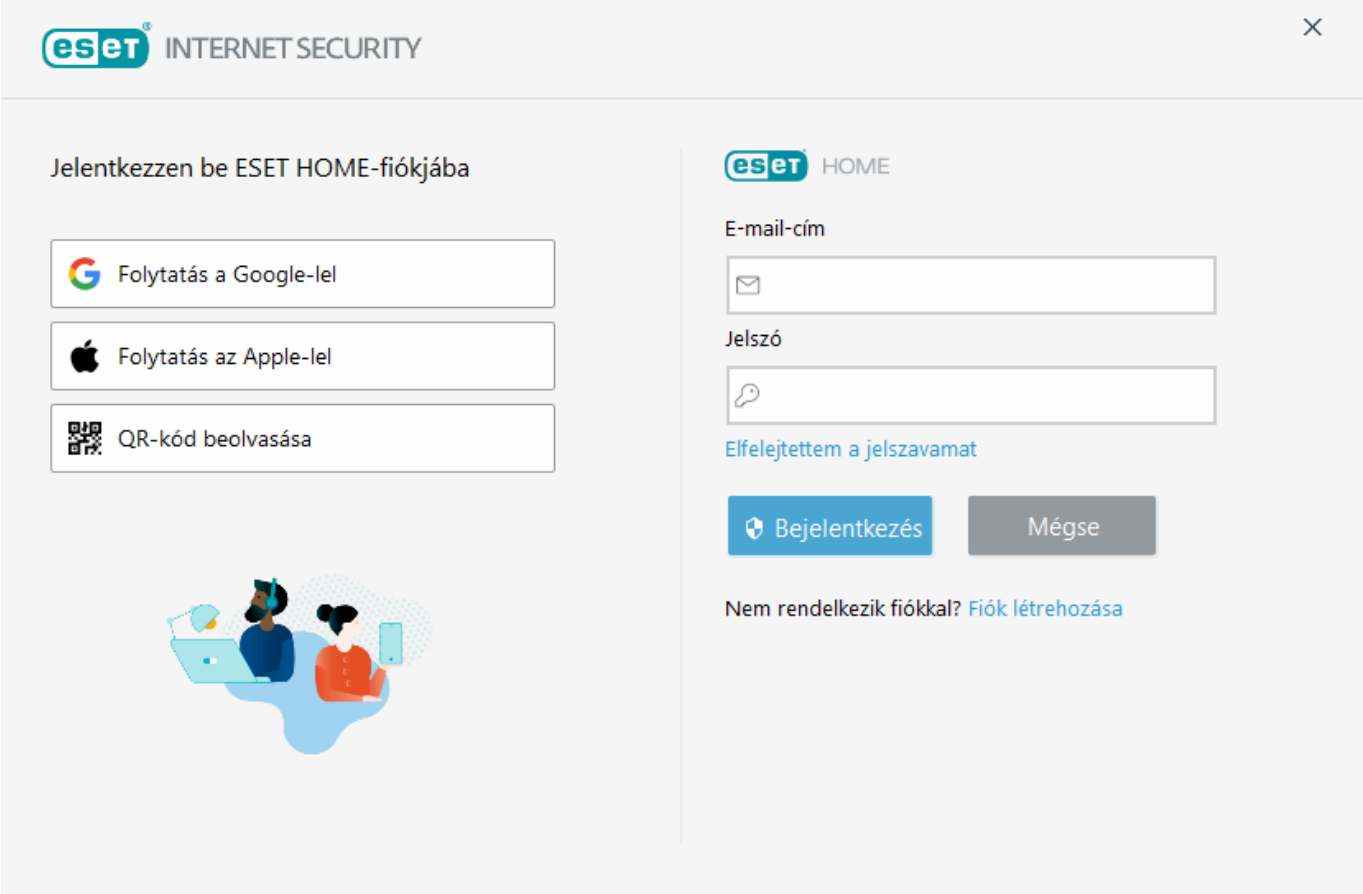
A pontosság érdekében javasoljuk, hogy az Önnek küldött regisztrációs e-mailből másolja és illessze be az adatokat.

Ha nem adta meg a licenckulcsot a telepítés után, a termék aktiválása nem történik meg. Az ESET Internet Security a fő programablak > **Súgó és támogatás** > **Licenc aktiválása** lapon aktiválható.

Az ESET Windows otthoni termékekhez használható teljes licencek nem ingyenesek.

A ESET HOME-fiók használata

Csatlakoztassa az eszközét a ESET HOME szolgáltatáshoz, ahol megtekintheti és kezelheti az összes aktivált ESET-licencet és eszközt. Megújíthatja, frissítheti vagy bővítheti licencét, és megtekintheti a fontos licencadatokat. A ESET HOME felügyeleti portálon vagy a mobilalkalmazásban szerkesztheti az Anti-Theft beállításait, különböző licenceket adhat hozzá, letölthet termékeket az eszközeire, ellenőrizheti a termékek biztonsági állapotát, illetve megoszthatja a licenceket e-mailben. További információkért látogasson el a ESET HOME online súgóoldalaira.



Miután kiválasztotta a **ESET HOME-fiók használata** aktiválási módszert, vagy amikor a ESET HOME-fiókhoz csatlakozik a telepítés során:

1. Jelentkezzen be az ESET HOME-fiókjába.

> Ha nincs ESET HOME-fiókja, kattintson a **Fiók létrehozása** gombra a regisztrációhoz, vagy tekintse meg az instrukciókat a ESET HOME online súgóban.
> Ha elfelejtette a jelszavát, kattintson az **Elfelejtettem a jelszavamat** szövegre, és kövesse a képernyőn látható lépéseket, vagy tekintse meg a ESET HOME online súgót.

2. Állítsa be annak az **eszköznek a nevét**, amelyet az összes ESET HOME-szolgáltatásban használni fog, majd kattintson a **Folytatás** gombra.

3. Válasszon ki egy licencet az aktiváláshoz, vagy adjon hozzá új licencet. Kattintson a **Folytatás** gombra az ESET Internet Security aktiválásához.

Aktiválás próba üzemmódban

Az ESET Internet Security próbaverziójának aktiválásához adja meg az érvényes e-mail-címét az **E-mail-cím** és az **E-mail-cím megerősítése** mezőben. Az aktiválást követően létrehozzuk és elküldjük a megadott e-mail-címre az ESET-licencet. Erre az e-mail-címre fogjuk küldeni a termék lejáratára vonatkozó értesítéseket, valamint az ESET általi egyéb tájékoztatásokat is. A próbaverzió csak egyszer aktiválható.

Az **Ország** legördülő listában jelölje ki a tartózkodási helyének megfelelő országot, hogy az ESET Internet Security terméket a helyi forgalmazónál regisztrálhassa, és igénybe vehesse a helyi terméktámogatást.

Ingyenes ESET-licenckulcs

Az ESET Internet Security teljes licence nem ingyenes.

Az ESET-licenckulcs betűk és számok egyedi sorozata, amelyet az ESET biztosít annak érdekében, hogy az ESET Internet Security legálisan használható legyen a Végfelhasználói licencszerződéssel összhangban. Minden Végfelhasználó csak abban a mértékben jogosult használni a Licenckulcsot, amennyi joga van használni az ESET Internet Security terméket az ESET által biztosított licencek számának alapján. A Licenckulcs bizalmas jellegű, és nem osztható meg. Megoszthatók azonban a licencegységek a ESET HOME segítségével.

Vannak olyan források az interneten, ahol esetlegesen hozzá lehet jutni „ingyenes” ESET-licenckulcsokhoz, de vegye figyelembe:

- Ha rákattint egy „Ingyenes ESET-licenckulcs” feliratú hirdetésre, akkor előfordulhat, hogy illetéktelenül hozzáférnek a számítógépéhez vagy eszközéhez, és kártevővel fertőzik meg. Kártevő rejtőzhet a nem hivatalos webes anyagokban (például videókban), olyan webhelyeken, ahol azt hirdetik, hogy a felhasználó pénzt kereshet a webhely meglátogatásával stb. Rendszerint ezek mind csapdák.
- Az ESET le tudja tiltani a kalózlicenceket, és ezt meg is teszi.
- A kalózlicenckulcs használata nem áll összhangban a Végfelhasználói licencszerződéssel, amelyet el kell fogadnia az ESET Internet Security telepítéséhez.
- Kizárólag hivatalos csatornákon keresztül vásároljon ESET-licencet, például a www.eset.com webhelyen, illetve ESET-forgalmazóktól vagy -viszonteladóktól (ne vásároljon licencet nem hivatalos, külső fél által működtetett webhelyen – például eBay –, illetve megosztott licencet külső féltől).
- Az ESET Internet Security ingyenesen letölthető, viszont érvényes ESET-licenckulcs szükséges a telepítés során történő aktiválásához (letöltheti és telepítheti, de aktiválás nélkül nem fog működni).
- Ne ossza meg licencét az interneten és közösségi oldalakon (továbbadhatják).

Tudásbáziscikkünk ismerteti, hogyan ismerhetők fel az ESET-kalózlicencek, és hogyan tehet róluk bejelentést.

Ha bizonytalan abban, hogy megvásároljon-e egy ESET biztonsági terméket, használhatja a próbaverzióját is egy ideig:

1. Aktiválja az ESET Internet Security terméket egy ingyenes próbaverzió-licenccel

2. Vegyen részt az ESET BÉTA Programban

3. Telepítse az ESET Mobile Security terméket (freemium), ha androidos mobileszközt használ.

Engedményért/a licenc meghosszabbításához:

- Ajánlja az ESET Internet Security terméket ismerősének
- Újítsa meg az ESET-licencet (ha rendelkezett aktív licenccel), vagy aktiválja hosszabb időre

Az aktiválás nem sikerült – gyakori forgatókönyvek

Ha nem sikerül az ESET Internet Security aktiválása, a leggyakoribb forgatókönyvek a következők:

- A licenckulcs már használatban van
- Érvénytelen licenckulcs. Hiba történt a licencaktiválási űrlappal kapcsolatosan
- Az aktiváláshoz szükséges kiegészítő adatok hiányoznak vagy nem érvényesek.
- Nem sikerült a kommunikáció az aktiválási adatbázissal. Próbálkozzon újból 15 perc múlva.
- Nincs vagy letiltott kapcsolat az ESET aktiválási szervereivel

Ellenőrizze, hogy a megfelelő licenckulcsot adta-e meg, majd próbálkozzon újra az aktiválással. Ha a ESET HOME-fiókot használja az aktiváláshoz, tekintse meg a ESET HOME Licenckezelés - Online súgót.

Ha nem sikerül az aktiválás, az ESET aktiválási hibaelhárító segítséget nyújt az aktiválással és licenceléssel kapcsolatos gyakori kérdésekhez, hibákhoz és problémákhoz (angolul és néhány egyéb nyelven áll rendelkezésre).

Az aktiválás nem sikerült túlhasznált licenc miatt

Hiba

- Lehet, hogy túlhasznált a licenc, vagy visszaéltek vele
- Az aktiválás nem sikerült túlhasznált licenc miatt

Megoldás

Több eszköz használja a licencet, mint amennyit megenged. Ön szoftverkalózkodás vagy hamisítás áldozata lehet. A licenc nem használható más ESET-termék aktiválására. A problémát közvetlenül akkor oldhatja meg, ha a ESET HOME-fiókjában kezelni tudja a licencet, vagy ha törvényes forrásból vásárolta a licencet. Ha még nem rendelkezik fiókkal, hozzon létre egyet.

Ha Ön a licenc tulajdonosa, és nem kapott felszólítást e-mail címének megadására:

1. Az ESET-licenc kezeléséhez nyissa meg a webböngészőjét, majd lépjen a https://home.eset.com oldalra. Lépjen az ESET License Managerbe, és távolítson el vagy deaktiválja egységeket. További információkért tekintse meg a Mi a teendő túlhasznált licenc esetén? című részt.

2. Az ESET-kalózlicencek felismeréséről és bejelentéséről szóló cikkünkben megtudhatja hogyan azonosíthatók be és jelenthetők be az ESET-kalózlicencek.

3. Ha nem biztos benne, kattintson a **Vissza** gombra, és küldjön e-mailt az ESET műszaki támogatási szolgálatának.

Ha nem Ön a licenctulajdonos, tájékoztassa a licenc tulajdonosát, hogy nem tudja aktiválni az ESET-terméket, mert túl sok eszköz használja a licencet. A tulajdonos a ESET HOME portálon tudja elhárítani a problémát.

Ha felszólítást kapott az e-mail-címe megerősítésére (csak néhány esetben), adja meg az ESET Internet Security megvásárlásához vagy aktiválásához használt e-mail-címet.

A licenc frissítése

Ez az értesítési ablak akkor jelenik meg, ha az ESET-termék aktiválásához használt licenc megváltozott. A megváltozott licenc segítségével egy több biztonsági funkcióval rendelkező terméket aktiválhat. Ha nem történt változtatás, az ESET Internet Security egyszer megjeleníti a **Váltás egy több funkcióval rendelkező termékre** riasztási ablakot.

Igen (ajánlott) – Automatikus végbemegy a több biztonsági funkcióval rendelkező termék telepítése.

Nem, köszönöm – Nincs változtatás, és az értesítés véglegesen eltűnik.

A termék későbbi módosításához tekintse meg ESET-tudásbáziscikkünket. Az ESET licenceiről további információkat a Licencelés – GYIK című témakörben talál.

Az alábbi táblázat felsorolja az egyes termékekben rendelkezésre álló funkciókat.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Keresőmotor	✔	✔	✔
Speciális gépi tanulás	✔	✔	✔
Exploit blokkoló	✔	✔	✔
Szkript-alapú támadások elleni védelem	✔	✔	✔
Adathalászat elleni védelem	✔	✔	✔
Webhozzáférés-védelem	✔	✔	✔
Behatolásmegelőző rendszer (Zsarolóprogram elleni védelem is)	✔	✔	✔
Levélszemétszűrő		✔	✔
Tűzfal		✔	✔
Hálózatfelügyelet		✔	✔
Webkamera-védelem		✔	✔
Hálózati támadások elleni védelem		✔	✔
Botnet elleni védelem		✔	✔
Netbank- és tranzakcióvédelem		✔	✔
Szülői felügyelet		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Lopásvédelem		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

A termék frissítése

Letöltött egy alapértelmezett telepítőt, és úgy döntött, hogy módosítja az aktiválandó terméket, vagy le szeretné váltani a telepített terméket egy több biztonsági funkcióval rendelkező termékre.

A termék módosítása a telepítés során.

Az alábbi táblázat felsorolja az egyes termékekben rendelkezésre álló funkciókat.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Keresőmotor	✔	✔	✔
Speciális gépi tanulás	✔	✔	✔
Exploit blokkoló	✔	✔	✔
Szkript-alapú támadások elleni védelem	✔	✔	✔
Adathalászat elleni védelem	✔	✔	✔
Webhozzáférés-védelem	✔	✔	✔
Behatolásmegelőző rendszer (Zsarolóprogram elleni védelem is)	✔	✔	✔
Levélszemétszűrő		✔	✔
Tűzfal		✔	✔
Hálózatfelügyelet		✔	✔
Webkamera-védelem		✔	✔
Hálózati támadások elleni védelem		✔	✔
Botnet elleni védelem		✔	✔
Netbank- és tranzakcióvédelem		✔	✔
Szülői felügyelet		✔	✔
Lopásvédelem		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

A licenc visszaléptetése

Ez a párbeszédpanel akkor jelenik meg, ha az ESET-termék aktiválásához használt licenc megváltozott. A megváltozott licenc csak egy másik, kevesebb biztonsági funkcióval rendelkező ESET-termékhez használható. A termék automatikusan megváltozott, hogy ne szűnjön meg a védelem.

Az ESET licenceiről további információkat a Licencelés – GYIK című témakörben talál.

Az alábbi táblázat felsorolja az egyes termékekben rendelkezésre álló funkciókat.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Keresőmotor	✔	✔	✔
Speciális gépi tanulás	✔	✔	✔
Exploit blokkoló	✔	✔	✔
Szkript-alapú támadások elleni védelem	✔	✔	✔
Adathalászat elleni védelem	✔	✔	✔
Webhozzáférés-védelem	✔	✔	✔
Behatolásmegelőző rendszer (Zsarolóprogram elleni védelem is)	✔	✔	✔
Levélszemétszűrő		✔	✔
Tűzfal		✔	✔
Hálózatfelügyelet		✔	✔
Webkamera-védelem		✔	✔
Hálózati támadások elleni védelem		✔	✔
Botnet elleni védelem		✔	✔
Netbank- és tranzakcióvédelem		✔	✔
Szülői felügyelet		✔	✔
Lopásvédelem		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

A termék visszaléptetése

A jelenleg telepített termék több biztonsági funkcióval rendelkezik, mint az aktiválni kívánt termék. A lopásvédelmi funkció nem fog működni, így nem fog hozzáférni a kapcsolódó adatokhoz a ESET HOME szolgáltatásban.

Az alábbi táblázat felsorolja az egyes termékekben rendelkezésre álló funkciókat.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Keresőmotor	✔	✔	✔
Speciális gépi tanulás	✔	✔	✔
Exploit blokkoló	✔	✔	✔
Szkript-alapú támadások elleni védelem	✔	✔	✔
Adathalászat elleni védelem	✔	✔	✔
Webhozzáférés-védelem	✔	✔	✔
Behatolásmegelőző rendszer (Zsarolóprogram elleni védelem is)	✔	✔	✔
Levélszemétszűrő		✔	✔
Tűzfal		✔	✔
Hálózatfelügyelet		✔	✔
Webkamera-védelem		✔	✔
Hálózati támadások elleni védelem		✔	✔
Botnet elleni védelem		✔	✔
Netbank- és tranzakcióvédelem		✔	✔
Szülői felügyelet		✔	✔
Lopásvédelem		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Telepítési hibaelhárító

Ha a telepítés során problémák merülnek fel, a Telepítő varázsló egy hibaelhárítót biztosít, amely lehetőség szerint elhárítja a problémát.

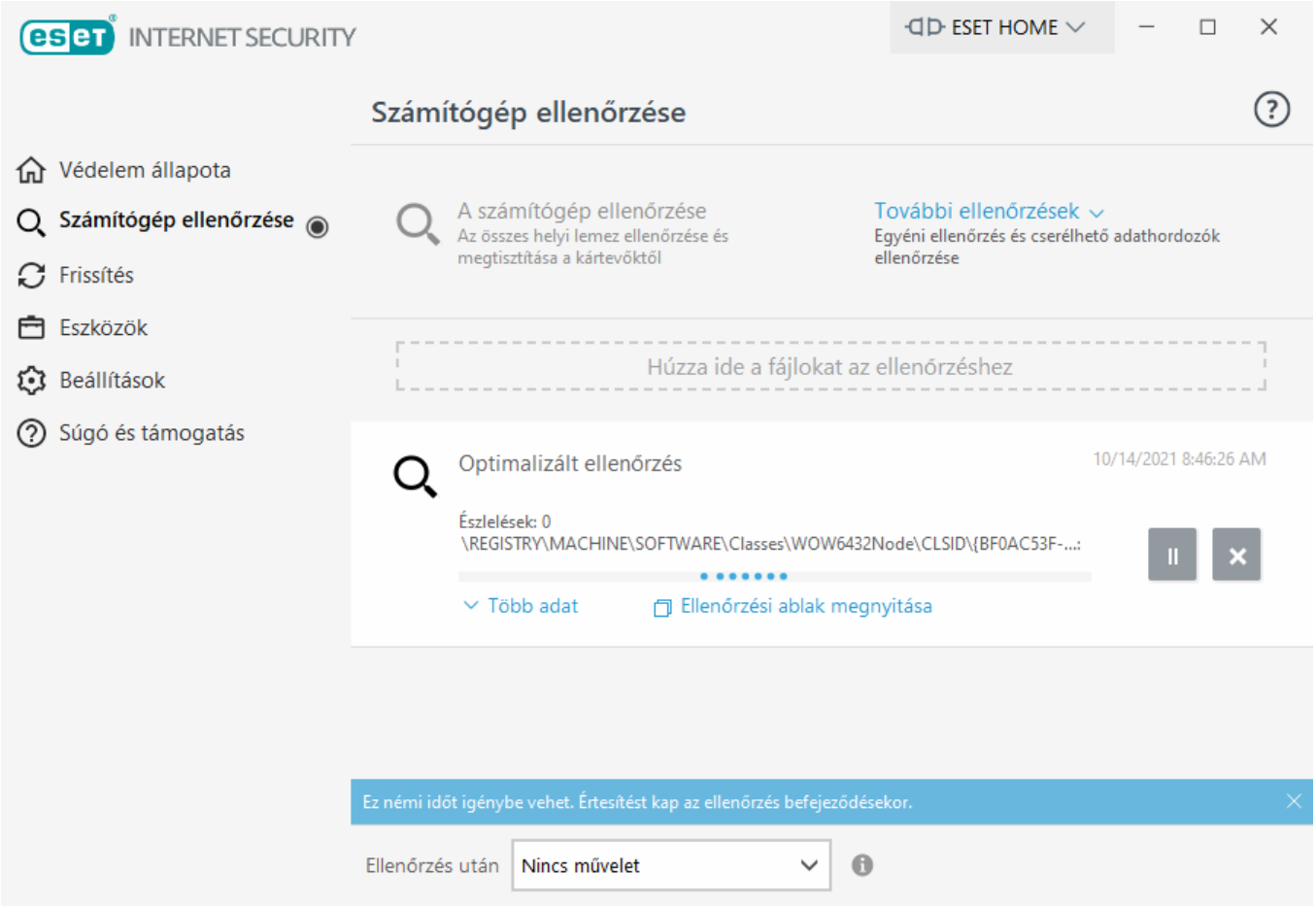
Kattintson a **Hibaelhárító futtatása** szövegre. Amikor a hibaelhárító befejezte a műveleteket, kövesse az ajánlott megoldást.

Ha a probléma továbbra is fennáll, tekintse meg a gyakori telepítési hibák és megoldások listáját.

Első ellenőrzés a telepítés után

Az ESET Internet Security telepítését követően, az első sikeres frissítés után az alkalmazás automatikusan ellenőrzi a számítógépet, hogy nem tartalmaz-e kártékony kódot.

A **Számítógép ellenőrzése** > **Optimalizált ellenőrzés** elemre kattintva a program főablakából kézzel is elindíthatja a számítógép ellenőrzését. A számítógép ellenőrzéséről a Számítógép ellenőrzése című témakörben részletesebben olvashat.



Frissítés egy újabb verzióra

Az ESET Internet Security új verziói továbbfejlesztett funkciókat tartalmaznak, és a programmodulok automatikus frissítésével nem megszüntethető problémákat orvosolnak. Többféleképpen lehet frissíteni egy újabb verzióra:

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 közvetlenül a kibocsátását követően újabb verzióra kell frissíteni, használja az alábbi módszerek egyikét.
Engedélyezze az **Alkalmazásfunkciók frissítése** funkciót a **További beállítások** (F5) > **Frissítés** > **Profilok** > **Frissítések** lapon.

2. Manuálisan a fő programablak **Frissítés** szakaszában a **Frissítések keresése** elemre kattintva.

3. Manuálisan, egy újabb verzió letöltésével és telepítésével (az előző verzióra).

További információkért és ábrákkal ellátott útmutatókért tekintse meg a következőket:

- Az ESET-termékek frissítése – a legújabb termékmodulok ellenőrzése
- Mik a különböző ESET-termékfrissítések és kiadási típusok?

Régi termék automatikus frissítése

Az ESET-termék Ön által használt verziója már nem támogatott, ezért frissítettük a legújabb verzióra.

A telepítéssel kapcsolatos általános problémák

Az ESET-termékek minden új verziója számos hibajavítást és fejlesztést tartalmaz. Azok a meglévő ügyfeleink, akik érvényes licenccel rendelkeznek az egyik ESET-termékhez, ingyenesen frissíthetnek az adott termék legújabb verziójára.

A telepítés befejezése:

1. Az **Elfogadás és folytatás** gombra kattintva fogadja el a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot. Ha nem fogadja el a Végfelhasználói licencszerződést, kattintson az **Eltávolítás** gombra. Nincs lehetőség az előző verzióra való visszatérésre.

2. **Az összes engedélyezése és folytatás** gombra kattintva engedélyezze az ESET LiveGrid® visszajelzési rendszert és a Felhasználói élmény javítását célzó programot, vagy kattintson a **Folytatás** gombra, ha nem szeretne részt venni benne.

3. Miután aktiválta az új ESET-terméket a licenckulccsal, megjelenik a kezdőoldal. Ha a licencadatok nem találhatók, folytassa a próbaverzió-licenccel. Ha az előző termékben használt licence nem érvényes, aktiválja az ESET-terméket.

4. A telepítés befejezéséhez újra kell indítani az eszközt.

ESET-termék ajánlása ismerősnek

Ez az ESET Internet Security-verzió ajánlási bónuszokat kínál, így lehetőséget adhat családjának és ismerőseinek, hogy kipróbáljanak egy ESET-terméket. Próbalicenccel aktivált termékből is küldhet ajánlást. Ha egy adott ajánlás termékaktiválást eredményez, akkor Ön és az ismerőse egy havi teljes védelmet kap ajándékba a próbalicenchez.

A telepített ESET Internet Security segítségével ajánlhat terméket. Attól függ, hogy milyen terméket ajánlhat, hogy melyik termékből adja le az ajánlást – lásd az alábbi táblázatot.

Telepített termék	Ajánlható termék
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Termék ajánlása

Ajánlási hivatkozás küldéséhez kattintson az **Ajánlás ismerősnek** elemre az ESET Internet Security főmenüjében. Kattintson az **Ajánlási hivatkozás megosztása** elemre. A termék ekkor generál egy ajánlási linket, amely egy új ablakban jelenik meg. Másolja át és küldje el a családjának és az ismerőseinek. Közvetlenül az ESET-termékből megoszthatja az ajánlási linket a **Megosztás a Facebookon**, az **Ajánlja gmailes ismerőseinek** és a **Megosztás a Twitteren** funkciók segítségével.

Ha ismerőse rákattint az Öntől kapott ajánlási linkre, akkor a rendszer átirányítja egy weboldalra, ahol letöltheti a

terméket, és INGYENESEN egy hónapos védelmet kap. Ön mint a próbaverzió felhasználója értesítést kap minden sikeresen aktivált ajánlási linkről, és a licenc automatikusan meghosszabbodik egy hónappal INGYENESEN. Ilyen módon akár 5 hónappal INGYENESEN meghosszabbíthatja a védelmet. Az ESET-termék **Ajánlás ismerősnek** ablakában megnézheti, hogy hány ajánlási linket aktiváltak sikeresen.

Előfordulhat, hogy az ajánlási funkció nem érhető el az Ön nyelvén/régiójában.

ESET Internet Security lesz telepítve

Ez a párbeszédablak a következő helyzetekben jelenhet meg:

- A telepítési folyamat során – Az ESET Internet Security telepítésének folytatásához kattintson a **Folytatás** gombra.
- Licenc módosításakor az ESET Internet Security szolgáltatásban – Kattintson az **Aktiválás** gombra a licenc módosításához és az ESET Internet Security aktiválásához.

A **Termékváltás** funkcióval válthat az ESET Windows otthoni termékek között az ESET-licencének megfelelően. További információkért tekintse meg a Melyik termékkel rendelkezem? című részt.

Váltson másik terméktípusra

ESET-licencének megfelelően válthat a különböző ESET Windows otthoni termékek között. További információkért tekintse meg a Melyik termékkel rendelkezem? című részt.

Regisztráció

Kérjük, hogy a regisztrációs űrlapon található mezőket kitöltve regisztrálja a licencét, és kattintson az Aktiválás gombra. A zárójelben kötelezőként megjelölt mezőket ki kell tölteni. Ez az információ csak az ESET licencéhez kapcsolódó műveletekhez használatos.

Aktiválási folyamat

Az aktiválási folyamat végrehajtása néhány másodpercet vesz igénybe (a szükséges idő változhat az internetkapcsolat sebességétől és számítógépétől függően).

Az aktiválás sikerült

Az aktiválási folyamat kész. Kövesse a telepítés utáni varázsló utasításait az ESET Internet Security beállításának befejezéséhez.

A modulfrissítés néhány másodpercen belül megtörténik. Az ESET Internet Security rendszeres frissítései azonnal elindulnak.

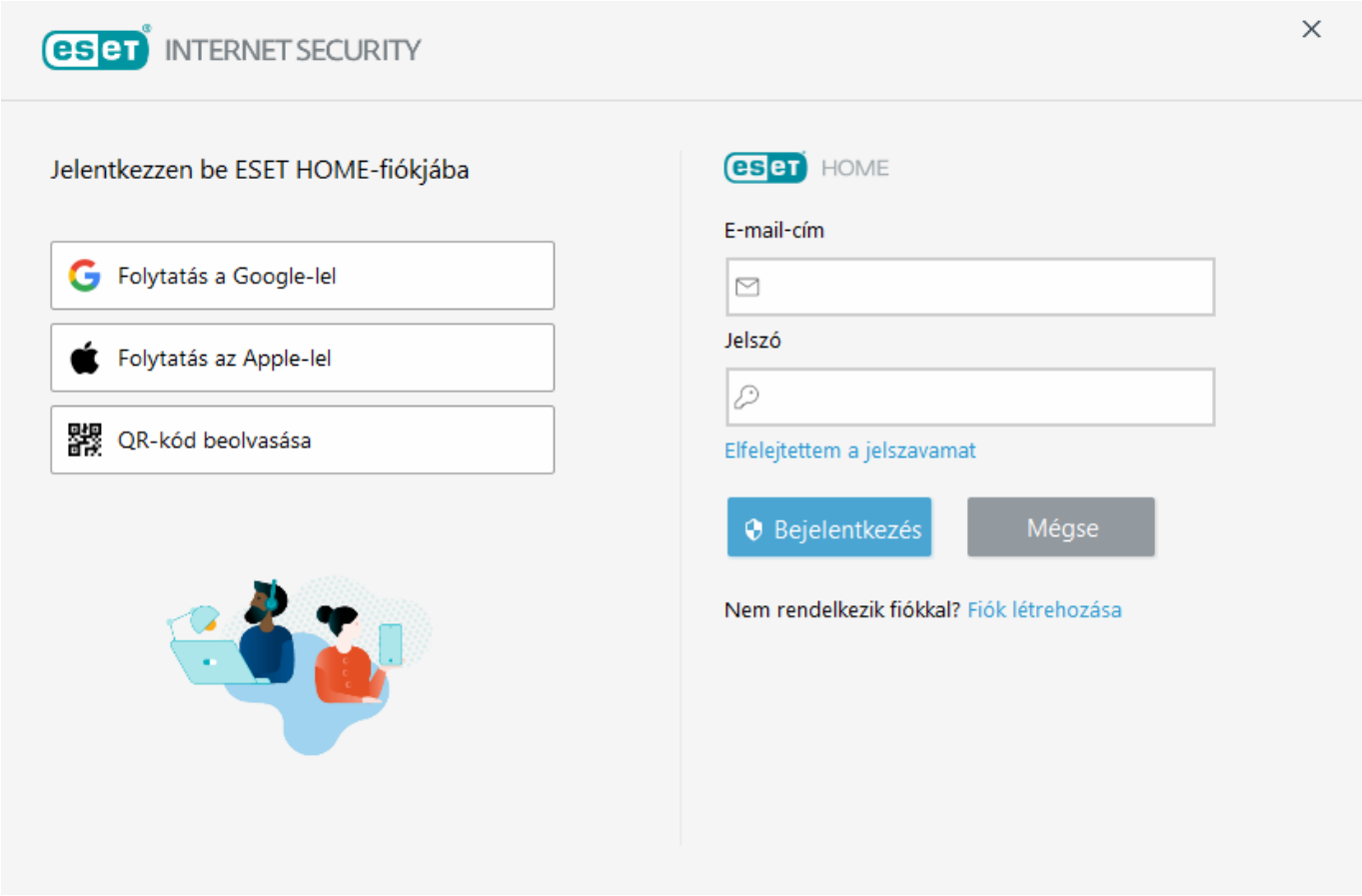
A modulfrissítést után 20 perccel automatikusan elindul az első ellenőrzés.

Útmutató kezdő felhasználók számára

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

Csatlakozzon a ESET HOME szolgáltatáshoz

Csatlakoztassa az eszközét a ESET HOME szolgáltatáshoz, ahol megtekintheti és kezelheti az összes aktivált ESET-licencet és eszközt. Megújíthatja, frissítheti vagy bővítheti licencét, és megtekintheti a fontos licencadatokat. A ESET HOME felügyeleti portálon vagy a mobilalkalmazásban szerkesztheti az Anti-Theft beállításait, különböző licenceket adhat hozzá, letölthet termékeket az eszközeire, ellenőrizheti a termékek biztonsági állapotát, illetve megoszthatja a licenceket e-mailben. További információkért látogasson el a ESET HOME online súgóoldalaira.



Csatlakoztassa eszközét az ESET HOME hoz:

> Ha telepítés során csatlakozik a ESET HOME szolgáltatáshoz, vagy amikor a **ESET HOME-fiók használata** aktiválási módszert választja, kövesse A ESET HOME-fiók használata témakörben ismertetett lépéseket. Ha az ESET Internet Security már telepítve és aktiválva van a ESET HOME-fiókjához hozzáadott licenccel, akkor csatlakoztathatja az eszközét a ESET HOME-fiókhoz a ESET HOME portál segítségével. Kövesse az ESET HOMEonline súgó instrukcióit, és engedélyezze a kapcsolatot az ESET Internet Security szolgáltatásban.

1. A fő programablakban kattintson a **ESET HOME** > **Csatlakozás a ESET HOME**-hez elemre, vagy kattintson a **Csatlakozás a ESET HOME**-hez **Az eszköz csatlakoztatása egy ESET HOME-fiókhoz** értesítésben.

2. Jelentkezzen be az ESET HOME-fiókjába.

Ha nincs ESET HOME-fiókja, kattintson a **Fiók létrehozása** gombra a regisztrációhoz, vagy tekintse meg az instrukciókat a ESET HOME online súgóban.
Ha elfelejtette a jelszavát, kattintson az **Elfelejtettem a jelszavamat** szövegre, és kövesse a képernyőn látható lépéseket, vagy tekintse meg a ESET HOME online súgót.

3. Adjon meg egy **eszköznevet**, majd kattintson a **Folytatás** gombra.

4. Sikeres kapcsolódás után megjelenik a részletező ablak. Kattintson a **Kész** gombra.

Bejelentkezés a ESET HOME szolgáltatásba

A ESET HOME fiókjába való bejelentkezéshez számos módszer áll rendelkezésére:

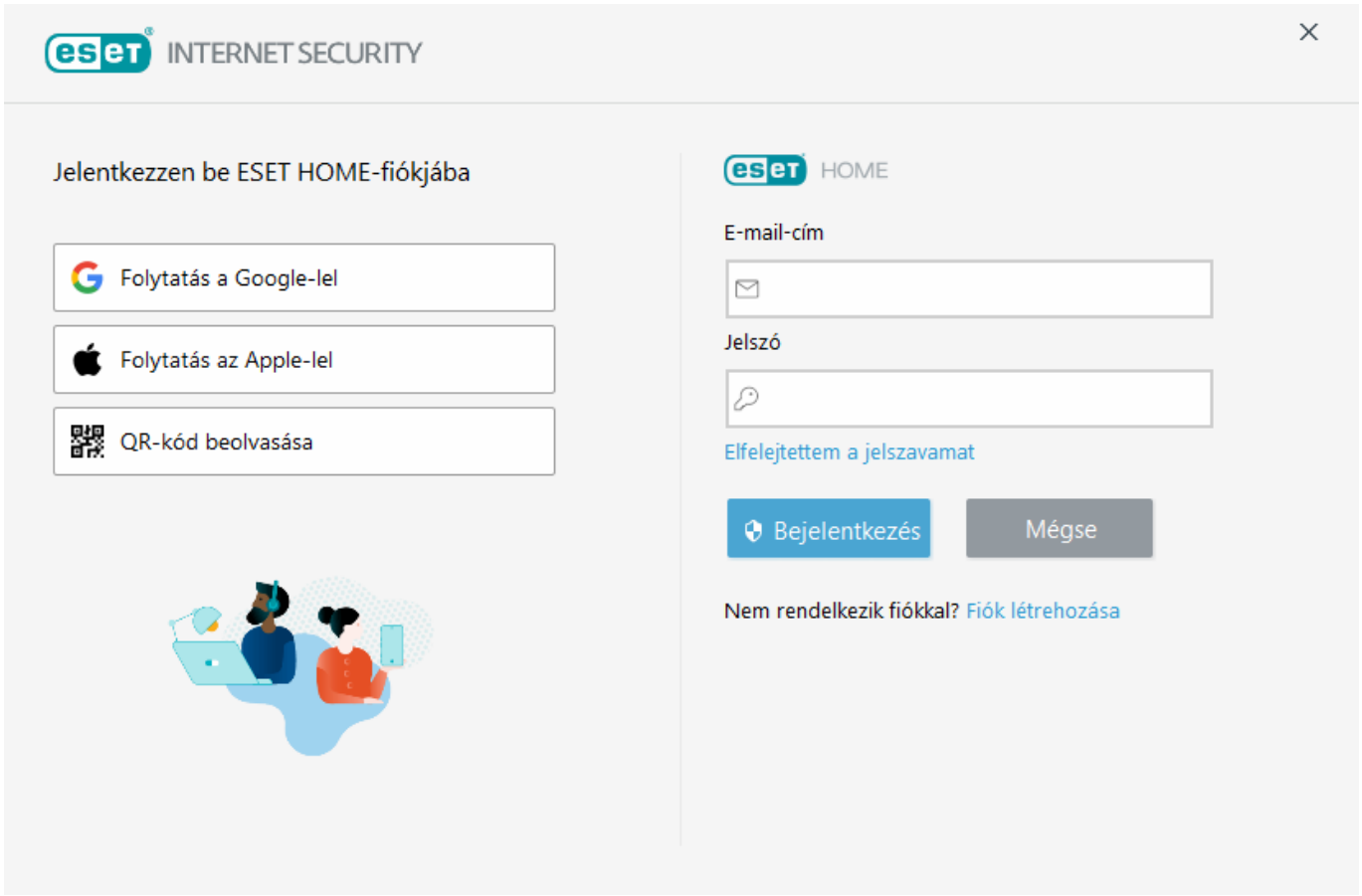
- **A ESET HOME e-mail-cím és jelszó használata** – Írja be a ESET HOME-fiók létrehozásához használt **e-mail-címet** és **jelszót**, majd kattintson a **Bejelentkezés** gombra.

- **Google-fiók/AppleID**-fiók használata – Kattintson a **Folytatás a Google**-lal vagy a **Folytatás az Apple**-lel elemre, és jelentkezzen be a megfelelő fiókba. Sikeres bejelentkezés után a rendszer átirányítja a ESET HOME megerősítő weboldalra. A folytatáshoz váltson vissza az ESET-termékablakra. A Google-fiók/AppleID segítségével történő bejelentkezésről a ESET HOME online súgójában olvashat bővebben.

- **QR-kód beolvasása** – Kattintson a **QR-kód beolvasása** gombra a QR-kód megjelenítéséhez. Nyissa meg a ESET HOME mobilalkalmazást, és olvassa be a QR-kódot, vagy irányítsa a készülék kameráját a QR-kódra. További információkért tekintse meg a ESET HOME online súgóját.

Ha nincs ESET HOME-fiókja, kattintson a **Fiók létrehozása** gombra a regisztrációhoz, vagy tekintse meg az instrukciókat a ESET HOME online súgóban.
Ha elfelejtette a jelszavát, kattintson az **Elfelejtettem a jelszavamat** szövegre, és kövesse a képernyőn látható lépéseket, vagy tekintse meg a ESET HOME online súgót.

Nem sikerült a bejelentkezés – gyakori hibák.



Nem sikerült a bejelentkezés – gyakori hibák

Nem találtunk olyan fiókot, amely megfelel a megadott e-mail-címnek

A megadott e-mail-cím nem egyezik egyetlen ESET HOME-fiókkal sem. Kattintson a **Vissza** gombra, és írja be a helyes e-mail-címet és jelszót.

A bejelentkezéshez létre kell hoznia egy ESET HOME-fiókot. Ha nincs ESET HOME-fiókja, kattintson az **Vissza** > **Fiók létrehozása** elemre, vagy tekintse meg az Új ESET HOME-fiók létrehozása című részt.

A felhasználónév és/vagy a jelszó nem megfelelő

A megadott jelszó nem egyezik a megadott e-mail-címmel. Kattintson a **Vissza** gombra, írja be a helyes jelszót, és ellenőrizze, hogy a megadott e-mail-cím helyes-e. Ha ezután sem tud bejelentkezni, kattintson az **Vissza** > **Elfelejtettem a jelszavam** elemre a jelszó visszaállításához, és kövesse a képernyőn látható lépéseket, vagy nézze meg az Elfelejtettem a ESET HOME-jelszavamat.

A kiválasztott bejelentkezési lehetőség nem egyezik a fiókjával

Fiókja kapcsolódik a közösségi fiókjához. A ESET HOME-fiókjába való bejelentkezéshez kattintson a **Folytatás a Google-lal** vagy a **Folytatás az Apple**-lel gombra, és jelentkezzen be a megfelelő fiókba. Sikeres bejelentkezés után a rendszer átirányítja a ESET HOME megerősítő weboldalra. A közösségi fiókját leválaszthatja a ESET HOME-fiókjáról a ESET HOME portálon.

Érvénytelen jelszó

Ez a hiba akkor fordulhat elő, ha az ESET Internet Security már csatlakoztatva van a ESET HOME-fiókhoz, és olyan módosításokat hajt végre, amelyek szükségessé teszik a bejelentkezést (például az Anti-Theft letiltását), és a megadott jelszó nem egyezik a fiókjával. Kattintson a **Vissza** gombra, és írja be a helyes jelszót. Ha ezután sem tud bejelentkezni, kattintson az **Vissza** > **Elfelejtettem a jelszavam** elemre a jelszó visszaállításához, és kövesse a képernyőn látható lépéseket, vagy nézze meg az Elfelejtettem a ESET HOME-jelszavamat.

Eszköz hozzáadása a ESET HOME szolgáltatásban

Ha az ESET Internet Security már telepítve és aktiválva van a ESET HOME-fiókjához hozzáadott licenccel, akkor csatlakoztathatja az eszközét a ESET HOME-fiókhoz a ESET HOME portál segítségével:

1. Kapcsolódási kérés küldése az eszközre.

2. Az ESET Internet Security megjeleníti **Az eszköz csatlakoztatása egy ESET HOME-fiókhoz** párbeszédablakot a ESET HOME-fiók nevével együtt. Az **Engedélyezés** gombra kattintva csatlakoztassa az eszközt az említett ESET HOME-fiókhoz.

Ha nincs interakció, a kapcsolódási kérés körülbelül 30 perc elteltével automatikusan törlődik.

A program főablaka

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

Ábrákkal ellátott útmutató
Tekintse meg az ESET Windows-termékek fő programablakának megnyitása című témakörben az angol és számos más nyelven elérhető illusztrált instrukciókat.

ESET HOME – Csatlakoztassa az eszközt a ESET HOME-hez. A ESET HOME segítségével megtekintheti és kezelheti az Anti-Theft beállításai és az aktivált ESET-licenceket és eszközöket.

Az alábbi szakaszok a főmenüben található lehetőségeket ismertetik.

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

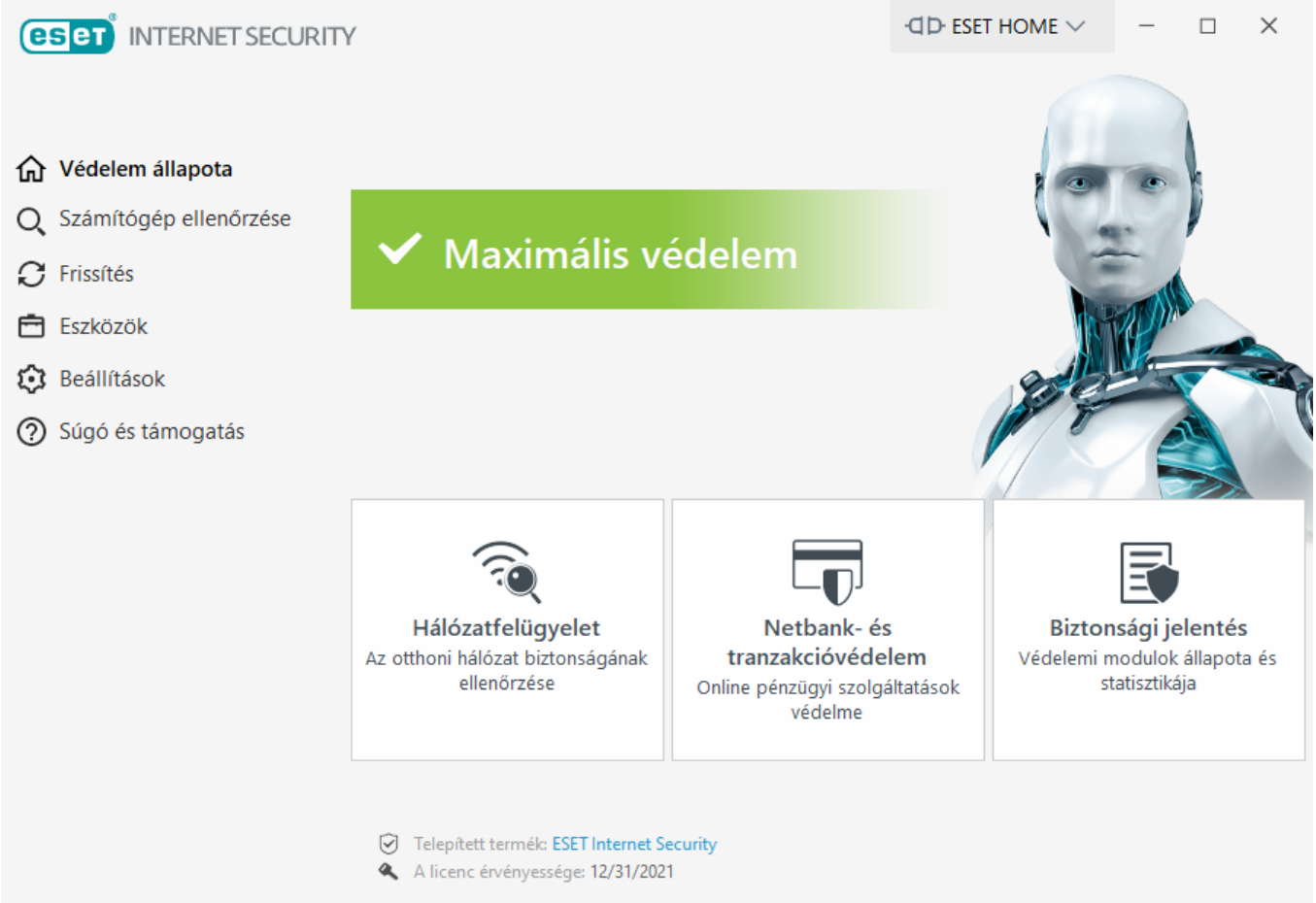
Számítógép ellenőrzése – A számítógép ellenőrzését konfigurálhatja és indíthatja el, vagy egyéni ellenőrzést hozhat létre.

Frissítés – A keresőmotor frissítéseiről jelenít meg információkat.

Eszközök – Hozzáférést biztosít a Hálózatfelügyelet, a Netbank- és tranzakcióvédelem, az Anti-Theft és egyéb modulokhoz, amelyek elősegítik a program adminisztrációjának leegyszerűsítését, és további lehetőségeket kínálnak a tapasztalt felhasználóknak. További információkért tekintse meg a következőt: Eszközök az ESET Internet Security szolgáltatásban.

Beállítások – Itt módosíthatja a biztonsági szintet a következők esetében: számítógép, internet,, hálózatvédelem és biztonsági eszközök.

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

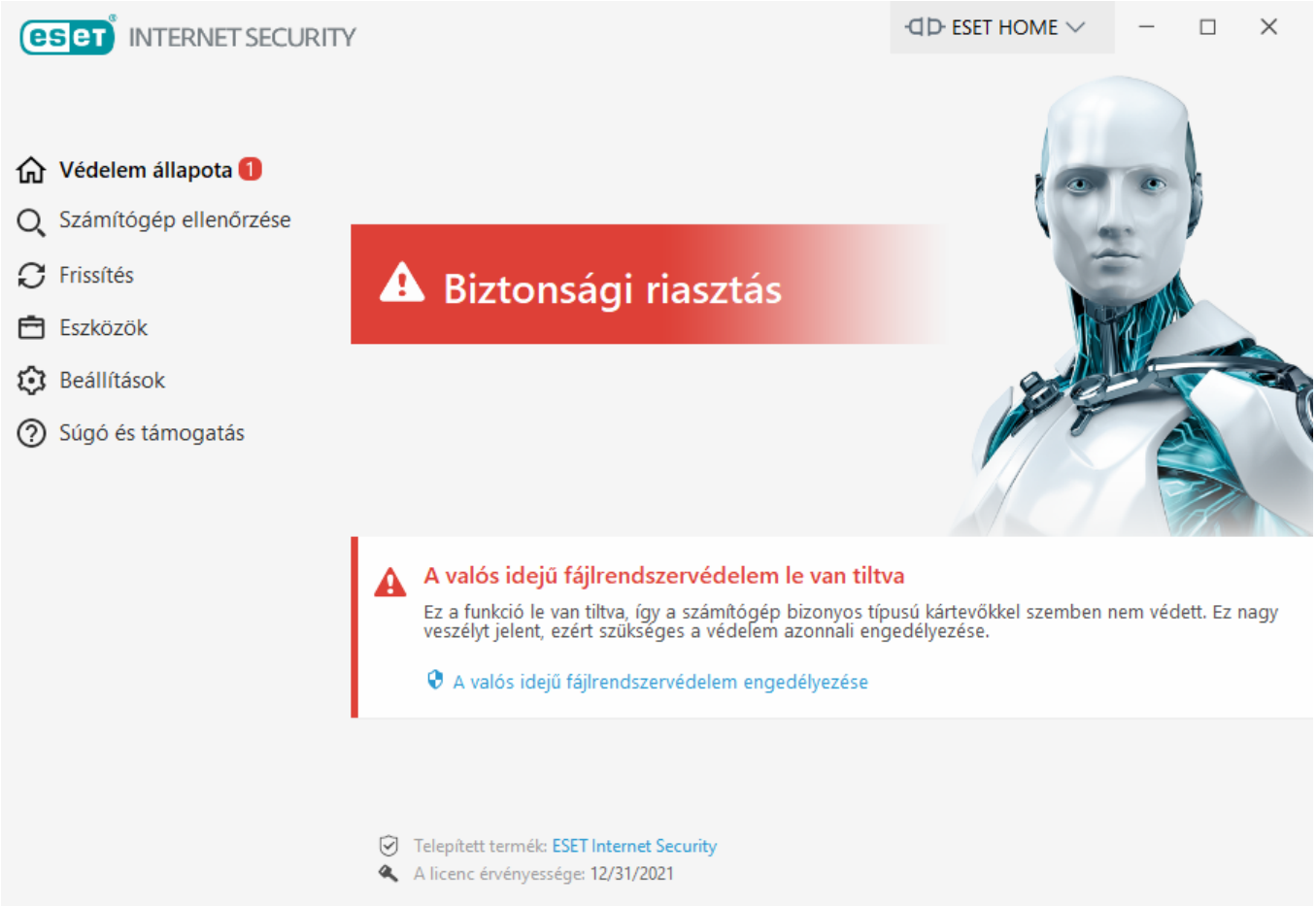


A **Védelem állapota** képernyő a számítógép aktuális védelmi szintjéről nyújt fontos információt. Az állapotablak az ESET Internet Security gyakran használt funkcióit jeleníti meg. És itt láthatók a legújabb frissítés adatai, valamint a program lejárati dátuma is. Kattintson az **ESET Internet Security** elemre, ha az ESET-termék egy másik verzióját szeretné telepíteni. További információk a funkciókról az egyes termékekben találhatók.

A zöld ikon és a zöld színű **A védelme biztosított** állapotüzenet azt jelzi, hogy biztosítva van a lehető legmagasabb szintű védelem.

Teendők, ha a program nem működik megfelelően?

Ha az aktív védelmi modul megfelelően működik, a védelmi állapot ikonja zöld lesz. Vörös felkiáltójel vagy narancssárga értesítő ikon jelzi, ha a számítógép veszélynek van kitéve. Az egyes modulok védelmi állapotára vonatkozó információk, valamint a teljes védelem visszaállítását célzó, ajánlott megoldások a **Védelem állapota** lapon jelennek meg. Az egyes modulok állapotának módosításához kattintson a **Beállítások** gombra, és válassza ki a kívánt modult.



A piros ikon és a piros színű **Biztonsági riasztás** állapotüzenet kritikus problémákat jelez.
Ezt az állapotot többek között például az alábbiak okozhatják:

- **A licenc nincs aktiválva** vagy **A licenc lejárt** – Ezt a védelem állapota ikon vörös színe jelzi. Ettől kezdve a program nem frissül. A licenc megújításához kövesse a riasztási ablakban látható utasításokat.
- **A keresőmotor elavult** – Ez a hiba a keresőmotor frissítésére tett több sikertelen kísérletet követően jelenik meg. Javasoljuk, hogy ellenőrizze a frissítési beállításokat. A hiba leggyakoribb oka a helytelenül megadott hitelesítési adatok, illetve a kapcsolati beállítások nem megfelelő konfigurációja.
- **A valós idejű fájlrendszervédelem le van tiltva** – A felhasználó letiltotta a valós idejű fájlrendszervédelmet. A számítógép nem védett a kártevőkkel szemben. A funkció újbóli engedélyezéséhez kattintson **A valós idejű fájlrendszervédelem engedélyezése** hivatkozásra.
- **A vírus- és kémprogramvédelem le van tiltva** – A vírus- és kémprogramvédelem **A vírus- és kémprogramvédelem engedélyezése** hivatkozásra kattintva engedélyezhető ismét.
- **Az ESET tűzfal le van tiltva** – Ezt a problémát is egy biztonsági értesítés jelzi a **Hálózat** elem mellett az asztalon. A hálózati védelem ismételt engedélyezéséhez kattintson **A tűzfal engedélyezése** hivatkozásra.

A narancssárga ikon a védelem korlátozott voltát jelzi. Ezt okozhatja például, ha probléma történt a program frissítése során, vagy a licenc a közeljövőben lejár.
Ezt az állapotot többek között például az alábbiak okozhatják:

- **Lopásvédelem optimalizálása** – Ez az eszköz nincs az Lopásvédelem szolgáltatáshoz optimalizálva. Ennek oka lehet például, ha a számítógépen nincs létrehozva fantomfiók (ez egy, az eszköz eltűntként való megjelölésekor automatikusan elindított biztonsági funkció). Ekkor az Lopásvédelem webes

felületén létrehozhatja azt az optimalizálási funkcióval.

- **A játékos üzemmód aktív** – A Játékos üzemmód engedélyezése egy lehetséges biztonsági kockázatot jelent. Ilyenkor a program letiltja az összes előugró ablakot, és leállítja az esetleges ütemezett feladatokat.
- **Az Ön licence hamarosan lejár** – Ezt a tényt a védelmi állapot ikonján a rendszer órája mellett látható felkiáltójel jelzi. A licenc lejárta után a program nem frissül, és a védelmi állapot ikonja vörös lesz.

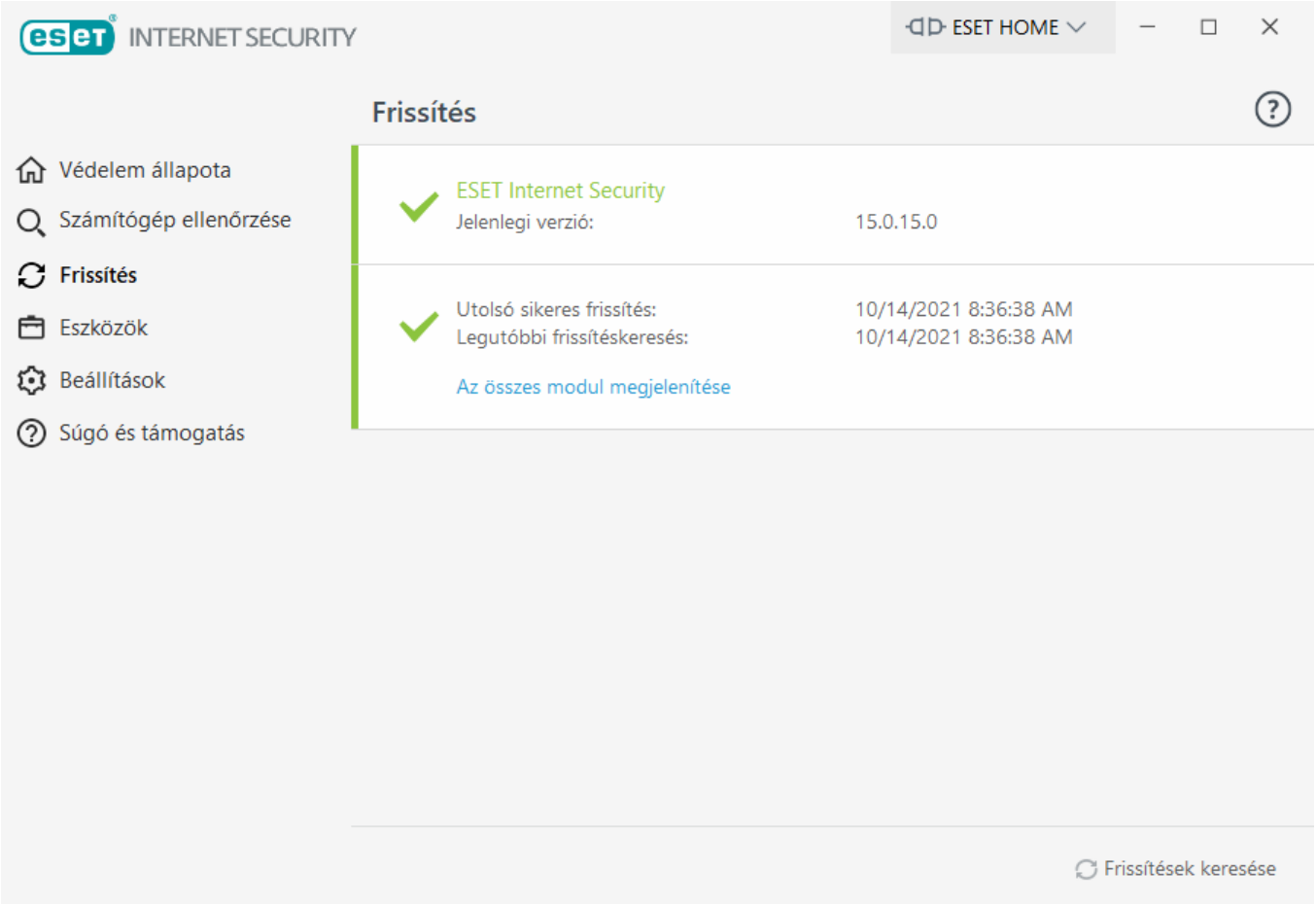
Ha a javasolt megoldásokkal nem szüntethető meg a probléma, a **Súgó és támogatás** hivatkozásra kattintva megnyithatja a súgófájlokat, illetve az ESET tudásbázisában is kereshet megoldást. Ha további segítségre van szüksége, elküldhet egy támogatási kérelmet. Az ESET műszaki támogatási szolgálat munkatársa gyorsan válaszol a kérdéseire, és segít a probléma megoldásában.

Frissítések

Az ESET Internet Security rendszeres frissítésével biztosítható a leghatékonyabban a számítógép maximális védelme. A Frissítés modul biztosítja, hogy a programmodulok és a rendszerösszetevők mindig naprakészek legyenek.

A program főablakának **Frissítés** elemére kattintva megjelenítheti az aktuális frissítési állapotot, beleértve az utolsó sikeres frissítés dátumát és időpontját, valamint azt, hogy szükség van-e frissítésre.

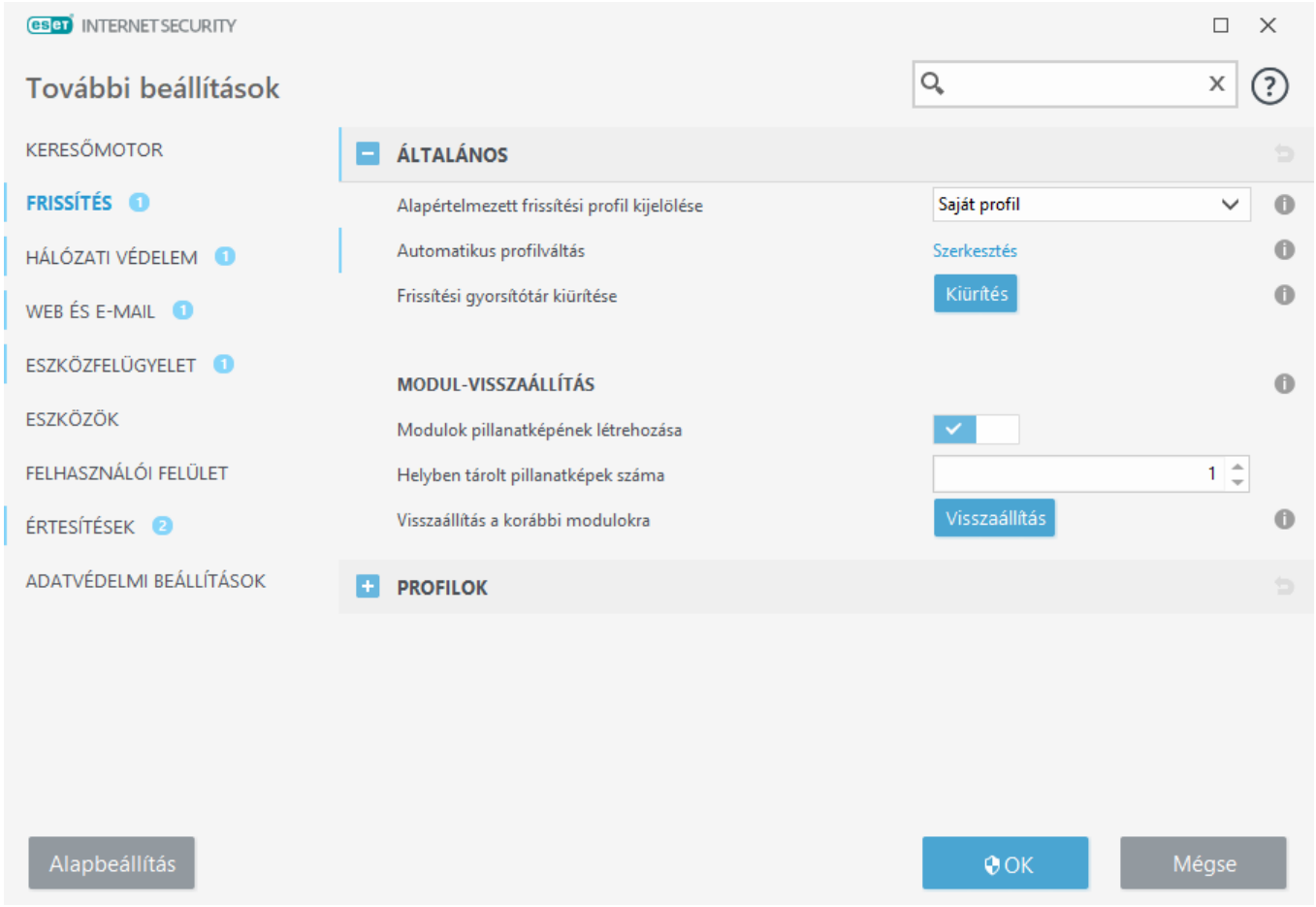
Az automatikus frissítések mellett manuális frissítést indíthat a **Frissítések keresése** gombra kattintva.



A További beállítások ablakban – amelyet a főmenü **Beállítások** parancsára, majd a **További beállítások** elemre

kattintva, vagy az **F5** billentyűt lenyomva érhet el – további frissítési beállítások találhatók. A további frissítési beállítások – például a frissítési mód, a proxyszerver elérhetőségi adatai és a helyi hálózati kapcsolatok – konfigurálásához kattintson a **Frissítés** elemre a További beállítások fában.

Ha egy frissítéssel kapcsolatban problémát tapasztal, a **Kiürítés** gombra kattintva ürítse ki a frissítési gyorsítótárat. Ha még mindig nem tudja frissíteni a programmodulokat, olvassa el A „Modulok frissítése sikertelen” üzenet hibaelhárítása című részt.



További biztonsági ESET-eszközök telepítése

Az ESET Internet Security használatbavétele előtt beállíthat további biztonsági eszközöket a védelem maximalizálása érdekében:

- Szülői felügyelet
- Lopásvédelem

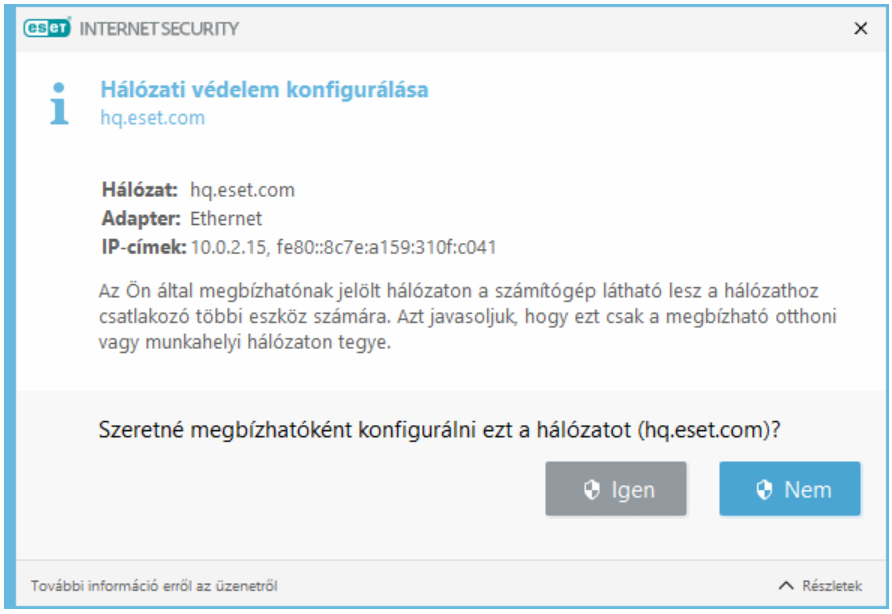
Ha további információra van szüksége a biztonsági eszközök ESET Internet Security alkalmazásban történő beállításáról, olvassa el ezt az ESET-tudásbáziscikket.

Hálózati védelem konfigurálása

Csatlakoztatott hálózatok beállításával biztosíthatja, hogy számítógépe hálózati környezetben is védett legyen. Hálózati védelmet állíthat be a megosztás engedélyezésére, hogy mások is hozzáférhessenek a számítógépéhez. Kattinson a **Beállítások** > **Hálózati védelem** > **Csatlakoztatott hálózatok** lehetőségre, és kattintson a

csatlakoztatott hálózat neve alatt látható hivatkozásra. Egy előugró ablakban megjelennek a beállítások, amelyek segítségével beállíthatja megbízhatóként a kiválasztott hálózatot.

Alapértelmezés szerint az ESET Internet Security a Windows-beállításokat alkalmazza egy új hálózat észlelésekor. Ha párbeszédpanelt szeretne megjeleníteni új hálózat észlelésekor, az Ismert hálózatok lapon módosítsa úgy az új hálózatok védelmi típusát, hogy a szolgáltatás megkérdezze a felhasználót. A hálózati védelem konfigurálása a számítógép új hálózathoz történő csatlakoztatásakor történik meg. Ezért általában nincs szükség megbízható zónák definiálására.



A hálózatvédelem konfigurálására szolgáló ablakban két hálózatvédelmi mód közül választhat:

- **Igen** – Megbízható hálózat esetén (otthoni vagy irodai hálózat). A számítógép és a számítógépen tárolt megosztott fájlok láthatók a többi hálózati felhasználó számára, és a rendszer erőforrásai elérhetők a hálózat többi felhasználója számára. Azt javasoljuk, hogy biztonságos helyi hálózat elérésekor használja ezt a beállítást.

- **Nem** – Nem megbízható hálózat esetén (nyilvános hálózat). A rendszer fájljai és mappái nincsenek megosztva a hálózat többi felhasználójával, nem láthatók a számukra, és a rendszer erőforrásainak megosztása inaktiválva van. Azt javasoljuk, hogy vezeték nélküli hálózatok elérésekor használja ezt a beállítást.

Ha helytelenül adja meg a hálózat beállításait, számítógépét biztonsági kockázatnak teszi ki.

A program alapértelmezés szerint engedélyezi a megbízható hálózatban lévő munkaállomásoknak a megosztott fájlok és nyomtatók elérését, a bejövő RPC-kommunikációt, valamint a távoli asztalok megosztását is.

A funkcióról az ESET alábbi tudásbáziscikkében talál további részleteket:

- A hálózati tűzfalbeállítások módosítása az ESET Windows otthoni termékekben

Engedélyezés Lopásvédelem

Otthonunktól a munkahelyre vagy más nyilvános helyre történő mindennapos utazásaink során személyes eszközeink folyamatosan ki vannak téve a kockázatnak, hogy elveszítjük vagy ellopják őket. Az Lopásvédelem növeli a felhasználó biztonságát az eszköz elvesztése vagy ellopása esetén. Az Lopásvédelem lehetővé teszi az eszközhasználat figyelését és az eltűnt eszköz nyomon követését az IP-cím alapján történő helymeghatározással a ESET HOME szolgáltatásban, ami elősegíti az eszköz visszaszerzését és a személyes adatok védelmét.

Az Lopásvédelem korszerű technológiák – például a földrajzi IP-cím keresése, a webkamerával történő képrögzítés, a felhasználói fiók védelme és a készülék figyelése – használatával segíti Önt és a rendvédelmi szerveket a számítógép vagy a készülék helyének meghatározásában annak elvesztése vagy ellopása esetén. A ESET HOME szolgáltatásban megtekintheti, hogy milyen tevékenység zajlik a számítógépén vagy az eszközén.

A ESET HOME Lopásvédelem funkciójáról a ESET HOME online súgójában olvashat bővebben.

Válasszon az alábbi lehetőségek közül az Lopásvédelem engedélyezéséhez és az eszköz védelméhez az elvesztése vagy ellopása esetén:

- A termék telepítése után kattintson az **EngedélyezésLopásvédelem** gombra az Lopásvédelem aktiválásához.
- Ha „Az ESET Anti-Theft rendelkezésre áll” üzenet látható a fő programablak > **Kezdőképernyőn**, kattintson az **Lopásvédelem engedélyezése** elemre.
- A fő programablakból kiindulva kattintson az **Eszközök** > **Lopásvédelem** elemre.
- A fő programablakból kiindulva kattintson a **Beállítások** > **Biztonsági eszközök** elemre. Kattintson a csúszka ikonra **Lopásvédelem**, majd kövesse a képernyőn megjelenő utasításokat.

Ha az eszköz nincs csatlakoztatva a ESET HOME szolgáltatáshoz, akkor a következőket kell tennie:
1. Jelentkezzen be a ESET HOME-fiókjába az Lopásvédelem engedélyezésekor.
2. Készüléknév beállítása.

Az Lopásvédelem nem támogatja a Microsoft Windows Home Server szoftvert.

Az Lopásvédelem engedélyezése után optimalizálhatja az eszköz biztonságát a fő programablak > **Eszközök** > **Lopásvédelem** lapon.

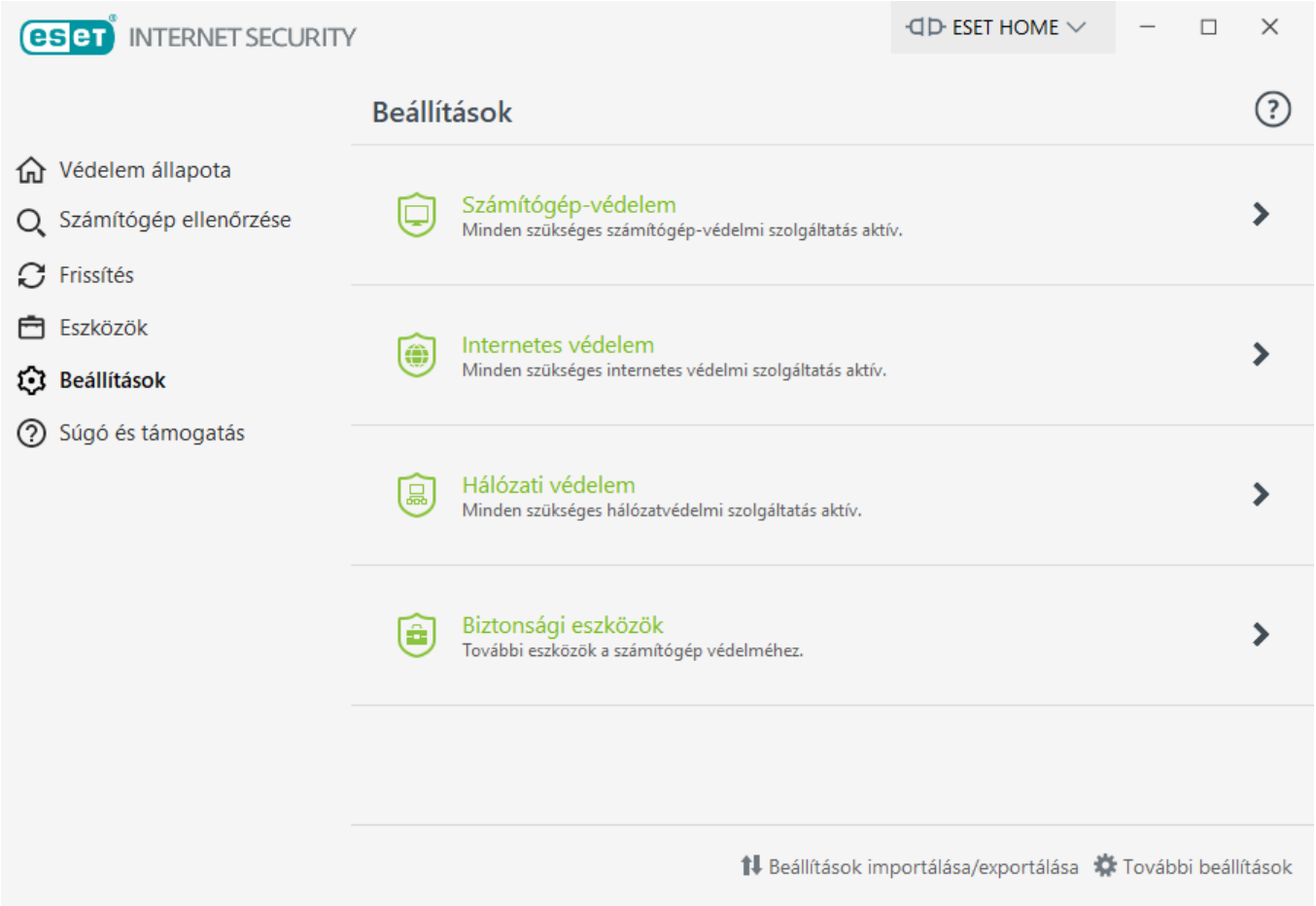
Szülői felügyeleti eszközök

Ha már engedélyezte a szülői felügyeletet az ESET Internet Security szolgáltatásban, az összes kapcsolódó felhasználói fiókokhoz is konfigurálnia kell.

Ha a szülői felügyelet aktív, és a felhasználói fiókok nincsenek konfigurálva, a **kezdőképernyőn** a „Szülői felügyelet nincs beállítva” üzenet látható. Kattintson a **Szabályok beállítása** elemre, és további információkért olvassa el a Szülői felügyelet című szakaszt.

Az ESET Internet Security használata

Az ESET Internet Security beállításai lehetővé teszik a számítógép és a hálózat védelmi szintjének megadását.



A **Beállítások** rész az alábbi szakaszokból áll:

A számítógép védelme

Internetes védelem

Hálózati védelem

Biztonsági eszközök

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 futtatásakor ellenőrzi, hogy nem tartalmaznak-e kártevő kódot.

- **Eszközfelügyelet** – 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

(CD/DVD/USB stb.).

• **Behatolásmegelőző rendszer (HIPS)** – A behatolásmegelőző rendszer felügyeli az operációs rendszeren belüli eseményeket, és a testre szabott 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 narancssárgára változik.

• **Webkamera-védelem** – A számítógéphez csatlakoztatott kamerához hozzáférő folyamatok és alkalmazások felügyeletére szolgál.

Az **Internetes védelem** beállításai között engedélyezheti vagy letilthatja az alábbi összetevőket:

• **Webhozzáférés-védelem** – Ha engedélyezi ezt a beállítást, a program a HTTP vagy a HTTPS protokoll teljes forgalmában keres kártevő szoftvereket.

• **E-mail-védelem** – A POP3(S) és az IMAP(S) protokollon keresztül érkező kommunikációt figyeli.

• **Levélszemétszűrő** – Kiszűri a kéretlen e-maileket, például a levélszemetet.

• **Adathalászat elleni védelem** – Kiszűri azokat a webhelyeket, amelyek gyaníthatóan a felhasználók manipulálására szolgáló tartalmat osztanak meg, és bizalmas információk kiszolgáltatására veszik rá a felhasználókat.

A **Hálózati védelem** csoportban engedélyezheti vagy letilthatja a tűzfalat, a hálózati támadások elleni védelmet (IDS) és a botnet elleni védelmet.

A **Biztonsági eszközök** beállítás lehetővé teszi a következő modulok beállítását:

• **Netbank- és tranzakcióvédelem** – A védelem egy újabb rétege a böngésző számára, amellyel megóvhatja pénzügyi adatait az online tranzakciók során. Az **Összes böngésző védelme** funkció engedélyezésével elindíthatja az összes támogatott webböngészőt biztonságos módban. További információkért tekintse meg a Netbank- és tranzakcióvédelem című részt.

• **Szülői felügyelet** – A Szülői felügyelet modul megvédi gyermekeit azáltal, hogy blokkolja a nem megfelelő vagy káros tartalmakat az interneten.

• **Anti-Theft** – Az Lopásvédelem engedélyezésével megvédheti számítógépét az elvesztése vagy ellopása esetén.

A szülői felügyelet lehetővé teszi az esetlegesen nem kívánt tartalmú weboldalak letiltását. Ezenkívül a szülők több mint 40 előre definiált webhely-kategória és több mint 140 alkategória elérését is megtilthatják.

Egy letiltott biztonsági összetevő újraengedélyezéséhez kattintson a csúszkára , hogy a zöld pipát  jelenítse meg.

> 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 **További beállítások** hivatkozással részletesebben megadhatja a paramétereket az egyes modulokhoz. A **Beállítások importálása és exportálása** gombra kattintva egy .xml konfigurációs fájl segítségével betöltheti a beállítási paramétereket, illetve egy konfigurációs fájlba mentheti az aktuális beállítási paramétereket.

A számítógép védelme

Kattintson a **Számítógép-védelem** elemre a **Beállítások** ablakban az összes védelmi modul áttekintéséhez:

- Valós idejű fájlrendszervédelem
- Eszközfelügyelet
- Behatolásmegelőző rendszer (HIPS)
- Játékos üzemmód
- Webkamera-védelem

Az egyes védelmi modulok szüneteltetéséhez vagy letiltásához kattintson a csúszkára .

A védelmi modulok kikapcsolása esetén csökkenhet a számítógép védelmi szintje.

Kattintson a fogaskerékre az egyik védelmi modul mellett a modul további beállításainak megjelenítéséhez.

A **Valós idejű fájlrendszervédelem** esetén kattintson a fogaskerékre , majd válasszon a következő lehetőségek közül:

- **Konfigurálás** – A Valós idejű fájlrendszervédelem További beállítások ablakának megnyitása.
- **Kivételek szerkesztése** – A Kivételek beállítása beállítási ablak megnyitása, ahol kizárhat fájlokat és mappákat az ellenőrzésből.

A **Webkamera-védelem** esetén kattintson a fogaskerékre , majd válasszon a következő lehetőségek közül:

- **Konfigurálás** – A Webkamera-védelem További beállítások ablakának megnyitása.
- **Minden hozzáférés letiltása újraindításig** – A számítógép újraindításáig a webkamerához való összes hozzáférés letiltása.
- **Minden hozzáférés letiltása véglegesen** – A webkamerához való összes hozzáférés blokkolása a beállítás letiltásáig.
- **Minden hozzáférés letiltásának megszüntetése** – A Webkamera-hozzáférés blokkolási lehetőségének letiltása. Ez a lehetőség csak akkor érhető el, ha a webkamera-hozzáférés le van tiltva.



A vírus- és kémprogramvédelem ideiglenes letiltása – Letiltja az összes vírus- és kémprogramvédelmi modult. A védelem letiltásakor megjelenik egy ablak, ahol az **Időpont** legördülő listából kiválasztott értékkel megadhatja, hogy mennyi ideig legyen letiltva a védelem. Csak akkor használja, ha tapasztalt felhasználó, vagy ha az ESET műszaki terméktámogatási szolgálat kérte meg erre.

Keresőmotor

A keresőmotor a fájlok, az e-mailek és az internetes kommunikáció ellenőrzésével megakadályozza a kártékony kódok bejutását a rendszerbe. Ha például a program felismer egy kártevőnek minősülő objektumot, megkezdődik a kezelése. A keresőmotor először letiltja, majd megtisztítja, törli vagy karanténba helyezi.

A keresőmotor részletes beállításához kattintson a **További beállítások** elemre, vagy nyomja le az **F5** billentyűt.

A Keresőmotor beállításainak módosítását csak tapasztalt felhasználóknak javasoljuk. A helytelen konfiguráció alacsonyabb szintű védelemhez vezethet.

Ebben a szakaszban:

- Valós idejű védelmi és gépi tanulási kategóriák
- Kártevő-ellenőrzések
- Jelentési beállítások
- Védelmi beállítások

Valós idejű védelmi és gépi tanulási kategóriák

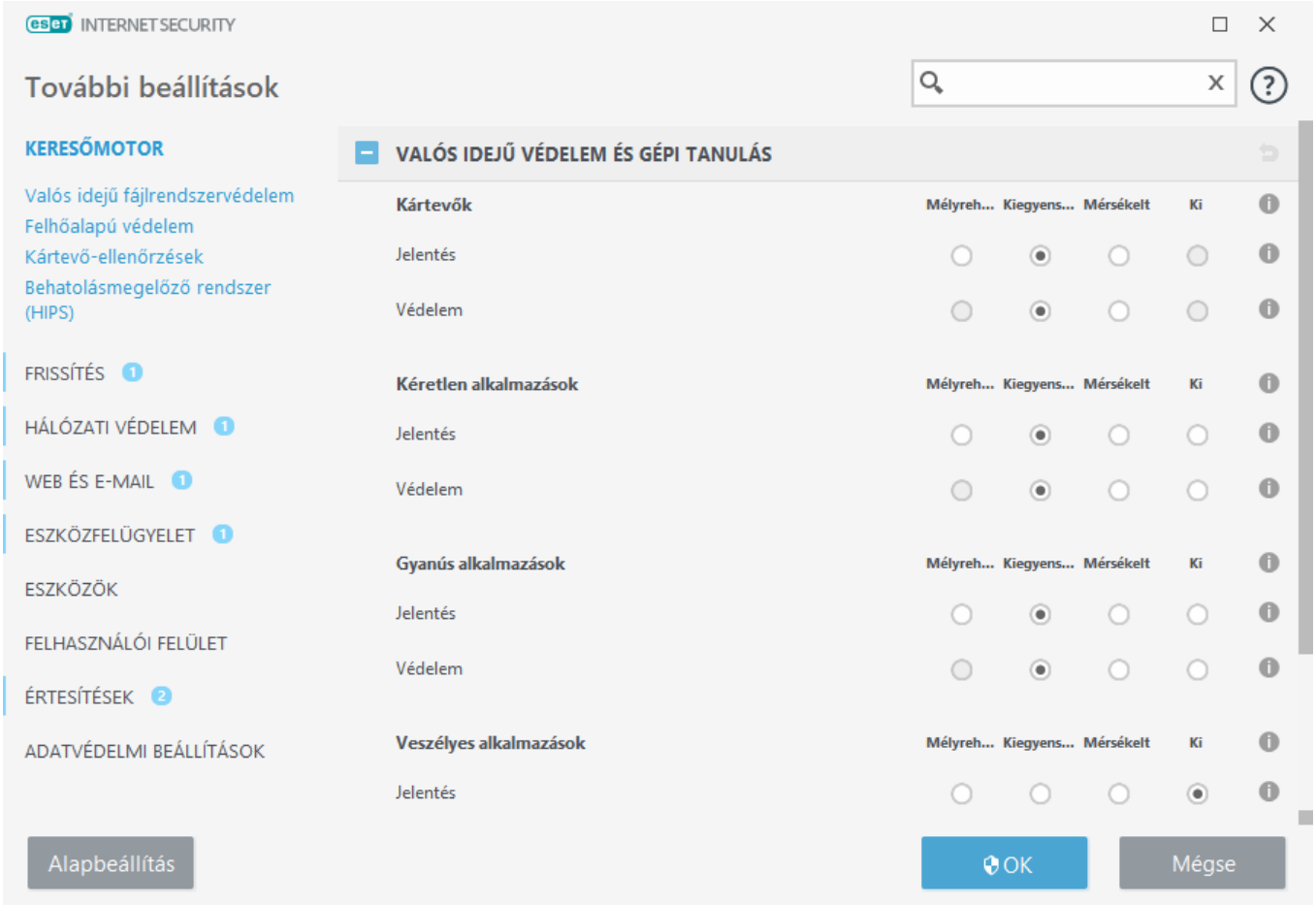
Az összes védelmi modulhoz (például Valós idejű fájlrendszervédelem és Webhozzáférés-védelem) rendelkezésre álló **Valós idejű és gépi tanulás védelem** segítségével konfigurálhatók jelentési és védelmi szintek a következő kategóriákban:

- **Kártevő** – A számítógépes vírusok olyan rosszindulatú kódok, amelyek a számítógépen lévő meglévő fájlok elejéhez vagy végéhez fűzik magukat. A „vírus” kifejezést azonban gyakran rosszul használják. A „kártevő” egy pontosabb kifejezés. A kártevőészlelést a keresőmotor végzi a gépi tanulás összetevővel együtt. A Szószedetben részletesen olvashat az ilyen típusú alkalmazásokról.

- **Kéretlen alkalmazások** – A „grayware” vagy kéretlen alkalmazások (PUA) kategória számos különböző szoftvert foglal magában. Az ilyen szoftverek nem annyira kártékonyak, mint a többi kártevő, például a vírusok és a trójaiak. További nemkívánatos szoftvereket telepíthetnek azonban, megváltoztathatják a digitális készülék viselkedését, illetve olyan tevékenységeket végezhetnek, amelyeket a felhasználó nem hagyott jóvá, vagy nem várt. A Szószedetben részletesen olvashat az ilyen típusú alkalmazásokról.

- A **gyanús alkalmazások** közé tartoznak a tömörítőkkel vagy védelmi modulokkal tömörített programok. Az ilyen típusú védelmi modulokat gyakran használják a kártevőprogramok fejlesztői arra, hogy segítségükkel elkerüljék az észlelést.

- **Veszélyes alkalmazások** – Ide a kereskedelemben kapható, törvényes szoftverek tartoznak, amelyekkel kártékony célokból visszaélhetnek. Veszélyes alkalmazások (PUA) például a távoli hozzáférést biztosító eszközök, a jelszófeltörő alkalmazások, valamint a billentyűzetfigyelők (a felhasználó minden billentyűleütését rögzítő programok). A Szószedetben részletesen olvashat az ilyen típusú alkalmazásokról.



Nagyobb fokú védelem

A Speciális gépi tanulás most már a keresőmotor része, és egy fejlett védelmi réteget biztosít, amely hatékonyabbá teszi a gépi tanulás alapú észlelést. A Szószedetben bővebben olvashat erről a típusú védelemről.

Kártevő-ellenőrzések

Az ellenőrzési beállítások külön konfigurálhatók a valós idejű víruskereső és a kézi indítású kereső esetén. Alapértelmezés szerint a **Valós idejű védelmi beállítások használata** funkció aktiválva van. Ha aktiválva van, a vonatkozó kézi indítású keresési beállítások a **Valós idejű védelem és gépi tanulás** szakaszból öröklődnek. További információkért tekintse meg a Kártevő-ellenőrzések című részt.

Jelentési beállítások

Észlelés esetén (pl. a program talált egy gyanús elemet, és kártevőnek minősíti) a rendszer rögzíti az adatokat az észlelési naplóban, és asztali értesítéseket is megjelenít, ha az ESET Internet Security programban ez konfigurálva van.

A jelentési küszöb mindegyik kategória („KATEGÓRIA”) esetén konfigurálható:

1. Kártevők

2.Kéretlen alkalmazások

3.Potenciálisan veszélyes

4.Gyanús alkalmazások

A keresőmotor által végzett jelentés, beleértve a gépi tanulás összetevőt is. Az aktuális védelmi küszöbértéknél magasabb jelentési küszöböt is be lehet állítani. Ezek a jelentési beállítások nem befolyásolják a letiltást, a tisztítást és az objektumok törlését.

Olvassa el a következőket, mielőtt módosítaná egy KATEGÓRIA jelentési küszöbét (vagy szintjét):

Küszöb	Magyarázat
Mélyreható	A KATEGÓRIA jelentés maximális érzékenységre lett állítva. Több kártevőészlelésről készül jelentés. A **Mélyreható** felismerési szint beállítása esetén, előfordulhat, hogy a rendszer tévesen KATEGÓRIA típusú kártevőnek észlel bizonyos nem kártékony objektumokat.
Kiegyensúlyozott	Az adott KATEGÓRIÁVAL kapcsolatos jelentés kiegyensúlyozottra van beállítva. Ez a beállítás az észlelési arány teljesítményének és pontosságának, illetve a hamisan jelentett objektumok számának kiegyensúlyozására van optimalizálva.
Mérsékelt	Az adott KATEGÓRIÁVAL kapcsolatos jelentés úgy van beállítva, hogy megfelelő szintű védelem mellett minimális legyen a tévesen beazonosított objektumok száma. A rendszer csak akkor jelenti a felismert objektumokat, ha a káros tartalom valószínűsége magas és megfelel az adott KATEGÓRIA viselkedési jellemzőinek.
Ki	Az adott KATEGÓRIÁVAL kapcsolatos jelentés nem aktív, és a rendszer nem ismeri fel, nem jelenti és nem tisztítja meg az ilyen típusú kártevőket. Ennek eredményeként a védelem nem biztosított. A Ki beállítási lehetőség nem áll rendelkezésre a kártevőjelentés esetén, és ez az alapértelmezett érték a veszélyes alkalmazások esetén.

Az ESET Internet Security védelmi modulok elérhetősége

Az adott KATEGÓRIÁNÁL kiválasztott küszöbérték elérhetősége (aktiválva vagy letiltva) a különböző védelmi modulok esetén:

	Mélyreható	Kiegyensúlyozott	Mérsékelt	Ki**
Speciális gépi tanulási modul*	✓ (mélyreható mód)	✓ (konzervatív mód)	X	X
Keresőmotor modul	✓	✓	✓	X
Egyéb védelmi modulok	✓	✓	✓	X

*Az ESET Internet Security 13.1-es és újabb verzióiban áll rendelkezésre.
** Nem javasolt

Termékverziók, programmodul-verziók és builddátumok meghatározása

1. Kattintson a **Súgó és támogatás** > **Az ESET Internet Security** névjegye elemre.

2. A **Névjegy** képernyőn a szöveg első sorában az ESET-termék verziószáma látható.

3. A **Telepített összetevők** elemre kattintva megtekintheti a különböző modulokkal kapcsolatos információkat.

Megjegyzések

Néhány megjegyzés a környezetnek megfelelő küszöb beállításához:

- A **Kiegyensúlyozott** a legtöbb telepítés esetén javasolt küszöb.
- A **Mérsékelt** küszöb az ESET Internet Security korábbi (13.0-es és korábbi) verzióihoz hasonló védelmi szintet nyújt. Olyan környezetben javasolt, ahol az elsődleges szempont az, hogy a biztonsági szoftver minél kevesebb tévesen azonosított objektumot jelentsen.
- Minél magasabb a jelentési küszöb, annál nagyobb az észlelési arány, viszont nagyobb az esélye a tévesen azonosított objektumoknak is.
- A valóságban nincs garancia a 100%-os észlelési arányra, illetve nincs 0%-os esélye a tiszta objektumok kártevőként való téves kategorizálásának.
- Tartsa az ESET Internet Security programot és a moduljait naprakészen, mert így maximalizálható az észlelési arány teljesítményének és pontossága, illetve a hamisan jelentett objektumok száma közötti egyensúly.

Védelmi beállítások

Ha egy adott KATEGÓRIÁNAK minősülő objektumot felismer, akkor a program blokkolja az objektumot, majd megtisztítja, törli, vagy karanténba helyezi.

Olvassa el a következőket, mielőtt módosítaná egy KATEGÓRIA védelmi küszöbét (vagy szintjét):

Küszöb	Magyarázat
Mélyreható	A rendszer letiltja a mélyreható (vagy alacsonyabb) felismerési szintű kártevőket, és elindul az automatikus eltávolítás (pl. tisztítás). Ez a beállítás akkor ajánlott, ha az összes végpont ellenőrzése mélyreható felismerési szinttel történt és a tévesen felismert objektumok hozzá lettek adva a kivételekhez.
Kiegyensúlyozott	A rendszer letiltja a kiegyensúlyozott (vagy alacsonyabb) felismerési szintű kártevőket, és elindul az automatikus eltávolítás (pl. tisztítás).
Mérsékelt	A rendszer letiltja a mérsékelt felismerési szintű kártevőket, és elindul az automatikus eltávolítás (pl. tisztítás).
Ki	Hasznos beállítás a tévesen jelentett objektumok azonosításához és kizárásához. A Ki beállítási lehetőség nem áll rendelkezésre a kártevők elleni védelem esetén, és ez az alapértelmezett érték a veszélyes alkalmazások esetén.

Átalakítási táblázat az ESET Internet Security 13.0-s és korábbi verzióihoz

A 13.0-es vagy korábbi verzióról a 13.1-es vagy újabb verzióra való frissítés után az új küszöbállapot a következő lesz:

Kategóriakapcsoló a frissítés előtt	✓	✗
A KATEGÓRIA új küszöbállapota a frissítés után	Kiegyensúlyozott	Ki

A keresőmotor további beállításai

Az **Anti-Stealth technológia** egy kifinomult rendszer, amely észleli azokat a veszélyes programokat (többek között a rootkiteket), amelyek képesek elrejtőzni az operációs rendszerben. Az elrejtőzés itt azt jelenti, hogy a szokásos vizsgálati eljárásokkal ezek a programok nem deríthetők fel.

AMSI-n keresztüli speciális ellenőrzés engedélyezése – Microsoft Antimalware Scan Interface eszköz, amely új védelmi lehetőséget ad az alkalmazásfejlesztők kezébe a kártevők ellen (csak Windows 10 esetén).

A program fertőzést észlelt

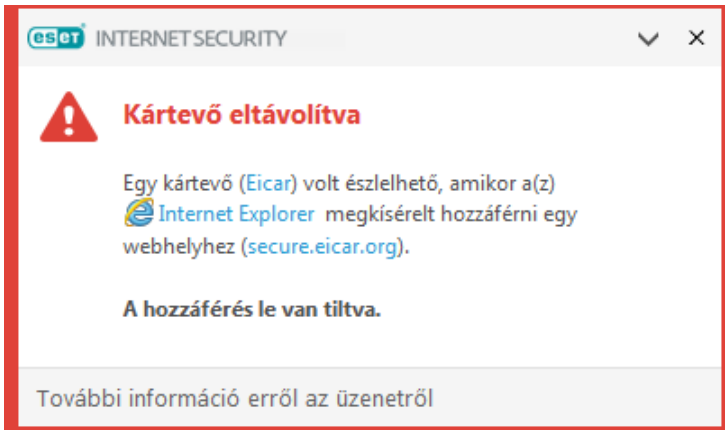
A fertőzések számos különböző ponton keresztül juthatnak be a rendszerbe, például weboldalakról, megosztott mappákból, e-mailen keresztül vagy cserélhető eszközökről (USB-eszközökről, külső lemezekről, CD, DVD vagy hajlékonylemezekről stb.).

Szokásos viselkedés

A fertőzések észleléséhez az ESET Internet Security az alábbi módszereket használhatja:

- Valós idejű fájlrendszervédelem
- Webhozzáférés-védelem
- E-mail védelem
- Kézi indítású számítógép-ellenőrzés

Ezek mindegyike a szokásos megtisztítási módot használja, megkísérli megtisztítani a fájlt, és áthelyezi a karanténba, vagy megszakítja a kapcsolatot. A képernyő jobb alsó sarkában lévő értesítési területen megjelenik egy értesítési ablak. Az észlelt/megtisztított objektumokról a Naplófájlok című fejezetben tájékozódhat bővebben. A megtisztítási szintekről és viselkedésről a Megtisztítási szintek című fejezetben olvashat bővebben.



Fertőzött fájlok keresése a számítógépen

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

1.Nyissa meg az ESET Internet Security programot, és kattintson a **Számítógép ellenőrzése** ikonra.

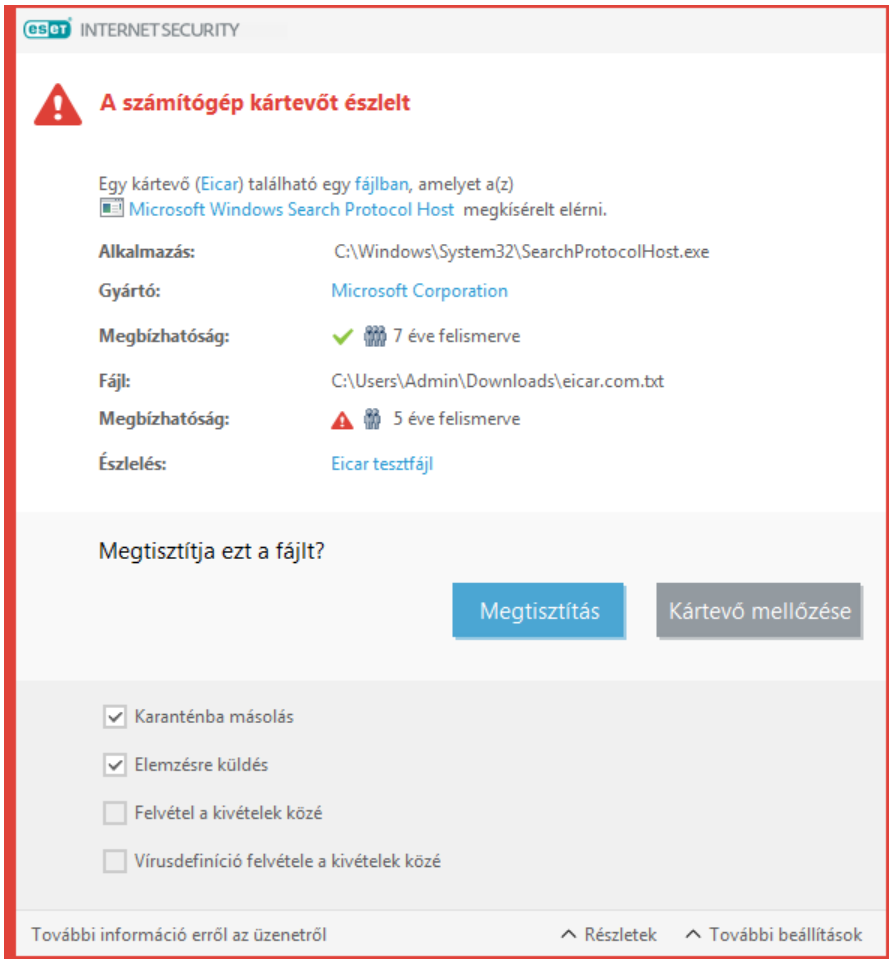
2.Kattintson **Optimalizált ellenőrzés** hivatkozásra (további információért lásd: Számítógép ellenőrzése).

3.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.

Megtisztítás és törlés

Ha nincs előre meghatározva, hogy a valós idejű fájlrendszervédelem milyen műveletet hajtson végre, a program egy riasztási ablakban kéri egy művelet megadását. Rendszerint a **Megtisztítás**, a **Törlés** és a **Nincs művelet** közül választhat. A **Nincs művelet** megadása nem javasolt, mivel ez megtisztítatlanul hagyja a fertőzött fájlokat. Kivételnek számít az a helyzet, ha az adott fájl biztosan ártalmatlan, és a program hibásan észlelte azt fertőzöttnek.



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).

Visszaállítás a karanténból

A karantén az ESET Internet Security fő programablakából érhető el az **Eszközök** > **További eszközök** > **Karantén** elemre kattintva.

A karanténba helyezett fájlok vissza is állíthatók az eredeti helyükre:

- Erre használja a **Visszaállítás** funkciót, amely a helyi menüből érhető el, azután hogy jobb gombbal az adott fájlra kattintott a Karanténban.
- Ha a fájl kéretlen alkalmazásként van megjelölve, akkor kiválasztható a **Visszaállítás és kizárás az ellenőrzésből** lehetőség. Lásd a Kivételek című részt is.
- A helyi menüben megtalálható a **Visszaállítás megadott helyre** menüpont is, mellyel a törlés helyétől különböző mappába is visszaállíthatók a fájlok.
- A visszaállítási funkció nem áll rendelkezésre bizonyos esetekben, például írásvédett hálózati megosztáson található fájlok esetén.

Többszörös fertőzés

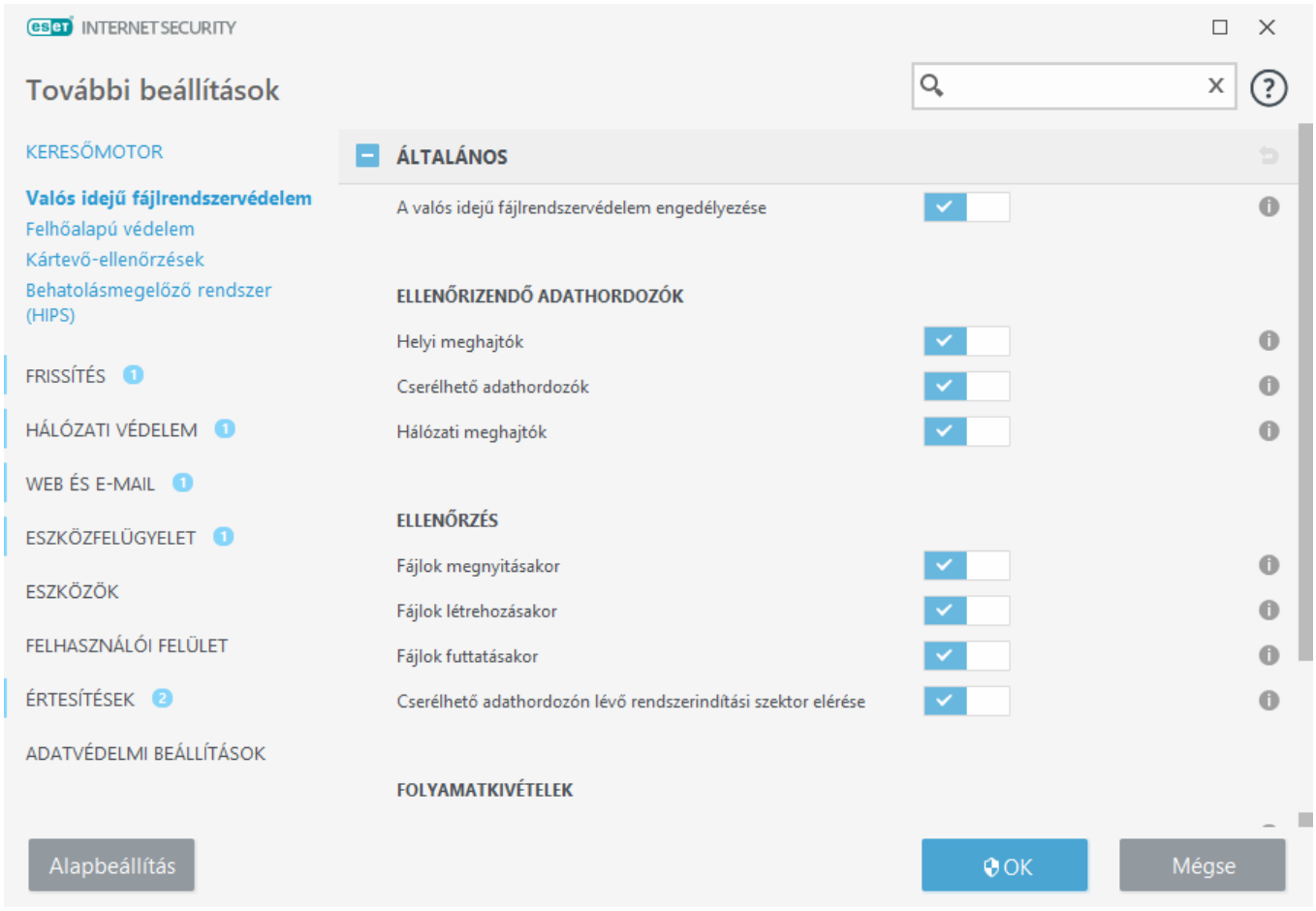
Ha a számítógép ellenőrzése után maradnak megtisztítatlan fertőzött fájlok (vagy az Automatikus megtisztítás szintje a **Mindig rákérdez** értékre van állítva), megjelenik egy riasztási ablak, amely a kérdéses fájlokon végrehajtandó műveletek kiválasztását kéri. Először válassza ki a fájlokon végrehajtandó műveleteket (ezeket a listában szereplő fájlok mindegyikéhez külön kell beállítani), majd kattintson a **Befejezés** gombra.

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 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.

Valós idejű fájlrendszervédelem

A Valós idejű fájlrendszervédelem ellenőrzi, hogy található-e rosszindulatú kód a rendszerben lévő összes fájlban megnyitáskor, létrehozáskor, illetve futtatáskor.



Alapértelmezés szerint a Valós idejű fájlrendszervédelem a rendszerindításkor indul el, és folyamatos ellenőrzést biztosít. Nem javasoljuk **A valós idejű fájlrendszervédelem automatikus engedélyezése** funkció letiltását a **További beállítások** lap **Keresőmotor** > **Valós idejű fájlrendszervédelem** > **Általános** szakaszában.

Ellenőrizendő adathordozók

A program alapértelmezés szerint minden típusú adathordozót ellenőriz a lehetséges kártevők felderítése érdekében:

- **Helyi meghajtók** – Az összes rendszer- és rögzített merevlemez ellenőrzése (például: *C:*\, *D:*\).
- **Cserélhető adathordozók** – CD/DVD lemezek, USB-tárolóeszközök, memórakártyák stb. ellenőrzése.
- **Hálózati meghajtók** – Az összes csatlakoztatott hálózati meghajtó (például: *H:*\ mint *store04*), illetve közvetlen hozzáférésű hálózati meghajtó ellenőrzése (például: *store08*).

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

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** – Ellenőrzés fájl megnyitásakor.

- **Fájlok létrehozásakor** – Létrehozott vagy módosított fájl ellenőrzése.
- **Fájlok futtatásakor** – Ellenőrzés fájl futtatásakor.
- **Cserélhető adathordozón lévő rendszerindítási szektor elérése** – Ha a felhasználó rendszerindítási szektorral rendelkező cserélhető adathordozót helyez az eszközbe, a program azonnal ellenőrzi a rendszerindítási szektort. Ez a beállítás nem teszi lehetővé a cserélhető adathordozókon lévő fájlok ellenőrzését. A cserélhető adathordozókon lévő fájlok ellenőrzése az **Ellenőrizendő adathordozók** > **Cserélhető adathordozók** lapon állítható be. Ahhoz, hogy megfelelően működjön a **cserélhető adathordozón lévő rendszerindítási szektor elérése**, hagyja aktivált állapotban a **Rendszerindítási szektorok/UEFI** funkciót a ThreatSense-paraméterekben.

A valós idejű fájlrendszervédelem a különböző rendszeresemények – például a fájlokhoz való hozzáférések – hatására ellenőrzi a különféle típusú adathordozókat. Az ellenőrzés a ThreatSense technológia észlelési módszereit alkalmazza (ezek leírása A ThreatSense keresőmotor beállításai című témakörben található). A valós idejű fájlrendszervédelem beállítható úgy, hogy másképpen kezelje az újonnan létrehozott, illetve a meglévő fájlokat. Beállíthatja például, hogy a valós idejű fájlrendszervédelem alaposabban figyelje az újonnan létrehozott fájlokat.

Az alacsony rendszerterhelés biztosítása érdekében a valós idejű védelem során a program csak akkor ellenőrzi újra a már ellenőrzött fájlokat, ha módosították őket. A program a keresőmotor minden egyes frissítése után azonnal újból ellenőrzi a fájlokat. Ennek működése **optimalizálással** szabályozható. Ha az **optimalizálás** le van tiltva, a fájlok ellenőrzése minden megnyitásuk esetén megtörténik. Ha módosítani szeretné ezt a beállítást, az **F5** billentyűt lenyomva nyissa meg a **További beállítások** párbeszédpanelt, és bontsa ki a **Keresőmotor** > **Valós idejű fájlrendszervédelem** csomópontot. Kattintson a **ThreatSense-paraméterek** > **Egyéb** elemre, és kapcsolja be vagy ki az **Optimalizálás engedélyezése** opciót.

Megtisztítási szintek

A kívánt védelmi modulhoz kapcsolódó megtisztítási szintek beállításainak eléréséhez bontsa ki a **ThreatSense-paramétereket** (például **Valós idejű fájlrendszervédelem**), majd lépjen a **Megtisztítás > Megtisztítás szintje** elemhez.

A ThreatSense-paraméterek a következő kezelési (vagyis tisztítási) szinteket teszik lehetővé.

Kezelés az ESET Internet Security termékben

Automatikus megtisztítás szintje	Leírás
Mindig kezelje a fertőzést	Az észlelt kártevő eltávolítása az objektumok tisztítása közben felhasználói beavatkozás nélkül. Egyes ritka esetekben (például rendszerfájlok esetén), ha az észlelt kártevő nem távolítható el, az objektum az eredeti helyén marad.
Fertőzés kezelése, ha ez biztonságos. Egyéb esetben megtartás	Az észlelt kártevő eltávolítása az objektumok tisztítása közben felhasználói beavatkozás nélkül. Egyes esetekben (például tiszta és fertőzött fájlokat egyaránt tartalmazó rendszerfájlok vagy archívumok esetén), ha az észlelt kártevő nem távolítható el, az objektum az eredeti helyén marad.
Fertőzés kezelése, ha ez biztonságos. Egyéb esetben rákérdezés	Az észlelt kártevő eltávolítása az objektumok tisztítása közben. Egyes esetekben, ha nem hajtható végre művelet, a végfelhasználó interaktív figyelmeztetést kap, és ki kell választania egy műveletet (például törlés vagy figyelmen kívül hagyás). Legtöbb esetben ez a beállítás ajánlott.

Automatikus megtisztítás szintje	Leírás
Mindig kérdezze meg a végfelhasználót	A végfelhasználónak megjelenik egy interaktív ablak az objektumok tisztítása során, és ki kell választania egy műveletet (például törlés vagy figyelmen kívül hagyás). Ez a szint a tapasztalt felhasználóknak ajánlott, akik tisztában vannak azzal, hogy mi a teendő a fertőzések esetén.

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.

Telepítése után az ESET Internet Security minden beállítást optimalizál, hogy a lehető legmagasabb szintű védelmet biztosítsa a rendszer számára. Az alapértelmezett beállítások visszaállításához kattintson az ablak ikonjára az egyes fülek mellett (**További beállítások** > **Keresőmotor** > **Valós idejű fájlrendszervédelem**).

A valós idejű védelem ellenőrzése

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

A fájl a következő weboldalról tölthető le: http://www.eicar.org/download/eicar.com
Miután megadta az URL-t a böngészőben, megjelenik egy üzenet, mely szerint megtörtént a kártevő eltávolítása.

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 egy felhasználó véletlenül letiltotta a valós idejű védelmet, akkor aktiválja újra a funkciót. A valós idejű védelem újbóli aktiválásához a program főablakában kattintson a **Beállítások** elemre, majd a **Számítógép-védelem** > **Valós idejű fájlrendszervédelem** lehetőségre.

Ha a valós idejű védelem nem indul el a rendszer indításakor, valószínűleg le van tiltva a **Valós idejű fájlrendszervédelem engedélyezése**. Ha engedélyezni szeretné ezt a beállítást, nyissa meg a **További beállítások** párbeszédpanelt (az **F5** billentyűvel), és válassza ki a **Keresőmotor** > **Valós idejű fájlrendszervédelem** elemet.

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 víruskereső program van telepítve, azok ütközésbe kerülhetnek egymással. Javasoljuk, hogy az ESET telepítése előtt távolítson el minden egyéb vírusvédelmi programot a rendszerről.

A valós idejű védelem nem indul el

Ha a valós idejű védelem nem indul el rendszerindításkor (és be van jelölve a **Valós idejű fájlrendszervédelem engedélyezése** jelölőnégyzet), akkor ennek valószínűleg más programokkal való ütközés az oka. A hiba elhárításához hozzon létre egy SysInspector-naplót, és elemzésre küldje el az ESET műszaki támogatási szolgálatának.

Folyamatkivételek

A Folyamatkivételek funkció lehetővé teszi, hogy alkalmazásfolyamatokat zárjon ki a valós idejű fájlrendszervédelmi ellenőrzésből. A biztonsági mentés gyorsaságának, a folyamatok integritásának és a szolgáltatások elérhetőségének fokozása érdekében néhány olyan technikát alkalmaznak a biztonsági mentés során, amelyek köztudottan problémát okoznak a fájlszintű kártevővédelemben. Az egyetlen hatékony módja ennek a két helyzetnek az elkerülésére a kártevőirtó szoftver deaktiválása. Bizonyos folyamatok kizárásával (például a biztonsági mentésre használt megoldás folyamatainak) a kizárt folyamat által végzett összes fájlműveletet figyelmen kívül hagyja és biztonságosnak tartja a rendszer, ezzel minimalizálva a biztonsági mentési folyamattal való ütközést. Azt javasoljuk, hogy körültekintéssel járjon el a kivételek létrehozásakor – a kizárt biztonsági mentési eszköz hozzá tud férni fertőzött fájlokhoz anélkül, hogy erről Ön riasztást kapna. Ez az oka annak, hogy kibővített kivételek csak a valós idejű védelmi modulban adhatók meg.

Nem összekeverendő a kizárt fájlkiterjesztésekkel, a HIPS-kiterjesztésekkel, az észlelési kivételekkel és a folyamatkivételekkel.

A Folyamatkivételek funkció elősegíti az esetleges ütközések kockázatának minimalizálását, és fokozza a kizárt alkalmazások teljesítményét, ami pozitív hatással van az operációs rendszer általános teljesítményére és stabilitására. Egy folyamat/alkalmazás kizárása a végrehajtható fájljának (*.exe*) kizárását jelenti.

A **További beállítások** (F5) > **Keresőmotor** > **Valós idejű fájlrendszervédelem** > **Folyamatkivételek** lapon adhat hozzá végrehajtható fájlokat a kizárt folyamatok listájához.

A funkció a biztonsági mentésre szolgáló eszközök kizárása céljából jött létre. A biztonsági mentésre szolgáló eszköz folyamatának kizárása nem csupán biztosítja a rendszer stabilitását, hanem a biztonsági mentés teljesítményére sincs hatással, mivel a biztonsági mentés nem lassul le, amikor fut.

A **Szerkesztés** elemre kattintva nyissa meg a **Folyamatkivételek** felügyeleti ablakot, ahol hozzáadhat kivételeket, és tallózással megkeresheti az ellenőrzésből kizárni kívánt végrehajtható fájlokat (például *Backup-tool.exe*).
Amint hozzáadja az *.exe* fájlt a kivételekhez, az ESET Internet Security leállítja az adott folyamat felügyeletét, és nem ellenőrzi a folyamat által végrehajtott fájlműveleteket.

Ha nem használja a tallózási funkciót a végrehajtható fájl kiválasztásakor, akkor manuálisan kell megadnia a teljes elérési útvonalát. Ha nem így jár el, akkor nem fog megfelelően működni a kivétel, és a Behatolásmegelőző rendszer hibákat jelezhet.

Szerkesztheti is a meglévő folyamatokat, illetve **törölhet** folyamatokat a kivételek közül.

A Webhozzáférés-védelem nem veszi figyelembe ezt a kivételt, így akkor is végbemegy a letöltött fájlok ellenőrzése, ha kizárja a webböngésző végrehajtható fájlját. Ilyen módon továbbra is észlelhetők a fertőzések. Mindezt csak példaként említettük – nem javasoljuk a webböngészők kizárását.

Folyamatkivételek felvétele vagy szerkesztése

Ezen a párbeszédpanelen **felvehet** olyan folyamatokat, amelyek ki vannak zárva a keresőmotorból. A Folyamatkivételek funkció elősegíti az esetleges ütközések kockázatának minimalizálását, és fokozza a kizárt alkalmazások teljesítményét, ami pozitív hatással van az operációs rendszer általános teljesítményére és stabilitására. Egy folyamat/alkalmazás kizárása a végrehajtható fájljának (*.exe*) kizárását jelenti.

Kiválaszthatja a kivételként felvenni kívánt alkalmazás elérési útvonalát a ... ikonra kattintva (például *C:\Program Files\Firefox\Firefox.exe*). NE írja be az alkalmazás nevét.
Amint hozzáadja az *.exe* fájlt a kivételekhez, az ESET Internet Security leállítja az adott folyamat felügyeletét, és nem ellenőrzi a folyamat által végrehajtott fájlműveleteket.

Ha nem használja a tallózási funkciót a végrehajtható fájl kiválasztásakor, akkor manuálisan kell megadnia a teljes elérési útvonalát. Ha nem így jár el, akkor nem fog megfelelően működni a kivétel, és a Behatolásmegelőző rendszer hibákat jelezhet.

Szerkesztheti is a meglévő folyamatokat, illetve **törölhet** folyamatokat a kivételek közül.

Felhőalapú védelem

Az ESET ThreatSense.Net korszerű korai riasztási rendszerre épülő ESET LiveGrid® felhasználja és az ESET víruslaborjába küldi az ESET felhasználói által szerte a világból beküldött adatokat. A gyanús minták és metaadatok biztosításával a ESET LiveGrid® lehetővé teszi, hogy azonnal választ adjunk ügyfeleink igényeire, és biztosítsuk az ESET hatékonyságát a legújabb kártevőkkel szemben.

A választható lehetőségek az alábbiak:

Az ESET LiveGrid® megbízhatósági rendszer engedélyezése

Az ESET LiveGrid® megbízhatósági rendszer felhőalapú engedélyező- és tiltólistákat biztosít.

Ellenőrizze a Futó folyamatok és megnyitott fájlok megbízhatóságát közvetlenül a program felületén, illetve az ESET LiveGrid® rendszerből származó járulékos információkat is megjelenítő helyi menükben.

Az ESET LiveGrid® visszajelzési rendszer engedélyezése

Az ESET LiveGrid® megbízhatósági rendszeren kívül az ESET LiveGrid® visszajelzési rendszer az újonnan felfedezett kártevőkkel kapcsolatos információkat gyűjt a számítógépről. Az információk között szerepelhetnek a következők:

- Az a minta vagy fájlmásolat, amelyben a kártevő megjelent
- A fájl elérési útja
- Fájlnév
- Dátum és időpont
- Az a folyamat, amely révén a kártevő megjelent a számítógépen
- Információk a számítógép operációs rendszeréről

Az ESET Internet Security alapértelmezés szerint elküldi a gyanús fájlokat elemzésre az ESET víruslaborjába. A küldött fájlok között néhány fájltípus – például a *.doc* és az *.xls* – sosem szerepel. Megadhat további kiterjesztéseket is, ha vannak olyan fájlok, amelyeket Ön vagy a szervezete nem szeretne elküldeni.

A releváns adatok elküldéséről az Adatkezelési szabályzatban részletesen olvashat.

Az ESET LiveGrid® engedélyezésének mellőzése mellett is dönthet

A szoftver funkciói megmaradnak, bizonyos esetekben azonban előfordulhat, hogy az ESET LiveGrid® engedélyezése esetén az ESET Internet Security a keresőmotor frissítésénél gyorsabban reagál az új kártevőkre. Ha korábban engedélyezett volt az ESET LiveGrid®, a letiltás után előfordulhat, hogy maradtak még elküldendő adatcsomagok. Ezeket a program a letiltás ellenére is elküldi az ESET cégnek a következő alkalommal. Az aktuális információk elküldését követően a későbbiekben már nem készülnek további adatcsomagok.

Az ESET LiveGrid® rendszerről a szószedetben olvashat további információkat.
Tekintse meg angol és sok más nyelven rendelkezésre álló, ábrákkal ellátott útmutatónkat arról, hogy miként lehet aktiválni és letiltani az ESET LiveGrid® rendszert az ESET Internet Security alkalmazásban.

Felhőalapú védelmi konfiguráció a További beállításokban

Az ESET LiveGrid®beállításainak eléréséhez nyissa meg a **További beállítások** (F5) > **Keresőmotor** > **Felhőalapú védelem** lapot.

- **Az ESET LiveGrid® megbízhatósági rendszer engedélyezése (javasolt)** – Az ESET LiveGrid® szolgáltatása összeveti az ellenőrzött fájlokat a felhőben tárolt engedélyező- és tiltólistaelemek adatbázisával, ezáltal fokozza az ESET kártevőirtó szoftvereinek a hatékonyságát.

- **Az ESET LiveGrid® visszajelzési rendszer engedélyezése** – Elküldi a megfelelő felismerési adatokat (lásd az alábbi **Minták elküldése** szakaszban), valamint a hibajelentéseket és statisztikákat az ESET víruslaborjába további elemzés céljából.

- **Összeomlási jelentések és diagnosztikai adatok küldése** – Az ESET LiveGrid® szolgáltatással kapcsolatos diagnosztikai adatok, például összeomlási jelentések és modul-memóriaképek elküldése. A funkció aktiválását javasoljuk, mert ezzel elősegíti, hogy az ESET ki tudja vizsgálni a problémákat, fejleszteni tudja termékeit, és hatékonyabb védelmet tudjon biztosítani a végfelhasználóknak.

- **Anonim statisztikai adatok küldése** – Az ESET összegyűjtheti az újonnan észlelt kártevőkre vonatkozó információkat, többek között a kártevő nevét, az észlelés dátumát és időpontját, az észlelési módot és a kapcsolódó metaadatokat, a program verzióját és konfigurációját, beleértve az Ön rendszerének adatait.

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

Minták elküldése

Minták manuális elküldése – Lehetővé teszi, hogy manuálisan küldjön mintákat elemzésre az ESET-nek a helyi menüből, a Karanténból vagy az Eszközök menüpontból.

Az észlelt vírusminták automatikus elküldése

Válassza ki, hogy milyen típusú mintákat szeretne elküldeni az ESET-nek elemzésre és a jövőbeli észlelés javítása céljából (az alapértelmezett maximális mintaméret 64 MB). A következő lehetőségek állnak rendelkezésre:

- **Az összes észlelt minta** – Az összes olyan objektum, amelyet észlelt a keresőmotor (a kéretlen alkalmazások is, ha ez aktiválva van a víruskereső-beállításokban).
- **Az összes minta a dokumentumok kivételével** – Az összes észlelt objektum a **dokumentumok** kivételével (lásd alább).
- **Ne küldje be** – Az észlelt objektumokat nem kapja meg az ESET.

Gyanús minták automatikus elküldése

Ezeket a mintákat akkor is megkapja az ESET, ha a keresőmotor nem észlelte őket. Például olyan mintákat, amelyeknek az észlelése majdnem meghiúsult, illetve ha az ESET Internet Security védelmi moduljainak egyike gyanúsnak vagy zavaros viselkedésűnek találja a mintákat (az alapértelmezett maximális mintaméret 64 MB).

- **Végrehajtható fájlok** – Például a következő végrehajtható fájlok: .exe, .dll, .sys.
- **Tömörített fájlok** – Például a következő archívumfájltípusok: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Szkriptek** – Például a következő szkriptfájltípusok: .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Egyéb** – Például a következő fájltípusok: .jar, .reg, .msi, .sfw, .lnk.
- **Potenciális levélszemét** – Ez esetben az ESET megkapja további elemzésre a potenciális levélszemét egyes részleteit vagy teljes egészében melléklettel együtt. A beállítás engedélyezésével növelhető a levélszemét globális észlelési hatékonysága, így javulni fog a levélszemét jövőbeli észlelési hatékonysága is.
- **Dokumentumok** – Aktív tartalommal rendelkező vagy nem rendelkező Microsoft Office-, illetve PDF-dokumentumok.

Az összes benne foglalt dokumentumfájltípus listájának kibontása

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Kivételek

A Kivételek szűrővek megadhatja, hogy mely fájlokat/mappákat ne küldjön el a rendszer elemzésre (hasznos lehet például a bizalmas jellegű adatokat tartalmazó fájlok, többek között dokumentumok vagy táblázatok kizárása). Az itt felsorolt fájlokat a program még abban az esetben sem küldi el az ESET víruslaborjába elemzésre, ha gyanús kódot tartalmaznak. A leggyakoribb fájltípusok alapértelmezés szerint ki vannak zárva (.doc stb.). A kizárt fájlok listája szükség szerint bővíthető.

A `download.domain.com` webhelyről letöltött fájlok kizárásához kattintson a **További beállítások** > **Keresőmotor** > **Felhőalapú védelem** > **Minták elküldése** elemre, majd kattintson a **Szerkesztés** elemre a **Kivételek** szöveg mellett. Adja hozzá a `.download.domain.com` kizárást.

Minták maximális mérete (MB) – A minták maximális mérete (1-64 MB) határozható meg.

Kivételszűrő a Felhőalapú védelemhez

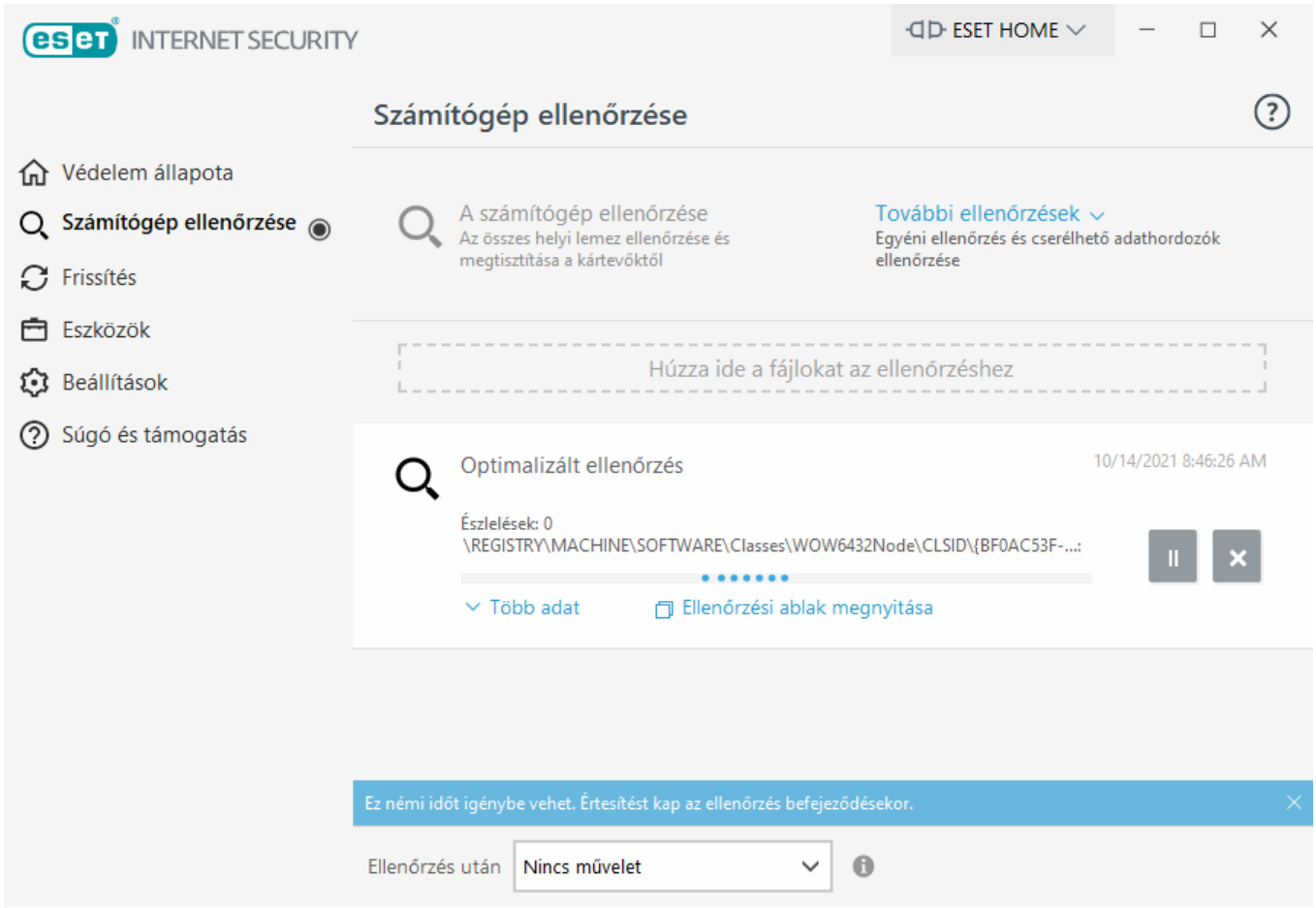
A Kivételszűrő segítségével megadhatja, hogy mely fájlokat vagy mappákat ne küldjön el a rendszer elemzésre. Az itt felsorolt fájlokat a rendszer még abban az esetben sem küldi el az ESET víruslaborjába elemzésre, ha azok gyanús kódot tartalmaznak. A gyakori fájltípusok (többek között a .doc stb.) alapértelmezés szerint ki vannak zárva.

Ez a funkció olyan fájlok kizárásához hasznos, amelyek bizalmas információkat tartalmazhatnak (például dokumentumok vagy táblázatok).

A download.domain.com webhelyről letöltött fájlok kizárásához kattintson a **További beállítások** > **Keresőmotor** > **Felhőalapú védelem** > **Minták elküldése** > **Kizárások** elemre, majd adja hozzá a *download.domain.com* kizárást.

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 a lemezre íráskor nem észlelt vírusok kiszűrése céljából. Ilyen akkor történhet, ha a Valós idejű fájlrendszervédelem ki van kapcsolva az adott időben, a keresőmotor elavult, illetve a lemezre íráskor a program nem ismeri fel vírusként a fájlt.



A **Számítógép ellenőrzése** lap kétféle ellenőrzési lehetőséget kínál A **Számítógép ellenőrzése** gyorsan átvizsgálja a rendszert; nincs szükség a vizsgálati paraméterek megadására. Az **Egyéni ellenőrzés** (a További ellenőrzések csoportban található) lehetőség esetén választhat az adott helyeket kijelölő, előre definiált ellenőrzési profilok közül, illetve kijelölhet ellenőrizendő célterületeket is.

Az ellenőrzési folyamatról Az ellenőrzés folyamata című fejezetben olvashat bővebben.

Alapértelmezés szerint az ESET Internet Security megpróbálja automatikusan megtisztítani vagy törölni a számítógép ellenőrzése során talált kártevőket. Bizonyos esetekben, ha nem hajtható végre művelet, interaktív figyelmeztetést kap, és ki kell választania egy megtisztítási műveletet (például törlés vagy figyelmen kívül hagyás). A megtisztítási szint módosításához és részletesebb információkért lásd a Tisztítás című részt. A korábbi ellenőrzések áttekintéséhez tekintse meg a Naplófájlok című részt.

A számítógép ellenőrzése

A **számítógép ellenőrzésével** gyorsan elindítható a számítógép átvizsgálása, és felhasználói beavatkozás nélkül megtisztíthatók a fertőzött fájlok. A **számítógép ellenőrzésének** előnye az egyszerű használhatóság, amely nem igényli az ellenőrzési beállítások részletes megadását. Ez az 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.

Használhatja az **Ellenőrzés húzással** funkciót egy fájl vagy mappa ellenőrzéséhez manuálisan. Ehhez húzza a fájlt vagy mappát, vigye az egérmutatót a megjelölt területre, közben tartsa lenyomva az egér gombját, majd engedje fel. Ezután az alkalmazás az előtérbe kerül.

A **További ellenőrzések** csoportban az alábbi ellenőrzési lehetőségek állnak rendelkezésre:

Egyéni ellenőrzés

Az **egyéni ellenőrzéshez** megadhatja az ellenőrzési paramétereket, többek között az ellenőrizendő célterületeket és a módokat. Az **Egyéni ellenőrzés** előnye a paraméterek részletes konfigurálásának lehetősége. A beállított paraméterek a felhasználó által definiált ellenőrizési profilokba menthetők, ami az ugyanazon beállításokkal végzett gyakori ellenőrzések során lehet hasznos.

Cserélhető adathordozók ellenőrzése

A **számítógép ellenőrzéséhez** hasonlóan gyorsan elindíthatja az aktuálisan a számítógéphez csatlakoztatott cserélhető adathordozók (például CD/DVD/USB) ellenőrzését. Ez különösen hasznos lehet akkor, ha egy USB flash meghajtót csatlakoztat egy számítógéphez, és ellenőrizni szeretné, hogy nem tartalmaz-e kártevőt, vagy nem jelent-e más miatt fenyegetést.

Az ilyen típusú ellenőrzéseket úgy is elindíthatja, hogy az **Egyéni ellenőrzés** elemre kattint, a **Cserélhető adathordozók** elemet választja az **Ellenőrizendő célterületek** legördülő listában, majd az **Ellenőrzés** gombra kattint.

Utolsó ellenőrzés megismétlése

Lehetővé teszi az előzőleg elvégzett ellenőrzés gyors elindítását a korábbi beállításokkal.

Az ellenőrzést követő művelet legördülő menüben megadhatja, hogy az ellenőrzés után milyen művelet menjen végbe automatikusan:

- **Nincs művelet** – Az ellenőrzés befejezését követően nincs végrehajtandó művelet.
- **Leállítás** – A számítógép kikapcsolása egy ellenőrzés befejezését követően.
- **Újraindítás** – Az összes program bezárása és a számítógép újraindítása egy ellenőrzés befejezését követően.
- **Újraindítás szükség esetén** – A számítógép csak akkor indul újra, ha erre szükség van az észlelt kártevők megtisztításához.
- **Újraindítás kényszerítése** – Az összes nyitott program bezárásának kényszerítése a felhasználói interakcióra való várakozás nélkül és a számítógép újraindítása az ellenőrzés befejezése után.
- **Szükség esetén az újraindítás kényszerítése** – A számítógép csak akkor indul újra, ha erre szükség van az észlelt kártevők megtisztításához.
- **Alvó állapot** – A munkamenet mentése és a számítógép alacsony energiájú állapotba állítása, hogy gyorsan folytathassa a munkát.
- **Hibernálás** – Mindent, ami a RAM-on fut, áthelyez egy adott fájlba a merevlemezen. A számítógép kikapcsol, de a legközelebbi indításakor az előző állapotot állítja vissza.

Az **Alvás** vagy **Hibernálás** művelet elérhetősége a számítógép operációs rendszerének Bekapcsolás és alvó állapot beállításaitól, illetve a számítógép/laptop funkcióitól függ. Vegye figyelembe, hogy az alvó állapotú számítógép továbbra is egy működő számítógép. Az alapfunkciók akkor is futnak és elektromos áramot használnak, amikor a számítógép csökkentett energiával működik. Az akkumulátor üzemidejének meghosszabbításához (például az irodán kívüli utazás esetén) javasoljuk, hogy használja a Hibernálás lehetőséget.

A kiválasztott művelet a futó ellenőrzések befejeződése után fog megkezdődni. A **Kikapcsolás** vagy az **Újraindítás** kiválasztása esetén a megerősítésre szolgáló párbeszédpanel megjeleníti a 30 másodperces visszaszámlálást (a **Mégse** gombra kattintva deaktiválhatja a kikapcsolást).

Javasolt legalább havonta egyszer ellenőrizni a számítógépet. Az ellenőrzés ütemezett feladatként konfigurálható az **Eszközök** > **További eszközök** > **Feladatütemező** elemre kattintva. Heti számítógép-ellenőrzés ütemezése

Egyéni ellenőrzés indítása

Egyéni ellenőrzés használatával a műveleti memóriát, a hálózatot vagy a lemez adott részeit ellenőrizheti a teljes lemez helyett. Ehhez kattintson a **További ellenőrzések** > **Egyéni ellenőrzés** elemre, majd a mappastruktúrában (fastruktúrában) jelöljön ki adott célterületeket.

Az **Profil** legördülő listában kiválaszthatja a célterületek ellenőrzéséhez használandó profilt. Az alapértelmezett profil az **Optimalizált ellenőrzés**. Három további előre megadott ellenőrzési profil áll még rendelkezésére: **Mindenre kiterjedő ellenőrzés**, **Helyi menüből indított ellenőrzés** és **Számítógép ellenőrzése**. Ezek az ellenőrzési profilok különböző ThreatSense-paramétereket használnak. A rendelkezésre álló beállítások a **További beállítások** (F5) > **Keresőmotor** > **Kártevő-ellenőrzések** > **Kézi indítású ellenőrzés** > ThreatSense-paraméterek lapon találhatók.

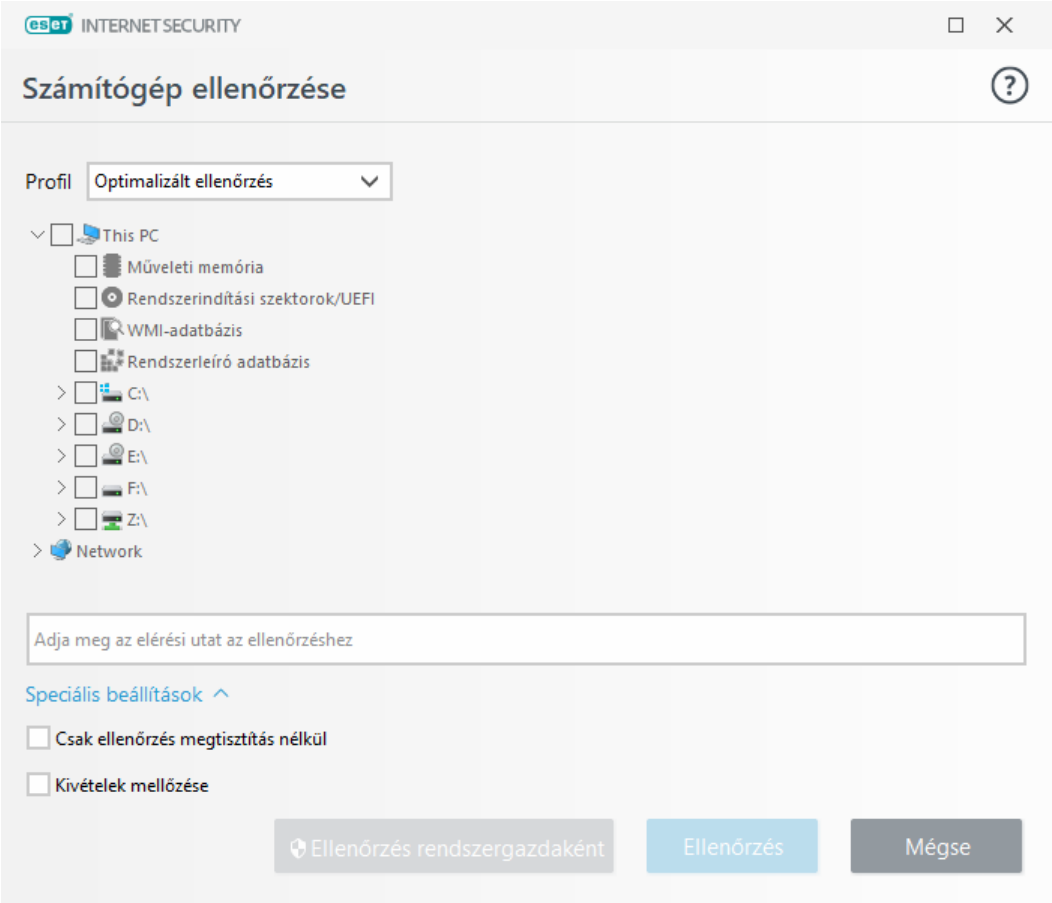
A mappa (fa) szerkezete adott ellenőrzési célterületeket is tartalmaz.

- **Műveleti memória** – A műveleti memória által aktuálisan használt összes folyamatot és adatot ellenőrzi.
- **Rendszerindítási szektorok/UEFI** – Ellenőrzi, hogy a rendszerindítási szektorokban és az UEFI-ban találhatók-e kártevők. A szószedetben bővebben olvashat az UEFI Scannerről.
- **WMI-adatbázis** – A teljes Windows Management Instrumentation WMI-adatbázis, az összes névtér, az összes osztálypéldány és az összes tulajdonság ellenőrzése. Az adatként beágyazott fertőzött fájlokra vagy kártevőkre mutató hivatkozásokat keres.
- **Rendszerleíró adatbázis** – Ellenőrzi a teljes rendszerleíró adatbázist, az összes kulcsot és alkulcsot. Az adatként beágyazott fertőzött fájlokra vagy kártevőkre mutató hivatkozásokat keres. Az észlelt elemek tisztításakor a hivatkozás a rendszerleíró adatbázisban marad, hogy ne vesszenek el fontos adatok.

Az ellenőrizendő célterülethez (fájl vagy mappa) való gyors navigálásához írja be az elérési útját a fastruktúra alatti szövegmezőbe. Az útvonal érzékeny a kis- és nagybetűkre. A célterület ellenőrzésbe való felvételéhez jelölje be a jelölőnégyzetét a fastruktúrában.

Heti számítógép-ellenőrzés ütemezése

Ha rendszeres feladatot szeretne ütemezni, olvassa el a következő fejezetet: Heti számítógép-ellenőrzés ütemezése.



Az ellenőrzés megtisztítási paramétereinek konfigurálását a következő helyen végezheti el: **További beállítások** (F5) > **Keresőmotor** > **Kézi indítású számítógép-ellenőrzés** > **ThreatSense-paraméterek** > **Megtisztítás**. Ha megtisztítás nélkül szeretne ellenőrzést futtatni, kattintson a **További beállítások** elemre, majd válassza ki a **Csak ellenőrzés megtisztítás nélkül** lehetőséget. Az ellenőrzési előzményeket a program az ellenőrzési naplóba menti.

Ha aktív a **Kivételek mellőzése** beállítás, akkor az olyan kiterjesztésű fájlok, amelyek korábban ki lettek hagyva az ellenőrzésből, most kivétel nélkül ellenőrizve lesznek.

Kattintson az **Ellenőrzés** gombra az ellenőrzés végrehajtásához a beállított egyéni paraméterek alapján.

Az **Ellenőrzés rendszergazdaként** gombbal a Rendszergazda fiókból hajthat végre ellenőrzést. Válassza ezt a lehetőséget, amennyiben az aktuális felhasználónak nincs elegendő jogosultsága az ellenőrizni kívánt fájlok eléréséhez. Ez a gomb nem érhető el akkor, ha az aktuális felhasználó nem hívhatja meg rendszergazdaként az UAC-műveleteket.

A számítógép-ellenőrzési naplót az ellenőrzés befejeződésekor a Napló megjelenítése hivatkozásra kattintva tekintheti meg.

Az ellenőrzés folyamata

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

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. További információk a tudásbáziscikkünkben találhatók.

Heti számítógép-ellenőrzés ütemezése

Ha rendszeres feladatot szeretne ütemezni, olvassa el a következő fejezetet: Heti számítógép-ellenőrzés ütemezése.

Az ellenőrzés folyamata – A folyamatjelző sáv a már ellenőrzött és az ellenőrzésre váró objektumok egymáshoz viszonyított állapotát jelzi. A program az ellenőrzési folyamat állapotát az ellenőrzésben szereplő objektumok teljes számából számítja ki.

Célterület – Az aktuálisan ellenőrzött objektum neve és helye.

Talált kártevők – Az ellenőrzött fájlok és az ellenőrzés során talált és megtisztított kártevők számát jeleníti meg.

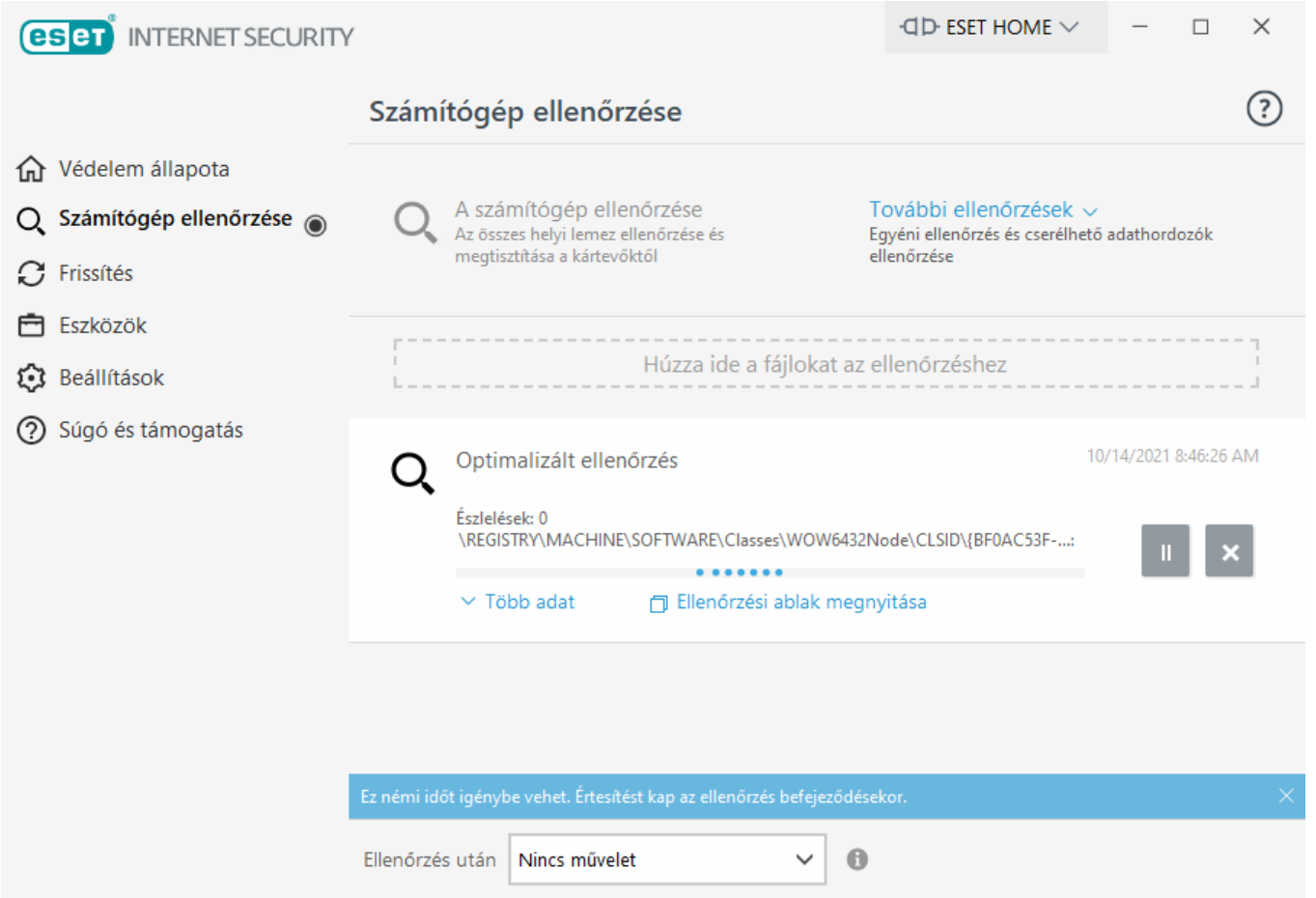
Felfüggesztés – Felfüggeszti az ellenőrzést.

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

Leállítás – Megszakítja az ellenőrzést.

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

A nagyítóra vagy a nyílra kattintva részleteket jeleníthet meg az aktuálisan futó ellenőrzésről. **A számítógép ellenőrzése** vagy a **További ellenőrzések** > **Egyéni ellenőrzés** lehetőségre kattintva párhuzamosan másik ellenőrzést is futtathat.



Az ellenőrzést követő művelet legördülő menüben megadhatja, hogy az ellenőrzés után milyen művelet menjen

végbe automatikusan:

- **Nincs művelet** – Az ellenőrzés befejezését követően nincs végrehajtandó művelet.
- **Leállítás** – A számítógép kikapcsolása egy ellenőrzés befejezését követően.
- **Újraindítás** – Az összes program bezárása és a számítógép újraindítása egy ellenőrzés befejezését követően.
- **Újraindítás szükség esetén** – A számítógép csak akkor indul újra, ha erre szükség van az észlelt kártevők megtisztításához.
- **Újraindítás kényszerítése** – Az összes nyitott program bezárásának kényszerítése a felhasználói interakcióra való várakozás nélkül és a számítógép újraindítása az ellenőrzés befejezése után.
- **Szükség esetén az újraindítás kényszerítése** – A számítógép csak akkor indul újra, ha erre szükség van az észlelt kártevők megtisztításához.
- **Alvó állapot** – A munkamenet mentése és a számítógép alacsony energiájú állapotba állítása, hogy gyorsan folytathassa a munkát.
- **Hibernálás** – Mindent, ami a RAM-on fut, áthelyez egy adott fájlba a merevlemezen. A számítógép kikapcsol, de a legközelebbi indításakor az előző állapotot állítja vissza.

> Az **Alvás** vagy **Hibernálás** művelet elérhetősége a számítógép operációs rendszerének Bekapcsolás és alvó állapot beállításaitól, illetve a számítógép/laptop funkcióitól függ. Vegye figyelembe, hogy az alvó állapotú számítógép továbbra is egy működő számítógép. Az alapfunkciók akkor is futnak és elektromos áramot használnak, amikor a számítógép csökkentett energiával működik. Az akkumulátor üzemidejének meghosszabbításához (például az irodán kívüli utazás esetén) javasoljuk, hogy használja a Hibernálás lehetőséget.

A kiválasztott művelet a futó ellenőrzések befejeződése után fog megkezdődni. A **Kikapcsolás** vagy az **Újraindítás** kiválasztása esetén a megerősítésre szolgáló párbeszédpanel megjeleníti a 30 másodperces visszaszámlálást (a **Mégse** gombra kattintva deaktiválhatja a kikapcsolást).

Számítógép-ellenőrzés naplója

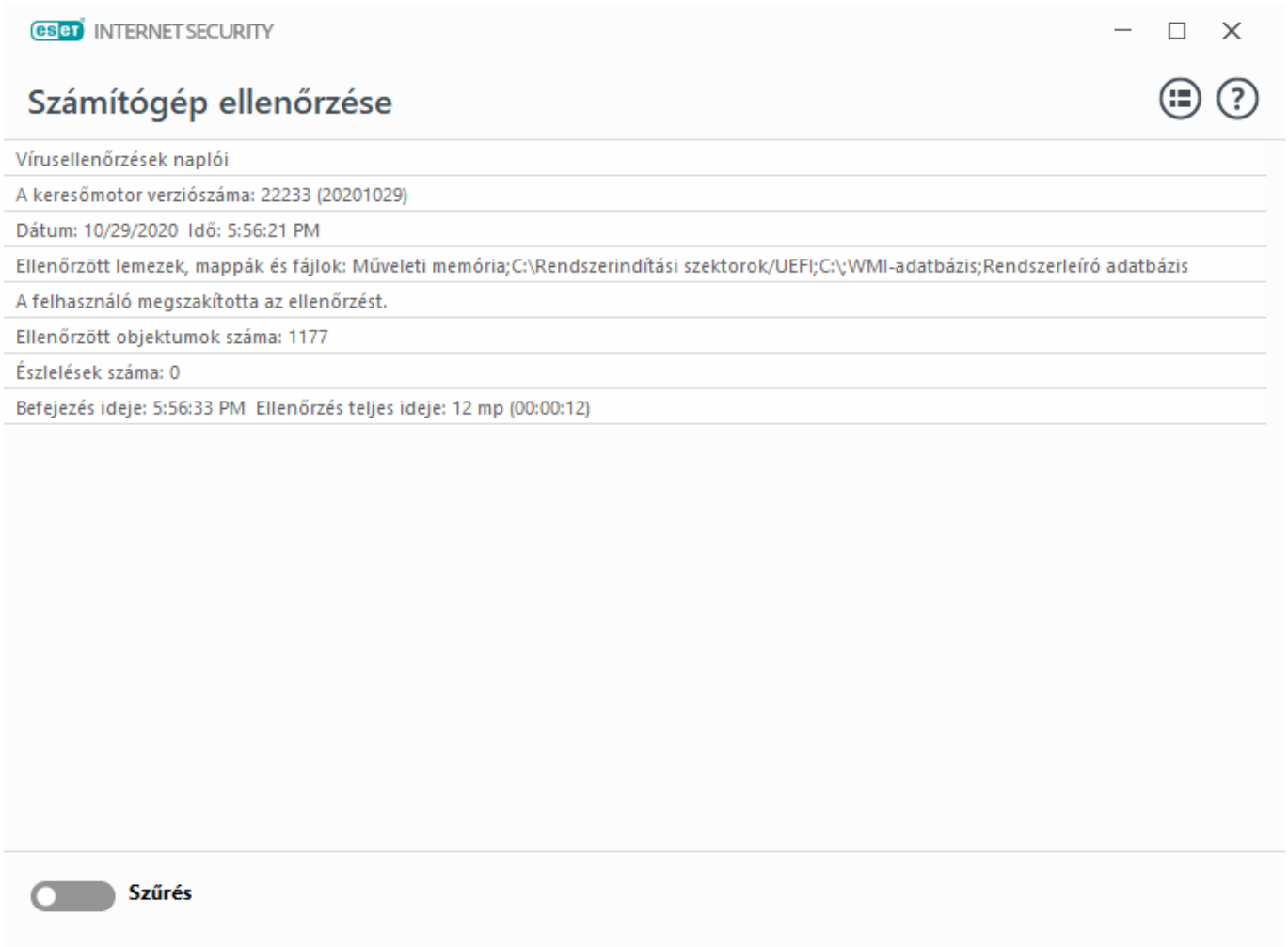
Az ellenőrzés befejeződése után megnyílik a Számítógép-ellenőrzés naplója ablak, amelyben megtalálható az adott ellenőrzéshez kapcsolódó összes információ. Az ellenőrzési napló például a következő információkat biztosítja:

- A keresőmotor verziószáma
- Kezdő dátum és időpont
- Az ellenőrzött lemezek, mappák és fájlok listája
- Ütemezett ellenőrzés neve (csak ütemezett ellenőrzés)
- Ellenőrzés állapota
- Ellenőrzött objektumok száma

- A talált kártevők száma
- Befejezés ideje
- Ellenőrzés teljes ideje

Az új ütemezett számítógép-ellenőrzési feladat elmarad, ha a korábban elindult ütemezett feladat még mindig fut. Az elmaradt ütemezett ellenőrzési feladat létrehoz egy Számítógép-ellenőrzési naplót 0 ellenőrzött objektummal és az **Az ellenőrzés nem indult el, mert még futott az előző ellenőrzés** állapottal.

A korábbi ellenőrzési naplók megkereséséhez a fő programablakban válassza ki az **Eszközök** > **További eszközök** > **Naplófájlok** menüpontot. A legördülő menüben válassza ki a **Számítógép ellenőrzése** menüpontot, majd kattintson duplán a kívánt rekordra.



Ha többet szeretne megtudni a „nem lehet megnyitni”, a „hiba a megnyitás közben”, illetve a „sérült archívum” rekordokról, olvassa el az ESET tudásbáziscikkét.

Kattintson a csúszkát ábrázoló ikonra **Szűrés** elemre a Naplószűrés ablak megnyitásához, ahol egyéni feltételek szerint szűkítheti a keresést. A helyi menü megtekintéséhez kattintson a jobb gombbal az egyik naplóbejegyzésre:

Művelet	Használat
Azonos rekordok szűrése	A naplószűrés aktiválása. A napló csak a kijelölttel megegyező típusú rekordokat jeleníti meg.

Művelet	Használat
Szűrő	Ezzel a paranccsal megnyithatja a Napló szűrése ablakot, és megadhatja bizonyos naplóbejegyzések szűrési feltételeit. Billentyűparancs: `Ctrl+Shift+F`
Szűrő letiltása	A szűrési beállítások aktiválása. Ha első alkalommal aktiválja a szűrőt, meg kell adnia a beállításokat, és megnyílik a Napló szűrése ablak.
Szűrő letiltása	A szűrő kikapcsolása (ugyanaz, mint a lenti kapcsolóra való kattintás).
Másolás	A kijelölt rekordok átmásolása a vágólapra. Billentyűparancs: `Ctrl+C`
Az összes másolása	Az ablakban lévő összes rekord bemásolása.
Exportálás	A kijelölt rekordok exportálása a vágólapra egy XML-fájlba.
Az összes exportálása	A paranccsal az ablakban lévő összes rekord átmásolható egy XML-fájlba.
Észlelt elem leírása	Megnyitja az ESET Threat Encyclopedia programot, amely részletes információkat tartalmaz a kijelölt beszivárgás veszélyeiről és tüneteiről.

Kártevő-ellenőrzések

A **Kártevőellenőrzések** szakasz a **További beállítások** (F5) > **Keresőmotor** > **Kártevőellenőrzések** útvonalon érhető el, és különböző ellenőrzési paramétereket tartalmaz. A csoportban az alábbiakban ismertetett beállítások láthatók.

Kiválasztott profil – A kézi indítású ellenőrzés által használt paraméterek csoportja. Új létrehozásához kattintson a **Szerkesztés** gombra a **Profilok listája** felirat mellett. További információkért tekintse meg az Ellenőrzési profilok című részt.

Ellenőrizendő célterületek – Ha csak egy meghatározott célterületet szeretne ellenőrizni, kattintson a **Szerkesztés** gombra az **Ellenőrizendő célterületek** felirat mellett, majd válasszon a legördülő menü elemei közül, vagy jelölje ki a kívánt célterületeket a mappastruktúrában (fastruktúrában). További információkért tekintse meg az Ellenőrizendő célterületek című részt.

A ThreatSense-paraméterek – Ebben a csoportban további beállítások találhatók (például az ellenőrizni kívánt fájlok kiterjesztése, az alkalmazott észlelési módok és így tovább). Rákattintva megnyithat egy további ellenőrzési beállításokat tartalmazó lapot.

Üresjárat idején történő ellenőrzés

Az üresjárat idején történő ellenőrzést a **További beállítások** lapon, a **Keresőmotor** > **Kártevő-ellenőrzések** > **Üresjárat idején történő ellenőrzés** szakaszban aktiválhatja.

Üresjárat idején történő ellenőrzés

A funkció engedélyezéséhez engedélyezze az **Üresjárat idején történő ellenőrzés engedélyezése** csúszkát. Ha a számítógép üresjáratban van, a program néma számítógép-ellenőrzést végez az összes helyi meghajtón.

Az üresjárat idején történő ellenőrzés alapértelmezés szerint nem fut, amikor a számítógép (hordozható számítógép) akkumulátorról működik. Felülírhatja ezt a beállítást, ha a További beállítások párbeszédpanelen engedélyezi a **Futtatás akkor is, ha a számítógép akkumulátorról működik** csúszkát.

A További beállítások lapon engedélyezze a **Naplózás engedélyezése** csúszkát, ha meg szeretné jeleníteni a

számítógép-ellenőrzés kimenetét a Naplófájlok szakaszban (a program főablakában kattintson az **Eszközök** > **További eszközök** > **Naplófájlok** elemre, majd a **Napló** legördülő listában válassza ki a **Számítógép ellenőrzése** lehetőséget.

Üresjárat idején történő ellenőrzés

Az Üresjárat idején történő ellenőrzés című részen található azoknak a feltételeknek a teljes listája, amelyeknek teljesülniük kell az üresjárat idején történő ellenőrzés kiváltásához.

A ThreatSense keresőmotor beállításai gombra kattintva módosíthatja az üresjárat idején történő ellenőrzés paramétereit (például az észlelési módokat).

Ellenőrzési profilok

Négy előre megadott ellenőrzési profilt biztosít az ESET Internet Security:

- **Optimalizált ellenőrzés** – Ez az alapértelmezett speciális ellenőrzési ellenőrzésprofil. Az intelligens ellenőrzési profil az Intelligens optimalizálási technológiát alkalmazza, amely kizárja azokat a fájlokat, amelyeket egy korábbi ellenőrzés tisztának talált, és amelyek az ellenőrzés óta nem módosultak. Ez gyorsabb ellenőrzést tesz lehetővé, ami minimális hatással van a rendszer biztonságára.

- **Helyi menüből indított ellenőrzés** – A helyi menüből elindíthatja bármely fájl kézi indítású ellenőrzését. A Helyi menü ellenőrzési profil lehetővé teszi egy ellenőrzési konfiguráció meghatározását, amely akkor fog érvényesülni, amikor ilyen módon indít ellenőrzést.

- **Mindenre kiterjedő ellenőrzés** – A részletes ellenőrzési profil alapértelmezés szerint nem használja az Intelligens optimalizálást, így egyetlen fájl sincs kizárva az ellenőrzésből a profil használatakor.

- **Számítógép ellenőrzése** – Ez a szabványos számítógépes ellenőrzés során használt alapértelmezett profil.

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

Új profil létrehozásához nyissa meg a További beállítások ablakot (az F5 billentyű lenyomásával), és kattintson a **Keresőmotor** > **Kártevőellenőrzések** > **Kézi indítású számítógép-ellenőrzés** > **Profilok listája** elemre. A **Profilkezelő** ablakban látható a meglévő ellenőrzési profilokat tartalmazó **Kiválasztott profil** legördülő lista, valamit a profilok létrehozására szolgáló lehetőség is. Ha segítségre van szüksége az igényeinek megfelelő ellenőrzési profil létrehozásával kapcsolatban, olvassa el az ellenőrzési beállítások egyes paramétereinek a leírását A ThreatSense keresőmotor beállításai című részben.

> Tegyük fel, hogy saját ellenőrzési profilt szeretne létrehozni, és **A számítógép ellenőrzése** konfiguráció részben megfelel az elképzeléseinek, nem kívánja azonban a futtatás közbeni tömörítőket vagy a veszélyes alkalmazásokat ellenőrizni, emellett **Mindig kezelje a fertőzést** szeretne alkalmazni. Írja be az új profil nevét a **Profilkezelő** ablakban, és kattintson a **Hozzáadás** gombra. Jelölje ki az új profilt a **Kiválasztott profil** legördülő menüben, és adja meg a fennmaradó paraméterek beállításait úgy, hogy megfeleljenek a követelményeknek, majd kattintson az **OK** gombra az új profil mentéséhez.

Ellenőrizendő célterületek

Az **Ellenőrizendő célterületek** legördülő listában előre definiált célterületeket választhat ki.

- **Profilbeállítások alapján** – A kijelölt ellenőrzési profilban meghatározott célterületeket ellenőrzi.
- **Cserélhető adathordozó** – A hajlékonylemezeket, USB-tárolóeszközöket, CD és DVD lemezeket ellenőrzi.
- **Helyi meghajtók** – Kijelöli az összes helyi meghajtót.
- **Hálózati meghajtók** – Kijelöli az összes csatlakoztatott hálózati meghajtót.
- **Egyéni kiválasztás** – Visszavonja az összes korábbi kiválasztást.

A mappa (fa) szerkezete adott ellenőrzési célterületeket is tartalmaz.

- **Műveleti memória** – A műveleti memória által aktuálisan használt összes folyamatot és adatot ellenőrzi.
- **Rendszerindítási szektorok/UEFI** – Ellenőrzi, hogy a rendszerindítási szektorokban és az UEFI-ban találhatók-e kártevők. A szószedetben bővebben olvashat az UEFI Scannerről.
- **WMI-adatbázis** – A teljes Windows Management Instrumentation WMI-adatbázis, az összes névtér, az összes osztálypéldány és az összes tulajdonság ellenőrzése. Az adatként beágyazott fertőzött fájlokra vagy kártevőkre mutató hivatkozásokat keres.
- **Rendszerleíró adatbázis** – Ellenőrzi a teljes rendszerleíró adatbázist, az összes kulcsot és alkulcsot. Az adatként beágyazott fertőzött fájlokra vagy kártevőkre mutató hivatkozásokat keres. Az észlelt elemek tisztításakor a hivatkozás a rendszerleíró adatbázisban marad, hogy ne vesszenek el fontos adatok.

Az ellenőrizendő célterülethez (fájl vagy mappa) való gyors navigálásához írja be az elérési útját a fastruktúra alatti szövegmezőbe. Az útvonal érzékeny a kis- és nagybetűkre. A célterület ellenőrzésbe való felvételéhez jelölje be a jelölőnégyzetét a fastruktúrában.

Eszközfelügyelet

Az ESET Internet Security lehetővé teszi a cserélhető adathordozók (CD/DVD/USB stb.) felügyeletét. Ez a modul lehetővé teszi a kiterjesztett szűrők/engedélyek 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 eszközöket használjanak.

Támogatott külső eszközök:

- Lemezes tárhely (HDD, USB-s cserélhető lemez)
- CD/DVD
- Nyomtató USB
- FireWire Tárhely

- Bluetooth Eszköz
- Intelligenskártya-olvasó
- Képeszköz
- Modem
- LPT/COM port
- Hordozható eszköz
- Minden eszköztípus

Az eszközfelügyelet beállítási lehetőségei a **További beállítások** (F5) > **Eszközfelügyelet** részen módosíthatók.

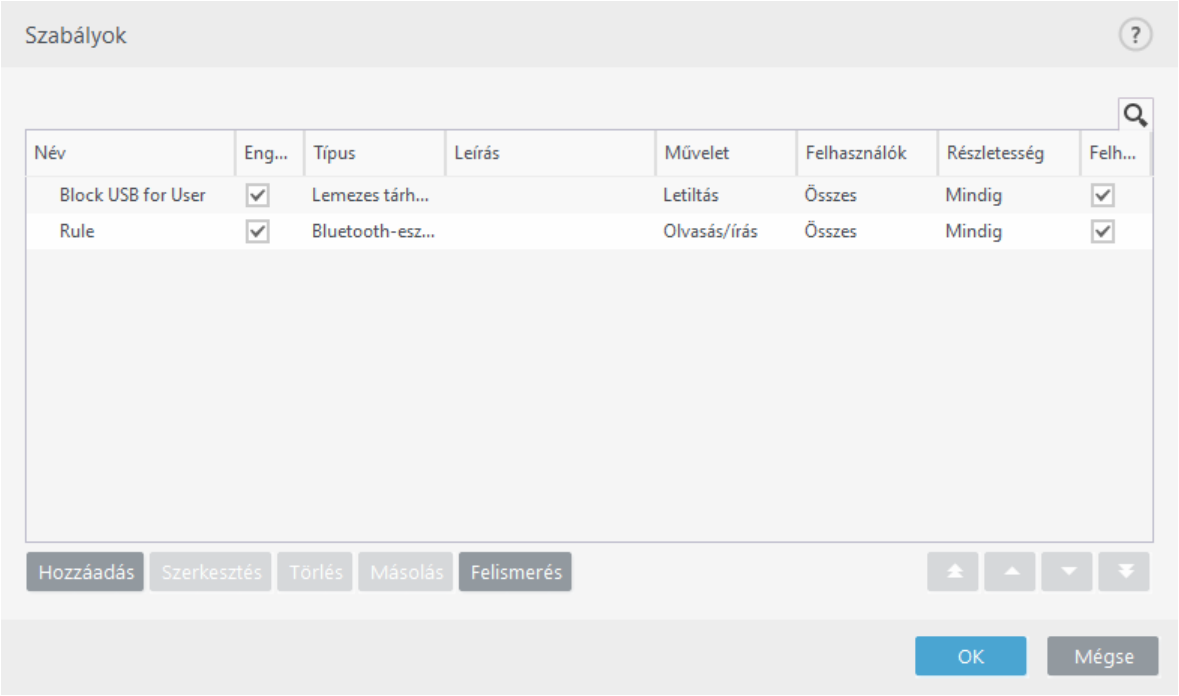
Az eszközfelügyelet engedélyezése szöveg melletti csúszka engedélyezésével aktiválható az ESET Internet Security Eszközfelügyelet funkciója; a módosítás érvénybelépéséhez újra kell indítani a számítógépet. Az Eszközfelügyelet engedélyezését követően aktív lesz a **Szabályok** gomb, amellyel megnyithatja a Szabályszerkesztő ablakot.

> Létrehozhat különböző eszközcsoportokat, amelyekre különböző szabályok vonatkoznak. Egyetlen csoportot is létrehozhat, amelyre az **Olvasás/írás** vagy a **Csak olvasás** műveletszabály vonatkozik. Ez biztosítja, hogy az Eszközfelügyelet letiltsa az ismeretlen eszközöket, amikor a számítógépéhez csatlakoznak.

Ha beszúr egy meglévő szabály által letiltott eszközt, megjelenik egy értesítési ablak, és megszűnik az eszközhöz való hozzáférés.

Eszközfelügyeleti szabályok szerkesztője

Az **Eszközfelügyeleti szabályok szerkesztője** ablak megjeleníti a külső eszközök meglévő szabályait, és lehetővé teszi a felhasználók által a számítógéphez csatlakoztatott külső eszközök pontos vezérlését.



A szabály konfigurációjában megadható további eszközparaméterek alapján adott eszközök engedélyezhetők vagy tilthatók le felhasználók vagy felhasználócsoportok szerint. A szabálylista az adott szabályokra vonatkozó leírásokat, többek között a külső eszköz nevét, típusát, a külső eszköz számítógéphez való csatlakoztatása után végrehajtandó műveletet és a napló súlyosságát tartalmazza. Tekintse meg a következőt is: Eszközfelügyeleti szabályok hozzáadása.

Szabály kezeléséhez kattintson a **Hozzáadás** vagy a **Szerkesztés** gombra. A **Másolás** gombra kattintva létrehozhat egy új szabályt egy másik kijelölt szabályhoz használt előre definiált beállításokkal. A szabályokra kattintáskor megjelenített XML-karakterláncok a vágólapra másolhatók vagy a rendszergazdákat segíthetik ezeknek az adatoknak az exportálásában/importálásában és használatában az programban.

A **CTRL** billentyűt lenyomva kattintással több szabályt is kijelölhet, és műveleteket alkalmazhat, többek között törölheti vagy a listában felfelé és lefelé helyezheti azokat, az összes kijelölt szabályhoz. Az **Engedélyezve** jelölőnégyzet bejelölése letiltja vagy engedélyezi ezt a szabályt; ez akkor lehet hasznos, ha a jövőben használni szeretné, ezért nem kívánja véglegesen törölni a szabályt.

A felügyelet szabályokkal végezhető el, amelyek a legnagyobb prioritásúval kezdődően, a prioritásuk sorrendben rendezettek.

A naplóbejegyzések az ESET Internet Security főablakában az **Eszközök** > **További eszközök** > **Naplófájlok** lehetőségére kattintva érhetők el.

Az Eszközfelügyelet naplója feljegyzi az eszközfelügyeletet kiváltó összes eseményt.

Észlelt eszközök

A **Felismerés** gombbal áttekintést kaphat az éppen csatlakoztatott eszközökről, az alábbi adatok formájában: eszköztípus, eszközgyártó, típus és sorozatszám (ha van).

Jelöljön ki egy eszközt az Észlelt eszközök listájában, majd kattintson az **OK** gombra kattintva adjon hozzá egy eszközfelügyeleti szabályt előre meghatározott információkkal (minden beállítás módosítható).

Az alacsony fogyasztású (alvó) üzemmódban lévő eszközöket figyelmeztető ikon jelöli . Az **OK** gomb engedélyezése és egy szabály hozzáadása az eszközhöz:

- Csatlakoztassa újra az eszközt
- Vegye használatba az eszközt (például indítsa el a Kamera alkalmazást a Windows rendszerben a webkamera felébresztéséhez)

Eszközcsoportok

A számítógépéhez csatlakoztatott eszközök biztonsági kockázatot jelenthetnek.

Az Eszközcsoportok ablak két részből áll. Az ablak jobb oldali részén az adott csoporthoz tartozó eszközök listája látható, a bal oldalon pedig létrehozott csoportok találhatók. Jelölje ki azt az eszközlistával rendelkező csoportot, amelyet a jobb oldali ablaktáblában meg szeretne jeleníteni.

Az Eszközcsoportok ablak megnyitásakor és egy csoport kijelölésekor felvehet a listára, illetve eltávolíthat róla eszközöket. Másik lehetőségként egy fájlból történő importálással is hozzáadhat eszközöket a csoporthoz. Ezenkívül kattinthat a **Felismerés** gombra is, és ezt követően a számítógépéhez csatlakoztatott összes eszköz listája látható lesz az **Észlelt eszközök** ablakban. Jelöljön ki egy eszközt a listában, és az **OK** gombra kattintva adja a csoporthoz.

Vezérlőelemek

Hozzáadás – A nevét megadva hozzáadhat egy csoportot, illetve egy eszközt a meglévő csoporthoz attól függően, hogy az ablak mely részén kattintott a gombra (részleteket, többek között a gyártó nevét, típust és sorozatszámot is megadhat).

Szerkesztés – Módosíthatja a kijelölt csoport nevét vagy az eszköz paramétereit (a gyártót, a típust, a sorozatszámot).

Törlés – A kijelölt csoport vagy eszköz törlése, attól függően, hogy az ablak mely részén kattintott a gombra.

Importálás – Eszközlista importálása szövegfájlból. Az eszközök szövegfájlból történő importálásához helyes formázás szükséges:

- Mindegyik eszköz új sorban kezdődik.
- A **gyártónak**, a **modellnek** és a **sorozatszámnak** minden eszköznél szerepelnie kell, és vesszővel kell elválasztani őket.

Íme egy példa a szövegfájl tartalmára:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exportálás – Eszközlisa exportálása fájlba.

A **Felismerés** gombbal áttekintést kaphat az éppen csatlakoztatott eszközökről, az alábbi adatok formájában: eszköztípus, eszközgyártó, típus és sorozatszám (ha van).

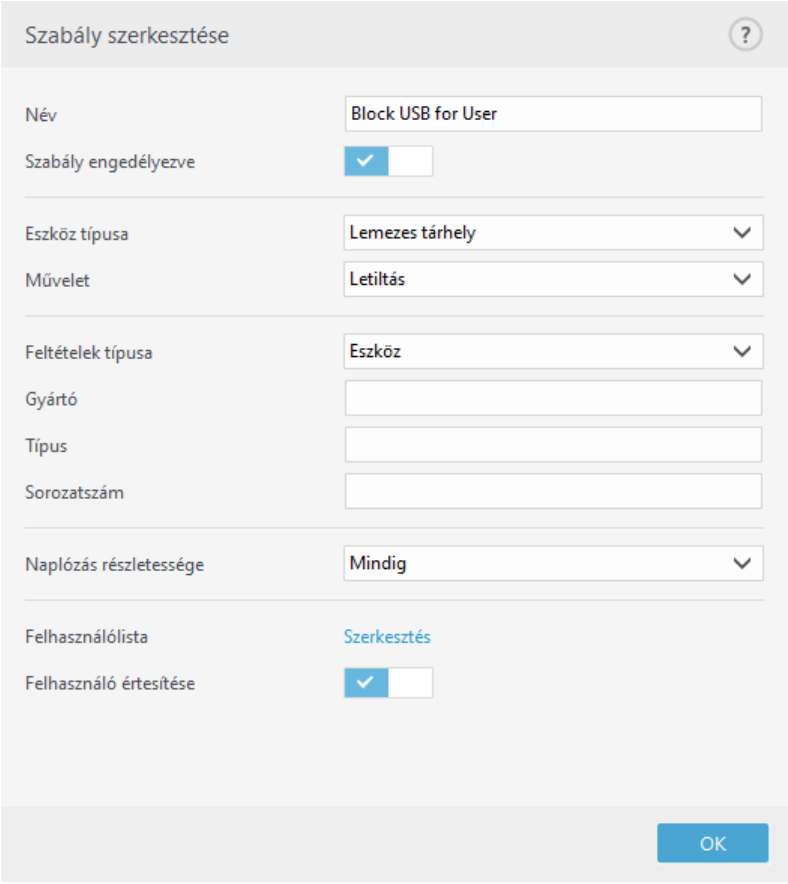
Amikor elkészült a testreszabással, kattintson az **OK** gombra. A **Mégse** gombra kattintva a módosítások mentése nélkül bezárhatja az **Eszközcsoportok** ablakot.

Létrehozhat különböző eszközcsoportokat, amelyekre különböző szabályok vonatkoznak. Egyetlen csoportot is létrehozhat, amelyre az **Olvasás/írás** vagy a **Csak olvasás** műveletszabály vonatkozik. Ez biztosítja, hogy az Eszközfelügyelet letiltsa az ismeretlen eszközöket, amikor a számítógépéhez csatlakoznak.

Vegye figyelembe, hogy nem minden művelet (engedély) érhető el az összes eszköztípushoz. Ha ez egy tároló típusú eszköz, mind a négy művelet elérhető. Nem tárolásra szolgáló eszközök esetén csak három művelet választható (a **Csak olvasás** például nem érhető el a Bluetooth-eszközök esetén, így azok csak engedélyezhetők, letilthatók vagy figyelmeztethetők).

Eszközfelügyeleti szabályok hozzáadása

Az eszközfelügyeleti szabályok határozzák meg, hogy milyen műveletet kell végrehajtani, amikor a szabályfeltételeket teljesítő eszköz csatlakozik a számítógéphez.



A **Név** mezőbe írt leírás segítségével a könnyebben azonosítható. A szabály letiltásához vagy engedélyezéséhez kattintson a **Szabály engedélyezve** felirat melletti csúszka. Ez akkor lehet hasznos, ha nem szeretné véglegesen törölni a szabályt.

Eszköz típusa

A legördülő menüben válassza ki a külső eszköz típusát (Lemezes tárhely/Hordozható eszköz/Bluetooth/FireWire/...). Az eszközök típusára vonatkozó információt az operációs rendszerből gyűjti össze a program, és a rendszer eszközkezelőjében látható, ha egy eszköz csatlakozik a számítógéphez. A tárolóeszközök közé tartoznak az USB-n vagy FireWire-eszközön keresztül csatlakoztatott külső lemezek vagy a hagyományos memóriakártya-olvasók. Az intelligenskártya-olvasók közé tartoznak a beágyazott integrált áramkörrel rendelkező

intelligens kártyák, például a SIM vagy a hitelesítési kártyák. Képeszközök többek között a képolvasók és a fényképezőgépek. Mivel ezek az eszközök csak a saját műveleteikről adnak meg információkat, a felhasználókról nem, csak globálisan tilthatók le.

Művelet

A nem tárolásra szolgáló eszközök hozzáférését lehet engedélyezni vagy letiltani. A tárolóeszközök szabályai esetén ezzel szemben választhat legalább egyet az alábbi jogosultságok közül:

- **Olvasás/Írás** – Teljes hozzáférést engedélyez az eszközhöz.
- **Tiltás** – Letiltja a hozzáférést az eszközhöz.
- **Csak olvasás** – Csak olvasási hozzáférést engedélyez az eszközhöz.
- **Figyelmeztetés** – Valahányszor csatlakozik egy eszköz, a rendszer értesíti a felhasználót, hogy az engedélyezett vagy letiltott-e, és készít egy naplóbejegyzést. A rendszer nem jegyzi meg az eszközöket, így ugyanazon eszköz következő kapcsolódásaikor is megjelenik egy értesítés.

Vegye figyelembe, hogy nem minden művelet (engedély) érhető el az összes eszköztípushoz. Ha ez egy tároló típusú eszköz, mind a négy művelet elérhető. Nem tárolásra szolgáló eszközök esetén csak három művelet választható (a **Csak olvasás** például nem érhető el a Bluetooth-eszközök esetén, így azok csak engedélyezhetők, letilthatók vagy figyelmeztethetők).

Feltételek típusa

– Az **Eszközcsoport** vagy az **Eszköz** elem közül választhat.

Az alább látható további paraméterek szabályok pontosításához és adott eszközök testreszabásához használhatók. A kis- és nagybetűk között minden paraméterben különbséget kell tenni:

- **Gyártó** – Szűrés a gyártói név vagy ID szerint.
- **Típus** – Az eszköz elnevezése.
- **Sorozatszám** – A külső eszközök rendszerint saját sorozatszámmal rendelkeznek. CD/DVD esetén ez nem a CD-meghajtó, hanem az adathordozó sorozatszáma.

Ha ezek a parancsok nincsenek megadva, a megfeleltetéskor a szabály mellőzi ezeket a mezőket. A szűrési paramétereknél egyik szöveges mező sem tesz különbséget a kis- és a nagybetűk között, és nem használhatók helyettesítő karakterek (*, ?).

Ha információkat szeretne megjeleníteni egy eszközről, hozzon létre egy szabályt az adott eszköztípushoz, csatlakoztassa az eszközt a számítógépéhez, majd ellenőrizze az eszköz adatait az Eszközfelügyelet naplójában.

Naplózás részletessége

Az ESET Internet Security a fontos eseményeket egy naplófájlba menti, amely közvetlenül a fő menüből megtekinthető. Kattintson az **Eszközök** > **További eszközök** > **Naplófájlok** hivatkozásra, majd a **Napló** legördülő menüben válassza ki az **Eszközfelügyelet** menüpontot.

- **Mindig** – Az összes esemény naplózása.

- **Diagnosztikai** – A program pontos beállításához szükséges információk naplózása.
- **Információk** – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett bejegyzéseket).
- **Figyelmeztetés** – Kritikus figyelmeztetések és figyelmeztető üzenetek rögzítése.
- **Nincs** – Nem rögzít naplókat.

Felhasználólista

A szabályok bizonyos felhasználókra vagy felhasználócsoportokra korlátozhatók, ha felveszi őket a felhasználólistára a **Szerkesztés** elemre kattintva, amely a **Felhasználólista** felirat mellett található.

- **Hozzáadás** – Megnyitja az **Objektumtípusok: Felhasználók és csoportok** párbeszédpanelt, amelyen kiválaszthatja a kívánt felhasználókat.
- **Eltávolítás** – Eltávolítja a szűrőből a kijelölt felhasználót.

Felhasználólistára vonatkozó korlátozások

A Felhasználólistánál nem definiálhatók szabályok bizonyos eszköztípusok esetén:

- USB-nyomtató
- Bluetooth-eszköz
- Intelligenskártya-olvasó
- Képeszköz
- Modem
- LPT/COM port

Felhasználó értesítése – Ha beszúr egy meglévő szabály által letiltott eszközt, megjelenik egy értesítési ablak.

Webkamera-védelem

A **Webkamera-védelem** funkció segítségével megtekintheti a számítógép webkamerájához hozzáférő folyamatokat és alkalmazásokat. Ha egy alkalmazás kísérel meg hozzáférni a kamerához, megjelenik egy értesítés ablak, ahol lehetősége van **engedélyezni** vagy **letiltani** a nemkívánatos folyamatok vagy alkalmazások hozzáférését a kamerához. Az értesítési ablak színe az adott alkalmazás megbízhatóságától függ.

A Webkamera-védelem beállítási lehetőségei a **További beállítások** (F5) > **Eszközfelügyelet** > **Webkamera-védelem** szakaszban módosíthatók.

A Webkamera-védelem funkció aktiválásához az ESET Internet Security szolgáltatásban engedélyezze a **Webkamera-védelem engedélyezése** felirat melletti csúszkát.

A Webkamera-védelem funkció engedélyezését követően aktív lesz a **Szabályok** gomb, amellyel megnyithatja a Szabályszerkesztő ablakot.

Ha ki szeretné kapcsolni az olyan alkalmazásokra vonatkozó figyelmeztetéseket, amelyek módosultak, de még mindig rendelkeznek érvényes digitális aláírással (például alkalmazásfrissítés), engedélyezze a **Webkamera-hozzáférési riasztások letiltása módosított alkalmazások esetén** melletti csúszkát.

Webkamera-védelem szabályszerkesztője

Ez az ablak a meglévő szabályokat jeleníti meg, és lehetőséget ad azoknak az alkalmazásoknak és folyamatoknak a szabályozása, amely az Ön által végzett művelet alapján hozzáfér a számítógép webkamerájához.

A választható műveletek az alábbiak:

- **Hozzáférés engedélyezése**
- **Hozzáférés letiltása**

- **Rákérdezés** (megkérdezi a a felhasználót minden alkalommal, amikor egy alkalmazás megpróbál hozzáférni a webkamerához)

Törölje a jelet az **Értesítés** oszlopban az értesítések fogadásának leállításához, ha egy alkalmazás hozzáfér a webkamerához.

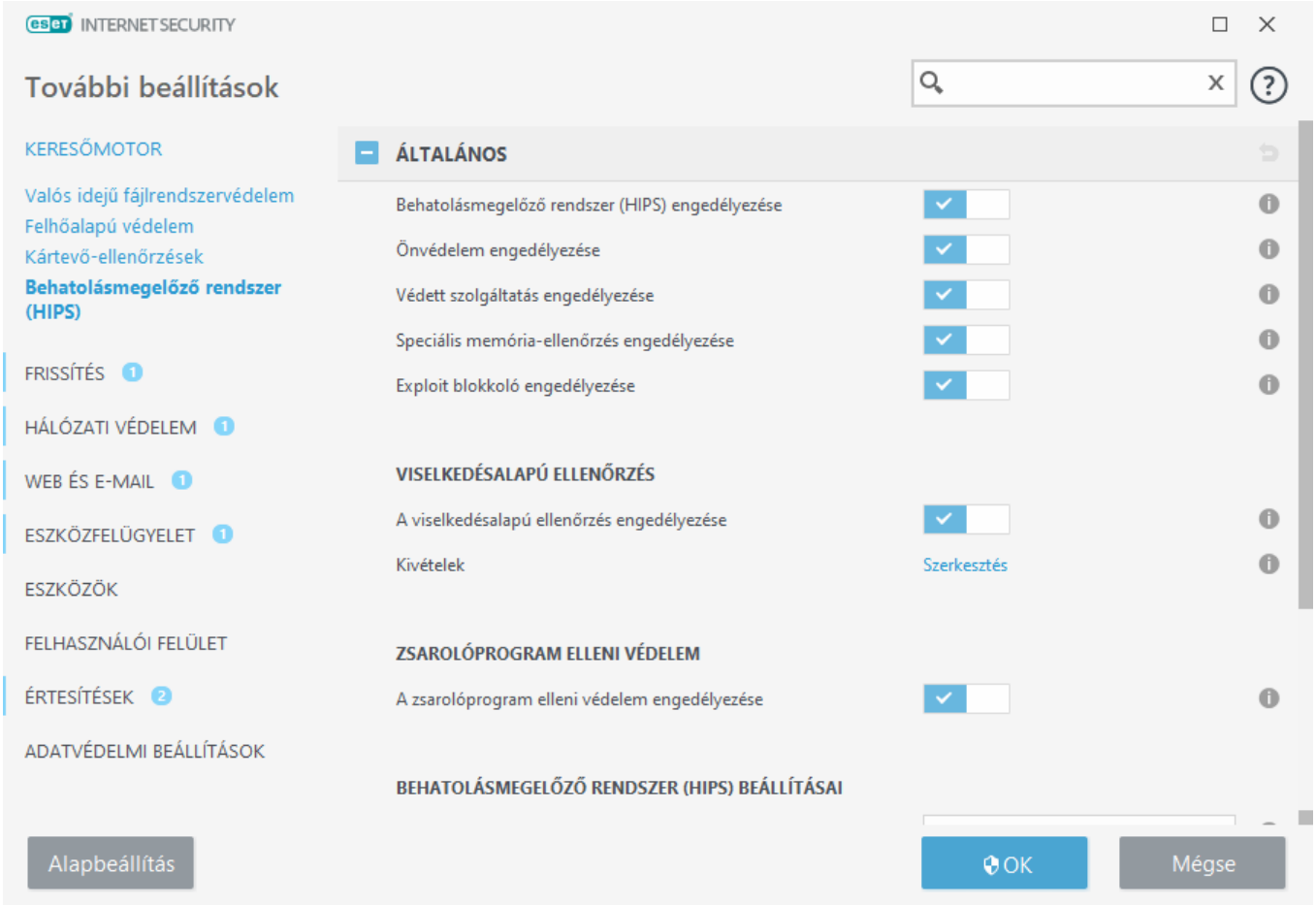
Ábrákkal ellátott útmutató
Webkamera-szabályok létrehozása és szerkesztése a ESET Internet Security szolgáltatásban.

Behatolásmegelőző rendszer (HIPS)

A behatolásmegelőző rendszer beállításainak módosítását csak tapasztalt felhasználóknak javasoljuk. A helytelen konfiguráció a rendszer instabilitásához vezethet.

A **Behatolásmegelőző rendszer (HIPS)** 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. A Behatolásmegelőző rendszer különbözik a valós idejű fájlrendszervédelemtől, és nem is tűzfal; csak az operációs rendszeren belül futó folyamatokat figyeli.

A Behatolásmegelőző rendszer beállításainak megjelenítéséhez válassza a **További beállítások** (F5) > **Keresőmotor** > **Behatolásmegelőző rendszer** > **Általános** elemet. A Behatolásmegelőző rendszer állapota (engedélyezve/letiltva) az ESET Internet Security fő programablakának **Beállítások** > **Számítógép-védelem** csoportjában látható.



Általános

Behatolásmegelőző rendszer engedélyezése – A Behatolásmegelőző rendszer engedélyezve van alapértelmezés szerint az ESET Internet Security programban. A Behatolásmegelőző rendszer kikapcsolásakor inaktiválódik a Behatolásmegelőző rendszer összes funkciója, például az Exploit blokkoló.

Önvédelem engedélyezése – Az ESET Internet Security beépített **önvédelmi** technológiával rendelkezik a behatolásmegelőző rendszer részeként, amely megakadályozza, hogy a kártevőprogramok károsítsák vagy letiltsák a vírus- és kémprogramvédelmet. Az önvédelem megakadályozza, hogy módosítani lehessen a rendkívül fontos rendszerfolyamatokat, az ESET folyamatait, a beállításkulcsokat és a fájlokat.

Védett szolgáltatás engedélyezése – az ESET szolgáltatás (ekrn.exe) megvédése. Ha engedélyezi a funkciót, akkor a szolgáltatás védett Windows-folyamatként indul el a kártevők támadásainak elhárítása érdekében. A funkció a Windows 8.1 rendszerben és az újabb verziókban áll rendelkezésre.

Speciális memória-ellenőrzés engedélyezése – az Exploit blokkolóval együttműködve erősíti a kártevőirtók általi észlelés elkerüléséhez összezavarást vagy titkosítást használó kártevőkkel szembeni védelmet. A speciális memória-ellenőrzés alapértelmezés szerint engedélyezve van. A védelem e típusáról a szószedetben olvashat bővebben.

Exploit blokkoló engedélyezése – a támadásoknak gyakran kitett alkalmazástípusok, például webböngészők, PDF-olvasók, levelezőprogramok és MS Office-összetevők megerősítésére szolgál. Az Exploit blokkoló alapértelmezés szerint engedélyezve van. A védelem e típusáról a szószedetben olvashat bővebben.

Viselkedésalapú ellenőrzés

A viselkedésalapú ellenőrzés engedélyezése – További védelmet biztosít, és a HIPS (Behatolásmegelőző rendszer) részeként működik. Ez a HIPS-bővítmény elemzi a számítógépen futó összes programot, és figyelmeztet, ha valamelyik folyamat viselkedése kártékony.

A HIPS-kivételek a viselkedésalapú ellenőrzés alól csoportban folyamatokat zárhat ki az elemzésből. Ha azt szeretné, hogy a program minden folyamatot megvizsgáljon a potenciális kártevők kiszűrése érdekében, azt javasoljuk, hogy csak akkor hozzon létre kivételeket, ha ez feltétlenül szükséges.

Zsarolóprogram elleni védelem

Zsarolóprogram elleni védelem engedélyezése – a védelem egy további rétege, amely a behatolásmegelőző funkció részeként működik. A Zsarolóprogram elleni védelem működéséhez engedélyeznie kell a ESET LiveGrid® értékelési rendszert. A védelem e típusáról itt olvashat bővebben.

HIPS-beállítások

A **Szűrési üzemmód** a következő üzemmódok egyikében használható:

Szűrési üzemmód	Leírás
Automatikus üzemmód	A műveletek a rendszer védelmét biztosító, előre megadott szabályok által tiltottak kivételével engedélyezettek.
Optimalizált mód	A felhasználó csak a nagyon gyanús eseményekről kap értesítést.
Interaktív üzemmód	A felhasználónak minden műveletet meg kell erősítenie.
Házirendalapú üzemmód	az összes olyan művelet letiltása, amelyet nem engedélyez egy adott szabály.
Tanuló mód	A műveletek engedélyezettek, és mindegyikhez létrejön egy szabály. Az ebben a módban létrehozott szabályok megtekinthetők a **Behatolásmegelőző rendszer (HIPS) szabályai** ablakban, prioritásuk azonban alacsonyabb a manuálisan és az automatikus módban létrehozott szabályokénál. Amikor kijelöli a **Tanuló módot** a **Szűrési üzemmód** legördülő menüben, **A tanuló mód befejezési időpontja** beállítás elérhetővé válik. Válassza ki a tanuló módhoz rendelni kívánt időtartamot. A maximális időtartam 14 nap. A megadott időtartam leteltét követően a program kérni fogja a tanuló módban a Behatolásmegelőző rendszer által létrehozott szabályok szerkesztését. Választhat másik szűrési üzemmódot, vagy elhalaszthatja a döntést, és tovább használhatja a tanuló módot.

A tanuló mód lejárata után beállított mód – Kiválaszthatja a tanuló mód lejárata után használandó szűrési módot. A lejáratot követően a **Rákérdez** beállítás esetén rendszergazdai jogosultságok szükségesek ahhoz, hogy módosítani lehessen a Behatolásmegelőző rendszer (HIPS) szűrési üzemmódját.

A behatolásmegelőző rendszer figyeli az operációs rendszerben zajló eseményeket, és a szabályoknak megfelelően reagál rájuk. A **Szabályok** felirat melletti **Szerkesztés** gombra kattintva megnyithatja a **Behatolásmegelőző rendszer (HIPS)** Párbeszédpaneljét, ahol kijelölheti, hozzáadhatja, szerkesztheti és eltávolíthatja a szabályokat. A szabályok létrehozásáról és a Behatolásmegelőző rendszer (HIPS) működéséről a következő rész tartalmaz további információkat: Behatolásmegelőző rendszer szabályainak szerkesztése.

A Behatolásmegelőző rendszer interaktív ablaka

A Behatolásmegelőző rendszer értesítő ablaka lehetővé teszi, hogy létrehozzon egy szabályt olyan új műveletekhez, amelyeket a Behatolásmegelőző rendszer észlel, majd megadja azokat a feltételeket, amelyek esetén engedélyezi, illetve megakadályozza az adott műveletet.

Az értesítő ablakban létrehozott szabályok egyenértékűek a manuálisan létrehozott szabályokkal. Az értesítő ablakban létrehozott szabályok lehetnek kevésbé pontosak, mint a párbeszédpanel megjelenítését kiváltó szabály. Ez azt jelenti, hogy a szabály párbeszédpanelen való létrehozása után ugyanaz a művelet megjelenítheti ugyanazt a párbeszédpanelt. További információkért tekintse meg a következő részt: A Behatolásmegelőző rendszer szabályainak prioritása.

Ha egy szabályhoz alapértelmezés szerint a **Mindig rákérdez** van megadva, a szabály aktiválásakor minden alkalommal megjelenik egy párbeszédpanel. Ezen választhatja a művelet **tiltását** vagy **engedélyezését** is. Ha a megadott időn belül nem választ műveletet, a rendszer a szabályok alapján dönt a végrehajtandó műveletről.

A **Művelet ideiglenes megjegyzése a jelenlegi munkamenetre** beállítás hatására a rendszer az **Engedélyezés/Tiltás** műveletet használja addig, amíg meg nem változtatja a szabályokat vagy a szűrési üzemmódot, nem frissíti a Behatolásmegelőző rendszer modult, illetve újra nem indítja a rendszert. E három művelet bármelyikét követően a program törli az ideiglenes szabályokat.

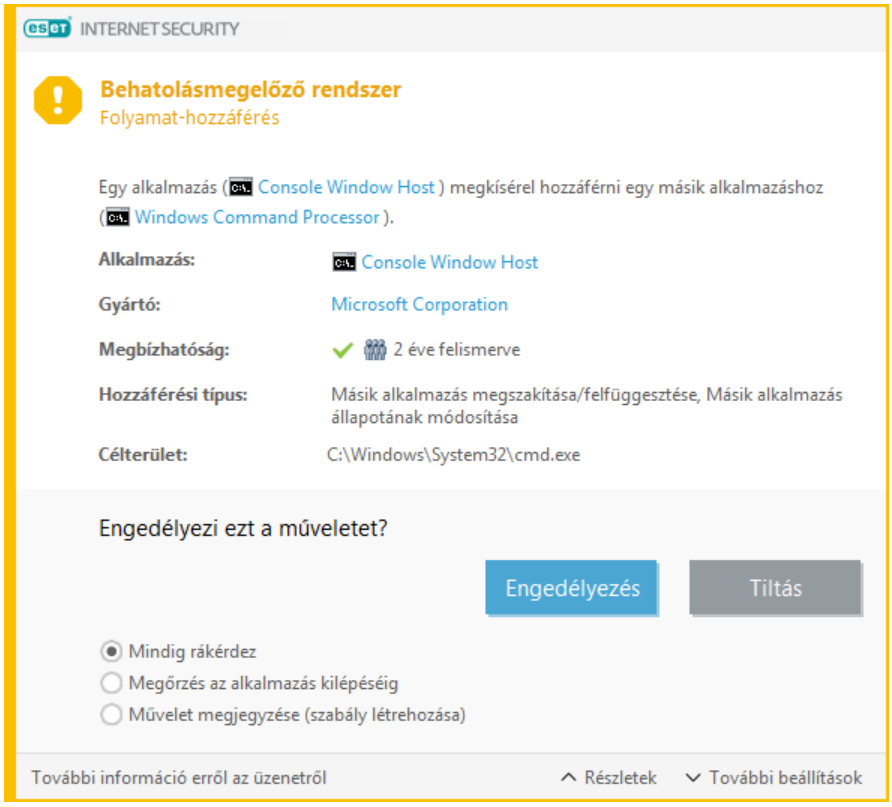
A **Művelet megjegyzése (szabály létrehozása)** funkció új Behatolásmegelőző rendszer-szabályt hoz létre, amely később módosítható a Behatolásmegelőző rendszer szabályainak kezelése szakaszban (rendszergazdai jogosultságra van szükség).

A lent található **Részletek** elemre kattintva megtekintheti, hogy mely alkalmazás váltja ki a műveletet, mennyire megbízható a fájl, illetve hogy Ön milyen műveletet engedélyez vagy tilt.

Részletesebb szabályok a **További beállítások** lapon adhatók meg. Az alábbi lehetőségek akkor állnak a rendelkezésére, ha kiválasztja a **Művelet megjegyzése (szabály létrehozása)** beállítást:

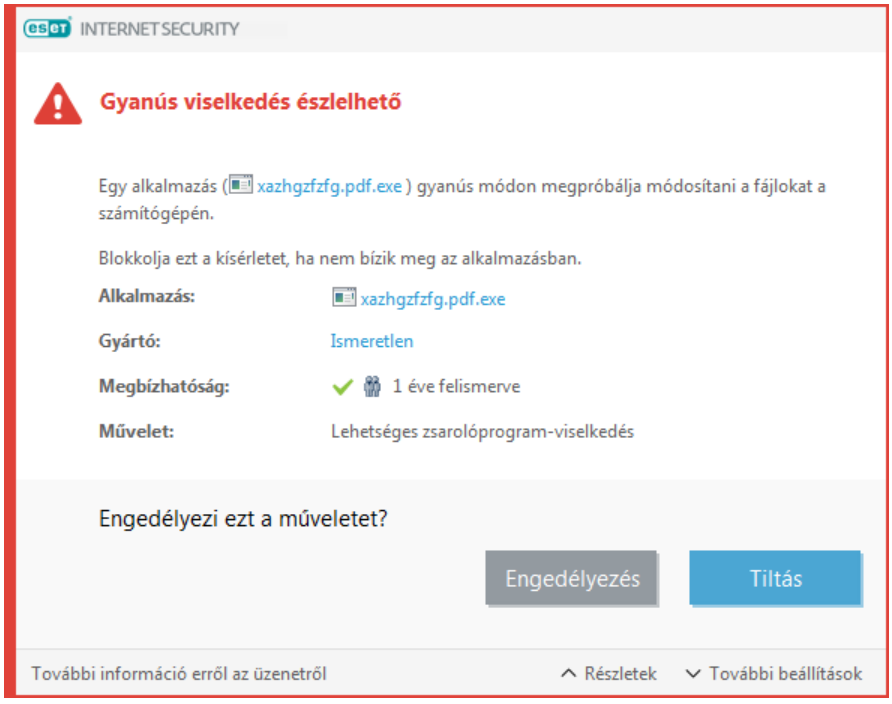
- **Csak erre az alkalmazásra érvényes szabály létrehozása** – Ha törli a jelet ebből a jelölőnégyzetből, a szabály az összes forrásalkalmazáshoz létrejön.
- **Csak a következő művelet esetén:** – Kiválaszthatja a szabályfájlt/alkalmazást/beállításjegyzék-műveletet. Itt megtekintheti a Behatolásmegelőző rendszer összes műveletének leírását.
- **Csak a következő cél esetén** – Kiválaszthatja a szabályfájlt/alkalmazást/beállításjegyzék-célt.

> **Túl sok értesítést küld a Behatolásmegelőző rendszer?**
> Ha nem szeretne értesítéseket kapni, módosítsa a szűrési módot **Automatikus üzemmódra** a **További beállítások** (F5) > **Keresőmotor** > **HIPS** > **Általános** lapon.



Lehetséges zsarolóprogram-viselkedés észlelve

Ez az interaktív ablak akkor jelenik meg, ha a program lehetséges zsarolóprogram-viselkedést észlel. Ezen választhatja a művelet **tiltását** vagy **engedélyezését** is.



A **Részletek** gombra kattintva megtekintheti az észlelési paramétereket. A párbeszédpanelen **elküldheti a fájlt elemzésre**, vagy **kizárhatja az észlelésből**.

a zsarolóprogram elleni védelem megfelelő működéséhez engedélyezni kell az ESET LiveGrid® szolgáltatást.

Behatolásmegelőző rendszer szabályainak kezelése

A párbeszédpanelen a behatolásmegelőző rendszer felhasználó által definiált, illetve automatikusan létrehozott szabályainak listája látható. A szabályok létrehozásáról és a behatolásmegelőző rendszer műveleteiről a Behatolásmegelőző rendszer szabálybeállításai című fejezetben olvashat részletesen. Tekintse meg A Behatolásmegelőző rendszer alapelvei című témakört is.

Oszlopok

Szabály – A szabály felhasználó által megadott vagy automatikusan választott neve.

Engedélyezve – Tiltsa le a csúszkát, ha szeretné a szabályt megőrizni a listában, de nem áll szándékában használni.

Művelet – A szabályok egy-egy műveletet – **Engedélyezés**, **Tiltás** vagy **Rákérdezés** – határoznak meg, amelyeket a feltételek teljesülése esetén a program végrehajt.

Források – A szabály alkalmazására csak akkor kerül sor, ha az eseményt ezek az alkalmazások váltották ki.

Célterületek – A szabály alkalmazására csak akkor kerül sor, ha a művelet adott fájlra, alkalmazásra vagy beállításértékre vonatkozik.

Naplózás részletessége – Ha bekapcsolja ezt a funkciót, a szabállyal kapcsolatos információkat a program bejegyzi a HIPS naplójába.

Értesítés – Esemény kiváltásakor egy kisméretű ablak jelenik meg képernyő jobb alsó sarkában.

Vezérlőelemek

Hozzáadás – Új szabály létrehozása.

Szerkesztés – A kijelölt bejegyzések szerkesztését teszi lehetővé.

Törlés – Ezzel a gombbal a kijelölt bejegyzéseket távolíthatja el.

A Behatolásmegelőző rendszer szabályainak prioritása

A tetejére/aljára gombokkal nem lehet megadni a Behatolásmegelőző rendszer szabályainak prioritási szintjét (mint a tűzfalszabályoknál, ahol a szabályok végrehajtása fentről lefelé történik).

- Az összes Ön által létrehozott szabály ugyanolyan prioritást kap
- Minél pontosabb egy szabály, annál magasabb prioritást kap (például egy adott alkalmazásra vonatkozó szabály magasabb prioritású, mint egy olyan, amely az összes alkalmazásra vonatkozik)
- A Behatolásmegelőző rendszer magasabb prioritású szabályokat foglal magában, amelyekhez Ön nem tud hozzáférni (például nem tud felülírni Önvédelem típusú szabályokat)
- A program nem alkalmaz olyan szabályt, amely miatt lefagyhat az operációs rendszer (a legalacsonyabb prioritású lesz)

A HIPS szabályainak szerkesztése

Először tekintse meg a Behatolásmegelőző rendszer szabályainak kezelése című részt.

Szabály neve – A szabály felhasználó által megadott vagy automatikusan választott neve.

Művelet – A szabályok egy-egy műveletet – **Engedélyezés**, **Tiltás** vagy **Rákérdezés** – határoznak meg, amelyet a feltételek teljesülése esetén a program végrehajt.

Műveletek által érintett – Ki kell jelölnie a művelet típusát, amelyre a szabály vonatkozni fog. A szabály csak az ilyen típusú műveletre és a kijelölt célterületre vonatkozik.

Engedélyezve – Tiltsa le csúszkát, ha meg szeretné őrizni a szabályt a listában, de nem kívánja alkalmazni.

Naplózás részletessége – Ha bekapcsolja ezt a funkciót, a szabállyal kapcsolatos információkat a program bejegyzi a HIPS naplójába.

Felhasználó értesítése – Ha bejelöli ezt a jelölőnégyzetet, a szabály alkalmazásakor egy kisméretű értesítés jelenik meg képernyő jobb alsó sarkában.

A szabály az azt kiváltó feltételeket leíró részekből áll:

Forrásalkalmazások – A szabály alkalmazására csak akkor kerül sor, ha az eseményt ezek az alkalmazások váltották ki. A legördülő listában válassza az **Adott alkalmazások** elemet, és kattintson a **Hozzáadás** műveletre új fájlok hozzáadásához, illetve ha az összes alkalmazást hozzá szeretné adni, a legördülő listában választhatja **Az összes alkalmazás** elemet is.

Célfájlok – A szabály alkalmazásához a műveletnek erre a célterületre kell vonatkoznia. A legördülő listában válassza ki az **Adott fájlok** elemet, és kattintson a **Hozzáadás** elemre új fájlok vagy mappák hozzáadásához, illetve ha az összeset hozzá szeretné adni, a legördülő listában kiválaszthatja a **Minden fájl** elemet is.

Alkalmazások – A szabály alkalmazásához a műveletnek erre a célterületre kell vonatkoznia. A legördülő listában válassza az **Adott alkalmazások** elemet, és kattintson a **Hozzáadás** műveletre új fájlok vagy mappák hozzáadásához, illetve ha az összes alkalmazást hozzá szeretné adni, a legördülő listában választhatja **Az összes alkalmazás** elemet is.

Beállításjegyzék bejegyzései – A szabály alkalmazásához a műveletnek erre a célterületre kell vonatkoznia. A legördülő listában válassza az **Adott bejegyzések** elemet, és kattintson a **Hozzáadás** elemre a kézi beíráshoz, illetve egy beállításkulcs választásához kattinthat a **Beállításszerkesztő megnyitása** elemre is. A legördülő listában választhatja a **Az összes bejegyzés** elemet is az összes alkalmazás hozzáadásához.

> A HIPS által előre létrehozott speciális szabályok egyes műveletei alapértelmezés szerint engedélyezettek, és nem tilthatók le. Emellett a HIPS nem figyel minden rendszerműveletet. A HIPS azokat figyeli, amelyek nem biztonságosak.

Az alábbi szakaszok a fontosabb műveleteket ismertetik.

Fájlműveletek

- **Fájl törlése** – Az alkalmazás engedélyt kér a célfájlok törléséhez.

• **Írás fájlba** – Az alkalmazás engedélyt kér a célfájlok írásához.

• **Közvetlen hozzáférés lemezhez** – Az alkalmazás a Windows szokásos eljárásainak megkerülésével, nem normál módon próbálja meg olvasni vagy írni a lemezt. Ilyenkor nem alkalmazhatók a megfelelő szabályok, és ellenőrizetlenül módosulnak a fájlok. Ilyen műveleteket az észlelést kerülni próbáló kártevők, a lemezekről pontos másolatot készítő biztonsági mentési szoftverek, illetve a lemezkötetek átszervezését végző partíciókezelő szoftverek is végrehajthatnak.

• **Globális beavatkozási rutin telepítése** – Az MSDN-könyvtár SetWindowsHookEx függvényének hívása.

• **Illesztőprogram betöltése** – Illesztőprogramok betöltése és telepítése a rendszerben.

Alkalmazásműveletek

• **Másik alkalmazás hibakeresése** – Hibakereső csatlakoztatása a folyamathoz. Hibakeresés közben megfigyelhető és módosítható a tanulmányozott alkalmazás viselkedése, továbbá elérhetők az adatai is.

• **Események elfogása másik alkalmazásból** – A forrásalkalmazás megpróbálja elfogni a célalkalmazásnak szóló eseményeket (például egy keylogger így kaphatja el a böngésző eseményeit).

• **Másik alkalmazás megszakítása/felfüggesztése** – Egy folyamat felfüggesztése, folytatása vagy befejezése (közvetlenül a folyamattallózóból vagy a Folyamatok lapról érhető el).

• **Új alkalmazás indítása** – Új alkalmazások vagy folyamatok indítása.

• **Másik alkalmazás állapotának módosítása** – A forrásalkalmazás megpróbál írni a célalkalmazás memóriájába, vagy a célalkalmazás nevében kísérel meg programkódot futtatni. Ez a műveletvédelmi beállítás az alapvető fontosságú alkalmazások védelmében használható különösen jól. Ehhez az alkalmazást célalkalmazásként kell beállítania egy szabályban, mely letiltja ezt a műveletet.

i A feldolgozó műveletek elfogása nem lehetséges 64 bites Windows XP rendszereken.

Beállításjegyzék-műveletek

• **Indítási beállítások módosítása** – A Windows indításakor futtatandó alkalmazásokkal kapcsolatos beállítások módosítása. A beállítások egy részét megtalálja, ha a Run kulcsra keres a Windows beállításjegyzékében.

• **Törlés a beállításjegyzékből** – Beállításkulcs vagy beállításazonosító törlése.

• **Beállításkulcs átnevezése** – A beállításkulcsok átnevezése.

• **Beállításjegyzék módosítása** – Új beállításazonosítók létrehozása a beállításkulcsokban, a beállításazonosítók módosítása, adatok áthelyezése a beállításjegyzék fájában, illetve felhasználói vagy csoportos jogosultságok beállítása beállításkulcsokra.

A célok megadásakor bizonyos korlátozásokkal, de használhat helyettesítő karaktereket is. A kulcsok pontos neve helyett a * karaktert is megadhatja, ami a beállításkulcs elérési útjában tetszőleges kulcsot jelent. Például a *HKEY_USERS*\software* kulcs magában foglalja a *HKEY_USER\.default\software* kulcsot, de a *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software* kulcsot nem. A *HKEY_LOCAL_MACHINE\system\ControlSet** nem érvényes beállításkulcs. A * rekurzív megadást tesz lehetővé, azaz magában foglalja a megadott elérési utat, illetve mindazon elérési utakat, melyeknek része a * előtti elérési út. Célfájloknál csak így használható helyettesítő karakter. A program előbb a megadott elérési utat értékeli ki, majd a helyettesítő karakter (*) utáni elérési utakat.

Ha nagyon általános szabályt hoz létre, a program figyelmeztetést jelenít meg erről a szabálytípusról.

Az alábbi példa egy adott alkalmazás nem kívánt működésének korlátozási módját szemlélteti:

1. Nevezze el a szabályt, és válassza ki a **Tiltás** elemet (vagy a **Rákérdezés** elemet, ha később szeretné kiválasztani) a **Művelet** legördülő listában.

2. Engedélyezze a **Felhasználó értesítése** szöveg melletti csúszkát, ha a szabályok alkalmazásakor értesítést szeretne megjeleníteni.

3. Válasszon ki legalább egy műveletet a **Műveletek által érintett** csoportban a szabályhoz.

4. Kattintson a **Tovább**gombra.

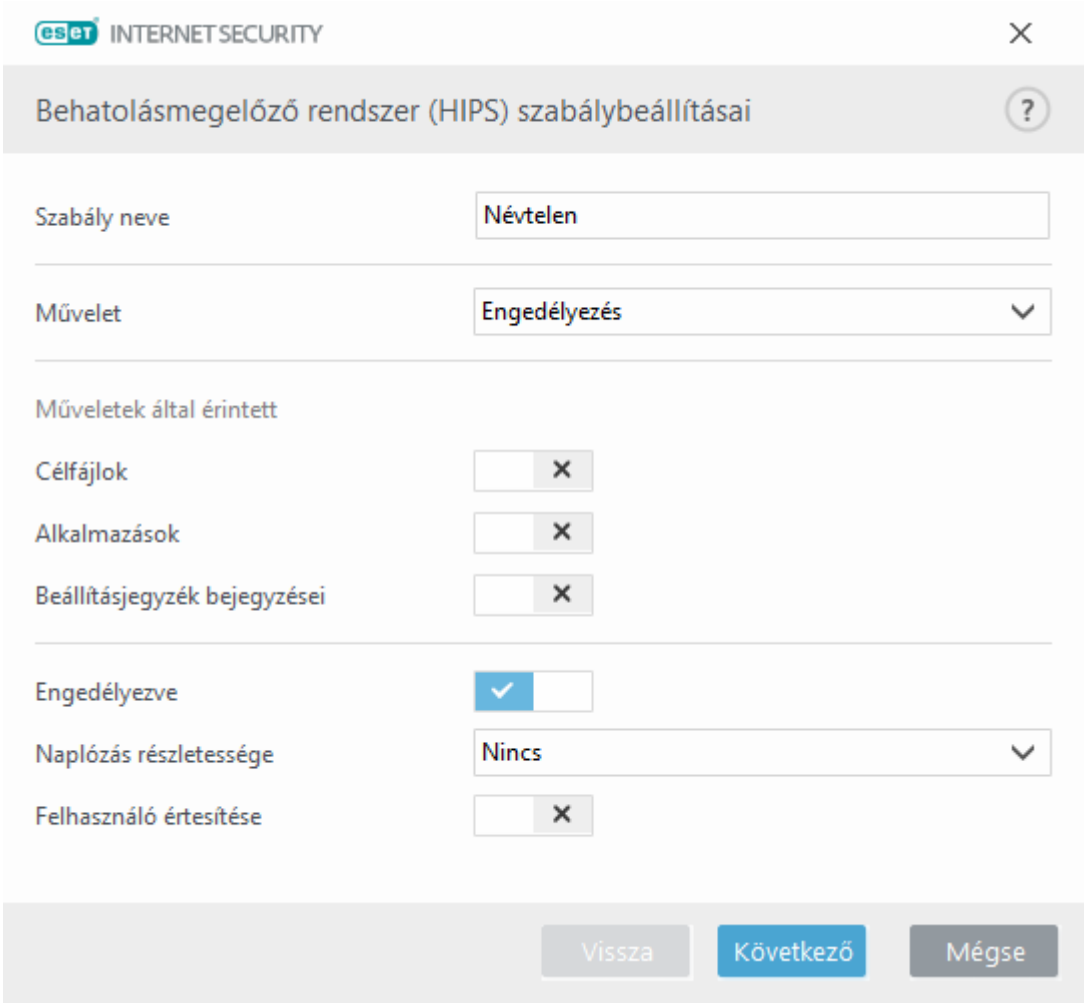
5. A **Forrásalkalmazások** ablak legördülő listájában válassza **Adott alkalmazások** elemet, ha azt szeretné, hogy az új szabály minden alkalmazásra vonatkozzon, amelyik megkísérli végrehajtani a kijelölt műveletek valamelyikét a megadott alkalmazásokon.

6. A **Hozzáadás**, majd a **...** elemre kattintva válassza ki az adott alkalmazáshoz vezető útvonalat, és ezután nyomja meg az **OK** gombot. Ha szeretne, adjon meg további alkalmazásokat.
Példa: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Válassza ki az **Írás fájlba** műveletet.

8. Válassza ki az **Összes fájl** menüpontot a legördülő menüben. Ezzel megakadályozza, hogy az előző lépésben kiválasztott alkalmazások írni tudjanak bármelyik fájlba.

9. A **Befejezés** gombra kattintva mentse az új szabályt.



Alkalmazás vagy beállításkulcs elérési útjának hozzáadása a HIPS-hez

A **...** gombra kattintva kijelölheti egy alkalmazás fájljának elérési útját. Ha mappát jelöl ki, azzal automatikusan kijelöl minden benne található alkalmazást.

A **Beállításszerkesztő megnyitása** gombra kattintva elindíthatja a Windows beállításszerkesztőjét (ez a Regedit.exe program). A beállításkulcsok megadásakor az **Érték** mezőben helyes kulcsot kell megadni.

Példa fájlelérési útra és beállításkulcsra:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

A Behatolásmegelőző rendszer haladó beállításai

Az alábbi beállítások az alkalmazások viselkedésének nyomon követésére és elemzésére szolgálnak.

Az illesztőprogramok mindig betölthetők – Az illesztőprogramok betöltése a beállított szűrési üzemmódtól függetlenül mindig engedélyezett, feltéve ha felhasználói szabály ezt kifejezetten nem tiltja le.

Összes tiltott művelet naplózása – Minden blokkolt művelet a HIPS naplóba kerül. Ezt a funkciót csak hibaelhárítás során vagy az ESET műszaki támogatási szolgálat kérésére használja, mivel egy hatalmas naplófájl jön létre, ami lelassíthatja a számítógépét.

Értesítés a rendszerindításkor futtatott alkalmazások módosításakor – Értesítést jelenít meg az asztalon, valahányszor alkalmazást vesz fel a rendszerindításba, illetve távolít el abból.

Az illesztőprogramok mindig betölthetők

A listában látható illesztőprogramok betöltése a HIPS szűrési üzemmódjától függetlenül mindig engedélyezett, hacsak egy felhasználói szabály ezt kifejezetten nem tiltja.

Hozzáadás – Új illesztőprogram hozzáadása.

Szerkesztés – Kijelölt illesztőprogram szerkesztése.

Eltávolítás – Illesztőprogram eltávolítása a listából.

Alaphelyzet – Rendszer-illesztőprogramok újbóli betöltése.

Kattintson az **Alaphelyzet** gombra, ha nem szeretné a kézzel hozzáadott illesztőprogramokat szerepeltetni. Ez akkor lehet hasznos, ha több illesztőprogramot felvett a listára, de nem tudja őket manuálisan törölni.

Játékos üzemmód

A játékos üzemmód azoknak a felhasználóknak hasznos, akiknek fontos a szoftverek megszakítás nélküli használata, és nem szeretnék, hogy előugró ablakok zavarják meg őket, illetve szeretnék minimalizálni a CPU terhelését. A játékos üzemmód olyan bemutatók során használható, amelyeket nem szakíthat meg semmiféle vírusvédelmi művelet. 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 üzemmód a program főablakában engedélyezhető, illetve tiltható le úgy, hogy a **Beállítások** > **Számítógép-védelem**, majd a  vagy a  elemre kattint a **Játékos üzemmód** szakaszban. A játékos üzemmód engedélyezése biztonsági kockázatot is jelent, amelyre a védelem állapotát jelző, a tálcán narancssárga színűre váltó állapotikon figyelmeztet. Ez a figyelmeztetés jelenik meg a program főablakában is, ahol a játékos üzemmód mellett **A játékos üzemmód aktív** narancssárga felirat látható.

A **További beállítások** (F5) > **Eszközök** > **Játékos üzemmód** csoportban jelölje be a **Játékos üzemmód engedélyezése automatikusan az alkalmazások teljes képernyős módban való futtatásakor** jelölőnégyzetet, ha azt szeretné, hogy a rendszer automatikusan játékos üzemmódba váltson, amint elindít egy teljes képernyős alkalmazást, majd az alkalmazás bezárásakor kilépjen ebből az üzemmódból.

A **Játékos üzemmód letiltása automatikusan** jelölőnégyzet bejelölése esetén megadhatja, hogy mennyi idő után kapcsoljon ki az üzemmód.

Ha a 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 kommunikáció engedélyezéséhez határozzon meg kommunikációs szabályt bármely olyan alkalmazás számára, amelyeknél felmerül ez a probléma, illetve használjon más Szűrési üzemmódot a tűzfalban. Ne feledje továbbá, hogy a játékos üzemmódban a meglátogatott webhelyek és a futtatott alkalmazások biztonsági kockázatot hordozhatnak, illetve előfordulhat, hogy a rendszer letiltja a webhelyeket vagy alkalmazásokat, de erről semmiféle tájékoztatást vagy figyelmeztetést nem kap, mivel a felhasználóval folytatott kommunikáció le van tiltva.

Rendszerindításkor futtatott ellenőrzés

A program rendszerindításkor vagy a keresőmotor frissítésekor alapértelmezés szerint elvégzi a rendszerindításkor automatikusan futtatott fájlok ellenőrzését. Az ellenőrzés a Feladatütemezőben meghatározott beállításoktól és feladatoktól függ.

A rendszerindításkor futtatott ellenőrzések beállítása a feladatütemező **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** feladatának a része. A beállítások módosításához keresse meg az **Eszközök** > **További eszközök** > **Feladatütemező** beállítást, és kattintson a **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése**, majd a **Szerkesztés** elemre. Az utolsó lépésben megjelenik a Rendszerindításkor automatikusan futtatott fájlok ellenőrzése ablak (erről bővebben a következő fejezetben olvashat).

Az ütemezett feladatok létrehozására és kezelésére vonatkozó utasítások az Új feladatok létrehozása című fejezetben találhatók.

Rendszerindításkor automatikusan futtatott fájlok ellenőrzése

A rendszerindításkor automatikusan futtatott fájlok ellenőrzése ütemezett feladat létrehozásakor többféleképpen módosíthatja az alábbi paramétereket:

Az **Ellenőrizendő célterületek** legördülő menü titkos, speciális algoritmus alapján adja meg a fájlok ellenőrzési mélységét a rendszer indításakor. A fájlok az alábbi feltételek szerint, csökkenő sorrendben rendezettek:

- **Minden regisztrált fájl** (legtöbb fájl ellenőrizve)
- **A ritkán használt fájlok**
- **A kevésbé gyakran használt fájlok**
- **A gyakran használt fájlok**
- **Csak a leggyakrabban használt fájlok** (legkevesebb fájl ellenőrizve)

Két speciális csoport is található itt:

- **A felhasználó bejelentkezése előtt futtatott fájlok** – Olyan helyekről származó fájlokat tartalmaz, amelyek lehetővé teszik a fájlok elérését anélkül, hogy a felhasználó bejelentkezne (tartalmazza szinte az összes rendszerindítási helyet, például szolgáltatásokat, böngésző segédobjektumait, Winlogon-értesítést, a Windows Ütemező bejegyzéseit, ismert dll-fájlokat stb.).

- **A felhasználó bejelentkezése után futtatott fájlok** – Olyan helyekről származó fájlokat tartalmaz, amelyek csak a felhasználó bejelentkezése után teszik lehetővé a fájlok elérését (beleértve az adott felhasználó által futtatott fájlokat, általában a *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* helyen lévőket).

Az ellenőrizendő fájlok listája minden fenti csoporthoz rögzítve van. Ha alacsonyabb ellenőrzési szintet választ a rendszerindításkor futtatott fájlok esetében, a nem ellenőrzött fájlok a megnyitásuk vagy a futtatásuk során lesznek ellenőrizve.

Ellenőrzés prioritása – A prioritás szintje, amellyel meghatározható az ellenőrzés indításának ideje.

- **Üresjárat idején** – a feladat csak üresjárat esetén megy végbe;

- **Alacsony** – a lehető legalacsonyabb rendszerterhelésnél,

- **Közepes** – alacsony rendszerterhelésnél,

- **Normál** – átlagos rendszerterhelésnél.

Dokumentumvédelem

A dokumentumvédelmi szolgáltatás még azt megelőzően ellenőrzi a Microsoft Office-dokumentumokat, valamint az Internet Explorer által automatikusan letöltött fájlokat, például Microsoft ActiveX-összetevőket, hogy megnyitná azokat. A dokumentumvédelem a valós idejű fájlrendszervédelem mellett további biztonságot nyújt, és a rendszer teljesítményének fokozása céljából letiltható abban az esetben, ha nem kell nagy mennyiségű Microsoft Office-dokumentumot kezelnie.

A dokumentumvédelem aktiválásához nyissa meg a **További beállítások** (F5) > **Keresőmotor** > **Kártevőellenőrzések** > **Dokumentumvédelem** lapot, majd kattintson a **Dokumentumvédelem engedélyezése** melletti csúszkára.

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

Kivételek

A **Kivételek** részen objektumokat zárhat ki az ellenőrzésből. Ha azt szeretné, hogy a program minden objektumot megvizsgáljon, azt javasoljuk, hogy csak akkor hozzon létre kivételeket, ha feltétlenül szükséges. Lehetnek olyan helyzetek, amikor valóban ki kell zárnia egy objektumot: a nagy adatbázis-bejegyzések ellenőrzése lelassíthatja a számítógép működését, akárcsak az olyan szoftverek, amelyek ütköznek az ellenőrzéssel.

A Teljesítménybeli kivételek részen fájlokat és mappákat zárhat ki az ellenőrzésből. A teljesítménybeli kivételekkel kizárható a játékalkalmazások fájlszintű ellenőrzése, illetve abnormális rendszerműködés vagy megnövekedett teljesítmény esetén.

Az Észlelési kivételek segítségével objektumokat zárhat ki az észlelésből az észlelt elem neve, az objektum elérési útvonala vagy kivonata segítségével. Az észlelési kivételek nem úgy zárnak ki fájlokat és mappákat az ellenőrzésből, mint a teljesítménybeli kivételek. Az észlelési kivételek csak akkor zárnak ki objektumokat, ha a keresőmotor észleli őket, és van egy megfelelő szabály a kizárási listában.

Nem összekeverendők más típusú kivételekkel:

- Folyamatkivételek – A kizárt folyamatok által végzett összes fájlművelet kimarad az ellenőrzésből (erre a biztonsági mentések gyorsaságának és a szolgáltatások elérhetőségének javítása miatt lehet szükség).
- Kizárt fájlkiterjesztések
- HIPS-kivételek
- Kivételszűrő felhőalapú védelemhez

Teljesítménybeli kivételek

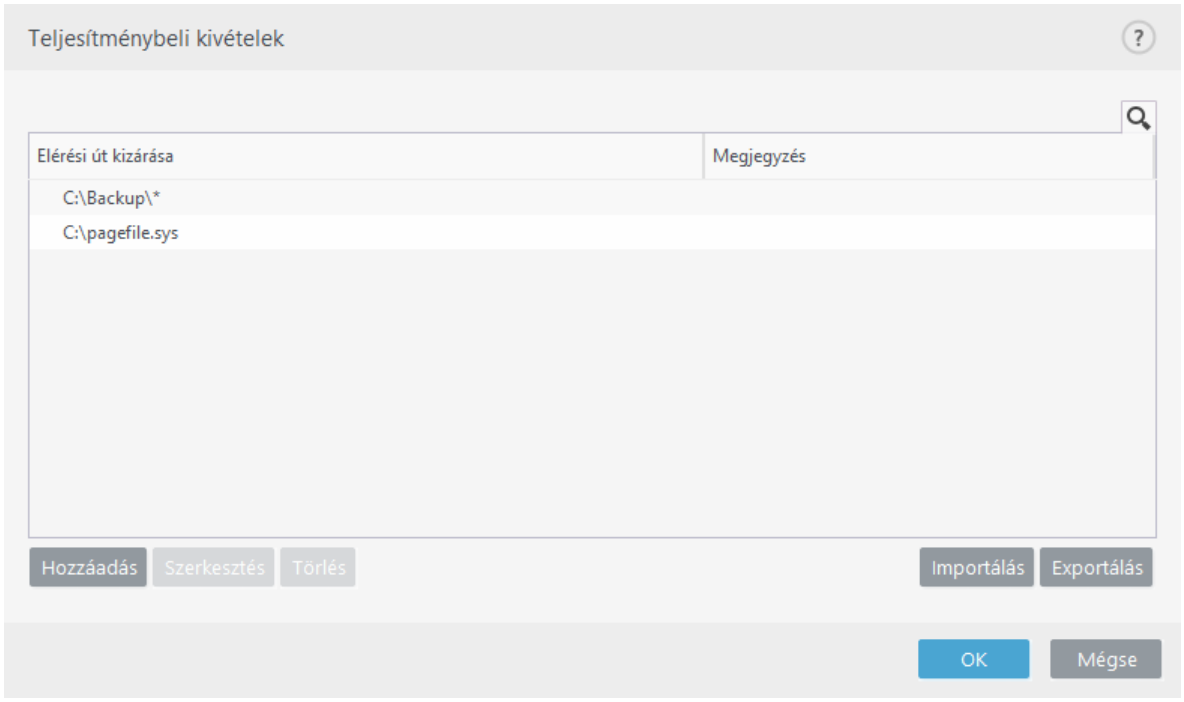
A Teljesítménybeli kivételek részen fájlokat és mappákat zárhat ki az ellenőrzésből.

Ha azt szeretné, hogy a program minden objektumot megvizsgáljon az esetleges kártevők kiszűrése érdekében, azt javasoljuk, hogy csak akkor hozzon létre kivételeket, ha feltétlenül szükséges. Lehetnek ugyanakkor olyan helyzetek, amikor valóban ki kell zárnia egy objektumot: a nagy adatbázis-bejegyzések ellenőrzése például lelassíthatja a számítógép működését, akárcsak az olyan szoftverek, amelyek ütköznek az ellenőrzéssel.

A **További beállítások** (F5) > **Keresőmotor** > **Kivételek** > **Teljesítménybeli kivételek** > **Szerkesztés** lapon adhatja hozzá az ellenőrzésből kizárni kívánt fájlokat és mappákat a kivételek listájához.

> Nem összekeverendő az észlelési kivételekkel, a kizárt fájlkiterjesztésekkel, a HIPS-kiterjesztésekkel és a folyamatkivételekkel.

Ha ki szeretne zárni egy objektumot (útvonalat, fájlt vagy mappát) az ellenőrzésből, kattintson a **Hozzáadás** elemre, majd írja be az elérési utat, vagy jelölje ki a fastruktúrában.



Ha egy fájl megfelel az ellenőrzésből való kizárás feltételeinek, az abban talált kártevőket nem észleli a **Valós idejű fájlrendszervédelem vagy** a **Számítógép ellenőrzése** modul.

Vezérlőelemek

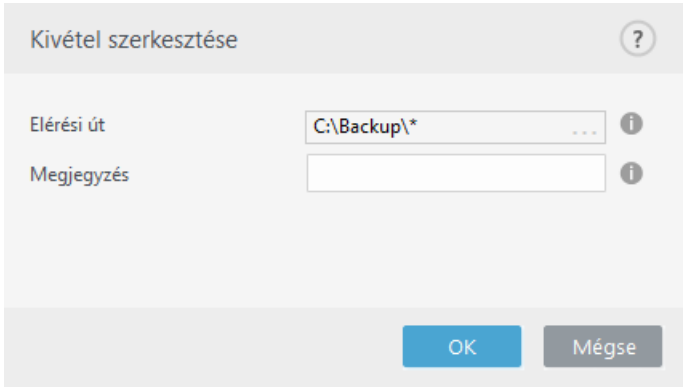
- **Hozzáadás** – Ezzel a gombbal zárhat ki objektumokat az ellenőrzésből.
- **Szerkesztés** – A kijelölt bejegyzések szerkesztését teszi lehetővé.
- **Törlés** – A kijelölt bejegyzések eltávolítása (több bejegyzés kijelöléséhez tartsa lenyomva a CTRL billentyűt, és kattintson a bejegyzésekre.

Teljesítménybeli kivételek felvétele vagy szerkesztése

Ez a párbeszédpanel kizár egy adott elérési utat (fájlt vagy könyvtárat) a számítógépen.

Elérési út kiválasztása vagy manuális megadás

A megfelelő elérési út kiválasztásához kattintson a **...** elemre az **Elérési út** mezőben. Manuális beírás esetén tekintsen meg lent további példákat kizárási formátumokra.



Helyettesítő karakterek használatával fájlcsoportokat is kizárhat. A kérdőjel (*?*) egyetlen karaktert jelöl, a csillag (***) pedig nulla vagy annál több karaktert.

Kivételek formátuma

- Ha egy mappa összes fájlját és almappáját 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 karaktert tartalmaz (és a karakterek eltérőek), de csak az elsőt ismeri biztosan (legyen ez a példában „D"), akkor használja a következő formátumot: *D????.exe* (a kérdőjelek hiányzó/ismeretlen karaktereket helyettesítenek).

Példák:

- *C:\Tools** – Az elérési útnak fordított perjellel (\) és csillaggal (*) kell végződnie, ami azt jelzi, hogy a mappa és a mappa összes tartalma (fájlok és almappák) lesz kizárva.
- *C:\Tools*.** – Ugyanaz a viselkedés, mint a *C:\Tools** esetén
- *C:\Tools* – A *Tools* mappa nem lesz kizárva. A víruskereső a *Tools* szót fájlnévként is kezelheti.
- *C:\Tools*.dat* – Ezzel kizárhatók a .dat fájlok a *Tools* mappában.
- *C:\Tools\sg.dat* – Ennek a fájlnak a kizárása, amely pontosan ezen az útvonalon érhető el.

Rendszerváltozók kivételekben

Használhat rendszerváltozókat – például %PROGRAMFILES% – az ellenőrzésből való kizáráshoz.

- A Program Files mappa fenti rendszerváltozóval való kizárásához használja a *%PROGRAMFILES%** útvonalat (ne felejtse el beírni a fordított perjelet és a csillagot az útvonal végére) a kivételek megadásakor.
- Ha a *%PROGRAMFILES%* alkönyvtár összes fájlját és mappáját ki szeretné zárni, a következő útvonalat használja: *%PROGRAMFILES%\Excluded_Directory**

Bontsa ki a támogatott rendszerváltozók listáját

A következő változók használhatók az útvonalkivétel formátumában:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Felhasználóspecifikus rendszerváltozók (például *%TEMP%* és *%USERPROFILE%*), illetve környezeti változók (például *%PATH%*) nem használhatók.

Helyettesítő karakterek nem támogatottak az elérési út közepén

Lehet helyettesítő karaktereket használni az elérési út közepén (például *C:\Tools*\Data\file.dat*), viszont hivatalosan nem támogatottak a teljesítménybeli kivételek esetén. További információkért tekintse meg ezt a tudásbáziscikket.

Nincsenek korlátozások a helyettesítő karakterek elérési út közepén történő használatára vonatkozólag észlelési kivételek használatakor.

A kivételek sorrendje

• A tetejére/aljára gombokkal nem lehet megadni a kivételek prioritási szintjét (mint a tűzfalszabályoknál, ahol a szabályok végrehajtása fentről lefelé történik).

• Ha az ellenőrző modul megfelelt az első alkalmazandó szabálynak, a rendszer nem értékeli ki a második alkalmazandó szabályt.

• Minél kevesebb a szabály, annál hatékonyabb lesz az ellenőrzés.

• Ne hozzon létre párhuzamos szabályokat.

Útvonalkivétel formátuma

Helyettesítő karakterek használatával fájlcsoportokat is kizárhat. A kérdőjel (*?*) egyetlen karaktert jelöl, a csillag (***) pedig nulla vagy annál több karaktert.

Kivételek formátuma

• Ha egy mappa összes fájlját és almappáját 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 karaktert tartalmaz (és a karakterek eltérőek), de csak az elsőt ismeri biztosan (legyen ez a példában „D”), akkor használja a következő formátumot: *D????.exe* (a kérdőjelek hiányzó/ismeretlen karaktereket helyettesítenek).

Példák:

• *C:\Tools** – Az elérési útnak fordított perjellel (\) és csillaggal (*) kell végződnie, ami azt jelzi, hogy a mappa és a mappa összes tartalma (fájlok és almappák) lesz kizárva.

• *C:\Tools*.** – Ugyanaz a viselkedés, mint a *C:\Tools** esetén

• *C:\Tools* – A *Tools* mappa nem lesz kizárva. A víruskereső a *Tools* szót fájlnévként is kezelheti.

• *C:\Tools*.dat* – Ezzel kizárhatók a .dat fájlok a *Tools* mappában.

• *C:\Tools\sg.dat* – Ennek a fájlnak a kizárása, amely pontosan ezen az útvonalon érhető el.

Rendszerváltozók kivételekben

Használhat rendszerváltozókat – például %PROGRAMFILES% – az ellenőrzésből való kizáráshoz.

• A Program Files mappa fenti rendszerváltozóval való kizárásához használja a *%PROGRAMFILES%** útvonalat (ne felejtse el beírni a fordított perjelet és a csillagot az útvonal végére) a kivételek megadásakor.

• Ha a *%PROGRAMFILES%* alkönyvtár összes fájlját és mappáját ki szeretné zárni, a következő útvonalat használja: *%PROGRAMFILES%\Excluded_Directory**

Bontsa ki a támogatott rendszerváltozók listáját

A következő változók használhatók az útvonalkivétel formátumában:

• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

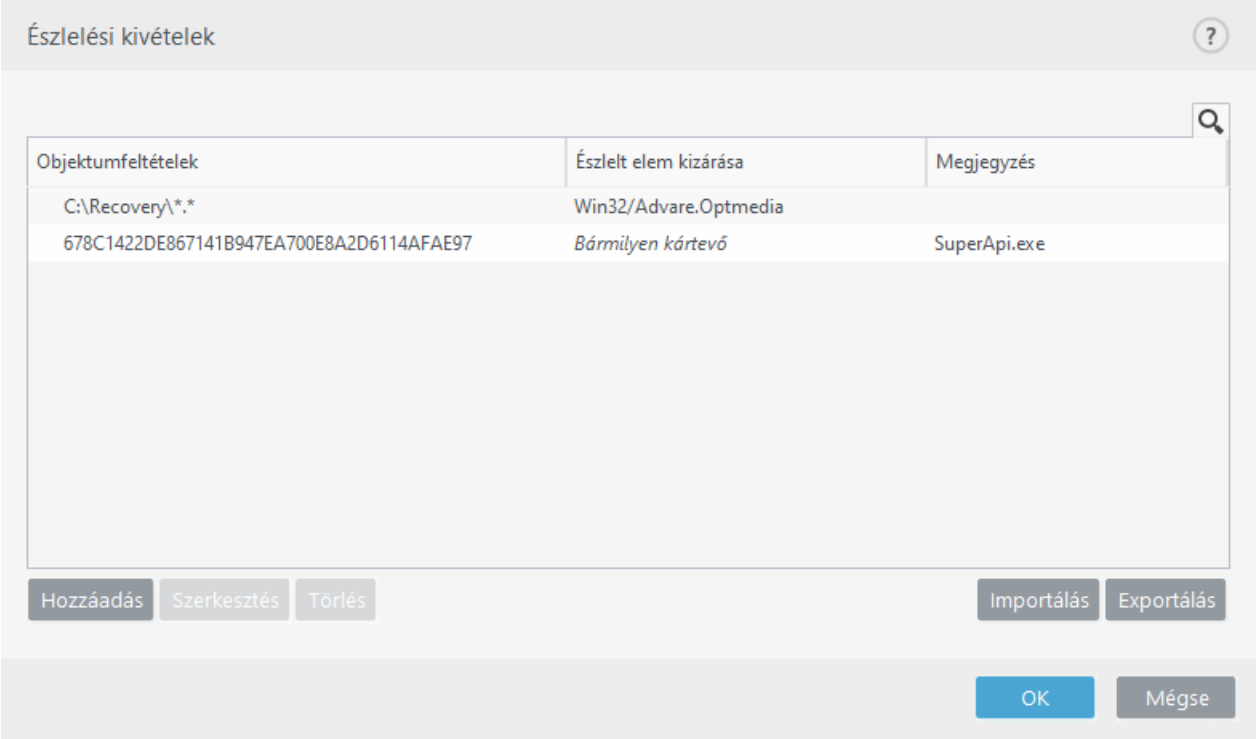
Felhasználóspecifikus rendszerváltozók (például *%TEMP%* és *%USERPROFILE%*), illetve környezeti változók (például *%PATH%*) nem használhatók.

Észlelési kivételek

Az Észlelési kivételek csoportban objektumokat zárhat ki az észlelésből az észlelt elem nevére, az objektum elérési útvonalára vagy a kivonatára szűrve.

Az észlelési kivételek működése

Az észlelési kivételek nem úgy zárnak ki fájlokat és mappákat az ellenőrzésből, mint a Teljesítménybeli kivételek. Az észlelési kivételek csak akkor zárnak ki objektumokat, ha a keresőmotor észleli őket, és van egy megfelelő szabály a kizárási listában.
Ha például (lásd az első sort az alábbi képen) az észlelt objektum neve Win32/Adware.Optmedia, az észlelt fájl neve pedig *C:\Recovery\file.exe*. A második sorban a megfelelő SHA-1 kivonattal rendelkező fájlok kizárása mindig megtörténik az észlelt elem nevétől függetlenül.



Annak érdekében, hogy a rendszer minden kártevőt észleljen, csak akkor javasoljuk az észlelési kivételek létrehozását, ha mindenképpen szükséges.

A **További beállítások** (F5) > **Keresőmotor** > **Kivételek** > **Észlelési kivételek** > **Szerkesztés** lapon adhatja hozzá az ellenőrzésből kizárni kívánt fájlokat és mappákat a kivételek listájához.

Nem összekeverendő a teljesítménybeli kivételekkel, a kizárt fájlkiterjesztésekkel, a HIPS-kiterjesztésekkel és a folyamatkivételekkel.

Ha ki szeretne zárni egy objektumot (neve vagy kivonata alapján) a keresőmotorból, kattintson a **Hozzáadás** gombra.

Kéretlen alkalmazások és veszélyes alkalmazások esetében észlelési név alapján történő kizárás is létrehozható:

- Az észlelt elemet jelentő riasztási ablakban (kattintson a **További beállítások megjelenítése** elemre, majd válassza ki a **Felvétel a kivételek közé** lehetőséget).
- A Naplófájlok helyi menüben található Varázsló létrehozása észlelési kivételekhez menüpont segítségével.

• Az **Eszközök** > **További eszközök** > **Karantén** elemre kattintva, majd jobb gombbal a karanténba helyezett fájlra kattintva és a helyi menü **Visszaállítás és kizárás az ellenőrzésből** menüpontját kiválasztva.

Objektumfeltételek az észlelési kivételek esetén

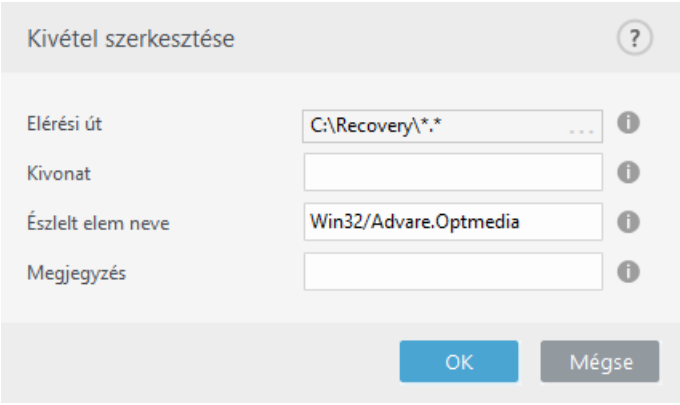
- **Elérési út** – Korlátozza az észlelési kivételt egy adott (vagy bármilyen) elérési úttal.
- **Észlelt elem neve** – Ha a kizárt fájl mellett egy észlelt elem neve látható, az azt jelenti, hogy a fájlt nem teljesen, hanem csak az adott észlelt elemet érintő ellenőrzésből zárja ki. Ha a fájlt később egy másik kártevő is megfertőzi, a rendszer ezt észlelni fogja.
- **Kivonat** – Fájl kizárása a megadott kivonat alapján SHA-1, függetlenül a fájl típusától, tárolási helyétől, nevétől és kiterjesztésétől.

Észlelési kivétel felvétele vagy szerkesztése

Észlelt elem kizárása

Érvényes ESET-fertőzésnevet kell megadni. Az érvényes fertőzésneveket tekintse meg a naplófájlokban, majd válassza ki az **Észlelések** menüpontot a Naplófájlok legördülő menüben. Ez akkor hasznos, ha egy tévesen jelentett minta észlelhető az ESET Internet Security alkalmazásban. A valós fertőzések kizárása nagyon veszélyes – lehetőleg csak az érintett fájlokat/könyvtárakat zárja ki a **...** ikonra kattintva az **Elérési út maszkja** mezőben, illetve csak átmeneti időre. A kivételek a kéretlen alkalmazásokra, a veszélyes alkalmazások és a gyanús alkalmazásokra is vonatkoznak.

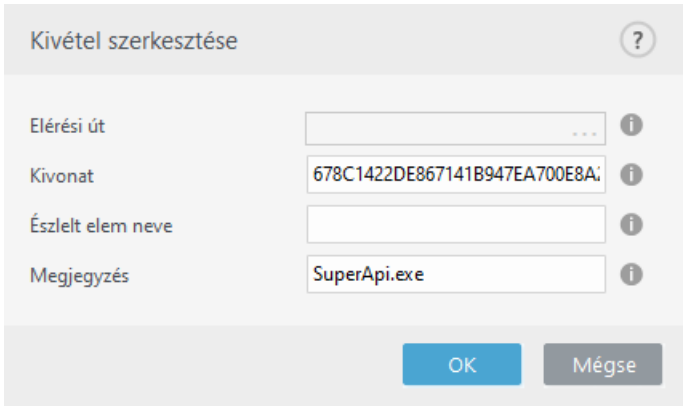
Tekintse meg az Útvonalkivétel formátuma című részt is.



Tekintse meg lent az Észlelési kivételekről szóló példát.

Kivonat kizárása

Fájl kizárása a megadott kivonat alapján SHA-1, függetlenül a fájl típusától, tárolási helyétől, nevétől és kiterjesztésétől.



Kivételek a kártevő neve szerint

Ha ki szeretne zárni egy kártevőt, adjon meg érvényes kártevőnevet:
Win32/Adware.Optmedia
A következő formátumot is használhatja, amikor kizár egy fertőzést az ESET Internet Security riasztási ablakában:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Vezérlőelemek

- **Hozzáadás** – Ezzel a gombbal zárhat ki objektumokat az ellenőrzésből.
- **Szerkesztés** – A kijelölt bejegyzések szerkesztését teszi lehetővé.
- **Törlés** – A kijelölt bejegyzések eltávolítása (több bejegyzés kijelöléséhez tartsa lenyomva a CTRL billentyűt, és kattintson a bejegyzésekre.

Varázsló létrehozása észlelési kivételekhez

A Naplófájlok helyi menüből is létre lehet hozni észlelési kivételt (erre nincs lehetőség kártevőkészlelések esetén):

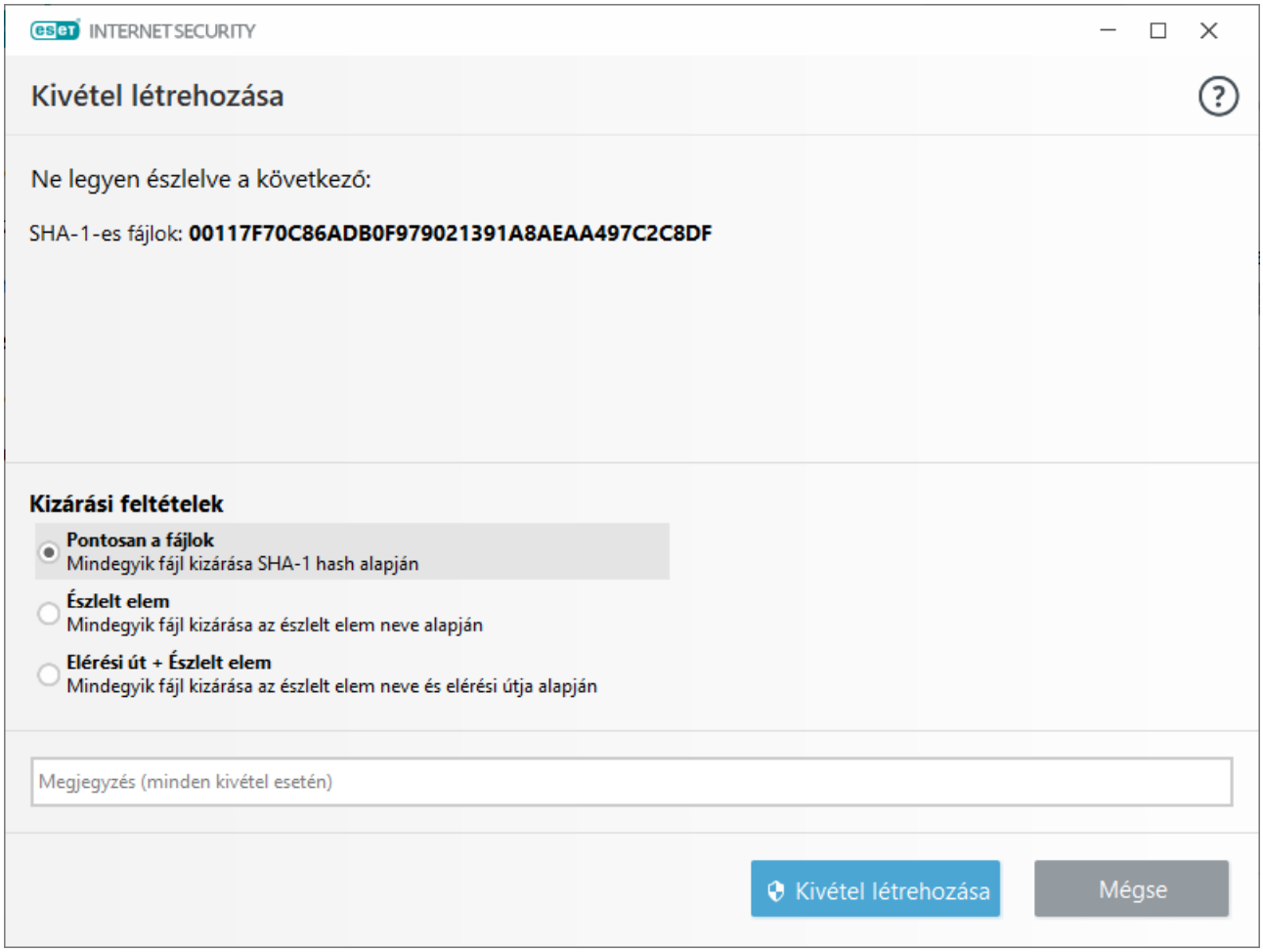
1. A program főablakában kattintson az **Eszközök** > **További eszközök** > **Naplófájlok**.
2. Kattintson a jobb gombbal az észlelt elemre az **Észlelési naplóban**.
3. Kattintson a **Kivétel létrehozása** elemre.

Egy vagy több észlelt elem **Kizárási feltételek** alapján való kizárásához kattintson a **Feltételek módosítása** elemre:

- **Pontosan a fájlok** – Mindegyik fájl kizárása SHA-1 hash alapján.
- **Észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve alapján.
- **Elérési út + Észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve és elérési útja alapján (pl. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Az ajánlott beállítás előre ki van választva az észlelt elem típusa alapján.

Opcionálisan megadhat egy **megjegyzést**, mielőtt a **Kivétel létrehozása** gombra kattint.



HIPS-kivételek

Kivételek megadásával megakadályozhatja, hogy bizonyos folyamatokat megvizsgáljon a HIPS (Behatolásmegelőző rendszer) Viselkedésalapú ellenőrzés funkciója.

A HIPS-kivételek szerkesztéséhez navigáljon a **További beállítások** (F5) > **Keresőmotor** > **HIPS** > **Általános** > **Kivételek** > **Serkesztés** lapra.

> Nem összekeverendő a kizárt fájlkiterjesztésekkel, az észlelési kivételekkel, a teljesítménybeli kivételek és a folyamatkivételekkel.

Ha ki szeretne zárni egy objektumot, kattintson a **Hozzáadás** elemre, majd írja be az objektum elérési útját, vagy jelölje ki a fastruktúrában. Szerkesztheti, illetve törölheti is a kijelölt bejegyzéseket.

ThreatSense paraméterek

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

A ThreatSense motor 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 **ThreatSense paraméterei** gombra a ThreatSense technológiát alkalmazó bármely modul További beállítások ablakában (lásd alább). A különböző biztonsági körülmények eltérő konfigurációkat igényelhetnek. Ennek érdekében a ThreatSense külön beállítható az alábbi védelmi modulokhoz:

- Valós idejű fájlrendszervédelem
- Üresjárat idején történő ellenőrzés
- Rendszerindításkor futtatott ellenőrzés
- Dokumentumvédelem
- E-mail védelem
- Webhozzáférés-védelem
- Számítógép ellenőrzése

A ThreatSense keresőmotor beállításai minden modulhoz nagymértékben optimalizáltak, módosításuk jelentősen befolyásolhatja a rendszer működését. Ha például úgy módosítja a paramétereket, 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 a ThreatSense paramétereit az alapértelmezett értékeken hagyni.

Ellenőrizendő objektumok

Ebben a csoportban állítható be, hogy a számítógép mely összetevőit, illetve milyen típusú fájlokat ellenőrizzen a keresőmotor.

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

Rendszerindítási szektorok/UEFI – A rendszerindítási szektorokban ellenőrzi, hogy a fő rendszerindító rekordban találhatók-e kártevők. További információk az UEFI-ről a szószedetben.

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 (SFX) olyan fájlok, amelyek 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 kódelemzést használva számos más típusú tömörítőt is képes felismerni.

Ellenőrzési beállítások

A rendszer fertőzésekkel kapcsolatos ellenőrzésének módjait adhatja meg itt. A választható lehetőségek az alábbiak:

Alapheurisztika használata – Az alapheurisztika a programok kártékony tevékenységének a felismerésére szolgál. Fő előnye, hogy a korábbi verziójú keresőmotorban még nem létező, illetve az által nem ismert kártevő szoftvereket is képes felismerni. Hátránya, hogy (nagyon ritkán) téves riasztásokat is küldhet.

Kiterjesztett heurisztika/DNA-vírusdefiníciók – A kiterjesztett heurisztika az ESET saját, a számítógépes férgek és trójai programok felismerésére optimalizált, magas szintű programozási nyelveken fejlesztett heurisztikus algoritmusa. A kiterjesztett heurisztika használata jelentősen javítja az ESET-termékek kártevő-észlelési hatékonyságát. 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.

Megtisztítás

A megtisztítási beállítások azt határozzák meg, hogy az ESET Internet Security mit tegyen a fertőzött objektumok megtisztítása során. A megtisztításnak az alábbi négy szintje áll rendelkezésre:

A ThreatSense-paraméterek a következő kezelési (vagyis tisztítási) szinteket teszik lehetővé.

Kezelés az ESET Internet Security termékben

Automatikus megtisztítás szintje	Leírás
Mindig kezelje a fertőzést	Az észlelt kártevő eltávolítása az objektumok tisztítása közben felhasználói beavatkozás nélkül. Egyes ritka esetekben (például rendszerfájlok esetén), ha az észlelt kártevő nem távolítható el, az objektum az eredeti helyén marad.
Fertőzés kezelése, ha ez biztonságos. Egyéb esetben megtartás	Az észlelt kártevő eltávolítása az objektumok tisztítása közben felhasználói beavatkozás nélkül. Egyes esetekben (például tiszta és fertőzött fájlokat egyaránt tartalmazó rendszerfájlok vagy archívumok esetén), ha az észlelt kártevő nem távolítható el, az objektum az eredeti helyén marad.
Fertőzés kezelése, ha ez biztonságos. Egyéb esetben rákérdezés	Az észlelt kártevő eltávolítása az objektumok tisztítása közben. Egyes esetekben, ha nem hajtható végre művelet, a végfelhasználó interaktív figyelmeztetést kap, és ki kell választania egy műveletet (például törlés vagy figyelmen kívül hagyás). Legtöbb esetben ez a beállítás ajánlott.
Mindig kérdezze meg a végfelhasználót	A végfelhasználónak megjelenik egy interaktív ablak az objektumok tisztítása során, és ki kell választania egy műveletet (például törlés vagy figyelmen kívül hagyás). Ez a szint a tapasztalt felhasználóknak ajánlott, akik tisztában vannak azzal, hogy mi a teendő a fertőzések esetén.

Kivételek

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

Egyéb

A kézi indítású számítógép-ellenőrzés beállítása során a ThreatSense keresőmotor paramétereinek a beállításai mellett az **Egyéb** csoportban az alábbiakat is megadhatja:

Változó adatfolyamok ellenőrzése (ADS) – 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.

Minden objektum naplózása – A Víruskeresési napló nem csak a fertőzött fájlokat, hanem önkicsomagoló archívumokban található összes ellenőrzött fájlt meg fogja jeleníteni (létrejöhet sok naplóadat, és megnövekedhet az ellenőrzési naplófájl mérete).

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.

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

Korlátok

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

Objektumok ellenőrzésének beállításai

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 a konténerobjektumokban (például RAR/ZIP-archívum vagy több mellékletet tartalmazó e-mail) található fájlok ellenőrzésének maximális időtartamát adhatja meg. A beállítás nem vonatkozik önálló fájlokra. Felhasználó által megadott érték és az időtartam lejárata esetén a víruskeresés leáll, függetlenül attól, hogy a konténerben található fájlok ellenőrzése befejeződött-e.
Nagy méretű fájlokat tartalmazó archívum esetén a víruskeresés csak akkor áll le, ha megtörtént az egyik fájl kibontása az archívumból (ha például a felhasználó által megadott változó 3 másodperc, a fájl kibontása viszont 5 másodpercig tart). Az archívumban lévő többi fájl ellenőrzése nem megy végbe, ha az adott időtartam lejárt.
A víruskeresési időtartam korlátozásához – ideértve a nagyobb archívumokat is – használja a **Maximális objektumméret** és a **Maximális fájlméret a tömörített fájlokon belül** lehetőséget (nem ajánlott a potenciális biztonsági kockázatok miatt).
Alapértelmezett érték: korlátlan.

Tömörített fájlok ellenőrzésének beállításai

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. Maximális érték: **3 GB**.

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

Ellenőrzésből kizárt fájlkiterjesztések

A kizárt fájlkiterjesztések a ThreatSense-paraméterek részét képezik. A kizárt fájlkiterjesztések konfigurálásához kattintson a **ThreatSense-paraméterek** elemre a Speciális beállítás ablakban minden olyan modulnál, amely a ThreatSense technológiát használja.

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

> Nem összekeverendő a folyamatkivételekkel, a HIPS-kivételekkel és a fájl-/mappakivételekkel.

Alapértelmezés szerint a program az összes fájlt ellenőrzi. Az ellenőrzésből kizárt fájlok listájára bármilyen kiterjesztés felvehető.

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.

> Új kivétel hozzáadásához kattintson a **Hozzáadás** gombra. Írja be a kivételt az üres mezőbe (például tmp), és kattintson az **OK** gombra. A **Több érték megadása** kiválasztása esetén hozzáadhat több fájlkiterjesztést, amelyeket vonallal, vesszővel vagy pontosvesszővel kell elválasztani egymástól (például válassza ki a **Pontosvessző** menüpontot a legördülő listából, majd írja be a következőt: `edb;eml;tmp`). Használhat különleges szimbólumot is: ? (kérdőjel). A kérdőjel tetszőleges szimbólumot jelent (például `?db`).

> Ha Windows operációs rendszerben meg szeretné nézni a fájlok pontos kiterjesztését (ha van), törölje az **Ismert fájltípusok kiterjesztéseinek elrejtése** opció bejelölését a **Vezérlőpult** > **Mappabeállítások** > **Nézet** (lap) beállításnál, és alkalmazza a módosítást.

További ThreatSense-paraméterek

Ezeknek a beállításoknak a szerkesztéséhez lépjen a **További beállítások** (F5) > **Keresőmotor** > **Valós idejű fájlrendszervédelem** >**További ThreatSense-paraméterek** lapra.

További ThreatSense-paraméterek az új és módosított fájlokhoz

A fertőzés valószínűsége az újonnan létrehozott vagy módosított fájlok esetén magasabb, mint a meglévő

fájloknál, ezért a program további ellenőrzési paraméterekkel ellenőrzi a fájlt. Az ESET Internet Security kiterjesztett heurisztikát használ, amely még a keresőmotor frissítésének megjelenése előtt a vírusdefiníció-alapú ellenőrzési módszerekkel együtt észleli az új kártevőket.

Az újonnan létrehozott fájlok mellett az ellenőrzés az **önkicsomagoló (.sfx) fájlokra** és a **futtatás közbeni tömörítőkre** (belsőleg tömörített végrehajtható fájlokra) is kiterjed. A tömörített fájlokat a program alapértelmezés szerint a 10. mélységi szintig ellenőrzi, 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

Kiterjesztett heurisztika a fájlok futtatásakor – A fájlok futtatásakor a program alapértelmezés szerint kiterjesztett heurisztikát használ. Ha be van jelölve, azt javasoljuk, hogy a rendszer teljesítményére gyakorolt hatás csökkentése végett tartsa meg az optimalizálás és az ESET LiveGrid® engedélyezését.

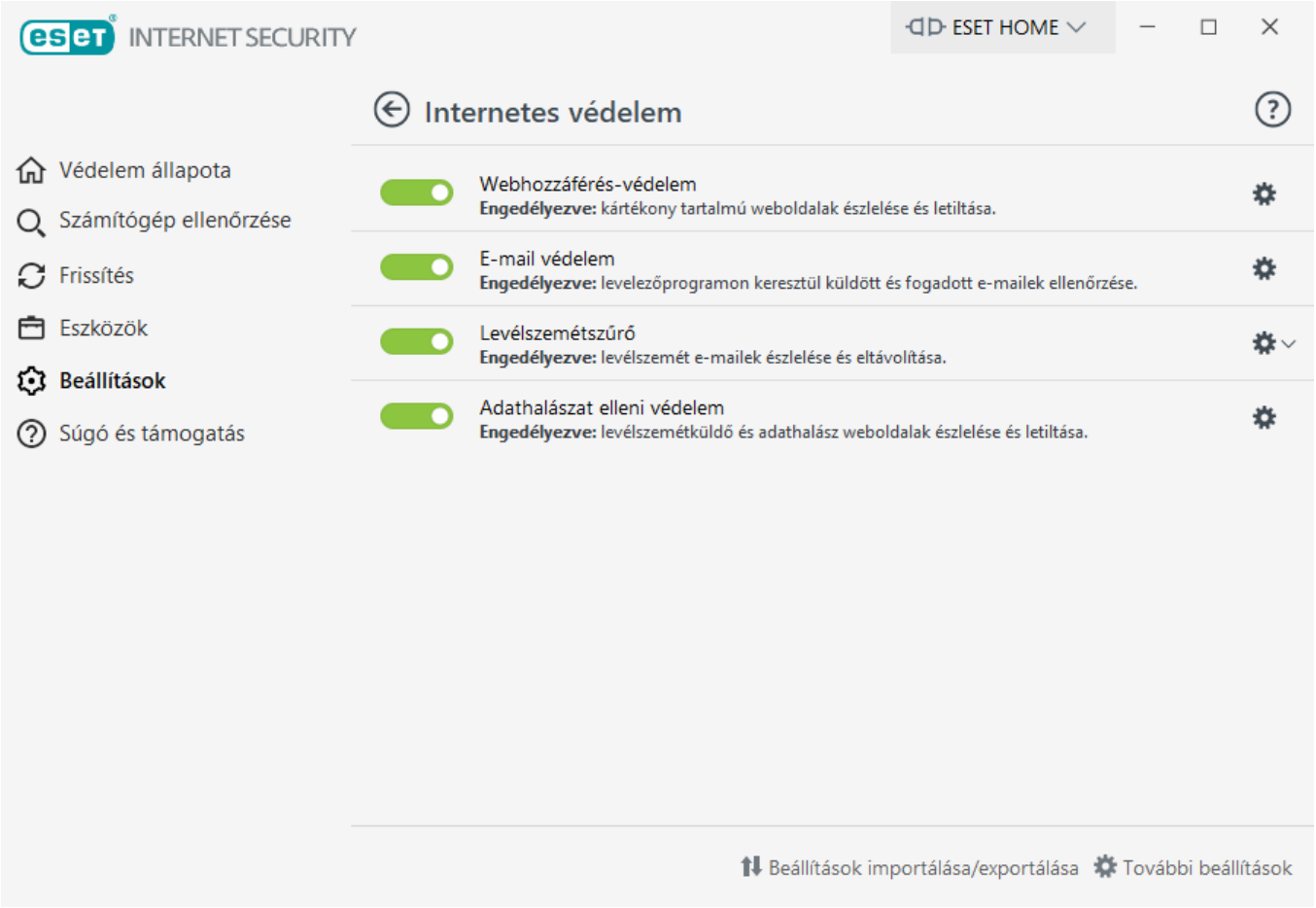
Kiterjesztett heurisztika a fájlok cserélhető adathordozóról történő futtatásakor - A kiterjesztett heurisztika virtuális környezetben emulálja a kódot, és a cserélhető adathordozóról való futtatása előtt értékeli a viselkedését.

Internetes védelem

A web- és e-mail-védelem konfigurálásához kattintson az **Internetes védelem** elemre a **Beállítások** ablakban. Innen a részletesebb programbeállításokat is elérheti.

Az egyes védelmi modulok szüneteltetéséhez vagy letiltásához kattintson a csúszkára .

A védelmi modulok kikapcsolása esetén csökkenhet a számítógép védelmi szintje.



Kattintson a fogaskerék ikonra a web/e-mail/adathalászat elleni védelem/levélszemétszűrő védelem beállításainak megnyitásához a További beállítások ablakban.

Az internetkapcsolatra való képesség a személyi számítógépek szabványos funkciója. Sajnos az internet mára a kártevő kódok terjesztésének elsődleges közegévé vált. Emiatt nagyon fontos a webhozzáférés-védelem beállításainak körültekintő konfigurálása.

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

A Levélszemétszűrő kiszűri a kéretlen e-maileket.

A **Levélszemétszűrő** esetén kattintson a fogaskerékre, majd válasszon a következő lehetőségek közül:

- **Konfigurálás** – Megnyitja a levélszemétszűrő speciális beállításait.

- **Felhasználói címlista** (ha engedélyezve van) – Megnyit egy párbeszédablakot, ahol címeket adhat hozzá, szerkesztheti vagy törölhet a levélszemétszűrő szabályok meghatározásához. A listában szereplő szabályok az aktuális felhasználóra fognak vonatkozni.

- **Globális címlista** (ha engedélyezve van) – Megnyit egy párbeszédablakot, ahol címeket adhat hozzá, szerkesztheti vagy törölhet a levélszemétszűrő szabályok meghatározásához. A listában szereplő szabályok minden felhasználóra vonatkozni fognak.

Adathalászat elleni védelem – Lehetővé teszi, hogy letiltson olyan weboldalakat, amelyek adathalászati tartalmat terjesztenek. Erősen javasoljuk, hogy hagyja bekapcsolva az adathalászat elleni védelmet.

Protokollszűrés

Az alkalmazásprotokollok vírusvédelmét az összes korszerű kártevőkereső technológiát zökkenőmentesen integráló ThreatSense keresőmotor biztosítja. A protokollszűrés az alkalmazott internetböngészőtől és levelezőprogramtól függetlenül, automatikusan működik. A titkosított (SSL/TLS-alapú) kommunikáció beállításainak módosításához keresse meg a **További beállítások** (F5) > **Web és e-mail**> **SSL/TLS** beállítást.

Protokollszűrés engedélyezése – A protokollszűrés letiltására használható. Ne feledje, hogy az ESET Internet Security számos összetevője (Webhozzáférés-védelem, E-mail védelem, Adathalászat elleni védelem, Szülői felügyelet) ettől függ, és nélküle nem működik.

Kizárt alkalmazások – Ez a beállítás lehetővé teszi adott alkalmazások kizárását a protokollszűrésből. Hasznosan alkalmazható, amikor a protokollszűrés kompatibilitási hibákat okoz.

Kizárt IP-címek – Ezzel a beállítással adott távoli címeket zárhat ki a protokollszűrésből. Hasznosan alkalmazható, amikor a protokollszűrés kompatibilitási hibákat okoz.

Hozzáadás (például *2001:718:1c01:16:214:22ff:fec9:ca5*).

Alhálózat– A szabály egy IP-cím és egy IP-maszk által meghatározott alhálózat (számítógépcsoport) tagjaira fog vonatkozni (például: *2002:c0a8:6301:1::1/64*).

Példa kizárt IP-címekre

IPv4-cím és -maszk:

- *192.168.0.10* – Ha ezt az opciót jelöli be, akkor a szabály arra az egyetlen számítógépre fog vonatkozni, amelynek címét megadja a címmezőben.
- *192.168.0.1 – 192.168.0.99* – A szabály a két címmezőben az érintett tartomány kezdő és záró IP-címének kijelölésével definiált IP-címtartományra (több számítógépre) fog vonatkozni.
- A szabály egy IP-cím és egy IP-maszk által meghatározott alhálózat (számítógépcsoport) tagjaira fog vonatkozni. A *255.255.255.0* maszk például a *192.168.1.0/24* előtag maszkja, és a *192.168.1.1* – 192.168.1.254 címtartományt adja meg.

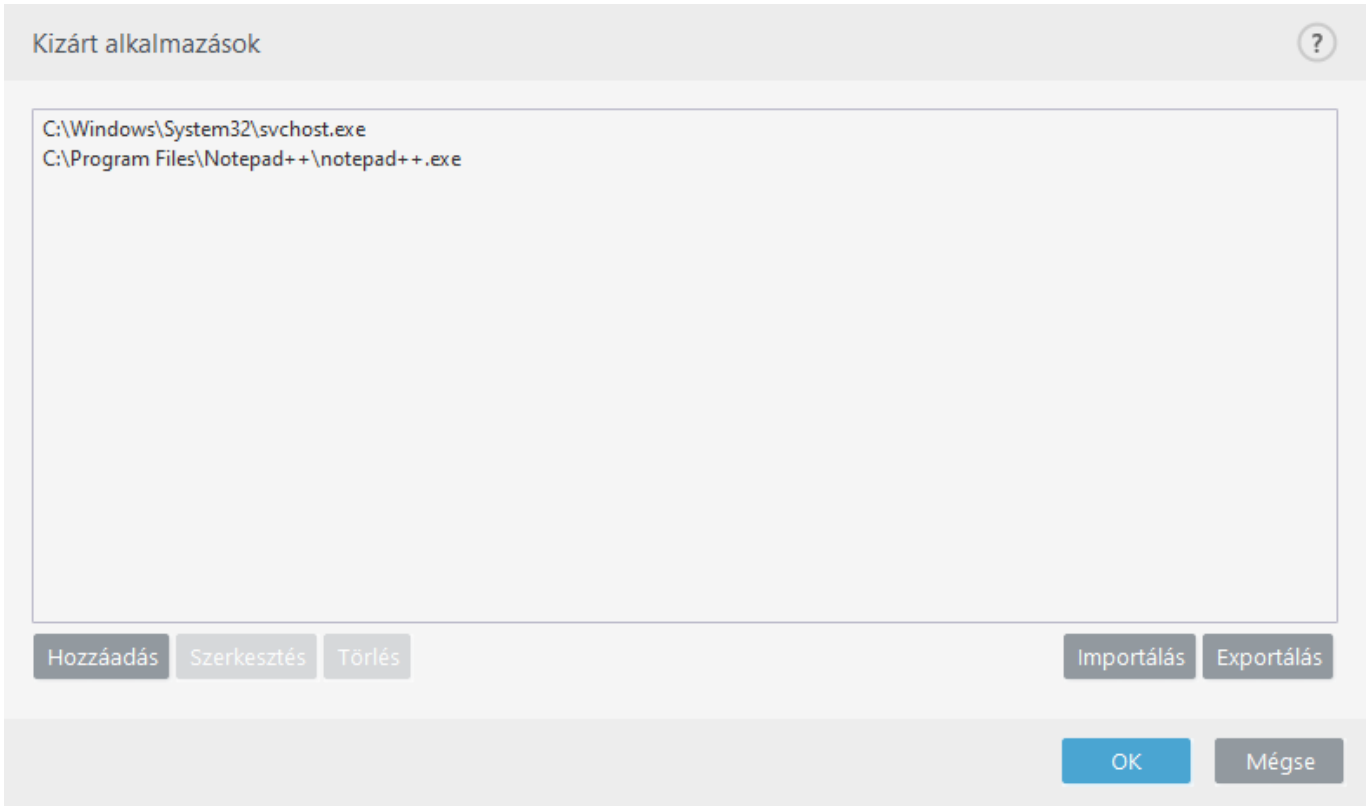
IPv6-cím és -maszk:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – Az IPv6-cím arra az egyetlen számítógépre fog vonatkozni, amelynek címét megadja a címmezőben.
- *2002:c0a8:6301:1::1/64* – 64 bites előtaghosszú IPv6-cím, vagyis *2002:c0a8:6301:0001:0000:0000:0000:0000 to 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

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/POP3/IMAP-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.



Kizárt IP-címek

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

A protokollszűrési listában meg nem jelenített távoli IP-cím/címtartomány/alhálózat kizárásához kattintson a **Hozzáadás** gombra.

A **Törlés** gombra kattintva távolítsa el a kijelölt bejegyzéseket a listáról.



IPv4-cím hozzáadása

Ezzel adhatja meg annak a távoli oldalnak az IP-címét, - címtartományát vagy -alhálózatát, amelyre a szabályt alkalmazni szeretné. Az IPv4 egy régebbi, de jelenleg is a leggyakrabban használt internetes címzési protokoll.

Egyetlen cím – Ha ezt az opciót jelöli be, akkor a szabály arra az egyetlen számítógépre fog vonatkozni, amelynek címét megadja a címmezőben (például *192.168.0.10*).

Címtartomány – A szabály a két címmezőben az érintett tartomány kezdő és záró IP-címének kijelölésével definiált IP-címtartományra (több számítógépre) fog vonatkozni (például *192.168.0.1 – 192.168.0.99*).

Alhálózat – A szabály egy IP-cím és egy IP-maszk által meghatározott alhálózat (számítógépcsoport) tagjaira fog vonatkozni.

A *255.255.255.0* maszk például a *192.168.1.0/24* előtag maszkja, és a *192.168.1.1* – 192.168.1.254 címtartományt adja meg.

IPv6-cím hozzáadása

Ezzel adhatja meg annak a távoli oldalnak az IPv6-címét vagy -alhálózatát, amelyre a szabályt alkalmazni szeretné. Az IPv6 az IP protokoll legújabb verziója, mely a korábbi 4-es verziót (IPv4) fogja felváltani.

Egyetlen cím – Ha ezt az opciót jelöli be, akkor a szabály arra az egyetlen számítógépre fog vonatkozni, amelynek a címét megadja a címmezőben (például *2001:718:1c01:16:214:22ff:fec9:ca5*).

Alhálózat– A szabály egy IP-cím és egy IP-maszk által meghatározott alhálózat (számítógépcsoport) tagjaira fog vonatkozni (például: *2002:c0a8:6301:1::1/64*).

SSL/TLS

Az ESET Internet Security kártevőkeresést tud végezni az SSL protokollt alkalmazó kommunikáció tartalmán. Az SSL protokollal védett kommunikáció ellenőrzéséhez többféle szűrési mód is beállítható. Az ellenőrzés a megbízható, az ismeretlen és az SSL protokollal védett kommunikáció ellenőrzéséből kizárt tanúsítványokon alapul.

SSL/TLS-protokollszűrés engedélyezése – A protokollszűrés letiltása esetén a program nem ellenőrzi az SSL protokollon keresztül folytatott kommunikációt.

Az **SSL/TLS-protokollszűrési mód** beállításához az alábbiak közül választhat:

Szűrési üzemmód	Leírás
Automatikus üzemmód	Alapértelmezett üzemmód, amely csak a megfelelő alkalmazásokat, például a böngészőket és a levelezőprogramokat vizsgálja. Ha felül szeretné bírálni, kiválaszthatja azon alkalmazásokat, amelyek kommunikációját ellenőrzi a program.
Interaktív üzemmód	Ha SSL protokollal védett, de ismeretlen tanúsítvánnyal rendelkező webhelyet keres fel, megjelenik egy műveletválasztási párbeszédpanel. Ez a mód lehetővé teszi, hogy tanúsítványokat/alkalmazásokat vegyen fel az ellenőrzésből kizárt SSL-tanúsítványok listájára.

Szűrési üzemmód	Leírás
Házirend üzemmód	Házirend üzemmód – Jelölje be ezt az opciót, 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 egy megbízhatóként megjelölt (a megbízható tanúsítványok listájához hozzáadott), azonban nem megbízható tanúsítvánnyal rendelkező szervert ér el, a program engedélyezi a kommunikációt a szerverrel, és szűri a kommunikációs csatornát.

Az **SSL/TLS szűrésű alkalmazások listája** lehetővé teszi az ESET Internet Security viselkedésének testreszabását adott alkalmazásokhoz.

Ismert tanúsítványok listája – Lehetővé teszi az ESET Internet Security viselkedésének testreszabását adott SSL tanúsítványokhoz.

Megbízható tartományokkal való kommunikáció kizárása – Ha engedélyezi ezt a funkciót, a megbízható tartományokkal folytatott kommunikáció nem lesz ellenőrizve. A tartományok megbízhatóságát beépített engedélyezőlista határozza meg.

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

Legfelső szintű tanúsítvány

Legfelső szintű tanúsítvány hozzáadása az ismert böngészőkhöz – Az SSL-alapú kommunikáció böngészőkben vagy levelezőprogramokban való megfelelő működéséhez az ESET legfelső szintű tanúsítványát hozzá kell adni az ismert legfelső szintű tanúsítványok (kibocsátók) listájához. Engedélyezésekor az ESET Internet Security automatikusan hozzáadja az ESET SSL Filter CA tanúsítványt az ismert böngészőkhöz (például Opera). A rendszer tanúsítványtárolóját használó böngészők esetén a tanúsítvány hozzáadása automatikusan történik. Például a Firefox automatikus konfigurációja szerint megbízik a rendszer tanúsítványtárolójában található gyökérszervezetekben.

Ha a tanúsítványt nem támogatott böngészőben szeretné beállítani, válassza a **Tanúsítvány megtekintése** > **Részletek** > **Másolás fájlba** lehetőséget, majd importálja manuálisan a böngészőbe.

Tanúsítvány érvényessége

Ha a tanúsítvány megbízhatósága nincs megállapítva – Egyes webhelytanúsítványok nem ellenőrizhetők a megbízható legfelső szintű hitelesítésszolgáltatók tárolójával. Ezek a tanúsítványok például egy webszerver vagy egy kisebb cég rendszergazdája által aláírt tanúsítványok, és megbízhatóként való kezelésük nem feltétlenül jelent kockázatot. A legtöbb nagy szervezet (például a bankok) a legfelső szintű hitelesítésszolgáltató által aláírt kibocsátott tanúsítványokat használ. Ha a **Kérdezzen rá a tanúsítvány érvényességére** választógomb van bejelölve (ez az alapbeállítás), a titkosított kapcsolatok létesítésekor választania kell egy műveletet. A **Tiltsa le a tanúsítványt használó kommunikációt** választógomb bejelölése esetén a program automatikusan letiltja a nem ellenőrzött tanúsítványokat használó webhelyek titkosított kapcsolatait.

Ha a tanúsítvány sérült – Ez azt jelenti, hogy a tanúsítvány vagy lejárt, vagy nem megfelelő az aláírása. Az ESET azt javasolja, hogy ilyen esetben hagyja bejelölve a **Tiltsa le a tanúsítványt használó kommunikációt** választógombot. Ha a **Kérdezzen rá a tanúsítvány érvényességére** választógomb van bejelölve, a felhasználónak választania kell

egy műveletet titkosított kapcsolat létesítésekor.

> **Ábrákkal ellátott példák**
> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> - Tanúsítványokkal kapcsolatos értesítések az ESET Windows otthoni termékekben
> - A „Titkosított hálózati forgalom: Nem megbízható tanúsítvány” üzenet jelenik meg weboldalak meglátogatásakor

Tanúsítványok

Az SSL-alapú kommunikáció böngészőkben vagy levelezőprogramokban való megfelelő működéséhez az ESET legfelső szintű tanúsítványát hozzá kell adni az ismert legfelső szintű tanúsítványok (kibocsátók) listájához. Erre szolgál a **Legfelső szintű tanúsítvány hozzáadása az ismert böngészőkhöz** jelölőnégyzet. Amelynek a bejelölésekor 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) a legfelső szintű hitelesítésszolgáltató által aláírt kibocsátott tanúsítványokat használ.

Ha a **Kérdezzen rá a tanúsítvány érvényességére** választógomb van bejelölve (ez az alapbeállítás), a titkosított kapcsolatok létesítésekor választania kell egy műveletet. A műveletválasztó párbeszédpanelen eldöntheti, hogy megbízhatóként vagy kizártként jelöl-e meg egy tanúsítványt. Ha a tanúsítvány nem szerepel a TRCA listában, az ablak piros lesz. Ha a tanúsítvány nem szerepel a TRCA listában, az ablak zöld lesz.

Amennyiben a **Tiltsa le a tanúsítványt használó kommunikációt** választógombot jelöli be, a program automatikusan letiltja 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.

Titkosított hálózati forgalom

Ha a rendszeren beállította az SSL protokollon alapuló kommunikáció ellenőrzését, az alábbi két helyzetben megjelenik egy párbeszédpanel, amely a megfelelő művelet kiválasztására kéri:

Ha egy webhely ellenőrizhetetlen vagy érvénytelen tanúsítványt használ, és ESET Internet Security úgy van beállítva, hogy ilyen esetekben kérdést tegyen fel a felhasználónak (amelyre ellenőrizhetetlen tanúsítványok esetén az alapértelmezett válasz igen, érvénytelenek esetén pedig nem), egy párbeszédpanel arra fogja kérni, hogy **engedélyezze** vagy **tiltsa le** a kapcsolatot. Ha a tanúsítvány nem található meg a Trusted Root Certification Authorities store gyűjteményben (TRCA), akkor a rendszer nem tekinti megbízhatónak.

Ha az **SSL-protokollszűrési mód interaktív üzemmódra** van állítva, minden egyes webhelyhez megjelenik egy párbeszédpanel, amelyen megadhatja, hogy **ellenőrizni** vagy **mellőzni** szeretné-e az adatforgalmat. Egyes alkalmazások ellenőrzik, hogy az SSL titkosítású adatforgalmat nem módosította vagy vizsgálta-e meg valaki. Ilyen esetekben az ESET Internet Security alkalmazásnak **mellőznie** kell az adott adatforgalmat ahhoz, hogy

működőképes maradjon.

> **Ábrákkal ellátott példák**
> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> - Tanúsítványokkal kapcsolatos értesítések az ESET Windows otthoni termékekben
> - A „Titkosított hálózati forgalom: Nem megbízható tanúsítvány” üzenet jelenik meg weboldalak meglátogatásakor

Mindkét esetben a felhasználó dönthet úgy, hogy a program megjegyezze a kijelölt műveletet. A mentett műveleteket a program az ismert tanúsítványok listájában tárolja.

Ismert tanúsítványok listája

Az **Ismert tanúsítványok listája** használható az ESET Internet Security viselkedésének testreszabására adott SSL tanúsítványokhoz és olyan műveletek megjegyzésére, amelyeket akkor választ ki, ha az **SSL/TLS-protokollszűrési mód Interaktív üzemmód** értékre van állítva. A lista a **További beállítások** (F5) > **Web és e-mail** > **SSL/TLS** > **Ismert tanúsítványok listája** részen tekinthető meg és szerkeszthető.

Az **Ismert tanúsítványok listája** ablak részei:

Oszlopok

Név – A tanúsítvány neve.

Tanúsítvány kibocsátója – A tanúsítvány létrehozójának neve.

Tanúsítvány tulajdonosa – A tulajdonosi mező azonosítja a tulajdonos nyilvános kulcsának mezőjében tárolt nyilvános kulccsal társított entitást.

Hozzáférés – Válassza az **Engedélyezés** vagy a **Tiltás** lehetőséget a **Hozzáférési művelet** értékeként a jelen tanúsítvánnyal (a megbízhatóságától függetlenül) védett kommunikáció engedélyezéséhez vagy letiltásához. Az **Automatikus** lehetőséget választva engedélyezheti a megbízható tanúsítványokat és kereshet nem megbízhatókat. Ha a **Rákérdezés** lehetőséget választja, a program mindig jóváhagyást kér a felhasználótól.

Ellenőrzés – Válassza az **Ellenőrzés** vagy a **Mellőzés** lehetőséget az **Ellenőrzési művelet** beállításaként a jelen tanúsítvánnyal védett kommunikáció ellenőrzéséhez vagy az ellenőrzés mellőzéséhez. Az **Automatikus** lehetőséget választva automatikus üzemmódban ellenőrizhet, interaktív üzemmódban pedig a program jóváhagyást kér. Ha a **Rákérdezés** lehetőséget választja, a program mindig jóváhagyást kér a felhasználótól.

Vezérlőelemek

Hozzáadás – Itt vehet fel új tanúsítványt, és módosíthatja a hozzáférésre és ellenőrzési lehetőségekre vonatkozó beállításokat.

Szerkesztés – Jelölje ki a konfigurálni kívánt tanúsítványt, és kattintson a **Szerkesztés** gombra.

Törlés – Jelölje ki az eltávolítandó tanúsítványt, majd kattintson az **Eltávolítás** gombra.

OK/Mégse – Az **OK** gombra kattintva menti a módosításait, a **Mégse** gombra kattintva pedig mentés nélkül kiléphet.

SSL/TLS szűrésű alkalmazások listája

Az **SSL/TLS szűrésű alkalmazások listája** használható az ESET Internet Security viselkedésének testreszabására adott alkalmazásokhoz és olyan műveletek megjegyzésére, amelyeket akkor választ ki, ha az **SSL/TLS-protokollszűrési mód** beállítás **Interaktív üzemmód** értékre van állítva. A lista a **További beállítások** (F5) > **Web és e-mail** > **SSL/TLS** > **SSL/TLS szűrésű alkalmazások listája** csoportban tekinthető meg és szerkeszthető.

Az **SSL/TLS szűrésű alkalmazások listája** ablak részei:

Oszlopok

Alkalmazás – Ebben a mezőben adhatja meg a futtatandó programot teljes elérési útjával. A mező melletti **Tallózás** gombra kattintva ki is jelölheti a fájlt.

Ellenőrzési művelet – Válassza az **Ellenőrzés** vagy a **Mellőzés** lehetőséget a kommunikáció ellenőrzéséhez vagy az ellenőrzés mellőzéséhez. Az **Automatikus** lehetőséget választva automatikus üzemmódban ellenőrizhet, interaktív üzemmódban pedig a program jóváhagyást kér. Ha a **Rákérdezés** lehetőséget választja, a program mindig jóváhagyást kér a felhasználótól.

Vezérlőelemek

Hozzáadás – Adja hozzá a szűrt alkalmazást.

Szerkesztés – Jelölje ki a konfigurálni kívánt alkalmazást, majd kattintson a **Szerkesztés** gombra.

Törlés – Jelölje ki a törölni kívánt alkalmazást, majd kattintson a **Törlés** gombra.

Importálás/Exportálás – Alkalmazások importálása fájlból vagy az aktuális alkalmazások listájának mentése fájlba.

OK/Mégse – Az **OK** gombra kattintva menti a módosításait, a **Mégse** gombra kattintva pedig mentés nélkül kiléphet.

E-mail védelem

Tekintse meg Az ESET Internet Security integrálása a levelezőprogrammal című részt az integráció konfigurálásához.

A levelezőprogram beállításait a **További beállítások** (F5) > **Web és e-mail** > **E-mail-védelem** > **Levelezőprogramok** lehetőséget választva érheti el.

Levelezőprogramok

Az e-mail védelem engedélyezése a beépülő modulon keresztül – Ha le van tiltva, a levelezőprogram beépülő moduljainak védelme ki van kapcsolva.

Ellenőrizendő e-mailek

Válassza ki az ellenőrizendő e-maileket:

- **Fogadott e-mailek**
- **Küldendő e-mailek**
- **Olvasott e-mailek**
- **Módosított e-mail**

Azt javasoljuk, hogy kapcsolja be az **E-mail védelem engedélyezése protokollszűrés szerint** funkciót. Ha az integrálás nem engedélyezett vagy nem működik, az e-mail-kommunikáció védelmét akkor is biztosítja a Protokollszűrés (IMAP/IMAPS és POP3/POP3S).

A fertőzött e-maileken végrehajtandó művelet

Nincs művelet – A választógomb bejelölése 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 fertőzött e-maileket a program automatikusan áthelyezi a Törölt elemek mappába.

E-mail áthelyezése a következő mappába (alapértelmezett művelet) – A fertőzött e-maileket a program automatikusan áthelyezi a megadott mappába.

Mappa – Itt adhatja meg, hogy az észlelésüket követően melyik mappába kerüljenek a fertőzött e-mailek.

Integrálás a levelezőprogramokkal

Az ESET Internet Security és az e-mail-kliens integrálása növeli az e-mailekben található rosszindulatú kódok elleni aktív védelem szintjét. A támogatott levelezőprogramok integrálása az ESET Internet Security programban engedélyezhető. Ha integrálva van a levelezőprogramba, az ESET Internet Security eszköztára közvetlenül a levelezőprogramban jelenik meg, ezzel még hatékonyabb védelmet nyújt a levelezés során. Az integrációs beállításokat a **További beállítások** (F5) > **Web és e-mail** > **E-mail védelem** > **Integrálás a levelezőprogramokkal** lehetőséget választva érheti el.

A jelenleg támogatott levelezőprogramok a következők: Microsoft Outlook, Outlook Express, Windows Mail és Windows Live Mail. Az E-mail-védelem a fenti programok beépülő 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. A támogatott levelezőprogramok és verzióik teljes listáját az ESET tudásbáziscikke tartalmazza.

Tiltsa le a **Mellékletkezelés optimalizálása** és a **Speciális levelezőprogram-feldolgozás** funkciót, ha az e-mailek beolvasásakor a rendszer lassulását tapasztalja.

Microsoft Outlook-eszköztár

A Microsoft Outlook védelme beépülő modulként működik. Az ESET Internet Security telepítését követően a vírusvédelmi,a levélszemétszűrő és a további védelmi funkciók megjelennek a Microsoft Outlook alkalmazásban:

Levélszemét – A gombra kattintva levélszemétként jelölheti meg a kijelölt üzenetet. A megjelölés után a program elküldi az e-mail ujjlenyomatát a levélszemét-definíciókat tároló központi szervernek. Ha több felhasználótól is hasonló ujjlenyomatok érkeznek a szerverre, az üzenet a továbbiakban levélszemétnek minősül.

Jó levél – A kijelölt üzenetet jó levélként jelöli meg.

Levélszemétküldő cím – Felveszi egy új feladó címét a tiltólistára, a levélszemétküldők címeinek listájára. A listán szereplő címekről érkező összes üzenet automatikusan levélszemétnek minősül.

Óvakodjon a hamisítástól, azaz amikor egy üzenetben hamisan másvalaki címe szerepel feladóként. Ennek célja, hogy a címzetteket az e-mail elolvasására és megválaszolására késztesse.

Megbízható cím – Felveszi egy új feladó címét az engedélyezőlistára, azaz a megbízható feladók címeinek listájára. Az engedélyezőlistán szereplő címekről érkező üzenetek sosem minősülnek automatikusan levélszemétnek.

ESET Internet Security – Kattintson duplán az ikonra az ESET Internet Security főablakának megnyitásához.

Üzenetek újraellenőrzése – Az e-mailek ellenőrzésének kézi indítása. Az ellenőrzéshez kijelölheti az ellenőrizendő üzeneteket, illetve újraellenőriztetheti a beérkezett e-maileket. További információt az E-mail védelem című témakörben talál.

Víruskereső beállításai – Az E-mail védelem beállítási lehetőségeit jeleníti meg.

Levélszemétszűrő beállításai – A Levélszemétszűrő beállítási lehetőségeit jeleníti meg.

Névjegyalbumok – Megnyitja a levélszemétszűrő ablakát, ahonnan elérheti a kizárt, a megbízható és a levélszemétküldő címek listáját.

Outlook Express- és Windows Mail-eszköztár

Az Outlook Express és a Windows Mail levelezőprogram védelme beépülő modulként valósul meg. Az ESET Internet Security telepítését követően a vírusvédelmi,a levélszemétszűrő és a további védelmi funkciók megjelennek az Outlook Express és a Windows Mail alkalmazásban:

Levélszemét – A gombra kattintva levélszemétként jelölheti meg a kijelölt üzenetet. A megjelölés után a program elküldi az e-mail ujjlenyomatát a levélszemét-definíciókat tároló központi szervernek. Ha több felhasználótól is hasonló ujjlenyomatok érkeznek a szerverre, az üzenet a továbbiakban levélszemétnek minősül.

Jó levél – A kijelölt üzenetet jó levélként jelöli meg.

Levélszemétküldő cím – Felveszi egy új feladó címét a tiltólista. A listán szereplő címekről érkező összes üzenet automatikusan levélszemétnek minősül.

Óvakodjon a hamisítástól, azaz amikor egy üzenetben hamisan másvalaki címe szerepel feladóként. Ennek célja, hogy a címzetteket az e-mail elolvasására és megválaszolására késztesse.

Megbízható cím – Felveszi egy új feladó címét az engedélyezőlistára. Az engedélyezőlistán szereplő címekről érkező üzenetek sosem minősülnek automatikusan levélszemétnek.

ESET Internet Security – Kattintson duplán az ikonra az ESET Internet Security főablakának megnyitásához.

Üzenetek újraellenőrzése – Az e-mailek ellenőrzésének kézi indítása. Az ellenőrzéshez kijelölheti az ellenőrizendő üzeneteket, illetve újraellenőriztetheti a beérkezett e-maileket. További információt az E-mail védelem című témakörben talál.

Víruskereső beállításai – Az E-mail védelem beállítási lehetőségeit jeleníti meg.

Levélszemétszűrő beállításai – A Levélszemétszűrő beállítási lehetőségeit jeleníti meg.

Felhasználói felület

Megjelenés testreszabása – A levelezőprogramhoz telepített eszköztár megjelenésének testreszabása. A parancs melletti pipa törlésével a levelezőprogram paramétereitől függetlenül szabhatja testre a program megjelenését.

Szöveg megjelenítése – Feliratok megjelenítése az ikonok mellett.

Szöveg jobbra – Az ikonfeliratok áthelyezése az ikonok jobb oldalára.

Nagy ikonok – Nagyméretű ikonok megjelenítése az eszköztáron.

Megerősítés

A program ezzel a párbeszédpanellel ellenőrzi, hogy a felhasználó valóban végre szeretné-e hajtani a választott műveletet. Ezzel kiküszöbölhetők a véletlenül indított műveletekből eredő problémák.

A párbeszédpanel mindazonáltal felajánlja a megerősítések letiltásának lehetőségét is.

Üzenetek újraellenőrzése

Az ESET Internet Security levelezőprogramokba integrált eszköztárán a felhasználók többféle e-mail ellenőrzési beállítást is megadhatnak. Az **Üzenetek újraellenőrzése** párbeszédpanelen két ellenőrzési mód közül választhat.

Az aktuális mappában lévő összes üzenetet – A levelezőprogramban megjelenített mappa üzeneteinek ellenőrzése.

Csak a kijelölt üzeneteket – Csak a felhasználó által kijelölt üzenetek ellenőrzése.

A már ellenőrzött üzenetek újraellenőrzése – A jelölőnégyzet bejelölése esetén újraellenőrizheti a korábban már ellenőrzött üzeneteket.

Levelezési protokollok

Az IMAP és POP3 a legelterjedtebb protokollok, amelyek segítségével fogadható az e-mail-kommunikáció a levelezőprogramokban. Az IMAP (Internet Message Access Protocol) egy másik internetes protokoll, amely az e-mailek beolvasására szolgál. Az IMAP-nek van néhány előnye a POP3 protokollal szemben, például több ügyfél egyszerre csatlakozhat ugyanahhoz a postaládához, és fenn tudják tartani az üzenetek állapotát, például azt, hogy az adott üzenetet elolvasták, megválaszolták, vagy törölték-e. A szabályozást biztosító védelmi modul automatikusan elindul a rendszer indításakor, majd ezután aktív marad a memóriában.

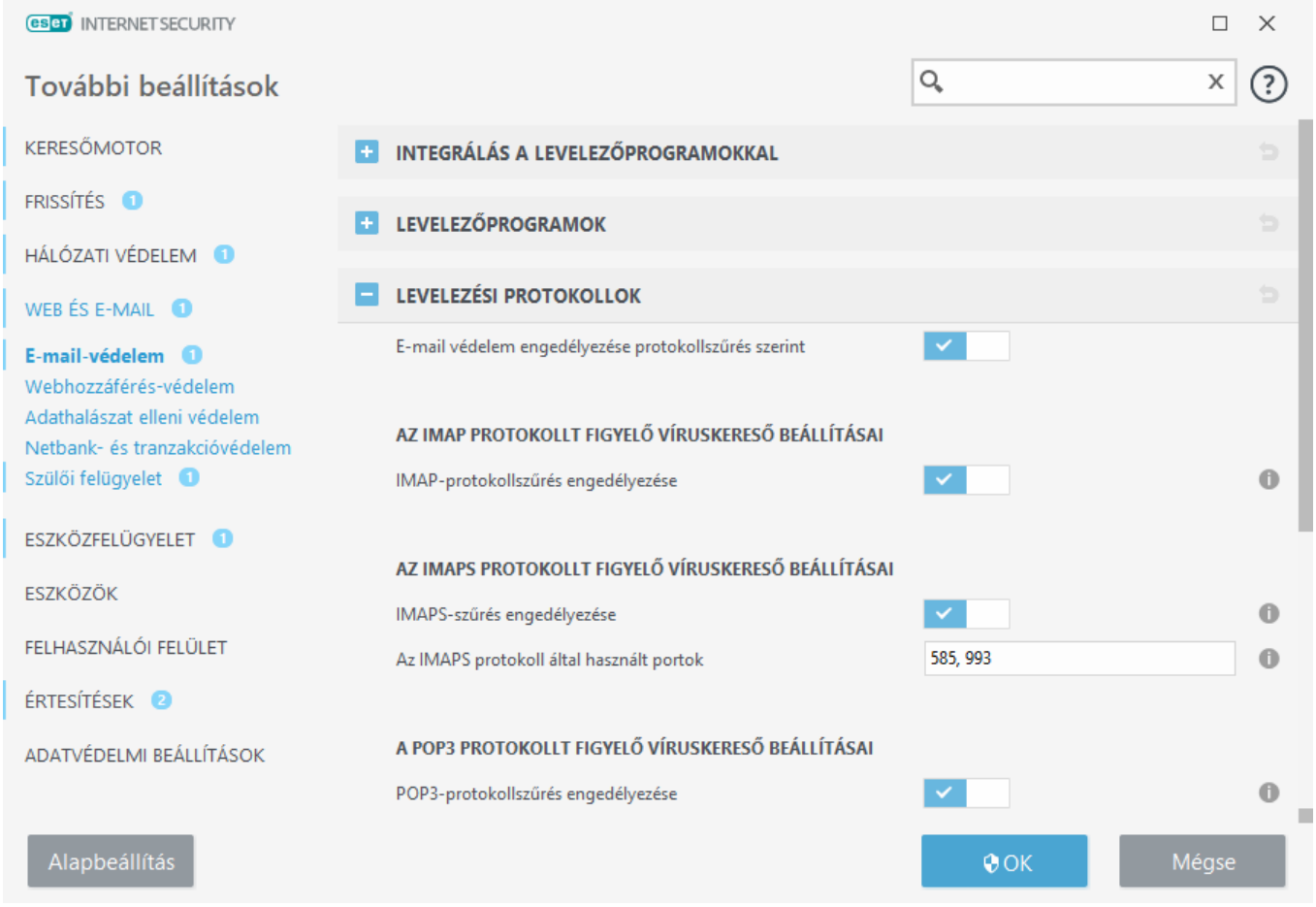
Az ESET Internet Security a levelezőprogramtól függetlenül képes védeni az ezeken a protokollokon keresztül zajló

kommunikációt anélkül, hogy szükség lenne a levelezőprogram újrakonfigurálására. Alapértelmezés szerint a POP3 és IMAP protokollon keresztül zajló kommunikáció is ellenőrzés alatt áll, az alapértelmezett POP3- és IMAP-portszámoktól függetlenül.
Az IMAP protokoll nem áll ellenőrzés alatt. A Microsoft Exchange szerverrel folytatott kommunikáció azonban ellenőriztethető az integrációs modullal az olyan levelezőprogramokban, mint a Microsoft Outlook.

Javasoljuk, hogy kapcsolja be az **E-mail-védelem engedélyezése protokollszűrés szerint** funkciót. Az IMAP/IMAPS és a POP3/POP3S protokoll ellenőrzését a **További beállítások** > **Web és e-mail** > **E-mail-védelem** > **Levelezési protokollok** elemet kiválasztva konfigurálhatja.

Az ESET Internet Security az IMAPS (585, 993) és a POP3S (995) protokoll ellenőrzését is támogatja, amelyek egy titkosított csatornán keresztül továbbítják az adatokat a szerver és a kliens között. Az ESET Internet Security képes az SSL és a TLS protokollon alapuló kommunikáció ellenőrzésére. A program az operációs rendszer verziójától függetlenül csak az **IMAPS/POP3S protokoll által használt portok** között megadott portokon fogja ellenőrizni az adatforgalmat. Szükség esetén más kommunikációs portok is hozzáadhatók. A portszámokat vesszővel kell elválasztani.

A program alapértelmezés szerint ellenőrzi a titkosított kommunikációt. A víruskereső beállításához nyissa meg a További beállítások > **Web és e-mail** > **SSL/TLS** lapot.



POP3/POP3S-szűrő

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

A szabályozást biztosító védelmi modul automatikusan elindul a rendszer indításakor, majd ezután aktív marad a

memóriában. Az automatikus POP3-ellenőrzéshez nincs szükség a levelezőkliens 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 kell elválasztani.

A program alapértelmezés szerint ellenőrzi a titkosított kommunikációt. A víruskereső beállításához nyissa meg a További beállítások > **Web és e-mail** > **SSL/TLS** lapot.

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

POP3-protokollszűrés engedélyezése – Az opció 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 Internet Security a POP3S protokoll ellenőrzését is támogatja. Ez a kommunikációtípus titkosított csatornán keresztül továbbítja az adatokat a szerver és a kliens között. Az ESET Internet Security képes az SSL és TLS protokollon alapuló kommunikáció ellenőrzésére.

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

POP3S-protokollszűrés a kijelölt portok esetén – Jelölje be ezt az opciót, 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 ellenőrizendő portok listája (alapértelmezés szerint a 995-ös port).

E-mail-címkék

A funkció beállításai a **További beállítások** lapon találhatók a **Web és e-mail** > **E-mail védelem** > **Riasztások és értesítések** részen.

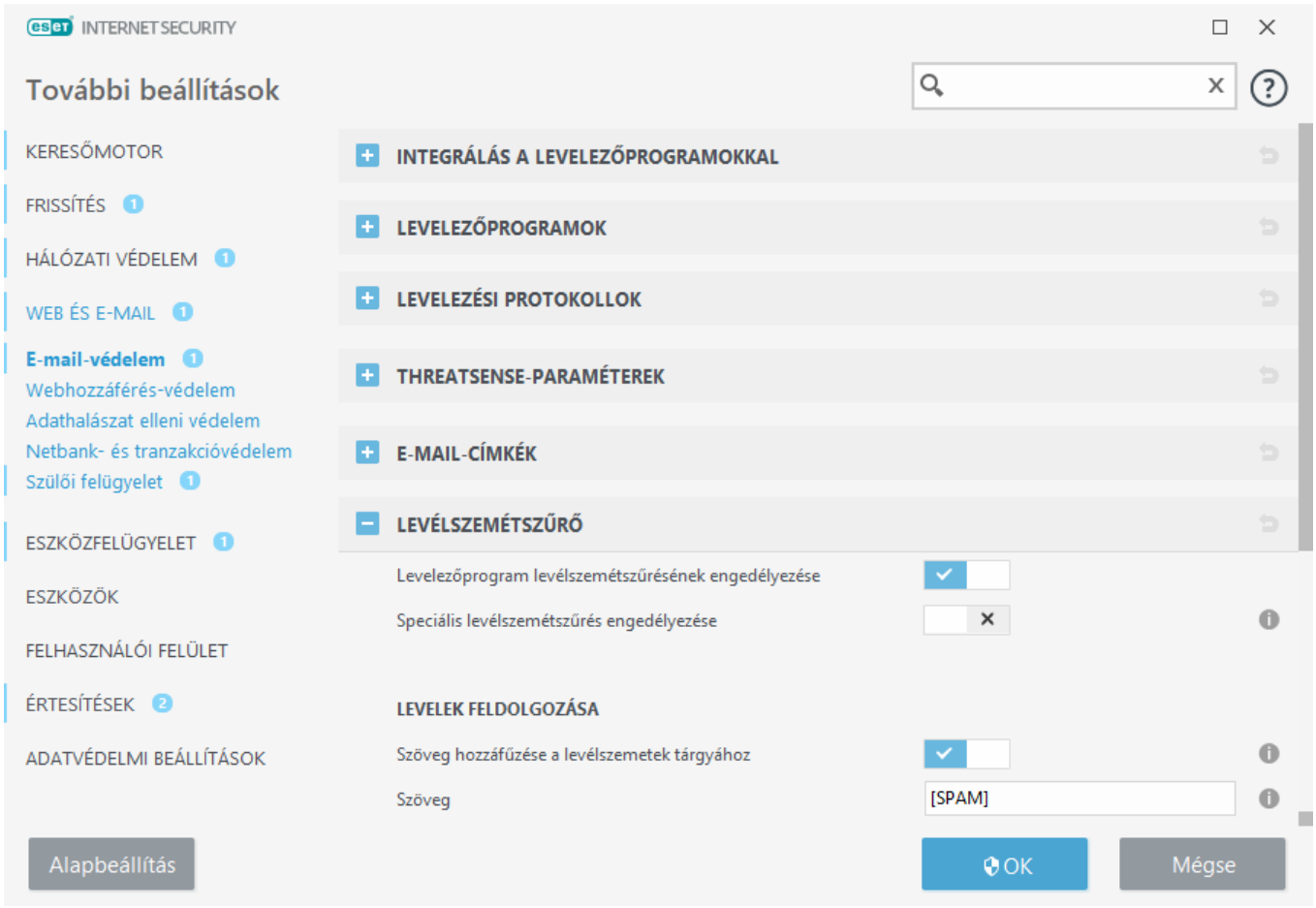
Miután a program ellenőriz egy-egy levelet, az ellenőrzés eredményét ismertető értesítést is hozzáfűzhet. Bejelölheti az **Értesítés hozzáfűzése a fogadott és elolvasott e-mailekhez** vagy az **Értesítés hozzáfűzése a kimenő e-mailekhez** jelölőnégyzetet. Ügyeljen arra, hogy a problémás HTML-üzenetekben az értesítések néha eltűnhetnek, illetve egyes kártevők képesek meghamisítani azokat. Az értesítések 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.
- **Kártevőészlelés esetén** – A program csak a kártékony szoftvert tartalmazó levelekhez fűz értesítést (alapértelmezett).
- **Minden e-mailhez ellenőrzéskor** – A program minden ellenőrzött levélhez értesítést fűz.

A fertőzött e-mailek tárgyához hozzáfűzendő szöveg – A sablon szerkesztésével módosíthatja a fertőzött e-mail tárgyában szereplő előtag formátumát. Ez a funkció az üzenet tárgyában szereplő "Hello" szót a következő formátumra cseréli: „[kártevő %KÁRTEVŐNEVE%] Hello”. Az %DETECTIONNAME% változó az észlelt kártevőt jelöli.

Levélszemétszűrő

Az elektronikus kommunikáció egyik legnagyobb problémáját a kéretlen levelek, más néven levélszemét áradata jelenti. A levélszemét a teljes levelezés mintegy 30 százalékát teszi ki. A levélszemétszűrés megoldást nyújt erre a problémára. A számos hatékony e-mailes biztonsági alapelvet kombináló Levélszemétszűrő modul egyedülálló szűrési képességekkel tartja tisztán postaládáját. A levélszemétszűrő konfigurálásához nyissa meg a **További beállítások** (F5) > **Web és e-mail** > **E-mail-védelem** > **Levélszemétszűrő** lapot.



A levélszemét észlelésének egyik fontos tényezője a kéretlen levelek felismerése előre definiált, megbízható címeket (engedélyezett), illetve tiltott címeket (tiltott) tartalmazó listák alapján.

A levélszemét észlelésének elsődleges módszere az e-mail-üzenetek 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.

Levelezőprogram levélszemétszűrésének engedélyezése – A jelölőnégyzet bejelölése esetén rendszerindításkor automatikusan aktiválódik a levélszemétszűrés.

Speciális levélszemétszűrés engedélyezése – A program további levélszemétszűrő-adatokat tölt le rendszeres időközönként, ezáltal növeli a levélszemétszűrő képességeit, és jobb eredményeket ér el.

Az ESET Internet Security levélszemétszűrője lehetővé teszi, hogy különböző paramétereket állítson be az üzenetekhez.

Levelek feldolgozása

Szöveg hozzáfűzése a levélszemetek tárgyához – Az opció bekapcsolása esetén egyéni szöveges előtagot fűzhet a levélszemétként azonosított levelek tárgyához. Az alapértelmezett előtag a „[SPAM]”.

Levelek áthelyezése a levélszemétmappába – Ha engedélyezve van az opció, akkor a program a levélszemétként azonosított leveleket áthelyezi az alapértelmezett levélszemétmappába, a jó levélként átminősített leveleket pedig a beérkezett üzenetek mappájába. Ha a jobb gombbal egy e-mailre kattint, és a helyi menüben kijelöli az ESET Internet Security elemet, választhat a rendelkezésre álló lehetőségek közül.

A következő mappa használata – Itt adhatja meg, hogy az észlelésüket követően melyik mappába kerüljenek a fertőzött e-mailek.

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

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

Levélszemétpontszám naplózása – az ESET Internet Security levélszemétszűrő motorja minden ellenőrzött üzenethez levélszemétpontszámot rendel. A program a levélszemétszűrő naplójában rögzíti az üzenetet (A program főablaka > **Eszközök** > **További eszközök** > **Naplófájlok** > **Levélszemétszűrő**).

- **Nincs** – A levélszemétszűrőtől származó pontszám nem kerül bele a naplóba.
- **Átminősítve és levélszemétként megjelölve** – Az opciót bejelölve rögzítheti a levélszemétként (SPAM) megjelölt üzenetek levélszemétpontszámát.
- **Összes** – A program minden üzenetet – a levélszemétpontszámmal együtt – rögzít a naplóban.

Ha kijelöl egy levelet a levélszemétmappában, a **Kiválasztott levelek átminősítése jó levéllé** lehetőséget választva áthelyezheti azt a beérkezett üzenetek mappájába. Amikor kijelöl egy levélszemétnek tekintett levelet a beérkezett üzenetek mappájában, az **Üzenetek átminősítése levélszeméttté** opciót választva a levelet áthelyezheti a levélszemétmappába. Több levelet is kijelölhet, és egyszerre elvégezheti rajtuk a műveletet.

Az ESET Internet Security támogatja a levélszemétszűrést a Microsoft Outlook, Outlook Express, Windows Mail és a Windows Live Mail esetén.

Címfeldolgozási eredmény

Új címek hozzáadásakor vagy egy e-mail-cím esetén végrehajtandó művelet módosításakor az ESET Internet Security értesítést jelenít meg. A tájékoztató üzenet tartalma a végrehajtani kívánt művelettől függ.

A **Ne kérdezzen rá újra** jelölőnégyzet bejelölve a későbbiekben a program nem teszi fel újra a kérdést, hanem automatikusan végrehajtja a most választott műveletet.

Levélszemét-címlisták

Az ESET Internet Security levélszemétszűrő szolgáltatása lehetővé teszi a névjegyalbumok különböző paramétereinek a beállítását.

Felhasználói címlista engedélyezése – A jelölőnégyzet bejelölésével aktiválhatja a felhasználói címlistát.

Felhasználói címlista – Azone-mail-címek listája, ahol címeket adhat hozzá, szerkeszthet vagy törölhet a levélszemétszűrő szabályok meghatározásához. A listában szereplő szabályok az aktuális felhasználóra fognak vonatkozni.

Globális címlista engedélyezése – A jelölőnégyzet bejelölésével aktiválhatja az eszközön az összes felhasználó által megosztott globális címlistát.

Globális címlista – Azone-mail-címek listája, ahol címeket adhat hozzá, szerkeszthet vagy törölhet a levélszemétszűrő szabályok meghatározásához. A listában szereplő szabályok minden felhasználóra vonatkozni fognak.

Automatikus engedélyezés és felvétel a felhasználói címlistára

A névjegyalbumban szereplő címek megbízhatóként való kezelése – A névjegyalbumában szereplő címek megbízhatóként lesznek kezelve a felhasználói címlistára való felvételük nélkül is.

Címzettek címeinek hozzáadása a kimenő levelekből – A címzettek címeinek felvétele a kimenő levelekből a felhasználói címlistára engedélyezettként.

Címek hozzáadása a JÓ levéllé átminősített levelekből – A feladók e-mail-címének felvétele a JÓ levéllé átminősített levelekből a felhasználói címlistára engedélyezettként.

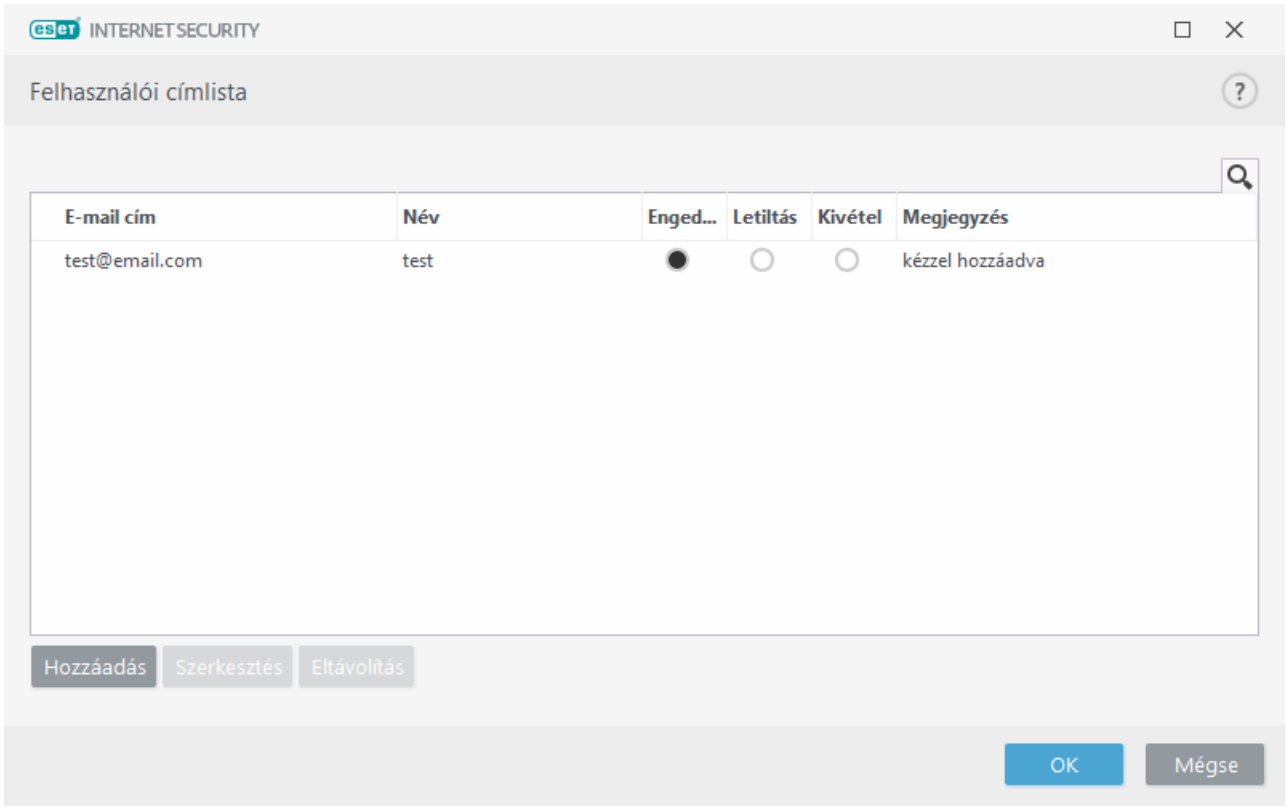
Automatikus hozzáadás a felhasználó címlistájához kivételként

Címek hozzáadása saját fiókokból – Címek felvétele a meglévő levelezőprogram fiókjaiból a felhasználói címlistára kivételként.

Címlisták

Az ESET Internet Security a kéretlen e-mailek elleni védelem biztosítására listák segítségével lehetővé teszi az e-mail-címek minősítését.

A címlisták szerkesztéséhez nyissa meg a **További beállítások** (F5) > **Web és e-mail** > **E-mail-védelem** > **Levélszemét-címlisták** lapot, majd kattintson a **Szerkesztés** elemre a **Felhasználói címlista** vagy a **Globális címlista** szöveg mellett.



Oszlopok

E-mail-cím – Az a cím, amelyre a szabály vonatkozni fog.

Név – Az egyéni szabály neve.

Engedélyezés/Letiltás/Kivétel – Az e-mail-cím esetén végrehajtandó művelet meghatározására szolgáló választógombok (kattintson a választógombra a kívánt oszlopban a művelet gyors módosításához):

- **Engedélyezés** – Olyan címek, amelyek biztonságosnak tekinthetők, és akiktől üzeneteket szeretne kapni.
- **Letiltás** – Olyan címek, amelyek nem biztonságosnak/levélszemétnek tekinthetők, és akiktől nem szeretne üzeneteket kapni.
- **Kivétel** – Olyan címek, amelyeknél mindig végbemegy a levélszemét ellenőrzése, és amelyeket meghamisíthatnak és kéretlen levelek küldésére használhatják.

Megjegyzés – Információ a szabály létrehozásának módjáról és arról, hogy a teljes tartományra/alacsonyabb szintű tartományokra vonatkozik-e.

A címek kezelése

- **Hozzáadás** – Ide kattintva hozzáadhat egy szabályt egy új címhez.
- **Szerkesztés** – Válasszon ki egy meglévő szabályt és kattintson rá a szerkesztéséhez.
- **Eltávolítás** – Válassza ki, majd kattintson rá, ha el szeretne távolítani egy szabályt a címlistáról.

Cím felvétele vagy módosítása

Ez az ablak lehetővé teszi egy cím hozzáadását vagy szerkesztését a levélszemetes címlistában, és konfigurálhatja a végrehajtandó műveletet:

E-mail-cím – Az a cím, amelyre a szabály vonatkozni fog.

Név – Az egyéni szabály neve.

Művelet – Végrehajtandó művelet, ha az adott e-mail-cím megegyezik az **E-mail-cím** mezőben megadott címmel:

- **Engedélyezés** – Olyan címek, amelyek biztonságosnak tekinthetők, és akiktől üzeneteket szeretne kapni.
- **Letiltás** – Olyan címek, amelyek nem biztonságosnak/levélszemétnek tekinthetők, és akiktől nem szeretne üzeneteket kapni.
- **Kivétel** – Olyan címek, amelyeknél mindig végbemegy a levélszemét ellenőrzése, és amelyeket meghamisíthatnak és kéretlen levelek küldésére használhatják.

Teljes tartomány – A jelölőnégyzet bejelölése esetén a szabály a megadott e-mail-címben szereplő teljes tartományra érvényes lesz – ha például az **E-mail-cím** mezőben a valaki@cim.info címet adta meg, a bejegyzés a teljes *cim.info* tartományra fog vonatkozni.

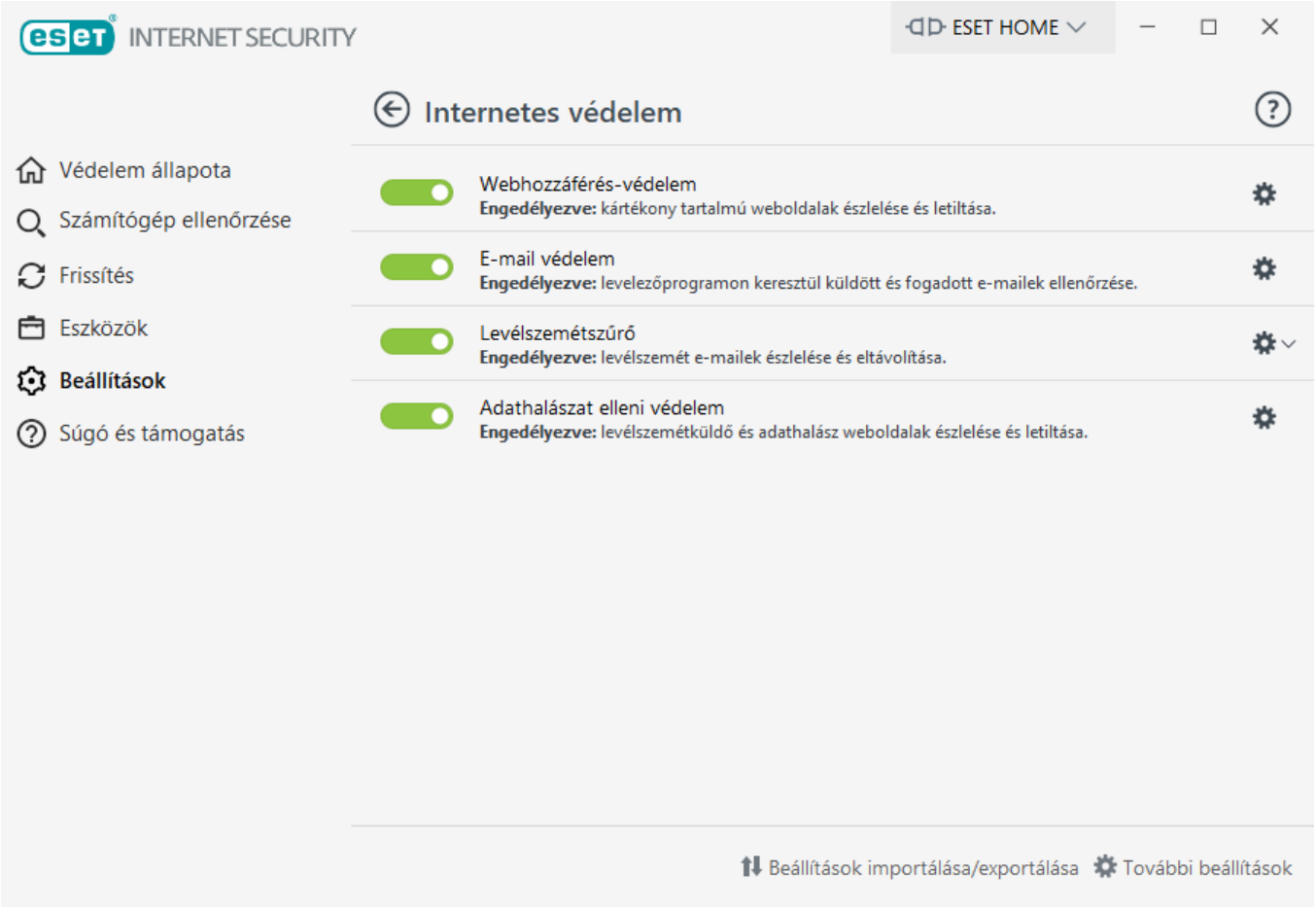
Alacsonyabb szintű tartományok – Ezt a jelölőnégyzetet bejelölve a szabály az alsóbb szintű tartományokra is érvényes lesz – a fenti példánál maradva a *cim.info* tartomány mellett a *sajat.cim.info* altartományra is.

Webhozzáférés-védelem

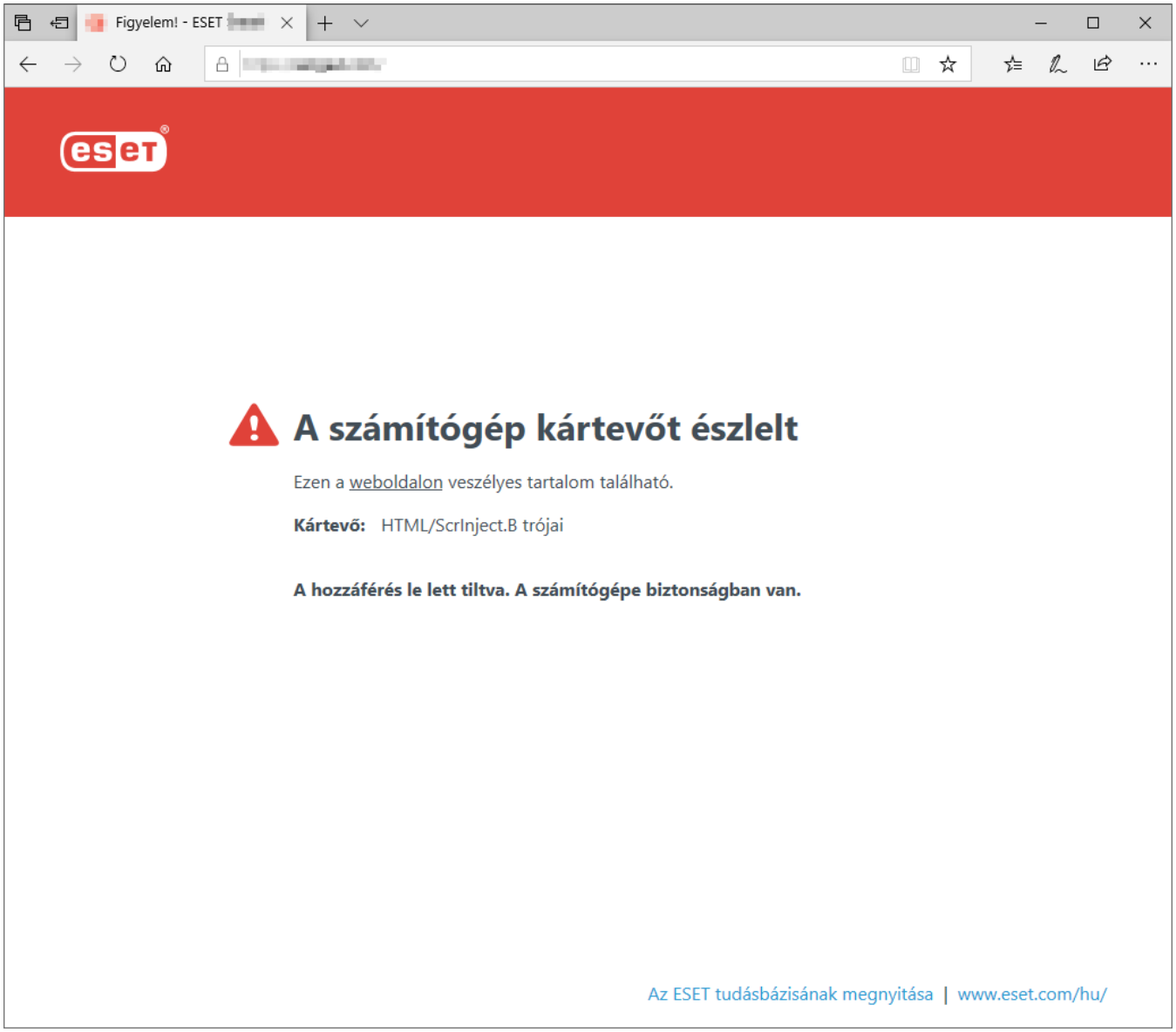
Az internetelérés a személyi számítógépek alapvető szolgáltatásaihoz tartozik. Sajnos a kártevők is ezt használják ki a terjedéshez. A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP és a HTTPS (titkosított kommunikáció) protokollon alapuló szabályokat.

A tartalom letöltése előtt a program letiltja a hozzáférést azokhoz a weboldalakhoz, amelyekről ismert, hogy nem kívánt tartalommal bírnak. A ThreatSense keresőmotor minden más weboldalon vírusellenőrzést hajt végre a weboldal megnyitásakor, és letiltja a weboldalt, ha kártékony tartalmat észlel. A webhozzáférés-védelem két védelmi szintet kínál: a tiltólista, illetve a tartalom alapján történő letiltást.

Kifejezetten javasoljuk, hogy engedélyezze a Webhozzáférés-védelem funkciót. A beállítás a fő programablak > **Beállítások** > **Internetes védelem** > **Webhozzáférés-védelem** útvonalon érhető el.



A webhozzáférés-védelem a következő üzenetet jeleníti meg a böngészőben, ha a webhely le van tiltva:



Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- Annak megakadályozása, hogy a Webhozzáférés-védelem letiltson egy biztonságos webhelyet
- Webhely letiltása az ESET Internet Security segítségével

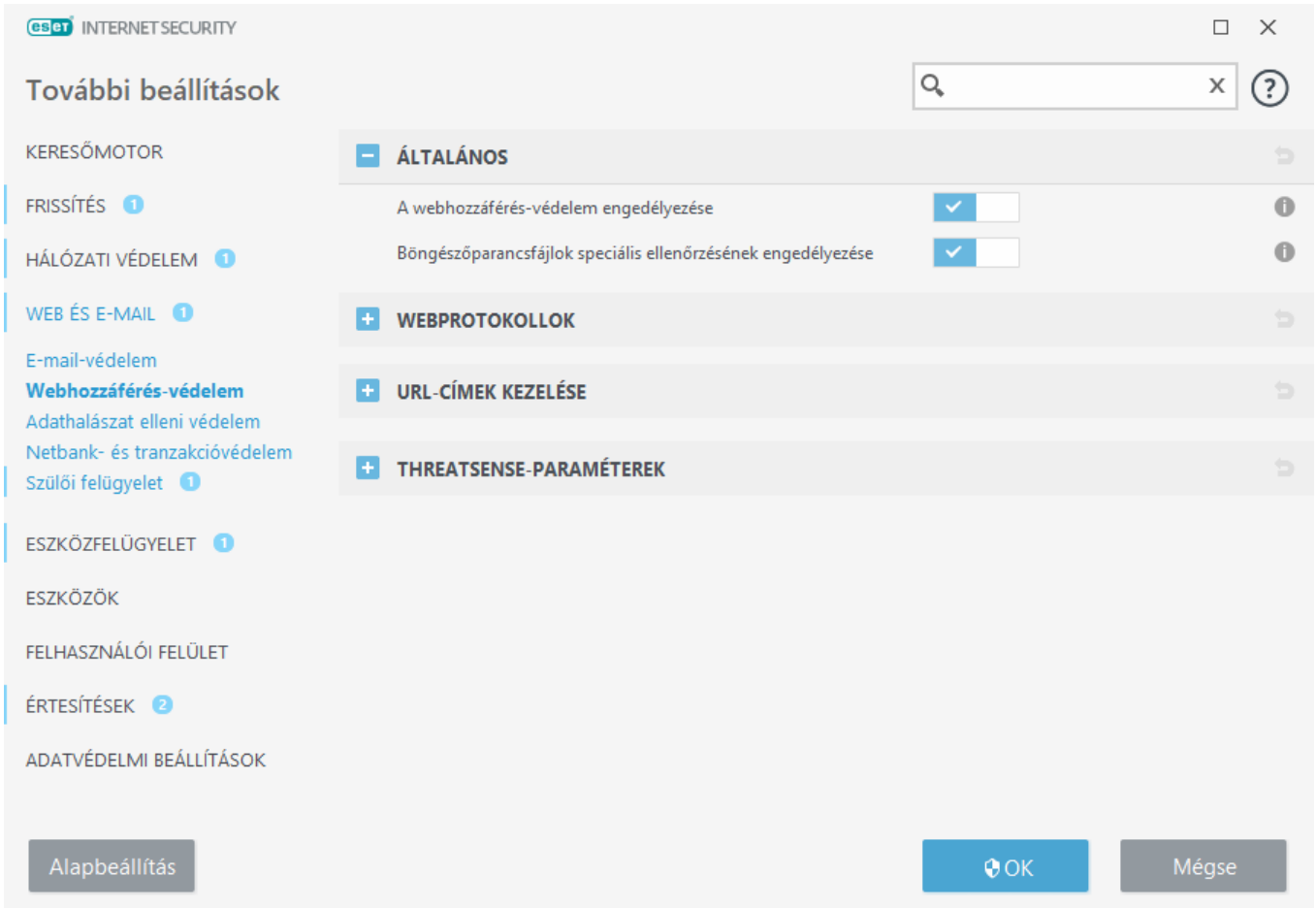
A **További beállítások** (F5) > **Web és e-mail** > **Webhozzáférés-védelem** lehetőséget választva az alábbi beállítások érhetők el:

Általános – A funkció engedélyezése vagy letiltása a További beállításokban.

Webprotokollok – Segítségével konfigurálhatja azoknak a szabványos protokolloknak a figyelését, amelyeket a legtöbb internetböngésző használ.

URL-címek kezelése – Segítségével letilthat, engedélyezhet és kizárhat az ellenőrzésből URL-címeket.

A ThreatSense paraméterei – Itt további víruskeresési beállításokkal megadhatja az ellenőrizendő objektumok típusát (e-mailek, archívumok stb.), a webhozzáférés-védelmi észlelési módszereket stb.



A webhozzáférés-védelem haladó beállításai

A **További beállítások** (F5) > **Web és e-mail** > **Webhozzáférés-védelem** > **Általános**lehetőséget választva az alábbi beállítások érhetők el:

A webhozzáférés-védelem engedélyezése – Ha letiltja, a rendszer nem futtatja a webhozzáférés-védelmet és az adathalászat elleni védelmet. Ez a beállítás akkor érhető el, ha az SSL/TLS-protokollszűrés engedélyezve van.

Böngészőparancsfájlok speciális ellenőrzésének engedélyezése – Ha engedélyezve van, a keresőmotor az internetböngészők által végrehajtott összes JavaScript programot ellenőrizni fogja.

Kifejezetten javasoljuk, hogy hagyja engedélyezve a Webhozzáférés-védelem funkciót.

Webprotokollok

Az ESET Internet Security alapértelmezés szerint be van állítva a legtöbb internetes böngészőben használt HTTP protokoll figyelésére.

A HTTP protokollt figyelő víruskereső beállításai

A HTTP-forgalmat mindig figyeli a rendszer az összes alkalmazás összes portján.

A HTTPS protokollt figyelő víruskereső beállításai

Az ESET Internet Security támogatja a HTTPS-protokollszűrést is. A HTTPS kommunikációtípus titkosított csatornán keresztül továbbítja az adatokat a szerver és a kliens között. Az ESET Internet Security képes az SSL és a TLS protokollon alapuló kommunikáció ellenőrzésére. A program az operációs rendszer verziójától függetlenül csak a **HTTPS protokoll által használt portok** között megadott portokon (443, 0-65535) fogja ellenőrizni az adatforgalmat.

A program alapértelmezés szerint ellenőrzi a titkosított kommunikációt. A víruskereső beállításához nyissa meg a További beállítások > **Web és e-mail** > **SSL/TLS** lapot.

URL-címek kezelése

A témakörből megtudhatja, miként tilthat le, engedélyezhet és zárhat ki a tartalomellenőrzésből HTTP-címeket.

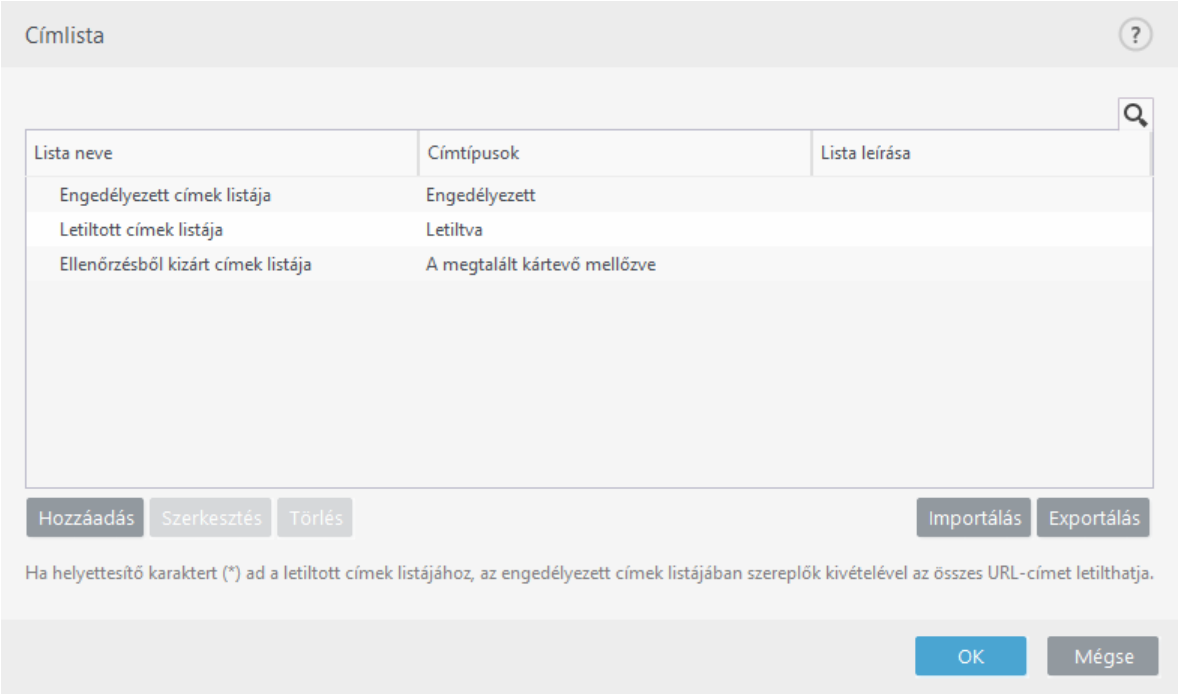
Ha a HTTP-weboldalak mellett a HTTPS-címeket is szeretné szűrni, jelölje be az SSL/TLS-protokollszűrés engedélyezése jelölőnégyzetet. Egyébként csak a felkeresett HTTPS-webhelyek tartományait veszi fel a program, a teljes URL-címet nem.

A **Letiltott címek listájában** szereplő webhelyek csak akkor érhetők el, ha az **Engedélyezett címek listája** is tartalmazza őket. Az **Ellenőrzésből kizárt címek listájában** található webhelyek elérése közben a program nem keres kártékony kódokat.

Ha az aktív **Engedélyezett címek listájában** szereplő címeken kívül az összes *-címet le szeretné tiltani, vegyen fel HTTP karaktert a **Letiltott címek listájára**.

A * (csillag) és a ? (kérdőjel) használható a listákban. 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 meg szeretné tudni, hogy miként lehet biztonságosan egyeztetni egy teljes tartományt az összes altartománnyal együtt, olvassa el a HTTP-címet vagy -tartományt meghatározó maszk hozzáadása című témakört. 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 az alkalmazásakor** jelölőnégyzetet.

> **Megbízható tartományok**
> Nem kerül sor a címek szűrésére, ha aktív a **Web és e-mail** > **SSL/TLS** > **Megbízható tartományokkal való kommunikáció kizárása** beállítás, és a tartomány megbízható.



Vezérlőelemek

Hozzáadás – Ezzel a gombbal az előre megadott listák mellett új listákat hozhat létre. Ez hasznos lehet, ha logikusan fel szeretné osztani a különféle címcsoportokat. A letiltott címek egyik listája például tartalmazhat külső nyilvános tiltólistákon szereplő címeket, míg egy másik tartalmazhatja a saját tiltólistáját, így egyszerűen frissítheti a külső listát úgy, hogy a sajátja változatlan maradjon.

Szerkesztés – A meglévő listák módosítására szolgál. Ide kattintva felvehet címeket, illetve eltávolíthatja őket a listáról.

Törlés – A meglévő listák törlésére használható. Csak a **Hozzáadás** gombbal létrehozott listákhoz használható, az alapértelmezett listáknál nem.

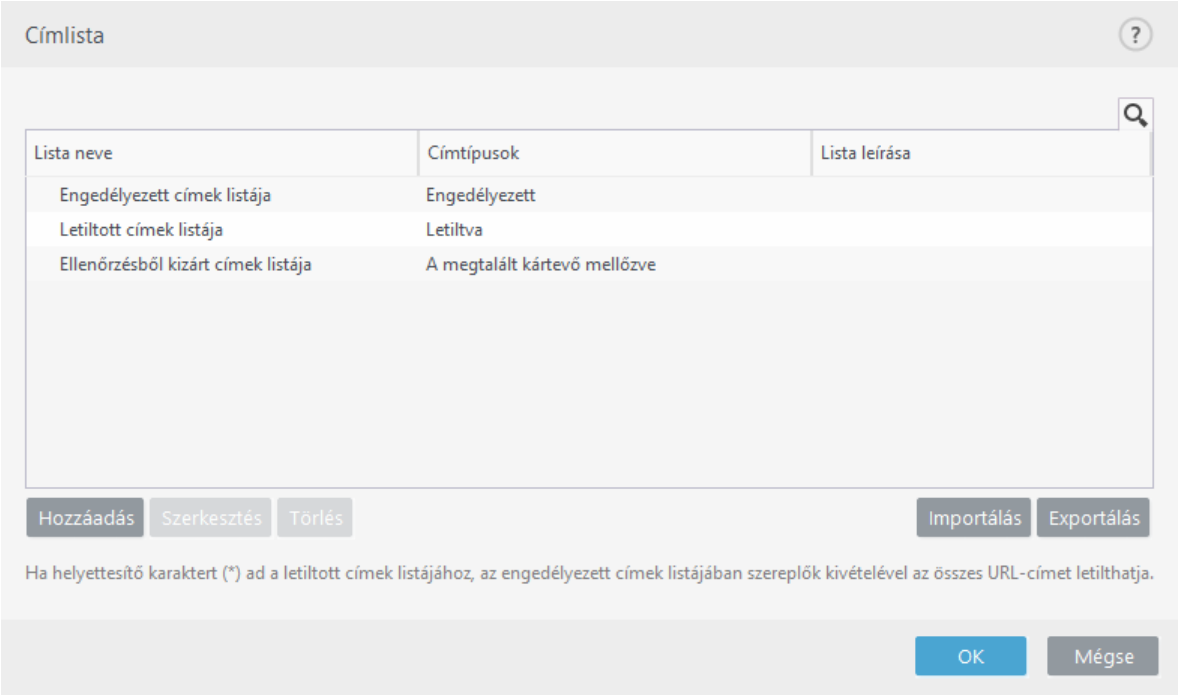
URL-címlista

Ezen a részen adhatja meg a letiltott vagy engedélyezett, illetve az ellenőrzésből kizárt HTTP-címek listáit.

Alapértelmezés szerint az alábbi három lista áll rendelkezésre:

- **Ellenőrzésből kizárt címek listája** – A program a listában szereplő egyetlen cím esetén sem keres kártevő kódokat.
- **Engedélyezett címek listája** – Ha csak az engedélyezett címek listájában szereplő HTTP-címekhez való hozzáférés van engedélyezve, és a letiltott címek listája * (mindent helyettesítő) karaktert tartalmaz, a felhasználónak csak az e listában megadott címekhez lesz hozzáférése. Az e listában található címek akkor is engedélyezettek, ha szerepelnek a letiltott címek listájában.
- **Letiltott címek listája** – A felhasználó csak akkor férhet hozzá az ebben a listában megadott címekhez, ha az engedélyezett címek listájában is szerepelnek.

A **Hozzáadás** gombra kattintva újabb listát készíthet. A kijelölt listák törléséhez kattintson a **Törlés** gombra.



Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- Annak megakadályozása, hogy a Webhozzáférés-védelem letiltson egy biztonságos webhelyet
- Webhely letiltása az ESET Windows otthoni termékek segítségével

További információt az URL-címek kezelése című témakörben talál.

Új URL-címlista létrehozása

Ebben a csoportban megadhatja a letiltott vagy engedélyezett, illetve az ellenőrzésből kizárt URL-címeket és -maszkokat definiáló listákat.

Új lista létrehozásakor az alábbi beállításokat adhatja meg:

Címlista típusa – Három listatípus áll rendelkezésre:

- **Ellenőrzésből kizárva** – A program a listában szereplő egyetlen cím esetén sem keres kártevő kódokat.
- **Letiltott** – Az ebben a listában szereplő címeket nem érheti el a felhasználó.
- **Engedélyezett** – Ha a „Hozzáférés engedélyezése csak az engedélyezett címek listájában szereplő HTTP-címekhez” opció van engedélyezve, és a letiltott címek listája * (mindent helyettesítő) karaktert tartalmaz, a felhasználónak csak az e listában megadott címekhez lesz hozzáférése. Az e listában található címek akkor is engedélyezettek, ha megegyeznek a letiltott címek listájában szereplő címekkel.

Lista neve – Ebben a mezőben adható meg a lista neve. A mező szürkén jelenik meg, ha éppen szerkeszti a három előre definiált lista egyikét.

Lista leírása – A mezőben rövid ismertetőt írhat a listához (nem kötelező). Szürkén jelenik meg, ha éppen szerkeszti a három előre definiált lista egyikét.

Ha aktiválni szeretne egy listát, jelölje be a kívánt lista melletti **Lista aktiválása** jelölőnégyzetet. Ha értesülni

szeretne arról, hogy egy adott listát felhasználnak egy Ön által már felkeresett HTTP-webhely értékeléséhez, jelölje be az **Értesítés az alkalmazásakor** jelölőnégyzetet. Ebben az esetben értesítést kap például arról, ha egy webhelyet letiltanak vagy engedélyeznek, mivel az szerepel a letiltott vagy az engedélyezett címek listáján. Az értesítésben szerepelni fog a szóban forgó webhelyet tartalmazó lista neve.

Vezérlőelemek

Hozzáadás – Új URL-cím hozzáadása a listához (több érték esetén használjon elválasztójelet).

Szerkesztés – A meglévő cím módosítása a listában. Csak a **Hozzáadás** gombbal létrehozott címek esetén használható.

Eltávolítás – Meglévő címek eltávolítása a listából. Csak a **Hozzáadás** gombbal létrehozott címek esetén használható.

Importálás – Fájl importálása URL-címekkel (az értékeket sortöréssel válassza el egymástól, például: UTF-8 kódolást használó *.txt).

URL-maszk hozzáadása

A kívánt cím- vagy tartománymaszk megadása előtt tanulmányozza a párbeszédpanelen megjelenő információkat.

Az ESET Internet Security lehetővé teszi bizonyos webhelyek elérésének és böngészőbeli megjelenítésének letiltását. Emellett az ellenőrzésből kizárni kívánt címek megadására is lehetőség van. A cím megadásakor helyettesítő karakterek is használhatók, így egyszerre weboldalak egész csoportját is le lehet tiltani, vagy fel lehet venni kivételként. A címmaszkok kérdőjeleket (?) és csillagokat (*) tartalmazhatnak:

- A kérdőjel egyetlen karaktert jelöl.
- A csillag tetszőleges hosszúságú karakterláncot helyettesít.

A *.c?m kifejezés például az összes olyan címet lefedi, amelynek utolsó része c betűvel kezdődik, m betűvel végződik, és a kettő között egyetlen karakter szerepel (például .com, .cam stb.).

A tartomány nevében a kezdő „*.” karaktersorozat speciálisan kezelendő, ha azt a tartománynév elején használják. A * helyettesítő karakter ebben az esetben nem felel meg a perjel („/”) karakternek. Ezzel elkerülhető a maszk megkerülése, a **.tartomany.hu* maszk például nem fog megfelelni a *http://barmelytartomany.hu/barmelyeleresiut#.tartomany.hu* címnek (ilyen utótag bármelyik URL-címhez hozzáfűzhető anélkül, hogy az hatással lenne a letöltésre). A „*.” továbbá egy üres sztringnek is megfelel ebben a speciális esetben. Ennek célja, hogy egyetlen maszk használatával lehessen engedélyezni egy teljes tartományt a hozzá tartozó esetleges altartományokkal együtt. A **.tartomany.hu* maszk például a *http://tartomany.hu* címnek is megfelel. A **tartomany.hu* használata helytelen lenne, mivel az a *http://masiktartomany.hu* címnek is megfelelne.

Adathalászat elleni védelem

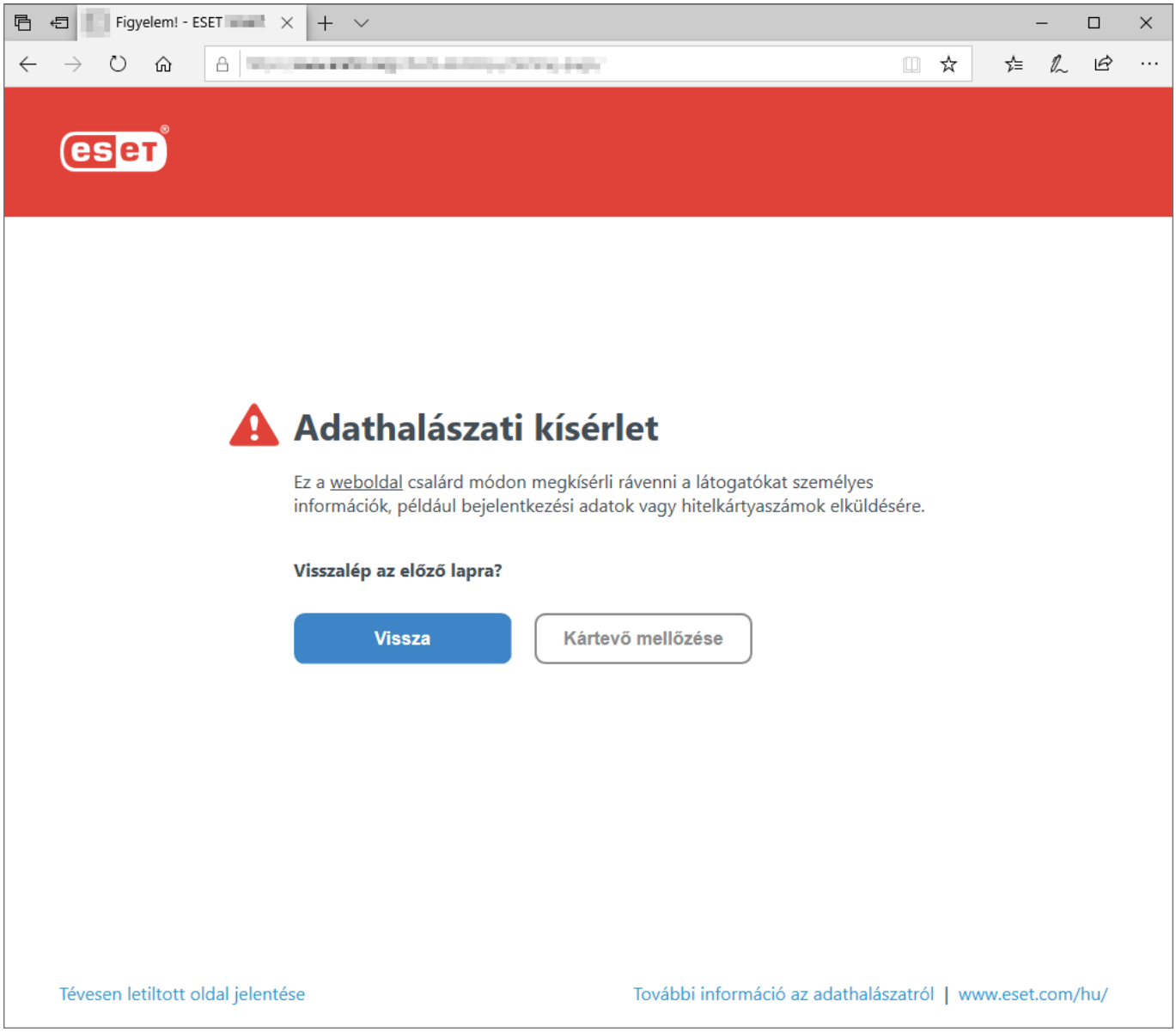
Az adathalászat kifejezés olyan bűnözői tevékenységet határoz meg, amely pszichológiai manipulációt alkalmaz (vagyis a felhasználót bizalmas információk kiszolgáltatására veszi rá). Az adathalászat gyakran bizalmas adatok, többek között bankszámlaszámok, PIN kódok vagy más adatok megszerzésére irányul. Erről a tevékenységről a szószedetben olvashat bővebben. Az ESET Internet Security az ilyen tartalommal rendelkező ismert weboldalak letiltásának lehetővé tételével támogatja az adathalászat elleni védelmet.

Javasoljuk, hogy engedélyezze az adathalászat elleni védelmet az ESET Internet Security alkalmazásban. Ehhez nyissa meg a **További beállítások** párbeszédpanelt (az F5 billentyű lenyomásával), és keresse meg a **Web és e-mail** > **Adathalászat elleni védelem** lehetőséget.

A tudásbáziscikkünk további információkat tartalmaz az ESET Internet Security adathalászat elleni védelméről.

Adathalász webhely elérése

Az ismert adathalász webhelyek megnyitásakor az alábbi párbeszédpanel jelenik meg a böngészőben. Ha továbbra is meg szeretné nyitni a webhelyet, kattintson a **Kártevő mellőzése** (nem javasolt) gombra.



Az engedélyezőlistán szereplő lehetséges adathalász webhelyek alapértelmezés szerint néhány óra múlva lejárnak. Webhelyek végleges engedélyezéshez használhatja az URL-címek kezelése eszközt. A **További beállítások** (F5) > **Web és e-mail** > **Webhozzáférés-védelem** > **URL-címek kezelése** > **Címlista** > **Szerkesztés** gombra, és vegye fel a szerkeszteni kívánt webhelyet erre a listára.

Adathalász webhely jelentése

A **Jelentés** hivatkozást használva jelenthet egy adathalász/kártevő webhelyet az ESET számára elemzés céljából.

Mielőtt egy webhelyet jelentene az ESET számára, ellenőrizze, hogy megfelel-e legalább az egyik alábbi feltételnek:
- A program egyáltalán nem észleli a webhelyet.
- A program tévesen kártevőként ismeri fel a webhelyet. Ilyenkor lehetősége van a tévesen letiltott oldal jelentésére.

A webhelyet e-mailben is elküldheti. Az e-mailt küldje a samples@eset.com címre. Az e-mail tárgyában írja le röviden és érthetően a problémát (angolul), az e-mailben pedig adjon meg minél több adatot a webhelyről (például mely webhelyről érte el, hogyan szerzett róla tudomást stb.).

Hálózati védelem

A hálózati védelem konfigurációja a **Hálózati védelem Beállítások** ablaktábláján található.

Az egyes védelmi modulok szüneteltetéséhez vagy letiltásához kattintson a csúszkára .

A védelmi modulok kikapcsolása esetén csökkenhet a számítógép védelmi szintje.



Tűzfal – Itt beállíthatja az ESET Tűzfal szűrési üzemmódját. A részletesebb beállítások eléréséhez kattintson a fogaskereket ábrázoló ikonra , majd a **Konfigurálás** elemre a **Tűzfal** felirat mellett, vagy nyomja le az **F5** billentyűt a További beállítások párbeszédpanel megnyitásához.

Konfigurálás – Megnyitja a Tűzfal ablakot a További beállítások párbeszédpanelen, ahol megadhatja, hogy a tűzfal hogyan kezelje a hálózati kommunikációt.

Tűzfal felfüggesztése (az összes forgalom engedélyezése) – Az összes forgalom tiltásával ellentétes hatással jár. Ha ezt a lehetőséget választja, a tűzfal összes szűrési beállítását kikapcsolja, és minden bejövő, illetve kimenő kapcsolatot engedélyez. Miközben a hálózati forgalom szűrése ebben a módban van, kattintson **A tűzfal engedélyezése** elemre a tűzfal újbóli engedélyezéséhez.

Minden forgalom letiltása – A tűzfal letiltja az összes bejövő és kimenő kommunikációt. Ezt a lehetőséget csak olyan különleges biztonsági kockázat felmerülése esetén alkalmazza, amely megköveteli a rendszer leválasztását a hálózatról. Miközben a hálózati forgalom szűrése **Minden forgalom letiltása** módban van, **Az összes forgalom letiltásának megszüntetése** elemre kattintva visszaállíthatja a személyi tűzfal normál működését.

Automatikus üzemmód (amikor egy másik szűrési mód van engedélyezve) – Az elemre kattintva automatikusra változtathatja a szűrési üzemmódot (felhasználó által definiált szabályokkal).

Interaktív üzemmód (amikor egy másik szűrési mód van engedélyezve) – Az elemre kattintva interaktívra változtathatja a szűrési üzemmódot (felhasználó által definiált szabályokkal).

Hálózati támadások elleni védelem (IDS) – Elemzi a hálózati forgalom tartalmát, és védelmet biztosít a hálózati támadásokkal szemben. A károsnak tűnő adatforgalmat letiltja. Az ESET Internet Security tájékoztatja Önt, ha egy védtelen vezeték nélküli hálózathoz vagy egy gyenge védelemmel rendelkező hálózathoz csatlakozik.

Botnet elleni védelem – Gyorsan és pontosan kiszúrja a kártékony programokat a rendszerben.

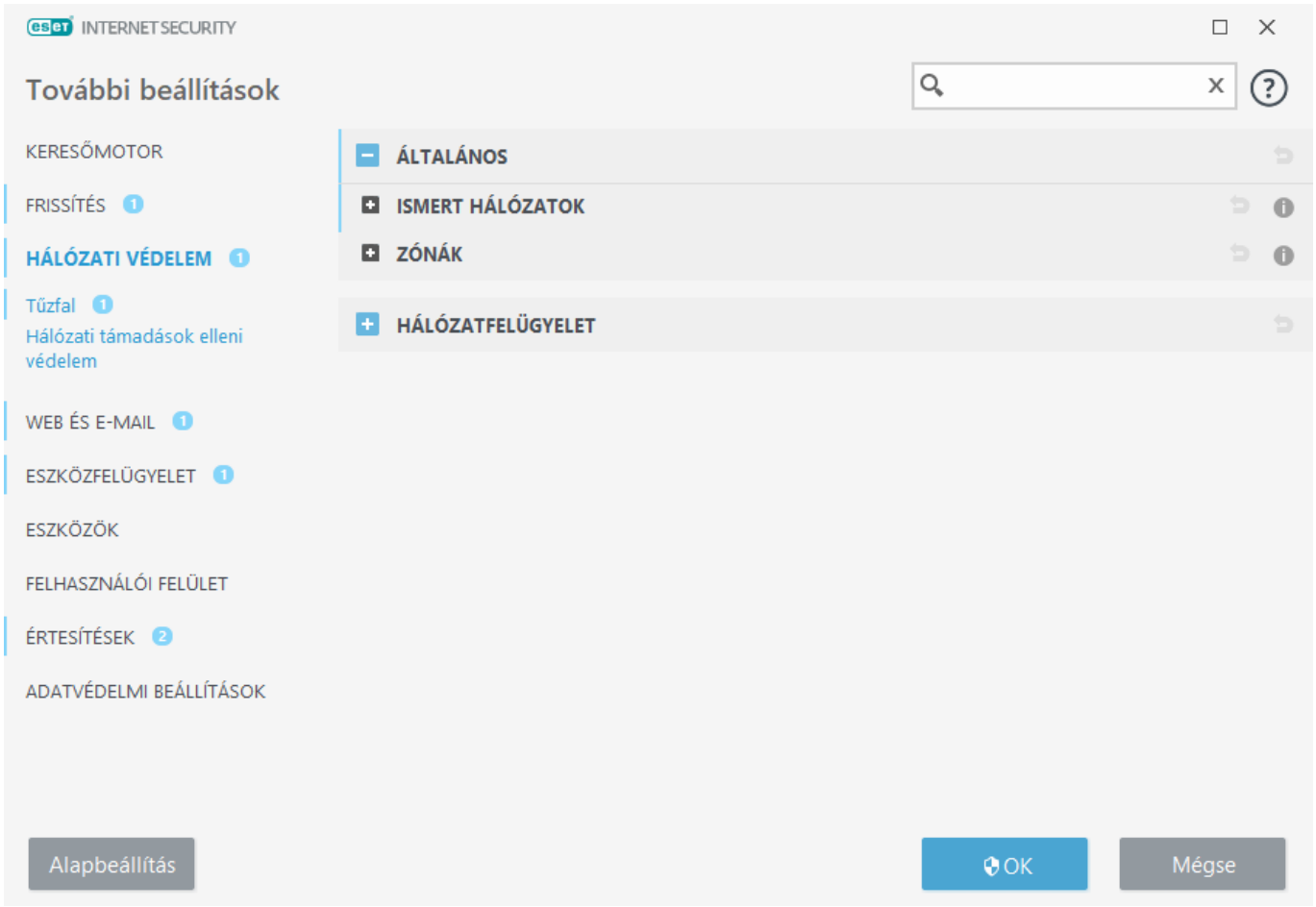
Csatlakoztatott hálózatok – Megjeleníti azokat a hálózatokat, amelyekhez hálózati adapterek vannak csatlakoztatva. Miután rákattintott a hálózat neve alatti linkre, egy felugró ablak lehetővé teszi a hálózat megbízhatóként történő konfigurálását.

IP-címek ideiglenes tiltólistája – Megjelenítheti azoknak az IP-címeknek a listáját, amelyeket támadások forrásaként észlelt a program, és felvett a tiltólistára, hogy bizonyos időtartamra letiltsa a kapcsolatot. Ha további információra van szüksége, jelölje ki a beállítást, és nyomja le az F1 billentyűt.

Hibaelhárítási varázsló – Segítségével megoldhatja az ESET Tűzfal által okozott kapcsolódási problémákat. Részletesebb információkért olvassa el a Hibaelhárítási varázsló című témakört.

Hálózatvédelem speciális beállítása

A program főablakában kattintson a **Beállítás** > **További beállítások** (F5) > **Hálózati védelem** elemre.



Általános

Ismert hálózatok

További információkért tekintse meg az Ismert hálózatok című részt.

Zónák

Egy-egy zóna olyan hálózati címek gyűjteménye, amelyek egy logikus csoportot alkotnak. További információkért tekintse meg a Zónák konfigurálása című részt.

Hálózatfelügyelet

Hálózatfelügyelet engedélyezése

A Hálózatfelügyelet segít beazonosítani az otthoni hálózaton a biztonsági réseket, például a nyitott portokat vagy a gyenge routerjelszót. A csatlakoztatott eszközök listáját is biztosítja, eszköztípus szerint kategorizálva.

Értesítés újonnan észlelt hálózati eszközökről

A program értesítést jelenít meg, ha a hálózaton új eszközt észlel.

Ismert hálózatok

Ha olyan számítógépet használ, amely gyakran csatlakozik nem megbízható vagy a megbízható (otthoni vagy munkahelyi) hálózatán kívüli hálózatokhoz, azt ajánljuk, hogy ellenőrizze azoknak az új hálózatoknak a megbízhatóságát, amelyekhez csatlakozni szeretne. Ha vannak definiálva hálózatok, az ESET Internet Security a **Hálózati azonosítás** párbeszédpanelen konfigurált hálózati paraméterek használatával képes felismerni a megbízható (otthoni vagy munkahelyi) hálózatokat. A számítógépek gyakran a megbízható hálózathoz hasonló IP-címekkel lépnek be a hálózatokra. Ilyen esetekben előfordulhat, hogy az ESET Internet Security megbízhatónak (otthoninak vagy munkahelyinek) tekint egy ismeretlen hálózatot. Ennek elkerülése érdekében tanácsos a **Hálózati azonosítás** használata. Az ismert hálózati beállítások eléréséhez lépjen a **További beállítások** (F5) > **Hálózatvédelem** > **Általános** > **Ismert hálózatok** menüpontba.

Amikor egy hálózati adaptert csatlakoztat egy hálózathoz vagy újrakonfigurálja az adapter hálózati beállításait, az ESET Internet Security ellenőrzi, hogy az ismert hálózatok listáján szerepel-e az új hálózatnak megfelelő rekord. Ha a **Hálózati azonosítás** és a **Hálózati hitelesítés** (nem kötelező) értéke megegyezik, a hálózat csatlakoztatottként lesz megjelölve ebben a kapcsolatban. Ha nincs ismert hálózat, a hálózati azonosítási beállítások egy új hálózati kapcsolatot hoznak létre, amely azonosítja a hálózatot a következő alkalommal, amikor kapcsolódik hozzá. Az új hálózati kapcsolat alapértelmezés szerint a Windows-beállításokban megadott védelmi típust használja. **A program új hálózati kapcsolatot észlelt** párbeszédpanelen választhat a **megbízható hálózat**, a **nem megbízható hálózat**, illetve a **Windows-beállítások használata** védelmi típus közül. Ha egy hálózati adapter **Megbízható hálózat** védelmi típusú ismert hálózathoz csatlakozik, az adapter helyi alhálózatai bekerülnek a megbízható zónába.

Új hálózatok védelmi típusa – Válassza ki az új hálózatokhoz alapértelmezettként használni kívánt lehetőséget: Alapértelmezés szerint a **Windows-beállítások használata**, a **Felhasználó megkérdezése** vagy a **Megjelölés nem megbízhatóként** beállítás érvényesül új hálózatok esetén.

Az **ismert hálózatok** lehetővé teszik a hálózat nevének, identitásának, védelmi típusának és más egyébnek a konfigurálását. Az Ismert hálózatok szerkesztése lap megnyitásához kattintson a **Szerkesztés** gombra.

> **i** A **Windows-beállítások használata** lehetőség választása esetén nem jelenik meg párbeszédpanel, és a program automatikusan a Windows-beállításoknak megfelelően fogja megjelölni a hálózatot, amelyhez kapcsolódik. Ennek hatására bizonyos funkciók (például a fájlmegosztás és a távoli asztal) elérhetővé válnak az új hálózatokról.

Ismert hálózatok szerkesztése

Az ismert hálózatokat kézzel a **További beállítások** > **Hálózatvédelem** > **Általános** > **Ismert hálózatok** , majd a **Szerkesztés** elemre kattintva konfigurálhatja.

Oszlopok

Név – Egy ismert hálózat neve.

Védelem típusa – Megjeleníti, hogy a hálózatnál a **megbízható**, **nem megbízható** vagy **Windows-beállítások használata** érték van-e beállítva.

Tűzfalprofil – A lapon a **Profil** legördülő listában kijelölt profilokhoz tartozó szabályok jelennek meg.

Frissítési profi – Lehetővé teszi a létrehozott frissítési profil alkalmazását, amikor ehhez a hálózathoz csatlakozik.

Vezérlőelemek

Hozzáadás – Új ismert hálózat létrehozása.

Szerkesztés – Meglévő ismert hálózat szerkesztése.

Eltávolítás – Ha el szeretne távolítani egy hálózatot az ismert hálózatok listájáról, jelölje ki, és kattintson az **Eltávolítás** gombra.

Tetejére/Fel/Le/Aljára – Az ismert hálózatok prioritási szintjének módosítása (az ismert hálózatok értékelése fentről lefelé történik).

A hálózati konfiguráció beállításai az alábbi négy lapon találhatók:

Hálózat

Itt megadhatja a **hálózat nevét**, és kiválaszthatja a **védelem típusát** (megbízható, nem megbízható vagy Windows-beállítások használata). A **Tűzfalprofil** legördülő listában kiválaszthatja a hálózat profilját. Ha a hálózat a **megbízható** védelmi típust használja, akkor a program az összes közvetlenül csatlakoztatott hálózati almappát megbízhatónak tekinti. Ha például egy hálózati adapter a 192.168.1.5 IP-címmel csatlakozik a hálózathoz, az alhálózati maszk pedig 255.255.255.0, a 192.168.1.0/24-es alhálózat bekerül az adapter megbízható zónájába. Ha az adapter több címmel/alhálózattal rendelkezik, mindegyik megbízható lesz, függetlenül az ismert hálózat **Hálózati azonosítás** lapon megadott beállításaitól.

Ezenkívül a **További megbízható címek** csoportban hozzáadott címek is mindig a hálózathoz csatlakoztatott adapterek megbízható zónájába fognak tartozni (a hálózat védelmi típusától függetlenül).

Figyelmeztetés gyenge WiFi-titkosításról – Az ESET Internet Security tájékoztatja Önt, ha egy védtelen vezeték nélküli hálózathoz vagy egy gyenge védelemmel rendelkező hálózathoz csatlakozik.

Tűzfalprofil – Kiválaszthatja azt a tűzfalprofilt, amelyet használni szeretne ehhez a hálózathoz kapcsolódva.

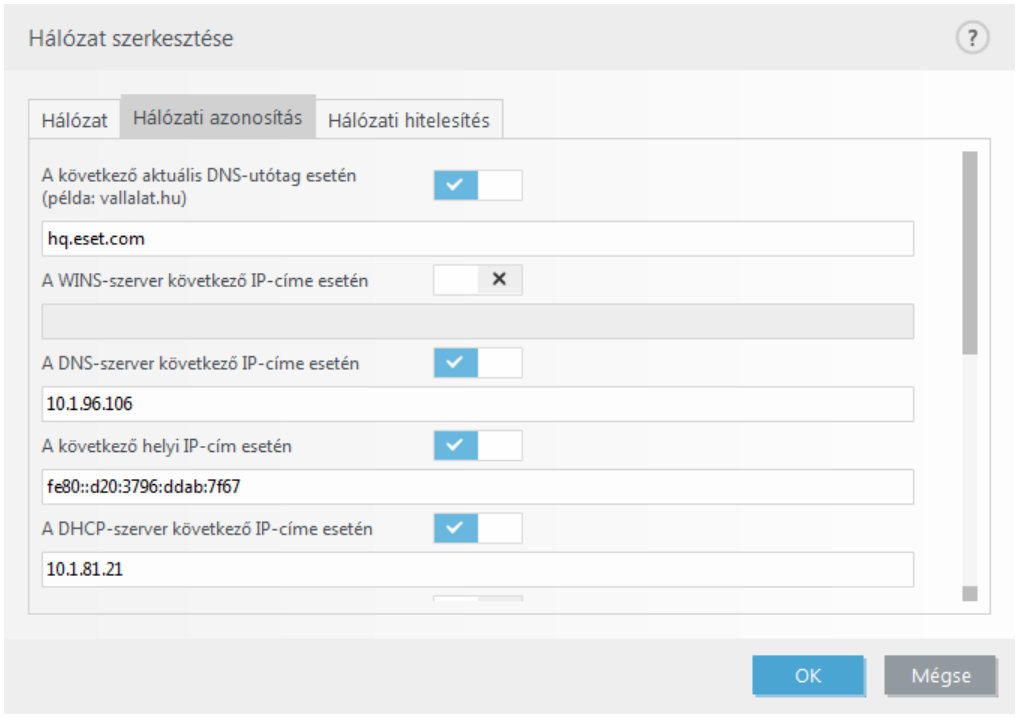
Profil frissítése – Kiválaszthatja azt a frissítési profilt, amelyet használni szeretne ehhez a hálózathoz kapcsolódva.

Ahhoz, hogy egy hálózatot csatlakoztatottként lehessen megjelölni a csatlakoztatott hálózatok listájában, az alábbi feltételeknek kell teljesülnie:

- **Hálózati azonosítás** – Minden megadott paraméternek meg kell felelnie az aktív kapcsolati paramétereknek.
- **Hálózati hitelesítés** – Hitelesítési szerver megadása esetén sikeres hitelesítésre van szükség az ESET hitelesítési szerverével.

Hálózati azonosítás

A hálózati azonosítás a helyi hálózati adapter paramétereinek megfelelően történik. A program minden kijelölt paramétert összevet az aktív hálózati kapcsolatok tényleges paramétereivel. Az IPv4- és az IPv6-címek egyaránt megengedettek.



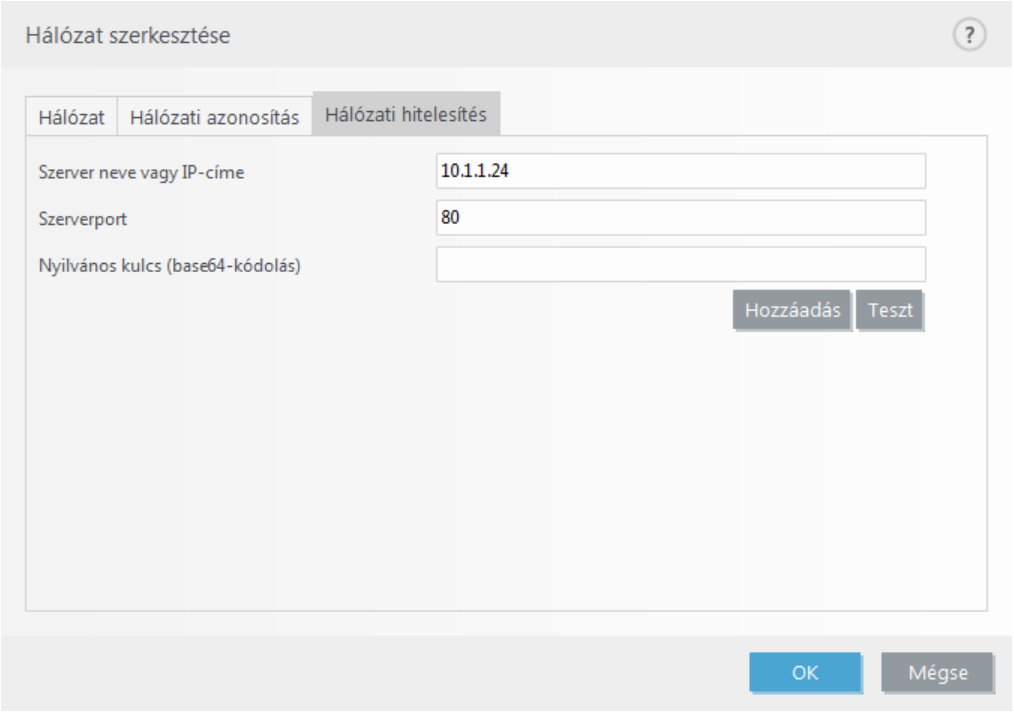
Hálózati hitelesítés

A hálózati hitelesítés adott szervert keres a hálózatban, és a szerver hitelesítéséhez aszimmetrikus titkosítást (RSA) használ. A hitelesítés alatt álló hálózat nevének meg kell egyeznie a hitelesítési szerver beállításai között megadott zónanévvel. A név érzékeny a kis- és nagybetűkre. Adja meg a szerver nevét és figyelőportját, valamint a titkos szerverkulcsnak megfelelő nyilvános kulcsot (erről további információt talál a Hálózati hitelesítés – Szerverkonfiguráció című témakörben). A szerveren tárolt kulcs nevét IP-címként, illetve DNS- vagy NetBios-névként, a szervernév után írt elérési úttal adhatja meg (például: szervernév/könyvtár1/könyvtár2/hitelesítés). Helyettesítő szervereket is megadhat az elérési út végén, egymástól pontosvesszővel elválasztva.

Töltse le az ESET hitelesítési szerverét,.

A nyilvános kulcs az alábbi fájltípusokból importálható:

- Titkosított nyilvános kulcsot tartalmazó, PEM formátumú (.pem) fájl – ezt a kulcsot az ESET hitelesítési szerverével lehet előállítani (további tudnivalók a Hálózati hitelesítés – Szerverkonfiguráció című témakörben találhatók).
- Titkosított nyilvános kulcsot tartalmazó fájl
- Nyilvános kulcsú tanúsítványt tartalmazó (.crt) fájl



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

Nem sikerült a szerverhitelesítés. Érvénytelen vagy nem egyező vírusdefiníció.
A szerver aláírása nem egyezik meg a megadott nyilvános kulccsal.

Nem sikerült a szerverhitelesítés. A hálózati név nem egyezik.
A megadott hálózatnév nem egyezik meg a hitelesítési szerver zónájának nevével. Ellenőrizze mindkét nevet, és gondoskodjon arról, hogy egyformák legyenek.

Nem sikerült a szerverhitelesítés. A szerverről érvénytelen válasz érkezett, vagy egyáltalán nincs válasz.
Nem érkezik válasz, ha a szerver nem fut, vagy nem érhető el. Érvénytelen válasz érkezhet például akkor, ha a megadott címen egy másik HTTP-szerver fut.

A megadott nyilvános kulcs érvénytelen.
Ellenőrizze, hogy nem sérült-e a megadott nyilvánoskulcs-fájl.

Hálózati hitelesítés – Szerverkonfiguráció

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

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

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.

Részletes információt az ESET tudásbáziscikkében talál.

Zónák konfigurálása

A zóna olyan hálózati címek gyűjteménye, amelyek az IP-címek egy logikai csoportját alkotják, és akkor lehet hasznos, ha több szabályban is fel kell használni ugyanazt a címkészletet. Egy csoport minden címére hasonló, a teljes csoport számára központilag definiált szabályok vonatkoznak. A **Megbízható zóna** például egy olyan címcsoport, amelybe a tűzfal által semmilyen módon nem korlátozott hálózati címek tartoznak. Megbízható zóna hozzáadása:

Megbízható zóna hozzáadása:

1. Nyissa meg a **További beállítások** (F5) > **Hálózati védelem** > **Általános** > **Zónák** lapot.
2. Kattintson a **Zónák** felirat melletti **Szerkesztés** gombra.
3. Kattintson a **Hozzáadás** gombra, írja be a zóna **nevét** és **leírását**, majd írjon be egy távoli IP-címet a **Távoli számítógép címe (IPv4/IPv6, tartomány, maszk)** mezőbe.
4. Kattintson az **OK** gombra.

További információkért tekintse meg a Tűzfalzónák című részt.

Tűzfalzónák

A zónákról további információt a Zónák konfigurálása című témakörben talál.

Oszlopok

Név – A távoli számítógépcsoport neve.

IP-címek – Egy zónához tartozó távoli IP-címek.

Vezérlőelemek

Amikor **hozzáad** vagy **szerkeszt** egy zónát, a következő mezők érhetők el:

Név – A távoli számítógépcsoport neve.

Leírás – A csoport általános leírása.

Távoli számítógép címe (IPv4, IPv6, tartomány, maszk) – Újabb távoli cím, címtartomány és alhálózat megadására szolgál.

Törlés – Zóna eltávolítása a listából.

> Ne feledje, hogy az előre definiált zónák nem távolíthatók el.

Tűzfal

A tűzfal ellenőrzi a rendszer 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 letilthatja a potenciálisan fenyegetést jelentő szolgáltatásokat.

Általános

A tűzfal engedélyezése

A rendszer biztonsága érdekében azt javasoljuk, hogy hagyja engedélyezve ezt a funkciót. Ilyenkor a program mindkét irányban ellenőrzi a hálózati forgalmat.

Windows tűzfalszabályok kiértékelése

Automatikus üzemmódban a Windows tűzfal szabályai szerint engedélyezett bejövő forgalom engedélyezése is, kivéve ha az ESET szabályai ezt kifejezetten nem tiltják le.

Szűrési üzemmód

A szűrési üzemmódtól függően változik a tűzfal működése. A szűrési üzemmódok a szükséges felhasználói beavatkozás szintjét is meghatározzák.

Az ESET Internet Security Tűzfalban az alábbi szűrési üzemmódok alkalmazhatók:

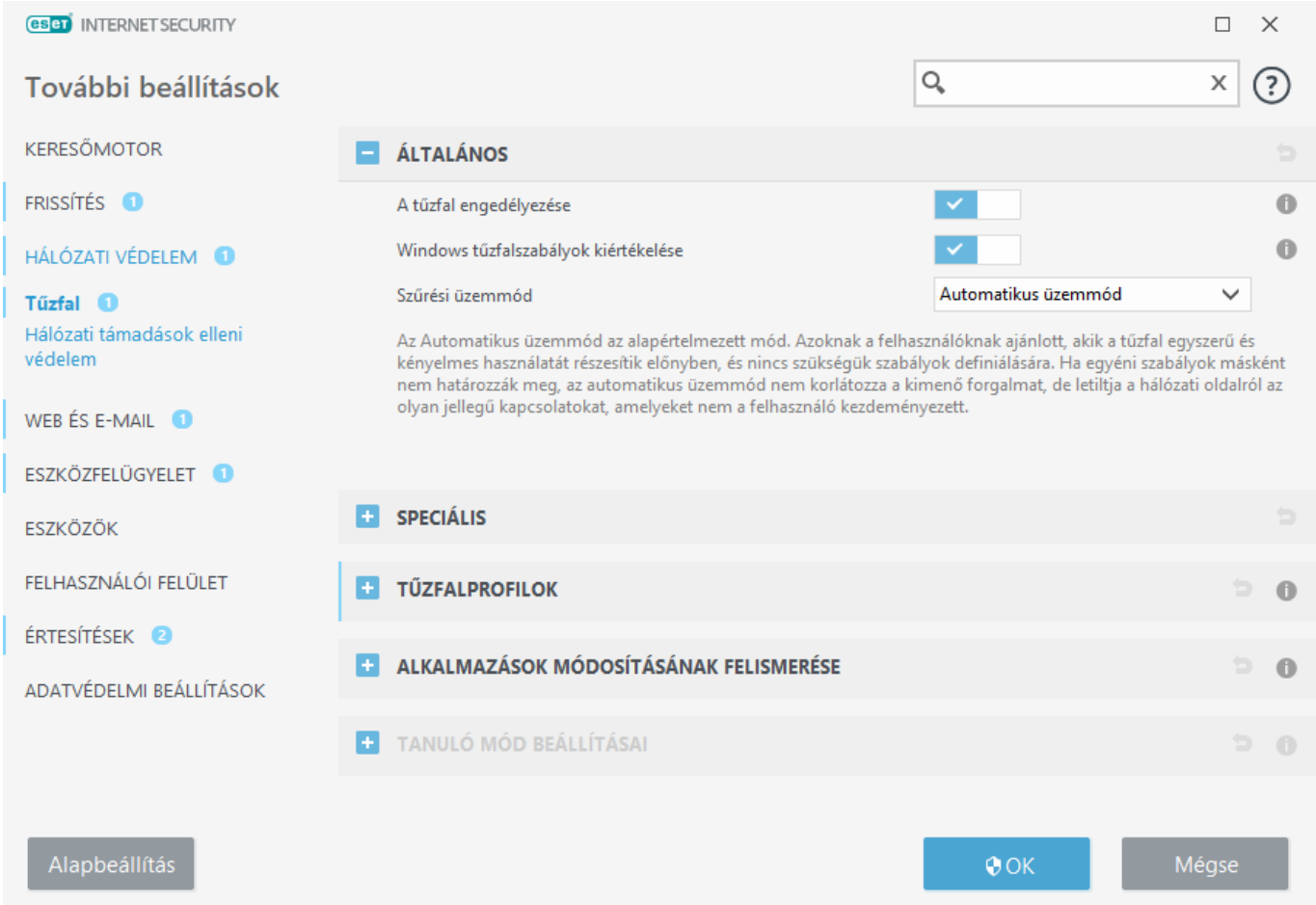
Szűrési üzemmód	Leírás
Automatikus üzemmód	Az alapértelmezett üzemmód. Ez az üzemmód azoknak a felhasználóknak ajánlott, akik a tűzfal egyszerű és kényelmes használatát részesítik előnyben, és nincs szükségük szabályok definiálására. Az **automatikus üzemmódban** lehetőség van egyéni, felhasználó által definiált szabályok létrehozására, de ez nem kötelező. Az automatikus üzemmód nem korlátozza a kimenő forgalmat a megadott rendszeren, de a legtöbb bejövő adatforgalmat letiltja (kivéve a megbízható zónából származó bizonyos adatforgalmakat, az IDS és további beállítások/Engedélyezett szolgáltatások között meghatározott beállítások alapján, valamint a nemrég zajlott kimenő kommunikációra adott válaszokat).
Interaktív üzemmód	Ez az üzemmód lehetővé teszi a 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 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 tűzfal az összes többi kapcsolatot letiltja.

Szűrési üzemmód	Leírás
Tanuló mód	A program automatikusan létrehozza és menti a szabályokat; ez a mód legjobban a tűzfal kezdeti konfigurációjakor használható, állandó használata nem ajánlott. Ebben a folyamatban nincs szükség felhasználói beavatkozásra, mert az ESET Internet Security előre definiált paraméterek szerint menti a szabályokat. A biztonsági kockázatok elkerülése érdekében csak addig tanácsos tanuló módot használni, amíg a program a szükséges kommunikációkhoz létre nem hozza az összes szabályt.

Speciális

Szabályok

A szabályok beállítási párbeszédpanelén megtekintheti az egyes alkalmazások által a megbízható zónákban és az interneten generált forgalomra vonatkozó összes szabályt.



Ha Botnet-támadás érte a számítógépét, létrehozhat egy IDS-szabályt. A szabály a **További beállítások** (F5) > **Hálózatvédelem** > **Hálózati támadások elleni védelem** > **IDS-szabályok** elemet kiválasztva, majd a **Szerkesztés** elemre kattintva módosítható.

Engedélyezett szolgáltatások

Konfigurálhatja a számítógépen futó közös hálózati szolgáltatásokhoz való hozzáférést. További információkért tekintse meg az Engedélyezett szolgáltatások című részt.

Tűzfalprofilok

A Tűzfalprofilok csoportban testre szabhatja az ESET Internet Security Tűzfal viselkedését, ha különböző szabálykészleteket definiál a különféle helyzetekhez.

Alkalmazások módosításának felismerése

Az Alkalmazások módosításának felismerése funkció értesítéseket jelenít meg, ha kapcsolatot próbálnak létesíteni azok a módosított alkalmazások, amelyekhez tartozik tűzfalszabály.

Tűzfalprofilok

A profilok használhatók az ESET Internet Security tűzfal működésének szabályozásához. A tűzfalszabályok létrehozásakor vagy szerkesztésekor megadhatja, hogy az adott szabály minden profilban érvényes legyen-e, vagy csak egy adott profilban. Amikor egy profil aktív egy hálózati kapcsolaton, a program csak a profilhoz nem rendelt globális szabályokat és a választott profillal társított szabályokat alkalmazza rá. Létrehozhat több olyan profilt, amelyben különböző szabályok vannak a hálózati adapterekhez, illetve a hálózatokhoz rendelve, és így könnyedén megváltoztathatja a tűzfal működését.

A **Profilok listája** mellett lévő Szerkesztés hivatkozásra kattintva nyissa meg a **Tűzfalprofilok** ablakot, ahol szerkesztheti a profilokat.

Beállíthatja a hálózati adaptereket úgy, hogy egy adott hálózathoz konfigurált profilt használjanak, amikor a szóban forgó hálózathoz vannak csatlakoztatva. Adott hálózaton való használatra a **További beállítások** (F5) > **Hálózati védelem** > **Ismert hálózatok** > **Szerkesztés** elemre kattintva is kijelölhet egy profilt. Ha kijelöl egy hálózatot az **Ismert hálózatok** listában, és a **Szerkesztés** gombra kattint, hozzárendelhet egy tűzfalprofilt a hálózathoz a **Tűzfalprofil** legördülő menü segítségével.

Ha a hálózathoz nincs profil rendelve, akkor az adapter alapértelmezett profilja lesz használatban. Ha az adapter úgy van beállítva, hogy ne használja a hálózat profilját, az alapértelmezett érték lesz használatos függetlenül attól, hogy az adapter melyik hálózathoz csatlakozik. Ha a hálózathoz vagy az adapterkonfigurációhoz nem tartozik profil, a rendszer a globális alapértelmezett profilt használja. Ha hozzá szeretne rendelni egy profilt egy hálózati adapterhez, jelölje ki a hálózati adaptert, kattintson a **Szerkesztés** gombra a **Hálózati adapterekhez rendelt profilok** felirat mellett, végezze el a kijelölt hálózati adapter szerkesztését, és jelölje ki a profilt az **Alapértelmezett tűzfalprofil** legördülő menüből.

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

Párbeszédablak – Tűzfalprofilok szerkesztése

A párbeszédpanel **Hozzáadás**, **Szerkesztés** és **Eltávolítás** gombjával létrehozhat, módosíthat és törölhet profilokat. Ahhoz, hogy a **Szerkesztés** és az **Eltávolítás** gomb elérhető legyen, ki kell jelölni a kívánt profilt a **Tűzfalprofilok** ablak legördülő listájában.

További tudnivalókat a Tűzfalprofilok című témakör tartalmaz.

Hálózati adapterekhez rendelt profilok

A profilváltással gyorsan érvényesíthet több változtatást a tűzfal viselkedésén. Egyéni szabályokat állíthat be és alkalmazhat adott profilokra. A számítógépen jelen lévő összes adapter hálózatiadapter-bejegyzései automatikusan felkerülnek a **Hálózati adapterek** listára.

Oszlopok

Név – A hálózati adapter neve.

Alapértelmezett tűzfalprofil – Az alapértelmezett profil akkor van használatban, amikor a hálózatnak, amelyhez csatlakozik, nincs konfigurált profilja, vagy amikor a hálózati adapter úgy van beállítva, hogy ne használjon hálózati profilt.

Hálózat profiljának előnyben részesítése – Amikor a **Csatlakoztatott hálózat tűzfalprofiljának előnyben részesítése** opció engedélyezve van, a hálózati adapter a csatlakoztatott hálózathoz hozzárendelt tűzfalprofilt fogja használni, amikor csak lehetséges.

Vezérlőelemek

Hozzáadás – Új hálózati adapter hozzáadása.

Szerkesztés – Meglévő hálózati adapter szerkesztése.

Eltávolítás – Ha el szeretne távolítani egy hálózati adaptert a listáról, jelölje ki, és kattintson az **Eltávolítás** gombra.

OK/Mégse – Az **OK** gombra kattintva mentheti a módosításokat, a **Mégse** gombra kattintva pedig kiléphet a módosítások mentése nélkül.

Szabályok beállítása és használata

A szabályok feltételegyüttesek, melyek célja a hálózati kapcsolatok ellenőrzése, és a feltételekkel társított műveletek végrehajtása. A Tűzfalszabályok használatával megadhatja a különböző típusú hálózati kapcsolatok létrehozásakor végrehajtandó műveletet. A szabályszűrési beállítások megjelenítéséhez nyissa meg a **További beállítások** (F5) > **Tűzfal** > **Speciális** lapot. Egyes előre megadott szabályok az **engedélyezett szolgáltatások** (IDS- és további beállítások) jelölőnégyzeteihez tartoznak, és közvetlenül nem, hanem csak a megfelelő jelölőnégyzetekkel kapcsolhatók ki.

Az ESET Internet Security előző verziójától eltérően a szabályok értékelése felülről lefelé történik. A program az első szabályegyezés műveletét használja az egyes értékelt hálózati kapcsolatokhoz. Ez egy fontos változás az előző verzióhoz képest, ahol a szabályok prioritása automatikus volt, és az egyedi szabályok nagyobb prioritást élveztek az általánosabbakkal szemben.

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 rendszer 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 tűzfallal észlelheti és bonthatja az ilyen kapcsolatokat.

Tűzfalszabályok listája

A tűzfalszabályok listáját úgy tekintheti meg, hogy a **További beállítások** (F5) > **Hálózati védelem** > **Tűzfal** > **Speciális** lapon a **Szerkesztés** gombra kattint a **Szabályok** felirat mellett.

Oszlopok

Név – A szabály neve.

Engedélyezve – Megjeleníti, hogy a szabály engedélyezve van-e vagy le van tiltva. Szabály aktiválásához be kell jelölnie a megfelelő jelölőnégyzetet.

Protokoll – Az a protokoll, amelyre az adott szabály vonatkozik.

Profil – Megjeleníti azt a tűzfalprofilt, amelyre az adott szabály vonatkozik.

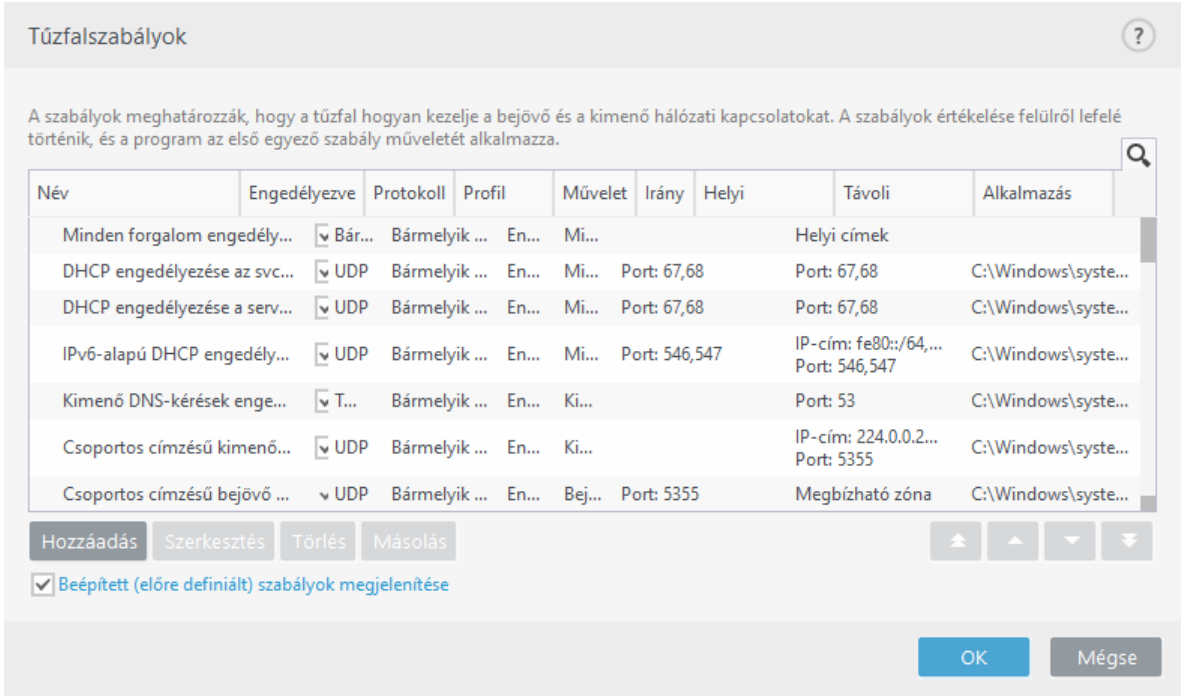
Művelet – Megjeleníti a kommunikáció állapotát (letiltás/engedélyezés/kérdés).

Irány – A kommunikáció iránya (bejövő/kimenő/mindkettő).

Helyi – A helyi számítógép távoli IPv4- vagy IPv6-címe/tartománya/alhálózata és portja.

Távoli – A távoli számítógép távoli IPv4- vagy IPv6-címe/tartománya/alhálózata és portja.

Alkalmazás – Az az alkalmazás, amelyre a szabály vonatkozik.



Vezérlőelemek

Hozzáadás – Új szabály létrehozása.

Szerkesztés – Meglévő szabály szerkesztése.

Törlés – Meglévő szabály eltávolítása.

Másolás – A kiválasztott szabály másolatának létrehozása.

Beépített (előre definiált) szabályok megjelenítése – Az ESET Internet Security által előre definiált szabályok, amelyek engedélyeznek vagy letiltanak bizonyos kommunikációkat. Ezek a szabályok letilthatók, előre megadott szabály azonban nem törölhető.

 **Tetejére/Fel/Le/Aljára** – A szabályok prioritási szintjének módosítása (a szabályok végrehajtása fentről lefelé történik).

Kattintson a keresési ikonra a szabály(ok) név, protokoll vagy port szerinti kereséséhez.

Tűzfalszabályok hozzáadása vagy szerkesztése

Ha egy szabály figyelt paraméterei változnak, módosítani kell a szabályt. Ha olyan változtatások történnek, amelyek miatt a szabály már nem tudja teljesíteni a feltételeket, és ezért a megadott művelet nem hajtható végre, a program visszautasíthatja a szóban forgó kapcsolatot. Ez problémákhoz vezethet annak az alkalmazásnak a működésében, amelyre a szabály hatással van. Ilyen esetre példa egy távoli oldali hálózati cím vagy portszám változása.

Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- Az ESET Tűzfalon egy adott port megnyitása vagy bezárása (engedélyezése vagy tiltása)
- Tűzfalszabály létrehozása naplófájlokból az ESET Internet Security alkalmazásban

A párbeszédpanel három lapból áll:

- **Általános** – Itt adható meg a szabály neve, a szabályozott kapcsolat iránya, a társított művelet (**Engedélyezés**, **Tiltás**, **Kérdés**), valamint a szabállyal felügyelt protokoll és profil.

- **Helyi** – A kapcsolat helyi oldalának adatait, beleértve a helyi portszámot vagy porttartományt, valamint a kommunikációt folytató alkalmazás nevét jeleníti meg. Emellett a **Hozzáadás** gombra kattintva előre megadott vagy létrehozott zóna hozzáadására is lehetősége van (IP-címek tartományával).

- **Távoli** – Ezen a lapon a távoli port (vagy porttartomány) adatai találhatók. Ugyanitt van lehetőség a szabályban érintett távoli IP-címek vagy zónák listájának megadására. Emellett a **Hozzáadás** gombra kattintva előre megadott vagy létrehozott zóna hozzáadására is lehetősége van (IP-címek tartományával).

Új szabály létrehozásakor a **Név** mezőben meg kell adni a szabály nevét. Az **Irány** legördülő listában kijelölheti, hogy milyen irányú kommunikációra vonatkozik a szabály, a **Művelet** legördülő listában pedig megadhatja, hogy milyen műveletet hajtson végre a program, amikor egy kommunikáció megfelel a szabálynak.

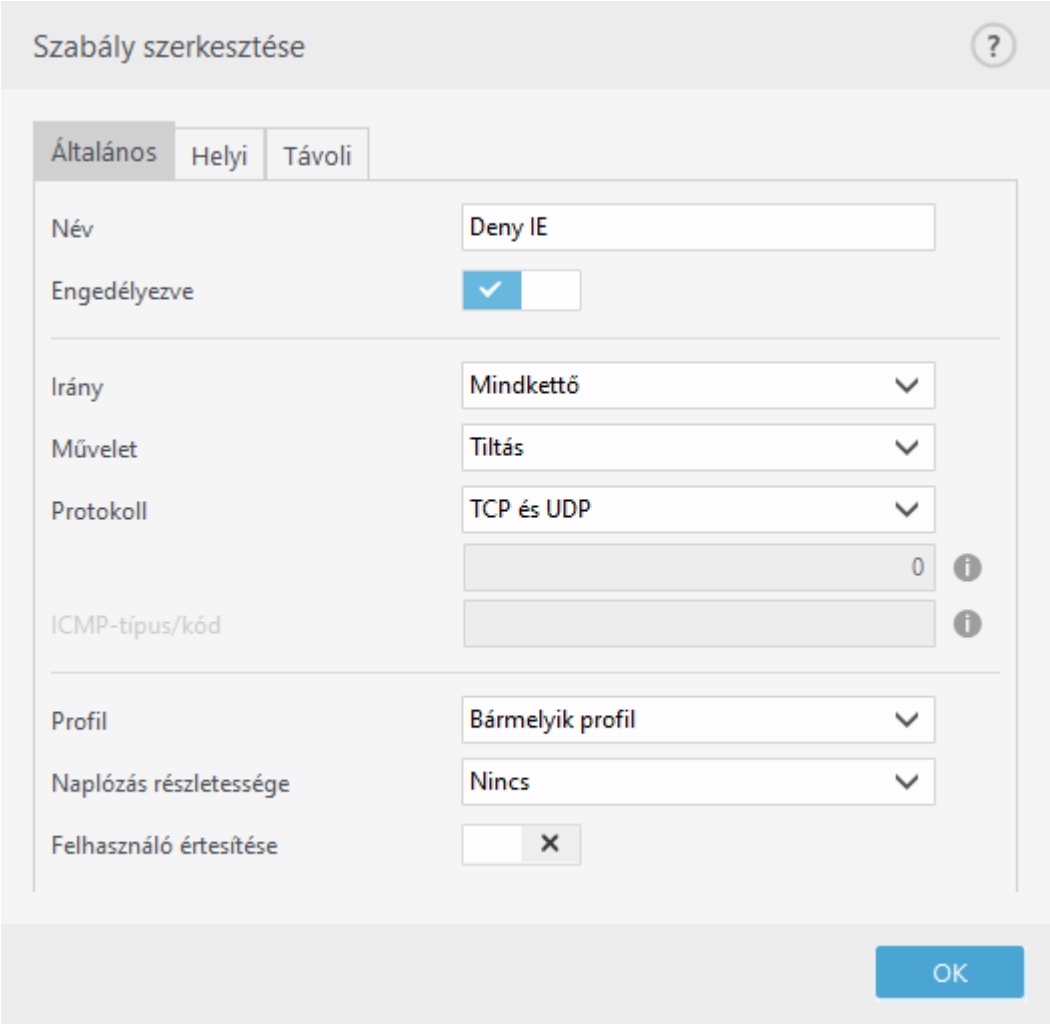
A **Protokoll** mezőben a szabállyal felügyelt átviteli protokoll adható meg. A legördülő menüből válassza ki azt a

protokollt, amelyet egy adott szabályhoz használni szeretne.

Az **ICMP-típus/-kód** egy számmal jelölt ICMP-üzenetet jelöl (a 0 például a visszhangválaszt (Echo Reply) képviseli).

Alapértelmezés szerint a **Bármelyik profil** profilban minden szabály engedélyezett. Ha ez nem megfelelő, a **Profil** legördülő listában válasszon egy egyéni tűzfalprofilt.

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



Létrehozunk egy olyan szabályt, amely engedélyezi a Firefox böngészőalkalmazásnak az Internethez/helyi hálózathoz való hozzáférést. A példában az alábbiakat kell megadni:
1.Az **Általános** lapon engedélyezni kell a TCP és UDP protokollon keresztüli kimenő irányú kommunikációt.
2.Kattintson a **Helyi** fülre.
3.Kiválaszthatja a használt böngésző elérési útvonalát a **...** ikonra kattintva (például *C:\Program Files\Firefox\Firefox.exe*). NE írja be az alkalmazás nevét.
4.A szabványos internetböngészés engedélyezéséhez a **Távoli** lapon engedélyezze a 80-as és a 443-as számú portot.

Vegye figyelembe, hogy az előre megadott szabályok módosításának lehetőségei korlátozottak.

Tűzfalszabály – Helyi

Itt adható meg a helyi alkalmazás neve, illetve az a helyi port vagy portegyüttes, amelyre a szabály vonatkozni fog.

Port – Helyi portszám(ok). Ha nincs megadva szám, a szabály minden portra vonatkozni fog. Egyetlen kommunikációs portot vagy porttartományt is hozzáadhat.

IP-cím – Lehetővé teszi távoli cím/címek, címtartomány vagy alhálózat megadását, amelyre a szabály vonatkozni fog. Ha nincs megadva érték, a szabály minden kommunikációra vonatkozni fog.

Zónák – A hozzáadott zónák listája.

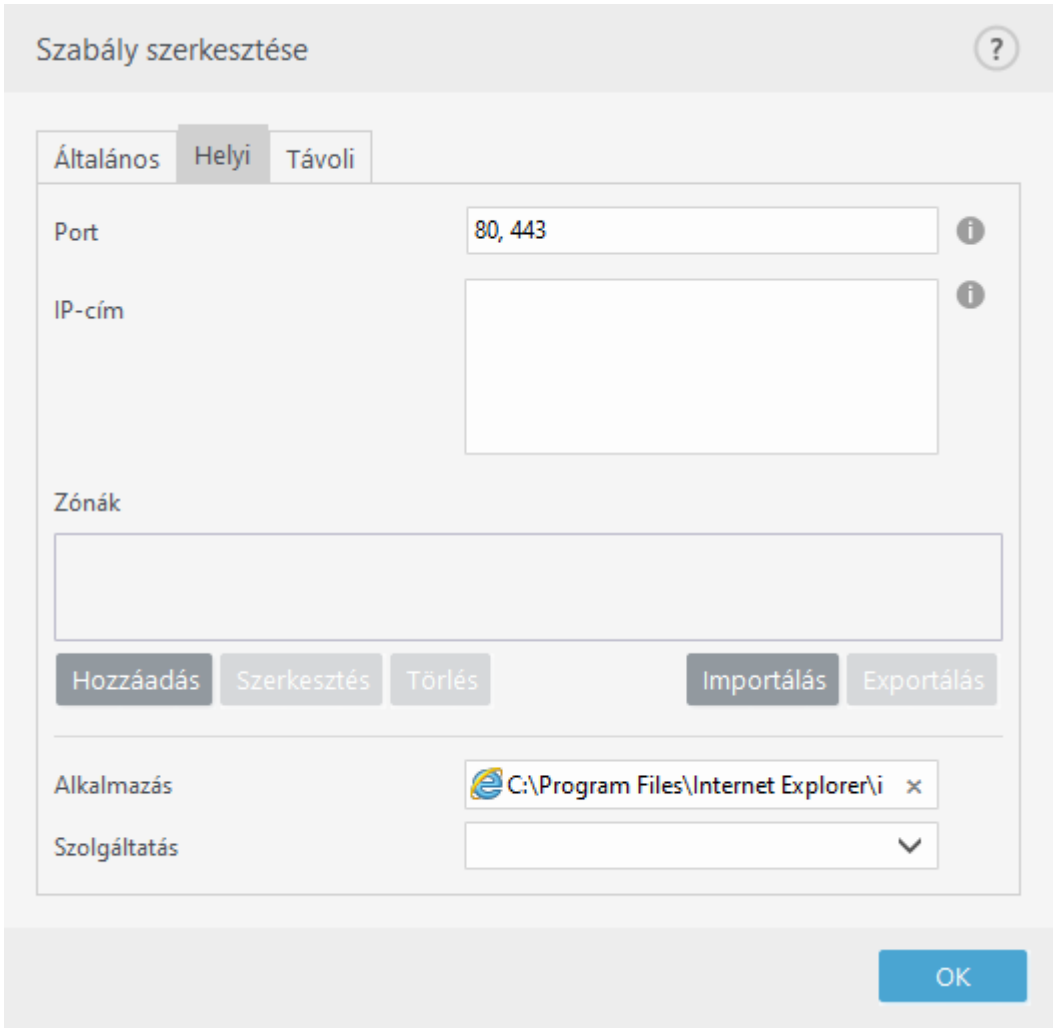
Hozzáadás – Létrehozott zóna hozzáadása a legördülő menüből. A zónák létrehozásáról a Zóna beállításai című témakörben tájékozódhat.

Eltávolítás – Zónák eltávolítása a listából.

Alkalmazás – Annak az alkalmazásnak a neve, amelyre a szabály vonatkozik. Hozzáadhatja annak az alkalmazásnak a helyét, amelyre a szabály vonatkozni fog.

Szolgáltatás – A legördülő listában rendszerszolgáltatások láthatók.

> Érdemes lehet létrehoznia egy szabályt a tükörhöz, amely frissítéseket biztosít a 2221-es porton keresztül a legördülő listában található kommunikációs EHttpSrv szolgáltatás használatával.



Tűzfalszabályok – Távoli

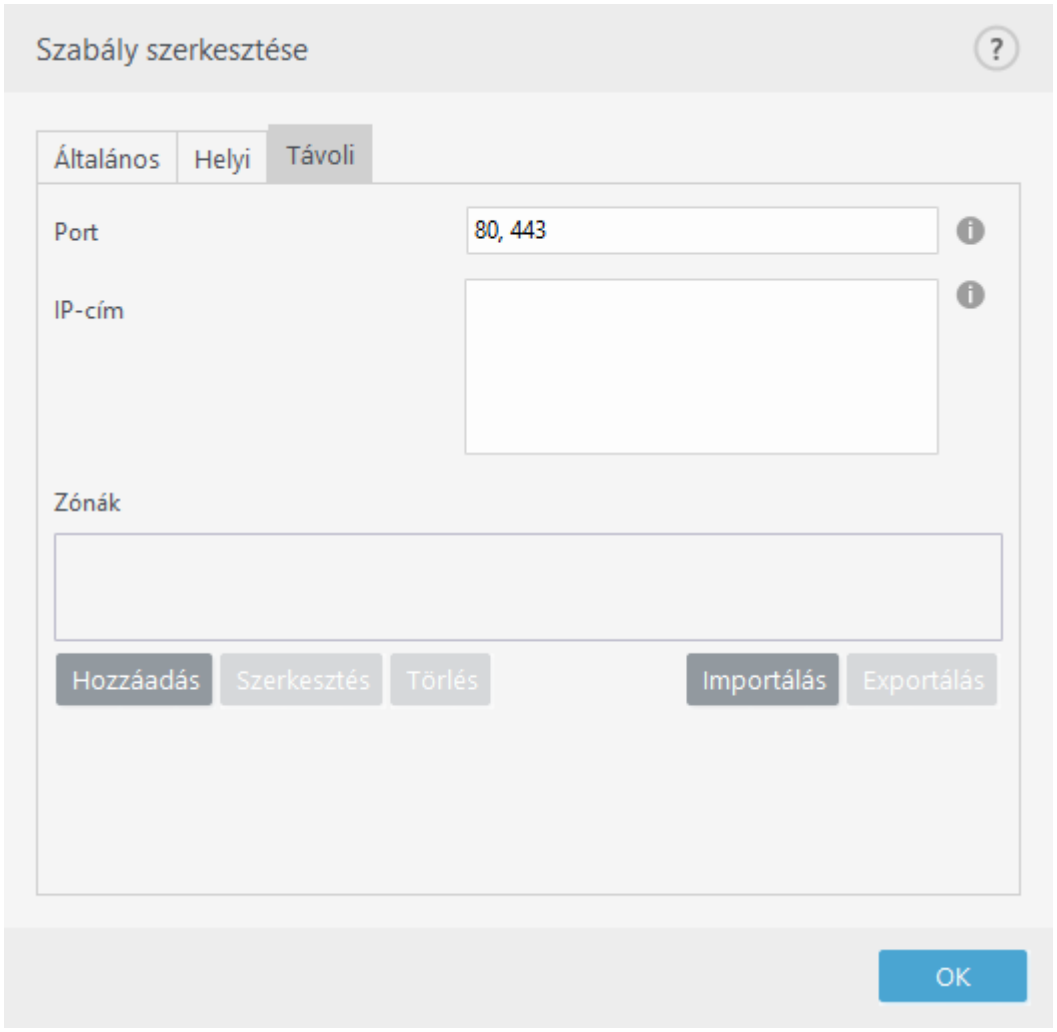
Port – Távoli portszám(ok). Ha nincs megadva szám, a szabály minden portra vonatkozni fog. Egyetlen kommunikációs portot vagy porttartományt is hozzáadhat.

IP – Lehetővé teszi újabb távoli cím/címek, címtartomány vagy alhálózat megadását. Az a cím, címtartomány, alhálózat vagy távoli zóna, amelyre a szabály vonatkozik. Ha nincs megadva érték, a szabály a teljes kommunikációra vonatkozik.

Zónák – A hozzáadott zónák listája.

Hozzáadás – Zóna hozzáadása a legördülő menüből. A zónák létrehozásáról a Zóna beállításai című témakörben tájékozódhat.

Eltávolítás – Zónák eltávolítása a listából.



Alkalmazások módosításának felismerése

Az Alkalmazások módosításának felismerése funkció értesítéseket jelenít meg, ha azok a módosított alkalmazások, amelyekhez tartozik tűzfalszabály, kapcsolatot próbálnak létesíteni. Az alkalmazásmódosítás egy olyan mechanizmus, amelynek során átmenetileg vagy véglegesen lecserélik az eredeti alkalmazást egy másik alkalmazásra egy végrehajtható fájl által (véd a tűzfalszabályokkal való visszaélés ellen).

Ne feledje, hogy ez a funkció nem arra szolgál, hogy általában, bármilyen alkalmazásban észlelje a módosításokat. Célja az, hogy elkerülje a meglévő tűzfalszabályok nem megfelelő használatát, és csak azokat az alkalmazásokat figyeli, amelyekhez adott tűzfalszabályok tartoznak.

Alkalmazásmódosítások felismerésének engedélyezése – Ha bejelöli ezt a jelölőnégyzetet, a program változások (frissítések, fertőzések és egyéb módosítások) szempontjából figyeli az alkalmazásokat. Ha egy módosított alkalmazás kapcsolatot próbál létesíteni, a tűzfal értesíti a felhasználót.

Aláírt (megbízható) alkalmazások módosításának engedélyezése – Nincs értesítés, ha az alkalmazás ugyanazzal az érvényes digitális aláírással rendelkezik a módosítás előtt és után.

Az ellenőrzésből kizárt alkalmazások listája – Ebben az ablakban hozzáadhat vagy eltávolíthat egyes alkalmazásokat, amelyek módosítása értesítés nélkül engedélyezhető.

Az ellenőrzésből kizárt alkalmazások listája

Az ESET Internet Security alkalmazásban a tűzfal észleli azoknak az alkalmazásoknak a módosításait, amelyekhez léteznek szabályok (lásd: Alkalmazások módosításának felismerése).

Ha egyes alkalmazások esetén nem szeretné használni ezt a funkciót, kizárhatja őket a tűzfal által végzett ellenőrzésből.

Hozzáadás – Segítségével megnyithat egy ablakot, ahol kiválaszthatja a módosítások felismeréséből kizárt alkalmazások listájára felvenni kívánt alkalmazást. Választhat az olyan futó alkalmazások listájából, amelyek nyitott hálózati kommunikációt folytatnak és tűzfalszabály szerint működnek, illetve megadhat egy adott alkalmazást is.

Szerkesztés – Segítségével megnyithat egy ablakot, ahol módosíthatja a módosítások felismeréséből kizárt alkalmazások listáján lévő egyik alkalmazás helyét. Választhat az olyan futó alkalmazások listájából, amelyek nyitott hálózati kommunikációt folytatnak és tűzfalszabály szerint működnek, illetve manuálisan is módosíthatja a helyet.

Eltávolítás – Ezzel a gombbal eltávolíthatja a listában kijelölt alkalmazást a módosítások felismeréséből kizárt alkalmazások listájáról.

Tanuló mód beállításai

A tanuló mód a rendszerben létesített minden kommunikációhoz automatikusan létrehoz és ment egy szabályt. Ebben a folyamatban nincs szükség felhasználói beavatkozásra, mert az ESET Internet Security előre definiált paraméterek szerint menti a szabályokat.

Ez a mód kockázatnak teheti ki a rendszert, és használata csak a tűzfal kezdeti konfigurációjához ajánlott.

Válassza ki a **Tanuló mód** menüpontot a legördülő menüben a **További beállítások**(F5) > **Tűzfal** > **Alapbeállítások** > **Szűrési üzemmód** lapon a **tanuló mód beállításainak** aktiválásához. A csoportban az alábbiakban ismertetett beállítások láthatók.

Tanuló módban a tűzfal nem szűri a kommunikációt. Ezért minden kimenő és bejövő kommunikáció engedélyezett. Ebben az üzemmódban a tűzfal nem nyújt teljes védelmet a számítógép számára.

A tanuló mód lejárata után beállított mód – Azon szűrési mód beállítása, amelyre az ESET Internet Security tűzfal visszaáll a tanuló mód időszakának lejárta után. Bővebben lásd a szűrési módok ismertetésénél. A lejáratot követően a **Rákérdez** beállítás esetén rendszergazdai jogosultságok szükségesek ahhoz, hogy módosítani lehessen a tűzfal szűrési üzemmódját.

Kommunikáció típusa – Különböző típusú kommunikációkhoz választhat adott szabálylétrehozási paramétereket. Négy kommunikációtípus létezik:

Bejövő forgalom a megbízható zónából – Megbízható zónabeli bejövő kapcsolatról van szó például, ha a megbízható zónában található egyik távoli számítógép kommunikálni próbál a számítógépen futó valamelyik helyi alkalmazással.

Kimenő forgalom a megbízható zónába – Ilyenkor egy helyi alkalmazás próbál meg kapcsolatot létesíteni a helyi hálózat vagy a megbízható zóna valamely hálózatának másik számítógépével.

Bejövő internetes forgalom – Egy távoli számítógép kommunikálni próbál a számítógépen futó egyik alkalmazással.

Kimenő internetes forgalom – Ilyenkor egy helyi alkalmazás próbál meg kapcsolatot létesíteni a helyi hálózat vagy a megbízható zóna valamely hálózatának másik számítógépével.

Ebben a csoportban határozhatók meg az újonnan létrehozott szabályok paraméterei:

Helyi port hozzáadása – A hálózati kommunikációban érintett helyi port számának felvétele a szabályokba. A kimenő kommunikációkhoz általában véletlenszerű számok jönnek létre. Ezért javasoljuk, hogy ezt az opciót csak a bejövő kommunikációkhoz engedélyezze.

Alkalmazás hozzáadása – A jelölőnégyzet bejelölésével a helyi alkalmazás neve is a szabályok részévé válik. Ez a beállítás alkalmas a jövőbeli alkalmazásszintű (egy teljes alkalmazás kommunikációját definiáló) szabályok kialakításához. Ez a beállítás ad például módot arra, hogy egy bizonyos típusú kommunikációt csak egy böngészőnek vagy levelezőprogramnak engedélyezzen.

Távoli port hozzáadása – Az opció bejelölésével a hálózati kommunikációban részt vevő távoli port számát is befoglalja a szabályba a rendszer. Ezzel a lehetőséggel engedélyezhet vagy tilthat le például egy szabványos portszámmal társított szolgáltatást. (A HTTP protokoll esetén például a 80-as, a POP3 esetén a 110-es port a szabványos port.)

Távoli IP-cím vagy megbízható zóna hozzáadása – A szabályparaméterként felvett távoli IP-címek és megbízható zónák a helyi rendszer és a távoli cím vagy zóna közötti összes kapcsolatra érvényes új szabályok definiálására alkalmasak. Ezt a jelölőnégyzetet érdemes bejelölni, ha egy adott számítógépre vagy hálózati számítógépek egy csoportjára vonatkozó műveleteket szeretne definiálni egy szabállyal.

Alkalmazás különböző szabályainak maximális száma – Ha egy alkalmazás különböző portokon keresztül, eltérő IP-címekkel stb. kommunikál, a tűzfal tanuló módban minden ilyen változat esetén létrehoz egy szabályt az alkalmazáshoz. Ezzel a beállítással azonban korlátozhatja az egy alkalmazáshoz létrehozható szabályok számát.

Hálózati támadások elleni védelem (IDS)

A Hálózati támadások elleni védelem (IDS) javítja az ismert biztonsági rések felismerését. A szószedetben bővebben olvashat a Hálózati támadások elleni védelemről.

Hálózati támadások elleni védelem (IDS) – Elemzi a hálózati forgalom tartalmát, és védelmet biztosít a hálózati támadásokkal szemben. Minden károsnak számító adatforgalmat letilt.

Botnet elleni védelem engedélyezése – Észleli és letiltja a kártevő parancsokkal folytatott kommunikációt, és tipikus minták alapján vezérli a szervereket, amikor a számítógépet megfertőzték, és egy bot kísérel meg kommunikálni. További információk a Botnet elleni védelemről a szószedetben.

IDS-szabályok – Ez a beállítás lehetővé teszi további szűrőbeállítások megadását a különböző típusú támadásokkal kapcsolatban.

> **Ábrákkal ellátott útmutató**
> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> - IP-cím kizárása az IDS-ből az ESET Internet Security alkalmazásban

A hálózati védelem által észlelt összes eseményt egy naplófájlba menti a szolgáltatás. További információkért

tekintse meg a hálózatvédelmi naplót.

Brute-force támadás elleni védelem

A brute-force támadás elleni védelem blokkolja a jelszótalálgatási kísérleteket az RDP és SMB szolgáltatások esetén. A brute-force támadás egy olyan módszer, amelynek során a cél a jelszó kiderítése azáltal, hogy szisztematikusan kipróbálják a betűk, számok és szimbólumok minden kombinációját a megfelelő kombináció kiderítéséhez. A brute-force támadás elleni védelem konfigurálásához a program főablakában kattintson a **Beállítás** > **További beállítások** (F5) > **Hálózati védelem** > **Hálózati támadások elleni védelem** > **Brute-force támadás elleni védelem** elemre.

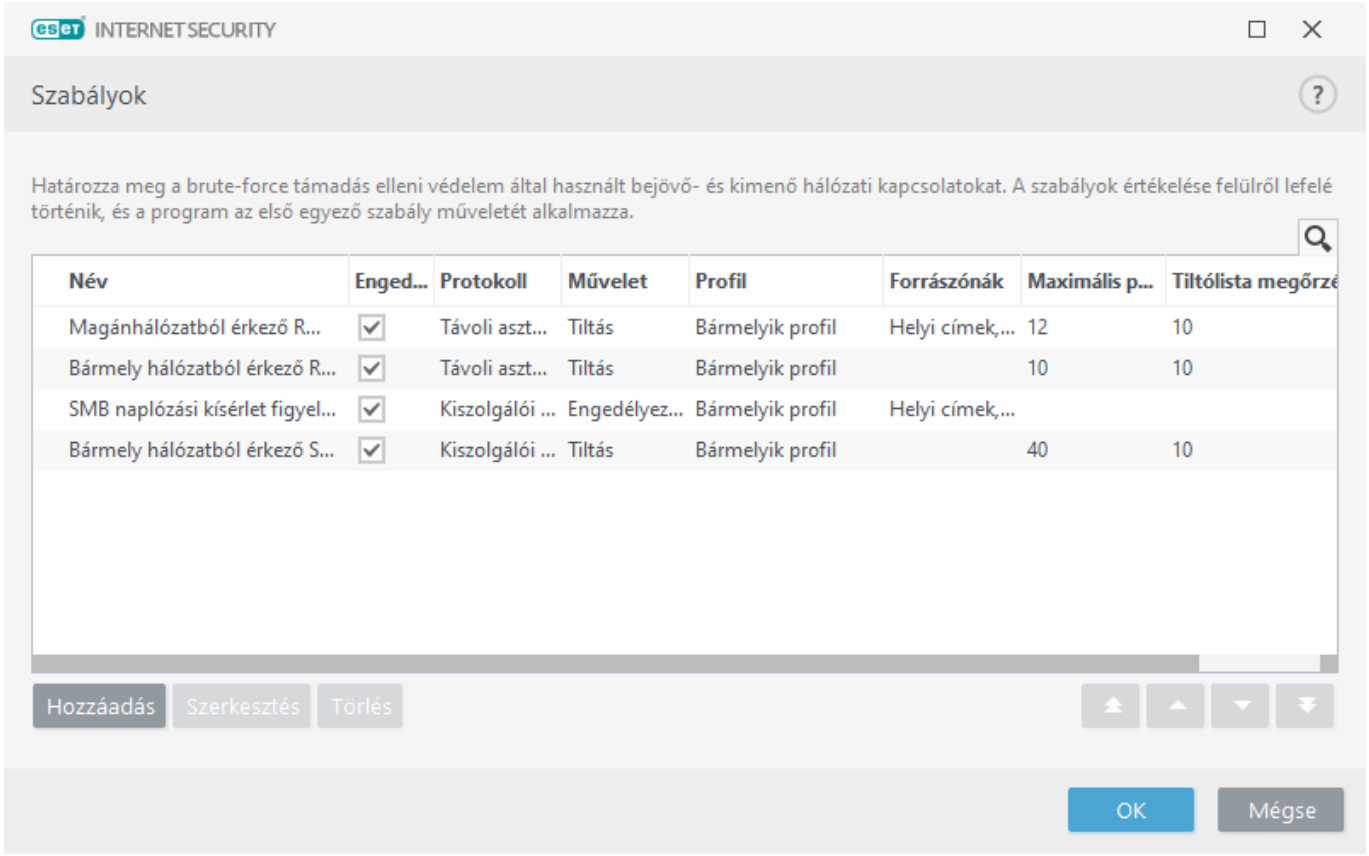
Brute-force támadás elleni védelem engedélyezése – Az ESET Internet Security ellenőrzi a hálózati forgalom tartalmát és blokkolja a jelszó-találgatási támadások keretében végzett próbálkozásokat.

Szabályok – Lehetővé teszik a bejövő és kimenő hálózati kapcsolatok szabályainak létrehozását, szerkesztését és megtekintését. További információkért tekintse meg a Szabályok fejezetet.

Szabályok

A brute-force támadás elleni védelem szabályai lehetővé teszik a bejövő és kimenő hálózati kapcsolatok szabályainak létrehozását, szerkesztését és megtekintését. Az előre megadott szabályok nem szerkeszthetők és törölhetők.

A brute-force támadás elleni védelem kezelése



Hozzáadás – Új szabály létrehozása.

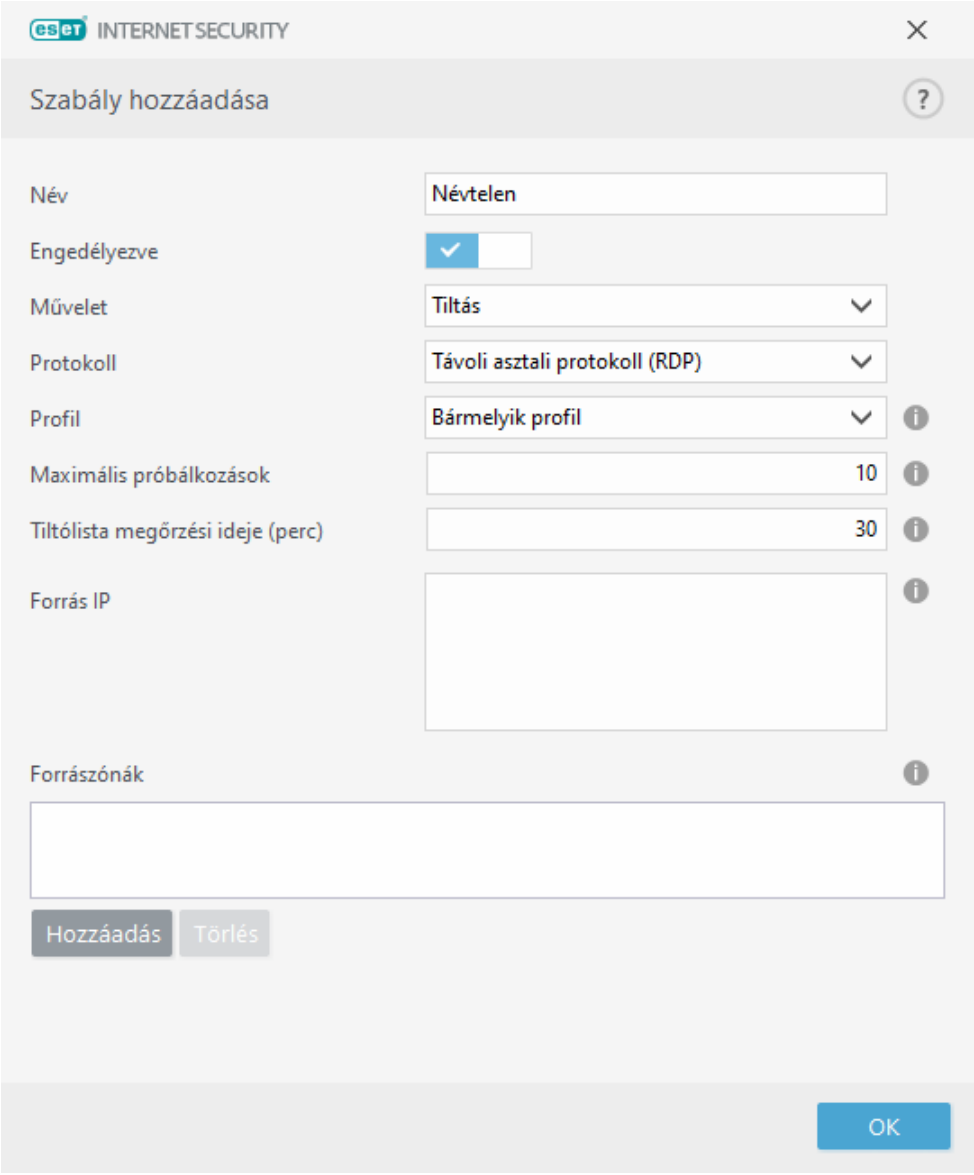
Szerkesztés – Meglévő szabály szerkesztése.

Törlés – Meglévő szabály eltávolítása a szabályok listájából.

 **Tetejére/Fel/Le/Aljára** – A szabályok prioritási szintjének módosítása.

> A lehető legnagyobb fokú védelem biztosítása érdekében a legkisebb **Maximális próbálkozási** értékkel rendelkező blokkolási szabály érvényesül akkor is, ha a szabály a Szabályok listában alacsonyabb helyen van, ha több blokkolási szabály is megfelel az észlelési feltételeknek.

Szabályszerkesztő



Név – A szabály neve.

Engedélyezve – Tiltsa le csúszkát, ha meg szeretné őrizni a szabályt a listában, de nem kívánja alkalmazni.

Művelet – Válassza ki, hogy **tiltja** vagy **engedélyezi** a kapcsolatot, ha a szabálybeállítások teljesülnek.

Protokoll – A kommunikációs protokoll, amelyet ez a szabály ellenőrizni fog.

Profil – Egyéni szabályok állíthatók be és alkalmazhatók bizonyos profilokra.

Maximális próbálkozások - A támadási ismétlési próbálkozások maximális száma addig, amíg az IP-cím blokkolva lesz, és hozzáadódik a tiltólistához.

Tiltólista megőrzési ideje (perc) – Annak az időtartamnak a beállítása, amikor a cím lejár a tiltólistán. A próbálkozások megszámlálására használt időtartam alapértelmezés szerint 30 perc.

Forrás IP – IP-címek/tartományok/alhálózatok listája. Több címet vesszővel kell elválasztani.

Forrászónák – Lehetővé teszi, hogy egy előre definiált vagy létrehozott zónát adjon hozzá IP-címtartományhoz a **Hozzáadás** gombra kattintva.

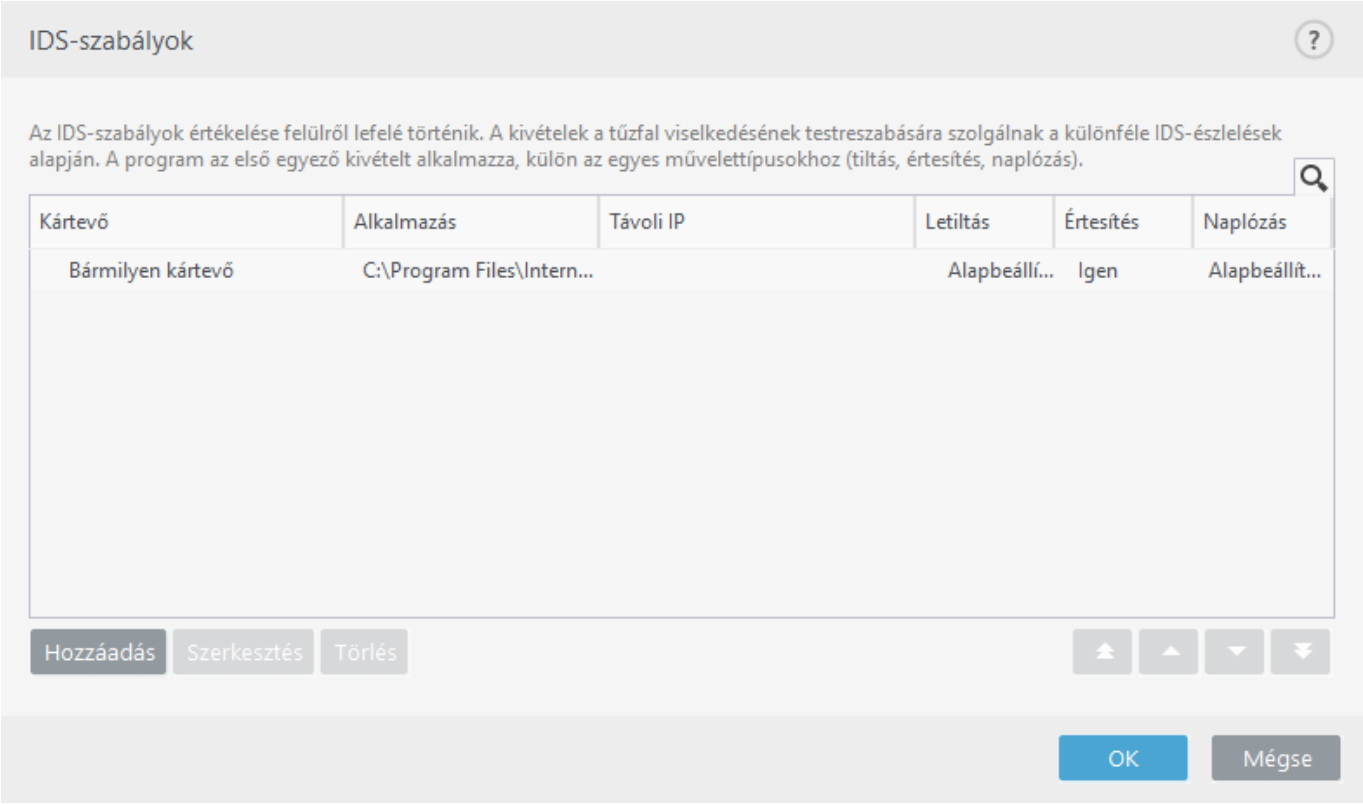
IDS szabályok

Bizonyos helyzetekben az IDS (Intrusion Detection Service) potenciális támadásként észleli a routerek és az egyéb belső hálózati eszközök közötti kommunikációt. Az IDS megkerüléséhez például hozzáadhatja az ismert biztonságos címet „Az IDS-észlelésből kizárt címek” listájához.

> **Ábrákkal ellátott útmutató**
> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> - IP-cím kizárása az IDS-ből az ESET Internet Security alkalmazásban

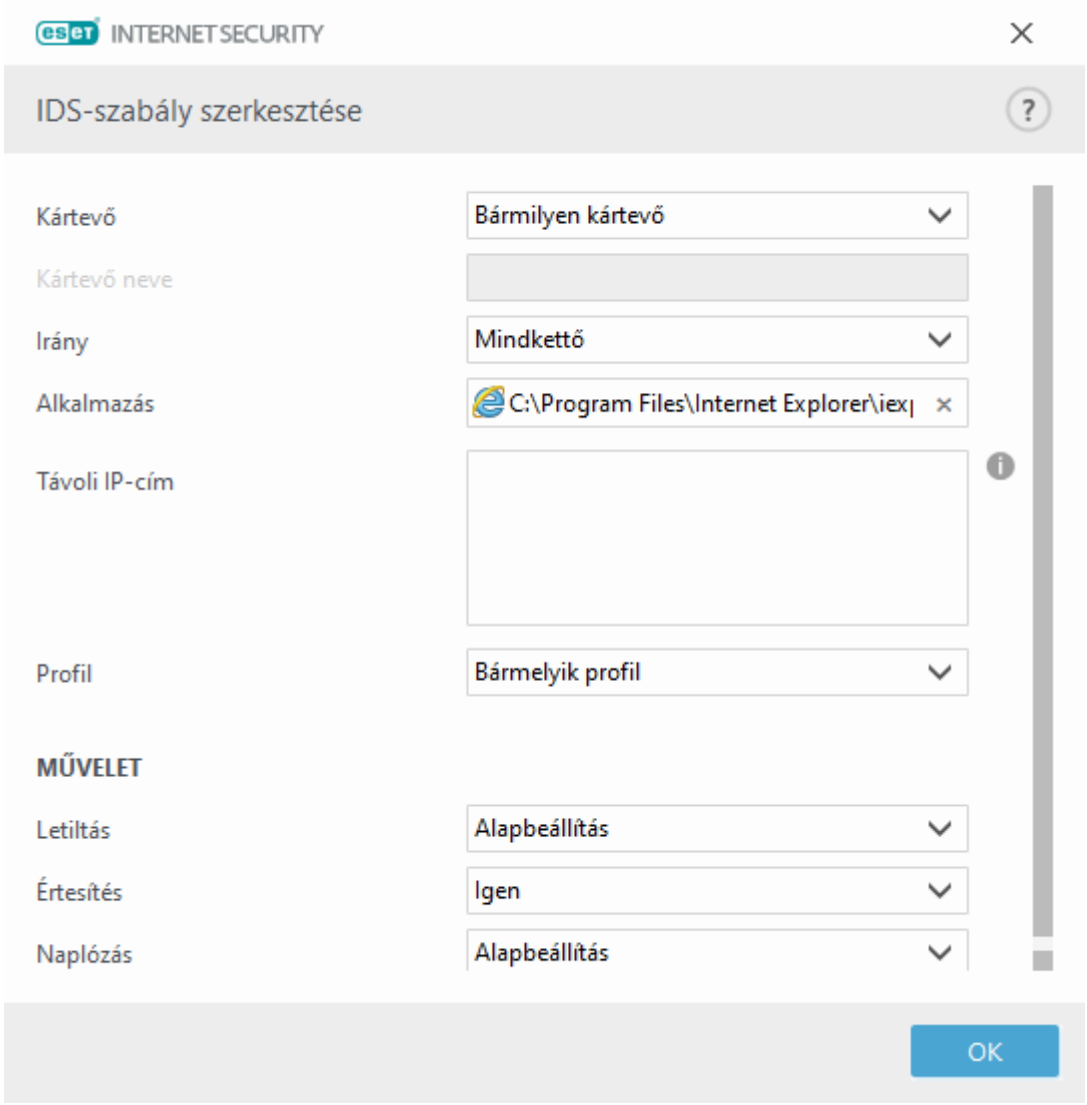
Oszlopok

- **Észlelés** – Az észlelt elem típusa.
- **Alkalmazás** – Kiválaszthatja a kivételként felvenni kívánt alkalmazás elérési útvonalát a ... ikonra kattintva (például C:\Program Files\Firefox\Firefox.exe). NE írja be az alkalmazás nevét.
- **Távoli IP-cím** – A távoli IPv4- vagy IPv6-címek/tartományok/alhálózatok listája. A címeket vesszővel elválasztva kell megadni.
- **Tiltás** – Minden rendszerfolyamathoz saját alapértelmezett viselkedés és hozzárendelt művelet (tiltás vagy engedélyezés) tartozik. Ha felül szeretné bírálni az ESET Internet Security alapértelmezett viselkedését, a legördülő menü segítségével letilthatja vagy engedélyezheti azt.
- **Értesítés** – Megjeleníthet asztali értesítéseket a számítógépén. A következő értékek közül választhat: **Alapértelmezett/Igen/Nem**.
- **Naplózás** – Naplózhatja az eseményeket az ESET Internet Security-naplófájlokba. A következő értékek közül választhat: **Alapértelmezett/Igen/Nem**.



Az IDS-szabályok kezelése

- **Hozzáadás** – Ide kattintva új IDS-szabályt hozhat létre.
- **Szerkesztés** – Ide kattintva egy meglévő IDS-szabályt szerkeszthet.
- **Eltávolítás** – Válassza ki, majd kattintson rá, ha el szeretne távolítani egy szabályt IDS-szabályok listájáról.
-  **Tetejére/Fel/Le/Aljára** – A szabályok prioritási szintjének módosítása (a szabályok értékelése felülről lefelé történik).



Ha értesítést szeretne megjeleníteni, és naplózni szeretne minden alkalommal, amikor az esemény fellép:
1.A **Hozzáadás** gombra kattintva adja hozzá az új IDS-szabályt.
2.Válassza ki a kívánt észlelt elemet az **Észlelés** legördülő menüben.
3.A **...** ikonra kattintva válassza ki az elérési útvonalat annál az alkalmazásnál, amely esetén ilyen riasztást szeretne kapni.
4.Hagyja meg az **Alapértelmezett** beállítást a **Tiltás** legördülő menüben. Ezzel az ESET Internet Security által alkalmazott alapértelmezett művelet fog érvényesülni.
5.Adja meg az **Értesítés** és a **Napló** legördülő menüben az **Igen** beállítást.
6.Az **OK** gombra kattintva mentse az értesítést.

Ha nem szeretne egy olyan ismétlődő értesítést megjeleníteni, amelyet nem tekint kártevőnek egy adott típusú **észlelés** esetén:
1.A **Hozzáadás** gombra kattintva adja hozzá az új IDS-szabályt.
2.Válassza ki a kívánt észlelt elemet az **Észlelés** legördülő menüben – például **Biztonsági bővítmények nélküli SMB-munkamenet**. **TCP-portszkennelés**.
3.Válassza ki a **Be** az irányt jelző legördülő menüben, ha bejövő kommunikációról van szó.
4.Adja meg az **Értesítés** legördülő menüben az **Igen** beállítást.
5.Adja meg az **Napló** legördülő menüben az **Igen** beállítást.
6.Hagyja üresen az **Alkalmazás** mezőt.
7.Ha a kommunikáció nem egy adott IP-címről érkezik, hagyja üresen a **Távoli IP-címek** mezőt.
8.Az **OK** gombra kattintva mentse az értesítést.

Lehetséges kártevő letiltva

Ez az eset akkor fordulhat elő, ha a számítógépen telepített alkalmazások valamelyike egy biztonsági rést kihasználva kártékony forgalmat próbál folytatni a hálózat másik számítógépével, illetve ha a program portszkennelési kísérletet észlel a rendszerben.

Kártevő – A kártevő neve.

Távoli cím – Távoli IP-cím.

Engedélyezés – Intrusion Detection Service (IDS) szabály létrehozása, amelyben előre be van állítva minden művelettípus (letiltás, értesítés, naplózás) mellőzése.

Letiltás fenntartása – Az észlelt kártevő letiltása. Ha az adott kártevőhöz IDS-szabályt szeretne létrehozni, jelölje be a **Ne értesítsen újból** jelölőnégyzetet, és a program értesítés, illetve naplózás nélkül adja hozzá a szabályt.

> Az értesítési ablakban megjelenő információk az észlelt kártevő típusától függően eltérhetnek.
> A kártevőkről és a kapcsolódó fogalmakról a Távolról kezdeményezett támadások típusai és a Kártevők típusai című témakörben talál további információt.
> Az **Ismétlődő IP-címek a hálózatban** esemény megoldásához olvassa el ESET-tudásbáziscikkünket.

Hálózati védelem hibájának elhárítása

A Hibaelhárítási varázslóval megoldhatja az ESET Tűzfal által okozott kapcsolódási problémákat. A legördülő menüből válassza ki azt az időszakot, amely alatt a kommunikáció nem működött. A legutóbbi nem működő kommunikációk listája áttekintést ad az alkalmazás vagy eszköz típusáról, a megbízhatóságról, valamint az adott időszakban tiltott alkalmazások és eszközök számáról. A tiltott kommunikációk részleteiért kattintson a **Részletek** elemre. A következő lépés a kapcsolati problémák által érintett alkalmazás vagy eszköz tiltásának megszüntetése.

Amikor a **Feloldás** lehetőségre kattint, az addig tiltott kommunikáció engedélyezve lesz. Ha továbbra is problémákat észlel egy alkalmazással kapcsolatban, vagy az eszköz nem működik megfelelően, kattintson **Az alkalmazás még mindig nem működik** lehetőségre; ekkor az adott eszközhöz addig tiltott minden kommunikáció engedélyezve lesz. Ha a probléma nem szűnik meg, indítsa újra a számítógépet.

A **Módosítások megjelenítése** elemre kattintva megtekintheti a varázsló által létrehozott szabályokat. A varázsló által létrehozott szabályokat itt is megtekintheti: **További beállítások** > **Hálózati védelem** > **Tűzfal** > **Speciális** > **Szabályok**.

Kattintson a **Másik feloldása** lehetőségre egy másik eszköz vagy alkalmazás kommunikációs hibáinak megoldásához.

Engedélyezett szolgáltatások és további beállítások

A Tűzfal és a Hálózati támadások elleni védelem szakaszban konfigurálhatja a számítógépen futó egyes szolgáltatásokhoz a megbízható zónából való hozzáférést.

Engedélyezheti vagy letilthatja több olyan támadás és biztonsági rés észlelését, amelyek károsíthatják a számítógépet.

Egyes esetekben nem kap kártevőkkel kapcsolatos értesítést a letiltott kommunikációkról. A Naplózás és szabályok vagy kivételek létrehozása naplóból című részből megtudhatja, hogy miként tekintheti meg az összes tiltott kommunikációt a tűzfal naplójában.

Az ablakban található egyes beállítások elérhetősége az ESET-szoftver típusától, a tűzfal modultól, valamint az operációs rendszer verziójától függ.

Engedélyezett szolgáltatások

E csoport beállításaival egyszerűbben konfigurálható a számítógép szolgáltatásaihoz a megbízható zónából való hozzáférés. Számos közülük előre definiált tűzfalszabályokat engedélyez vagy tilt le. Az engedélyezett szolgáltatások a **További beállítások** (F5) > **Hálózati védelem** > **Tűzfal** > **Speciális** > **Engedélyezett szolgáltatások** lapon szerkeszthetők.

- **Fájl- és nyomtatómegosztás engedélyezése a Megbízható zónában** – A jelölőnégyzet bejelölésével engedélyezhető, hogy a megbízható zóna számítógépei hozzáférjenek a helyi számítógép megosztott fájljaihoz és nyomtatóihoz.

- **UPNP engedélyezése a rendszerszolgáltatásoknak a Megbízható zónában** – A jelölőnégyzet bejelölésével engedélyezhető az UPnP protokoll összes bejövő és kimenő kérelme a rendszerszolgáltatásokhoz. Az UPnP (Universal Plug and Play, más néven Microsoft Hálózat felderítése) a Windows Vista és az újabb operációs rendszerekben használt funkció.

- **Bejövő RPC-kommunikáció engedélyezése a megbízható zónában** – A beállítással engedélyezhetők az MS RPC Portmapper és RPC/DCOM szolgáltatáson keresztül létesített TCP-kapcsolatok a megbízható zónán belül.

- **Távoli asztal engedélyezése a megbízható zónában** – Ezt az opciót bejelölve lehetővé teszi a Microsoft RDP protokollon keresztüli kapcsolatokat, és engedélyezi a megbízható zónában lévő számítógépeknek, hogy az RDP-t használó programokkal (például a Távoli asztali kapcsolat alkalmazással) hozzáférjenek ehhez a számítógéphez.

- **Naplózás engedélyezése csoportcímes küldési csoportokba az** IGMP protokollon keresztül – Ezzel az opcióval engedélyezheti az **IGMP** protokollt használó bejövő vagy kimenő, illetve az UDP protokollt használó bejövő csoportos küldésű adatfolyamokat, például az IGMP protokollt használó programok által létrehozott video-adatfolyamokat.

- **Hálózati hídkapcsolatok kommunikációjának engedélyezése** – A jelölőnégyzet bejelölésével elkerülheti a hálózati hídkapcsolatok megszakítását. A hálózati hídkapcsolatokkal egy virtuális gép csatlakoztatható egy hálózathoz a gazdaszámítógép Ethernet-adaptere segítségével. Hálózati hídkapcsolatok használatakor a virtuális gép el tud érni más eszközöket a hálózaton – és ez fordított irányban is lehetséges – épp úgy, mintha egy fizikai számítógép lenne a hálózaton.

- **Automatikus Web Services Discovery- (WSD) kérések engedélyezése a rendszerszolgáltatásoknak a megbízható zónában** – Az opció bejelölésével engedélyezheti a megbízható zónából a tűzfalon keresztül bejövő WSD- (Web Services Discovery) kéréseket. A WSD a helyi hálózaton a szolgáltatások keresésére szolgáló protokoll.

- **Csoportos IP-címek feloldásának engedélyezése a megbízható zónában (LLMNR)** – Az LLMNR (Link-local Multicast Name Resolution – Kapcsolati szintű csoportos küldés névfeloldása) egy DNS-csomagon alapuló protokoll, amely az IPv4 és az IPv6 rendszerű állomásokon egyaránt lehetővé teszi az azonos helyi hálózaton lévő állomások címének feloldását DNS-szerver és DNS-klienskonfiguráció igénybevétele nélkül. Ez a beállítás átengedi a tűzfalon a Megbízható zónából érkező bejövő csoportos DNS-kérelmeket.

- **A Windows otthoni csoport támogatása** – A jelölőnégyzet bejelölésével engedélyezheti a Windows 7 vagy újabb operációs rendszerben megjelent otthoni csoportok funkciójának támogatását. Az otthoni csoportok révén fájlok és nyomtatók oszthatók meg az otthoni hálózatokban. Az otthoni csoport beállításához válassza a **Start** > **Vezérlőpult** > **Hálózat és internet** > **Otthoni csoport** lehetőséget.

Behatolásfelismerés

A behatolásészlelés figyeli, hogy az eszköz hálózati kommunikációjában folynak-e rosszindulatú tevékenységek. Ezek a beállítások a **További beállítások** (F5) > **Hálózati védelem** > **Hálózati támadások elleni védelem** > **További beállítások Behatolásfelismerés** szakaszban szerkeszthetők.

- **SMB protokollSMB** – Számos biztonsági problémát észlel és blokkol az SMB protokollban.

- **RPC Protokoll** – Észleli és letiltja a különféle gyakori biztonsági réseket és kitettségeket az elosztott számítógépes környezethez (DCE) kifejlesztett távoli eljáráshívási rendszerben.

- **RDP protokollRDP** – Észleli és letiltja a gyakori biztonsági réseket és kitettségeket az RDP protokollban (lásd fent).

- **ARP-mérgezés felismerése** – A betolakodó illetéktelen személyek általi támadások vagy a hálózati kapcsolónál az elemzésészlelés által kiváltott ARP-mérgezés felismerése. Az ARP (Address Resolution Protocol) protokollt a hálózati alkalmazás vagy eszköz használja az Ethernet-cím meghatározására.

- **TCP/UDP-portszkennelés felismerése** – Portszkenneléses szoftverek támadásait észleli. Ezek olyan alkalmazások, amelyek az állomásokon próbálnak nyitott portokat keresni úgy, hogy klienskérelmeket küldenek portcímek tartományára abból a célból, hogy aktív portokat találjanak, és kihasználják a szolgáltatás biztonsági réseit. Erről a támadástípusról további információt a szószedetben olvashat.

- **Nem biztonságos címek letiltása a támadások felismerése után** – A támadások forrásaként felismert IP-címeket a program felveszi a tiltólistára, így bizonyos időszakra megakadályozza a kapcsolatot.

- **Értesítés megjelenítése támadás felismerése után** – A jelölőnégyzet bejelölésével kikapcsolhatja a képernyő jobb alsó sarkában, a tálcán megjelenő értesítéseket.

- **Értesítések megjelenítése a biztonsági réseket kihasználó támadások esetén is** – Riasztást jelenít meg a biztonsági rések elleni támadások észlelésekor, illetve ha egy kártevő ily módon kísérel meg belépni a rendszerbe.

Csomagellenőrzés

Olyan csomagelemzési típus, amely szűri a hálózaton keresztül továbbított adatokat. Ezek a beállítások a **További beállítások** (F5) > **Hálózati védelem** > **Hálózati támadások elleni védelem** > **További beállítások Csomagellenőrzés** szakaszban szerkeszthetők.

- **Rendszergazdai megosztások bejövő kapcsolatainak engedélyezése az SMB protokollban** – A rendszergazdai megosztások azok az alapértelmezett hálózati megosztások, amelyek megosztják a merevlemez-partíciókat (*C$, D$*...) a rendszerben a rendszermappákkal (*ADMIN$*). A rendszergazdai megosztásokkal fennálló kapcsolat letiltása számos biztonsági kockázatot csökkent. A Conficker féreg például szótáras támadásokkal próbál meg a rendszergazdai megosztásokhoz kapcsolódni.

- **Régi (nem támogatott) SMB-dialektusok tiltása** – Letiltja az IDS által nem támogatott régi SMB-dialektust

használó SMB-munkameneteket. A modern Windows operációs rendszerek a korábbi operációs rendszerekkel (például Windows 95) való visszamenőleges kompatibilitásnak köszönhetően támogatják az SMB-dialektusokat. A támadó használhat régi dialektust az SMB-munkamenetben annak érdekében, hogy elkerülje a forgalom vizsgálatát. Tiltsa le a régi SMB-dialektusokat, ha számítógépének nem kell fájlokat megosztania (vagy általában használjon SMB-kommunikációt) a Windows korábbi verzióját futtató számítógéppel.

- **Biztonsági bővítmények nélküli SMB-munkamenetek tiltása** – A kibővített biztonságot az SMB-munkamenet használata során lehet egyeztetni a LAN Manager kérdés-válasz hitelesítésénél biztonságosabb hitelesítési módszerek biztosítása céljából. A LAN Manager séma gyengének számít, és a használata nem javasolt.

- **Végrehajtható fájlok megbízható zónán kívüli szerveren való megnyitásának tiltása az SMB protokollban** – Megszakad a kapcsolat, amikor megkísérli egy végrehajtható fájl (.exe, .dll) futtatását egy olyan szerveren lévő megosztott mappából, amely nem tartozik a tűzfal megbízható zónájához. Vegye figyelembe, hogy a végrehajtható fájlok megbízható forrásokból történő másolása törvényes lehet. A végrehajtható fájlok megbízható forrásokból való másolása szabályszerű lehet ugyan, ez a felismerés azonban csökkenti a kártékony szervereken lévő fájlok nem kívánt megnyitásából származó kockázatokat (például egy megosztott kártékony végrehajtható fájlra mutató hivatkozásra kattintva megnyitott fájl esetén).

- **NTLM-hitelesítés tiltása a megbízható zónában lévő/megbízható zónán kívüli szerver eléréséhez az SMB protokollban** – Az NTLM (mindkét verziójának) hitelesítési sémáit használó protokollok ki vannak téve a hitelesítő adatok továbbításával járó (az SMB protokoll esetében SMB-továbbításos néven ismert) támadásnak. A megbízható zónán kívüli szerverrel való NTLM-hitelesítés tiltása csökkenti a megbízható zónán kívüli kártékony szerver által történő hitelesítőadat-továbbításból származó kockázatokat. Hasonlóképpen, a megbízható zónában lévő szerverekkel való NTLM-hitelesítés is tiltható.

- **A Biztonsági fiókkezelő szolgáltatással (SAM) való kommunikáció engedélyezése** – A szolgáltatásról további információt itt talál: [MS-SAMR].

- **A Helyi biztonsági szervezet (LSA) szolgáltatással való kommunikáció engedélyezése** – A szolgáltatásról további információt itt talál: [MS-LSAD] és [MS-LSAT].

- **A Távoli beállításjegyzék szolgáltatással való kommunikáció engedélyezése** – A szolgáltatásról további információt itt talál: [MS-RRP].

- **A Szolgáltatásvezérlő szolgáltatással való kommunikáció engedélyezése** – A szolgáltatásról további információt itt talál: [MS-SCMR].

- **A Kiszolgáló szolgáltatással való kommunikáció engedélyezése** – A szolgáltatásról további információt itt talál: [MS-SRVS].

- **Más szolgáltatásokkal való kommunikáció engedélyezése** – Egyéb MSRPC-szolgáltatások.

Csatlakoztatott hálózatok

Megjeleníti azokat a hálózatokat, amelyekhez hálózati adapterek vannak csatlakoztatva. A **Csatlakoztatott hálózatok** lap a **Beállítás** > **Hálózati védelem** útvonalon érhető el. Miután a hálózatnév alatti hivatkozásra kattintott, a rendszer arra kéri, hogy válasszon ki egy védelmi típust ahhoz a hálózathoz, amelyhez kapcsolódik.

A hálózatvédelem konfigurálására szolgáló ablakban két hálózatvédelmi mód közül választhat:

- **Igen** – Megbízható hálózat esetén (otthoni vagy irodai hálózat). A számítógép és a számítógépen tárolt

megosztott fájlok láthatók a többi hálózati felhasználó számára, és a rendszer erőforrásai elérhetők a hálózat többi felhasználója számára. Azt javasoljuk, hogy biztonságos helyi hálózat elérésekor használja ezt a beállítást.

• **Nem** – Nem megbízható hálózat esetén (nyilvános hálózat). A rendszer fájljai és mappái nincsenek megosztva a hálózat többi felhasználójával, nem láthatók a számukra, és a rendszer erőforrásainak megosztása inaktiválva van. Azt javasoljuk, hogy vezeték nélküli hálózatok elérésekor használja ezt a beállítást.

Kattintson a hálózat melletti fogaskerék ikonra a következő lehetőségek közül való választáshoz (nem megbízható hálózatok esetén csak a **Hálózat szerkesztése** opció érhető el):

• **Hálózat szerkesztése** – A Hálózatszerkesztő megnyitása.

• **Hálózat ellenőrzése a Hálózatfelügyelet segítségével** – A Hálózatfelügyelet megnyitása hálózati ellenőrzés futtatásához.

• **Megjelölés „Saját hálózat" névvel** – A Saját hálózat címke hozzáadása a hálózathoz. A címke a hálózat mellett fog megjelenni az ESET Internet Security szolgáltatásban a könnyebb beazonosítás és a biztonság áttekintése érdekében.

• **„Saját hálózat" jelölés törlése** – A Saját hálózat címke eltávolítása. Csak akkor érhető el, ha a hálózat már fel van címkézve.

Az egyes hálózati adapterek, valamint a hozzájuk rendelt tűzfalprofil és megbízhatósági zóna megtekintéséhez kattintson a **Hálózati adapterek** elemre. Részletesebb információkért olvassa el a Hálózati adapterek című témakört.

Hálózati adapterek

A Hálózati adapterek ablak az alábbi információkat jeleníti meg a hálózati adapterekről:

• A hálózati adapter neve és a kapcsolat típusa (vezetékes, virtuális stb.)

• IP-cím MAC-címmel

• Csatlakoztatott hálózat (a Saját hálózat címke látható)

• A megbízható zóna IP-címe alhálózattal

• Aktív profil (lásd: Hálózati adapterekhez rendelt profilok)

IP-címek ideiglenes tiltólistája

A támadások forrásaként felismert IP-címeket a program felveszi a tiltólistára, így bizonyos időszakra letiltja a kapcsolatot. A címek megtekintéséhez lépjen az ESET Internet Security programból a **Beállítások** > **Hálózati védelem** > **IP-címek ideiglenes tiltólistája** lapra. Az átmenetileg letiltott IP-címeket 1 óra hosszáig tiltja le a rendszer.

Oszlopok

IP-cím – Letiltott IP-címet jelenít meg.

Letiltás oka – Itt látható a címről indított, de megakadályozott támadás típusa (például TCP-portszkennelés).

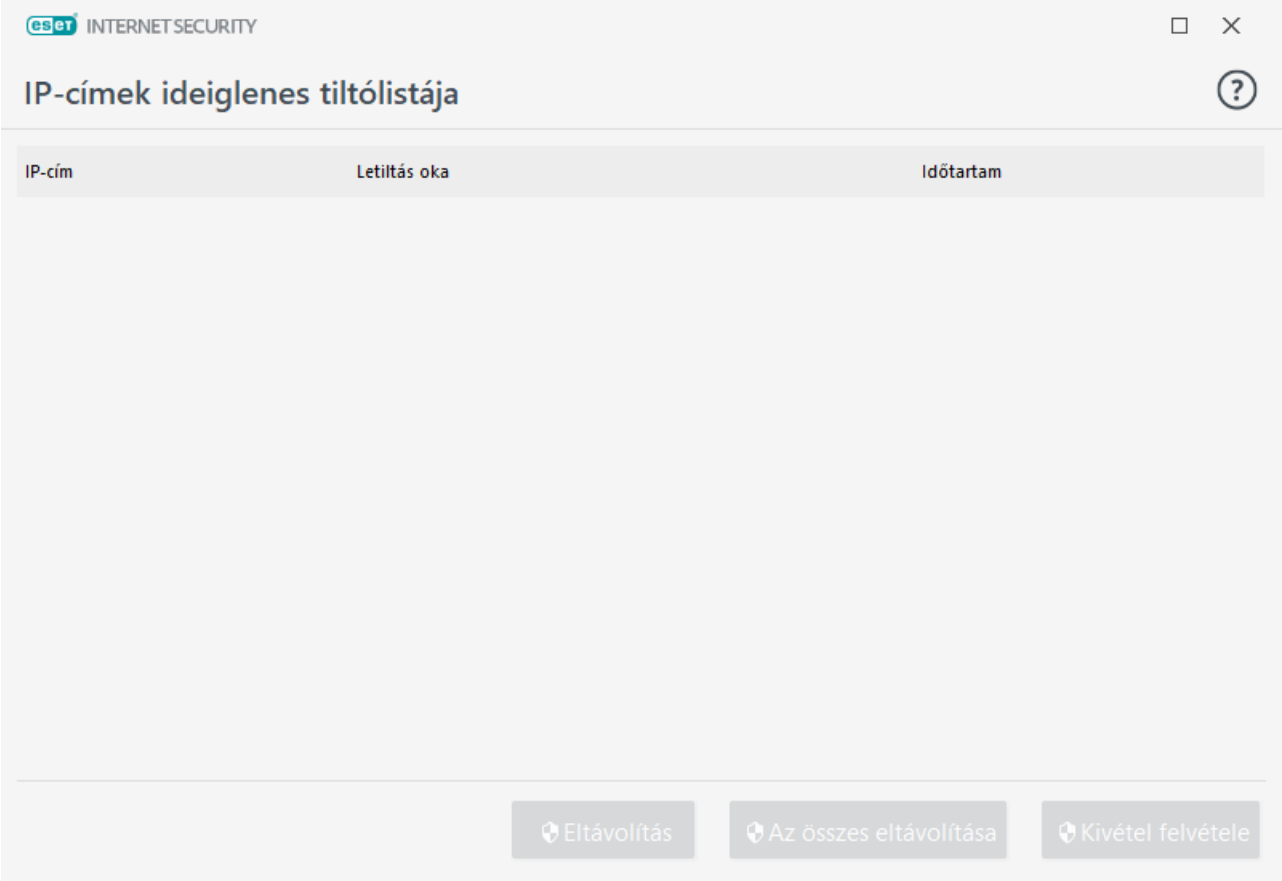
Időpont – Itt látható az a dátum és időpont, ameddig a cím a tiltólistán marad.

Vezérlőelemek

Eltávolítás – Erre a gombra kattintva eltávolíthatja a címet a tiltólistáról a lejárata előtt.

Összes eltávolítása – Erre a gombra kattintva azonnal eltávolíthatja az összes címet a tiltólistáról.

Kivétel felvétele – Erre a gombra kattintva tűzfalkivételt vehet fel az IDS-szűrésbe.



Hálózatvédelmi napló

Az ESET Internet Security hálózatvédelme a fontos eseményeket egy naplófájlba menti, amely közvetlenül a fő menüből megtekinthető. Kattintson az **Eszközök** > **További eszközök** > **Naplófájlok** elemre, majd a **Napló** legördülő listában válassza ki **Hálózati védelem** elemet.

A naplófájlok segítségével észlelhetők a hibák és felfedhetők a rendszerbe történő behatolások. Az ESET hálózatvédelmi naplók az alábbi adatokat tartalmazzák:

- Az esemény dátuma és időpontja
- Az esemény neve

- 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

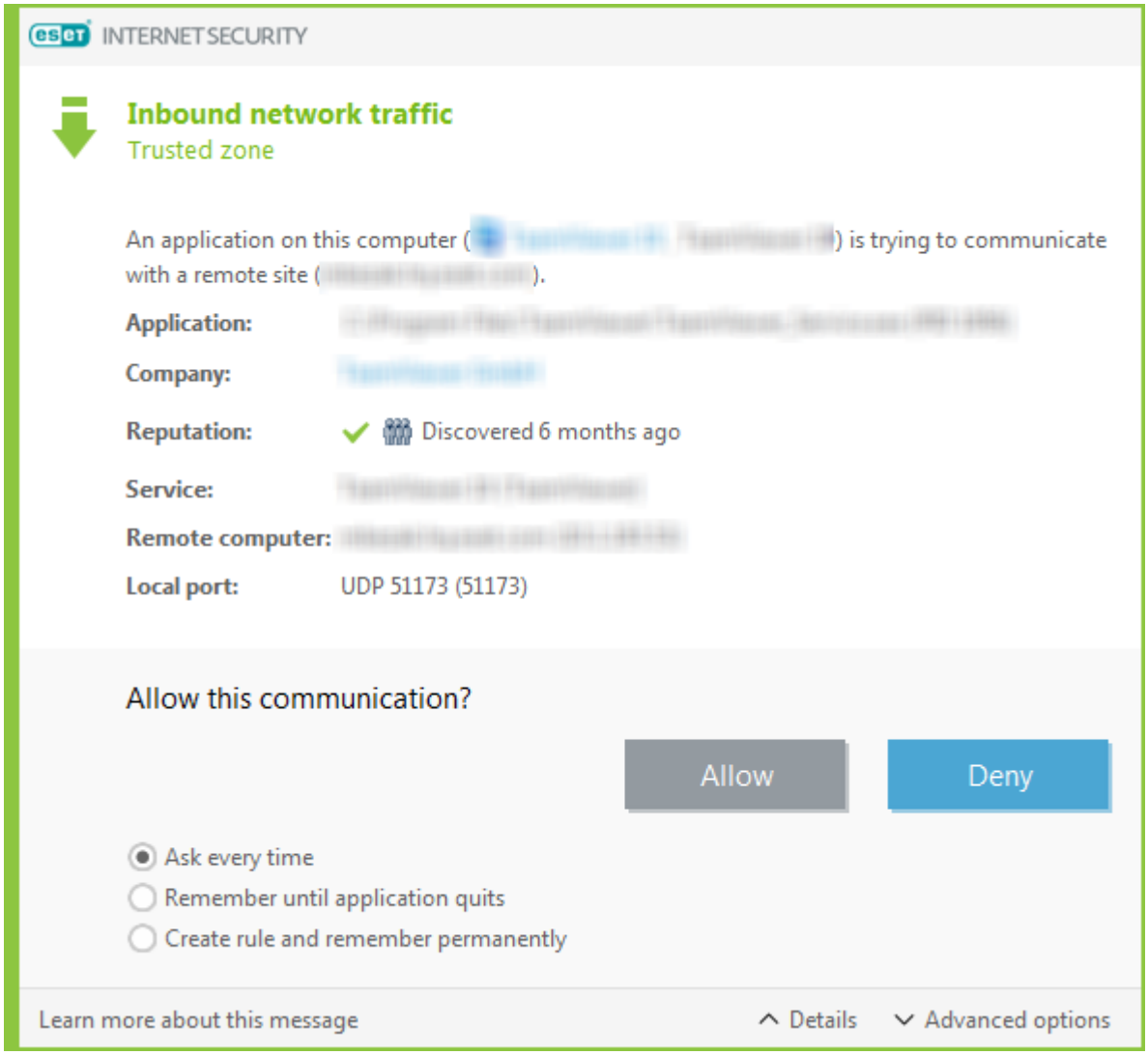
Ezeknek az adatoknak az alapos elemzésével felderítheti a rendszerbiztonság megsértésére tett kísérleteket. Számos tényező utal a lehetséges biztonsági kockázatokra, amelyek negatív hatását így a lehető legkisebbre csökkentheti. Ilyen például, ha ismeretlen helyek túl gyakran kezdeményeznek kapcsolatot,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

> **Biztonsági rés kihasználása**
> A biztonsági rés kihasználásáról szóló üzenet naplózásra kerül akkor is, ha az adott rést már kijavították a támadási kísérlet észlelése óta, és hálózati szinten blokkolták, mielőtt tényleges támadásra kerülhetett volna sor.

Kapcsolat létesítése – észlelés

A 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 tűzfal előre megadott műveleteket fog végrehajtani, felhasználói beavatkozás nélkül.

Interaktív üzemmódban a program egy tájékoztató ablakban részletes információkat is tartalmazó értesítést küld az új kapcsolat észleléséről. Választhatja a kapcsolat **engedélyezését** vagy **elutasítását** (tiltását). Ha többször engedélyezi ugyanazt a kapcsolatot a párbeszédpanelen, ajánlatos új szabályt létrehozni a kapcsolathoz. Ehhez válassza a **Művelet megjegyzése (szabály létrehozása)** lehetőséget, és a tűzfal új szabályaként mentse a műveletet. Ha a tűzfal a jövőben ugyanezt a kapcsolatot észleli, felhasználói beavatkozás nélkül is a meglévő szabályt alkalmazza rá.



Új szabályok létrehozásakor csak biztonságosnak tartott kapcsolatokat engedélyezzen. Ha minden kapcsolatot engedélyez, a tűzfal nem tölti be a rendeltetését. A kapcsolatok fontos jellemzői az alábbiak:

Alkalmazás – A végrehajtható fájl helye és folyamatazonosítója. Ne engedélyezzen kapcsolatot ismeretlen alkalmazásoknak és folyamatoknak.

Vállalat – Az alkalmazás kiadójának neve. Kattintson a szövegre a vállalat biztonsági tanúsítványának megjelenítéséhez.

Hírnév – A kapcsolat kockázati szintje. A kapcsolatok kockázati szintet kapnak: Elfogadható (zöld), Ismeretlen (narancssárga) vagy Kockázatos (piros), heurisztikus szabályok alkalmazásával, amelyek megvizsgálják az egyes kapcsolatok jellemzőit, a felhasználók számát és az észlelési időtartamot. Ezt az információt az ESET LiveGrid® technológia gyűjti.

Szolgáltatás – A szolgáltatás neve, ha az alkalmazás egy Windows-szolgáltatás.

Távoli számítógép – A távoli eszköz címe. Csak megbízható és ismert címekkel engedélyezzen kapcsolatot.

Távoli port – Kommunikációs port. A szokásos portokon (például webes kapcsolatok esetében a 80.443-as számú porton) zajló kommunikáció általában engedélyezhető.

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

kódok támadása elleni védelemben.

Az ESET Tűzfallal kapcsolatos problémák megoldása

Ha a telepített ESET Internet Security szoftverrel kapcsolatos problémákat tapasztal, többféleképpen is megállapíthatja, hogy azok az ESET Tűzfal miatt léptek-e fel. Az ESET Tűzfal emellett a kapcsolódási problémák megoldásához hozzájáruló új szabályok vagy kivételek létrehozását is segítheti.

Az ESET Tűzfallal kapcsolatos problémák megoldásához olvassa el az alábbi témaköröket:

- Hibaelhárítási varázsló
- Naplózás és szabályok vagy kivételek létrehozása naplóból
- Kivételek létrehozása a tűzfal értesítéseiből
- A hálózati védelem speciális naplózása
- Protokollszűrési problémák megoldása

Hibaelhárítási varázsló

A Hibaelhárítási varázsló értesítések küldése nélkül figyeli a letiltott kapcsolatokat, és végigvezeti Önt a hibaelhárítási eljáráson a tűzfal adott alkalmazásokkal vagy eszközökkel kapcsolatos problémáinak megoldása érdekében. Ezt követően a varázsló új szabályokat javasol alkalmazásra, amennyiben Ön jóváhagyja őket. A **Hibaelhárítási varázsló** a főmenüben a **Beállítások** > **Hálózati védelem** elemre kattintva érhető el.

Naplózás és szabályok vagy kivételek létrehozása naplóból

Alapértelmezés szerint az ESET Tűzfal nem naplózza az összes letiltott kapcsolatot. Ha meg szeretné tekinteni, hogy milyen elemeket tiltott le a Hálózati védelem, engedélyezze a naplózást a **További beállítások** lapon, amely az **Eszközök** > **Diagnosztika** > **Részletes naplózás** > **A hálózati védelem speciális naplózásának engedélyezése** lehetőséget választva érhető el. Ha a naplóban az látható, hogy a tűzfal nem kívánt elemet tilt le, egy szabályt vagy IDS-szabályt létrehozva orvosolhatja ezt. Ehhez kattintson a jobb gombbal az elemre, és válassza a **Ne tiltson le hasonló eseményeket a jövőben** parancsot. Ne feledje, hogy az összes letiltott kapcsolatot tartalmazó naplóban több ezer elem is szerepelhet, így nehézségekbe ütközhet egy adott kapcsolat megkeresése. A probléma megoldása után kikapcsolhatja a naplózást.

A naplóról további információt a Naplófájlok című témakörben talál.

> A naplózás használatával megtekintheti, hogy a Hálózati védelem milyen sorrendben tiltotta le a kapcsolatokat. Ezenkívül szabályokat is létrehozhat a naplóból, így pontosan azt teheti, amit szeretne.

Új szabály létrehozása naplóból

Az ESET Internet Security új verziója lehetővé teszi új szabály létrehozását a naplóból. A főmenüben kattintson az **Eszközök** > **További eszközök** > **Naplófájlok** pontra. A legördülő listában válassza a **Tűzfal** elemet, a jobb gombbal kattintson a kívánt naplóbejegyzésre, és a helyi menüben válassza a **Ne tiltson le hasonló eseményeket a jövőben** parancsot. Egy értesítési ablakban megjelenik az új szabály.

Az új szabályok naplóból történő létrehozásának engedélyezéséhez az ESET Internet Security alkalmazásban az alábbi beállításokat kell megadni:

1. A naplózás minimális részletességi szintjét állítsa **Diagnosztikai** értékre a **További beállítások** (F5) > **Eszközök** > **Naplófájlok** részen;

2. Engedélyezze az **Értesítések megjelenítése a biztonsági réseket kihasználó támadások esetén is** funkciót a **További beállítások** (F5) > **Hálózati védelem** > **Hálózati támadások elleni védelem** > **További beállítások Behatolásfelismerés** szakaszban.

Kivételek létrehozása a tűzfal értesítéseiből

Amikor az ESET Tűzfal kártékony hálózati tevékenységet észlel, megjelenít egy értesítést, amelyben az esemény leírása látható. Az értesítés tartalmaz egy hivatkozást is, amelyre kattintva további információkhoz juthat az eseményről, és szabályt is beállíthat az eseményhez, ha szeretne.

> **i** Ha egy hálózati alkalmazás vagy eszköz nem implementálja helyesen a hálózati szabványokat, a tűzfal ismétlődő IDS-értesítéseket jeleníthet meg. Létrehozhat egy kivételt közvetlenül az értesítésből, amellyel megakadályozhatja, hogy az ESET Tűzfal észlelje az adott alkalmazást vagy eszközt.

A hálózati védelem speciális naplózása

Ezzel a funkcióval összetettebb naplófájlok készülhetnek az ESET műszaki támogatási szolgálata számára. Mivel a funkció hatalmas naplófájlt hoz létre és lelassítja a számítógépet, csak az ESET műszaki támogatási szolgálatának kérésére használja.

1. A **További beállítások** > **Eszközök** > **Diagnosztika** részen kapcsolja be **A hálózati védelem speciális naplózásának engedélyezése** opciót.

2. Próbálja meg reprodukálni a tapasztalt problémát.

3. Tiltsa le a hálózati védelem speciális naplózását.

4. A hálózati védelem speciális naplózása által létrehozott PCAP-naplófájl ugyanabban a könyvtárban található, amelyben a diagnosztikai memóriakép létrejön: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Protokollszűrési problémák megoldása

Ha problémákat tapasztal a böngésző vagy a levelezőprogram használata során, első lépésként állapítsa meg, hogy nem a protokollszűrés-e a felelős a hibákért. Ehhez tiltsa le átmenetileg az alkalmazás protokollszűrését a

további beállítások között (ne felejtse el visszakapcsolni a beállítást, miután végzett, mert különben a böngésző és a levelezőprogram védtelen marad a támadásokkal szemben). Ha a probléma megszűnik a protokollszűrés kikapcsolása után, az alábbi gyakori problémák jöhetnek szóba:

A frissítéssel vagy a biztonságos kommunikációval kapcsolatos probléma

Ha az alkalmazás arról értesíti, hogy nem tud frissíteni, vagy hogy a kommunikációs csatorna nem biztonságos:

- Ha engedélyezve van az SSL-protokollszűrés, kapcsolja ki azt átmenetileg. Ha ez segít, továbbra is használhatja az SSL-szűrést, a frissítés működésének biztosításához pedig kizárhatja a problémás kommunikációt:
  Állítsa az SSL-protokollszűrést interaktív üzemmódra. Futtassa újra a frissítést. Ekkor megjelenik egy titkosított hálózati adatforgalomról tájékoztató párbeszédpanel. Győződjön meg arról, hogy az alkalmazás megegyezik azzal az alkalmazással, amelynek a hibaelhárítását végzi, és hogy a tanúsítvány arról a kiszolgálóról származik, amelyről a frissítést végzi. Ezután mentse a tanúsítványhoz megadott műveletet, és kattintson a Mellőzés gombra. Ha nem jelenik meg több hibát jelző párbeszédpanel, visszakapcsolhatja a szűrési üzemmódot automatikusra, mivel ez azt jelenti, hogy a probléma megoldódott.

- Ha a kérdéses alkalmazás nem böngésző vagy levelezőprogram, teljesen kizárhatja azt a protokollszűrésből (ha böngésző vagy levelezőprogram esetében tenne így, azzal támadásoknak tenné ki magát). Minden olyan alkalmazás, amelynek a kommunikációjára szűrőt alkalmazott a múltban, szerepel a kivétel hozzáadásakor kapott listában, így elvileg nincs szükség az alkalmazás kézi hozzáadására.

Hálózati eszköz elérésével kapcsolatos probléma

Ha nem tudja használni egy hálózati eszköz egyik funkcióját sem (megnyitni a webkamera egy weboldalát, vagy videót lejátszani az otthoni médialejátszón), próbálkozzon azzal, hogy felveszi az eszköz IPv4- és IPv6-címét a kizárt címek listájára.

Egy adott webhellyel kapcsolatos problémák

Kizárhat adott webhelyeket a protokollszűrésből az URL-címkezelés használatával. Ha például nem tudja elérni a https://www.gmail.com/intl/en/mail/help/about.html webhelyet, próbálkozzon azzal, hogy felveszi a *gmail.com* elemet a kizárt címek listájára.

Egyes, legfelső szintű tanúsítványok importálására képes alkalmazások futásakor fellépő hiba

Az SSL-protokollszűrés engedélyezésekor az ESET Internet Security meggyőződik arról, hogy a telepített alkalmazások megbíznak abban a módban, ahogyan a program az SSL-szűrést végzi. Ehhez egy tanúsítványt importál azok tanúsítványtárába. Egyes alkalmazások esetében ez nem lehetséges, amíg fut az alkalmazás. Ilyen például a Firefox és az Opera. Győződjön meg arról, hogy ezek közül egyik sem fut (a legegyszerűbb, ha megnyitja a Feladatkezelőt, és ellenőrzi, hogy a Folyamatok lapon szerepel-e a firefox.exe vagy az opera.exe), majd kattintson az Újra gombra.

Nem megbízható tanúsítvánnyal vagy érvénytelen aláírással kapcsolatos probléma

Ebben az esetben az a legvalószínűbb, hogy a fent ismertetett importálás meghiúsult. Elsőként győződjön meg

arról, hogy nem fut a fent említett alkalmazások egyike sem. Ezután tiltsa le, majd engedélyezze újra az SSL-protokollszűrést. Ezzel újrafuttatja az importálást.

Tudásbáziscikkünkből megtudhatja, hogy hogyan kezelhető a protokoll-/SSL-/TLS-szűrés az ESET Windows otthoni termékben?

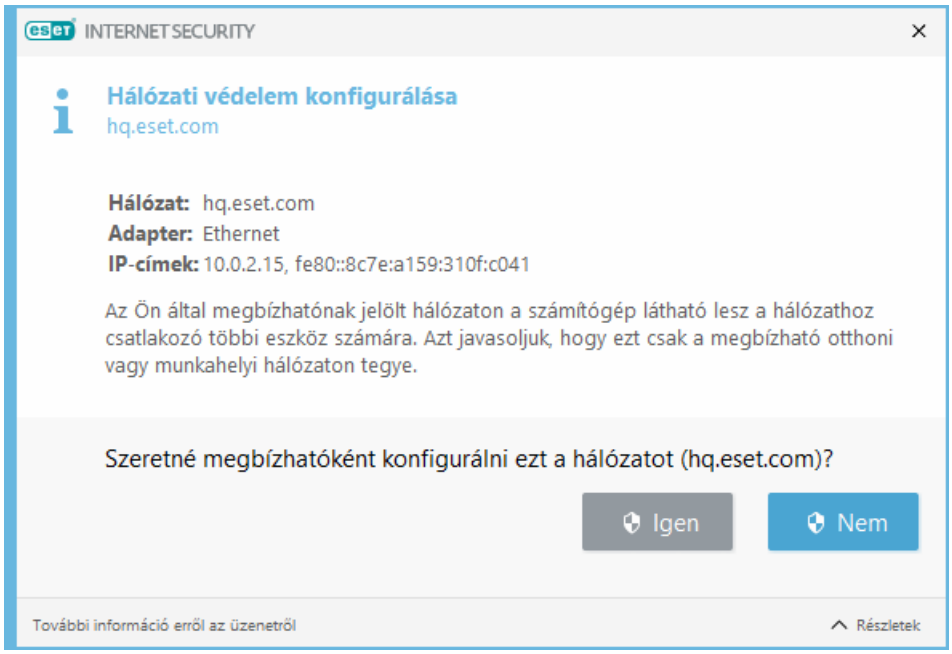
A program új hálózatot észlelt

Alapértelmezés szerint az ESET Internet Security a Windows-beállításokat alkalmazza egy új hálózat észlelésekor. Ha párbeszédpanelt szeretne megjeleníteni új hálózat észlelésekor, az Ismert hálózatok lapon módosítsa úgy az új hálózatok védelmi típusát, hogy a szolgáltatás megkérdezze a felhasználót. Ezután ha a program új hálózattal létesített kapcsolatot észlel, lehetővé teszi a felhasználónak a védelmi szint megválasztását. Ez a beállítás az adott hálózatban lévő összes távoli számítógéppel létesített kapcsolatra érvényes lesz.

A hálózatvédelem konfigurálására szolgáló ablakban két hálózatvédelmi mód közül választhat:

- **Igen** – Megbízható hálózat esetén (otthoni vagy irodai hálózat). A számítógép és a számítógépen tárolt megosztott fájlok láthatók a többi hálózati felhasználó számára, és a rendszer erőforrásai elérhetők a hálózat többi felhasználója számára. Azt javasoljuk, hogy biztonságos helyi hálózat elérésekor használja ezt a beállítást.

- **Nem** – Nem megbízható hálózat esetén (nyilvános hálózat). A rendszer fájljai és mappái nincsenek megosztva a hálózat többi felhasználójával, nem láthatók a számukra, és a rendszer erőforrásainak megosztása inaktiválva van. Azt javasoljuk, hogy vezeték nélküli hálózatok elérésekor használja ezt a beállítást.



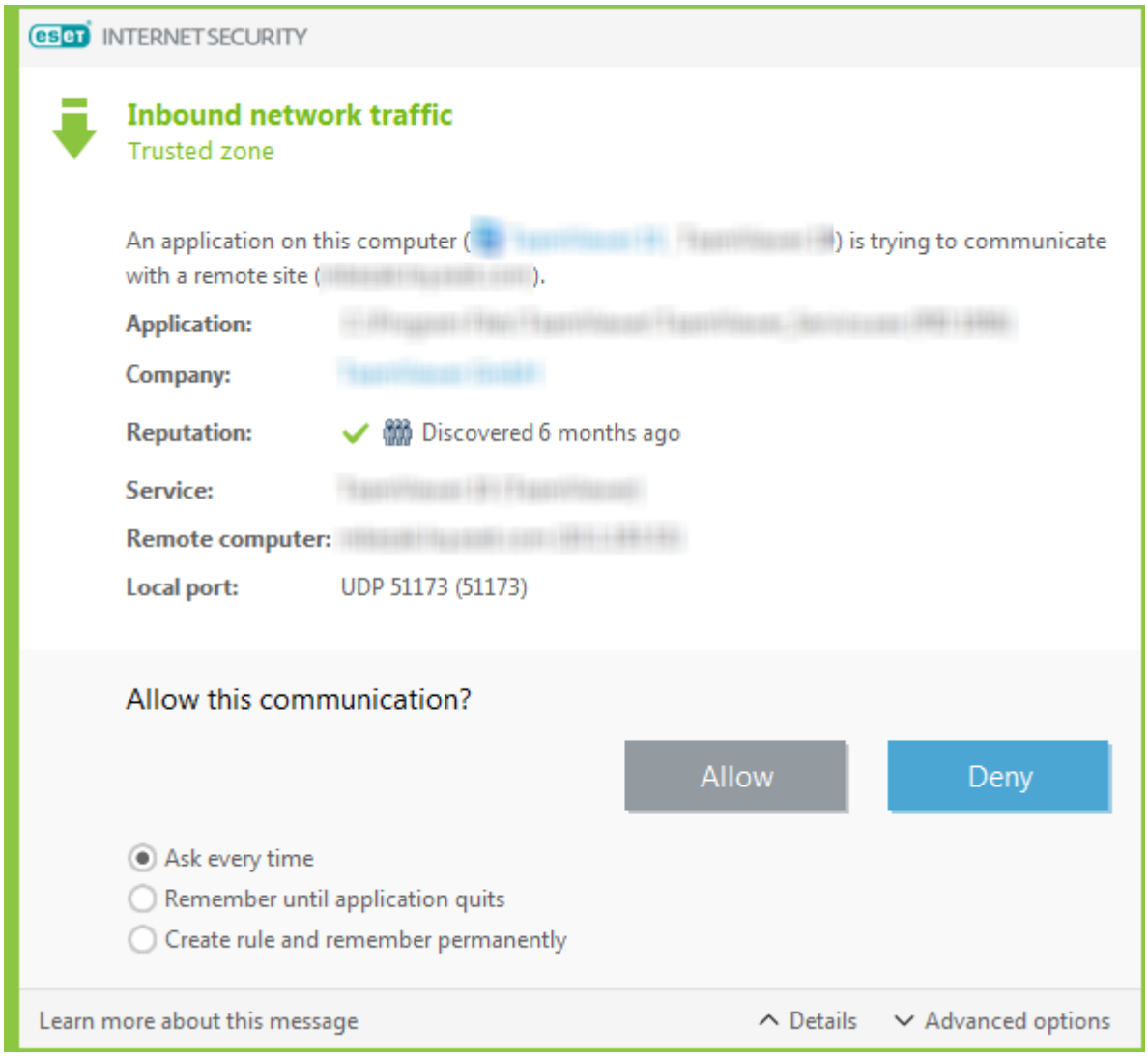
Ha a hálózat megbízhatónak van beállítva, akkor a közvetlenül csatlakoztatott alhálózatok automatikusan megbízhatónak minősülnek.

Alkalmazásmódosulás

A tűzfal változást észlelt egy alkalmazásban, amely kimenő kapcsolatokat létesít a számítógépen. Elképzelhető, hogy egyszerűen csak új verzióra frissült az alkalmazás. Másrészről azonban kártevő is okozhatja a változást. Ha nincs tudomása szándékos módosításról, ajánlott letiltani a kapcsolatot, majd ellenőrizni a számítógépet a legfrissebb vírusdefiníciós adatbázissal.

Bejövő megbízható kommunikáció

Példa a megbízható zónából bejövő kapcsolatra:
A megbízható zónában található egyik távoli számítógép kommunikálni próbál a számítógépen futó egyik helyi alkalmazással.



Alkalmazás – Az az alkalmazás, amellyel egy távoli számítógép kapcsolatot kísérel meg létesíteni.

Gyártó – Az alkalmazás gyártója.

Megbízhatóság – Az alkalmazás megbízhatósága az ESET LiveGrid® technológiának köszönhetően..

Szolgáltatás – A számítógépen éppen futó szolgáltatás neve.

Távoli számítógép – Az a távoli számítógép, amely kapcsolatot kísérel meg létesíteni a számítógépen futó alkalmazással.

Helyi port – A kommunikációhoz használt port.

Mindig rákérdez – Ha egy szabályhoz alapértelmezés szerint **rákérdezés** van beállítva, a szabály aktiválásakor minden alkalommal megjelenik egy párbeszédpanel.

Megőrzés az alkalmazás kilépéséig – Az ESET Internet Security emlékezni fog a kiválasztott műveletre a rendszer következő újraindításáig.

Szabály létrehozása és végleges megőrzése – Ha a kommunikáció engedélyezése vagy letiltása előtt bejelöli ezt a választógombot, az ESET Internet Security emlékezni fog a műveletre, és azt használja, ha a távoli számítógép ismét megpróbál kapcsolatba lépni az alkalmazással.

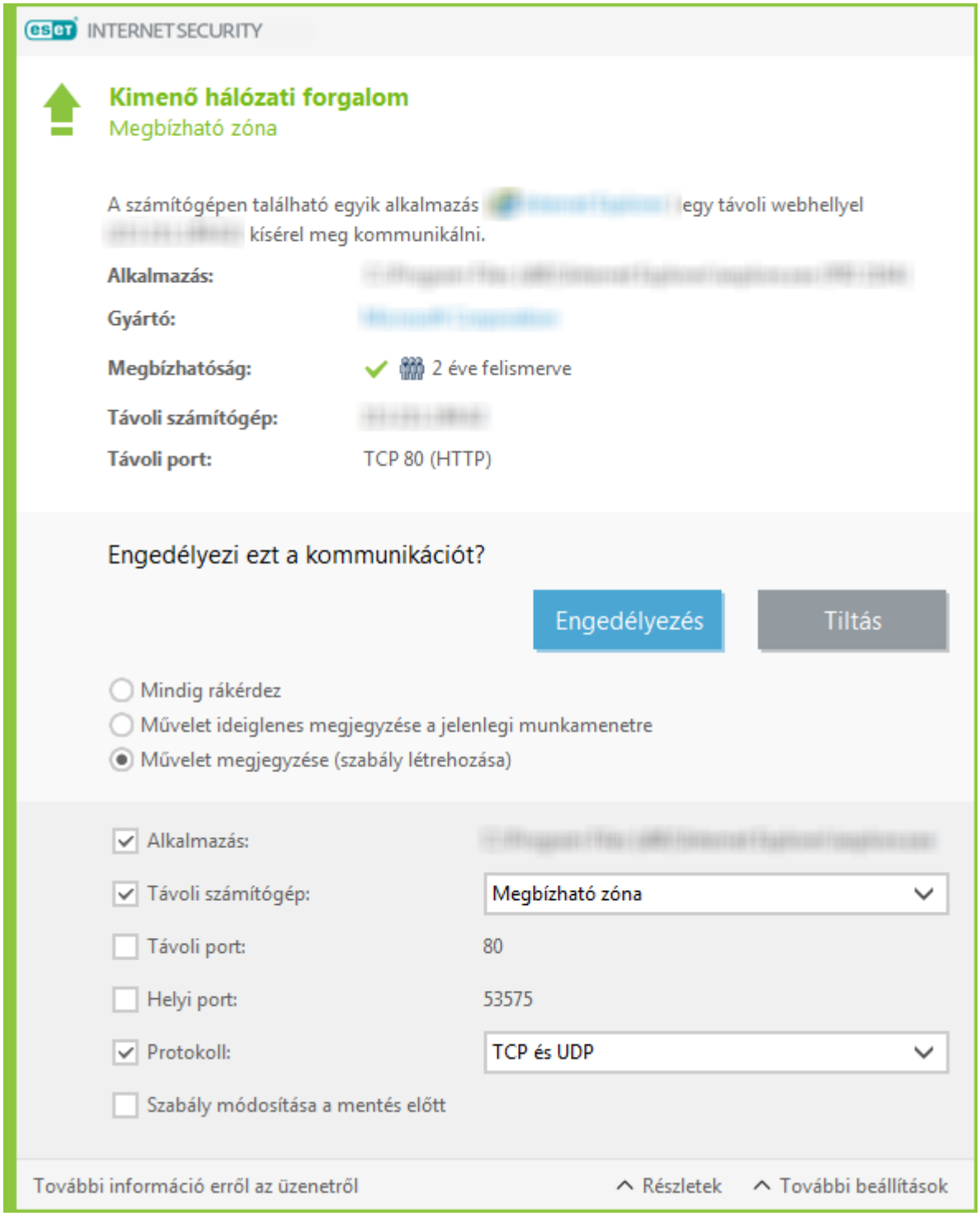
Engedélyezés – Ezzel a beállítással engedélyezheti a bejövő kommunikációt.

Tiltás – Ezzel a beállítással letilthatja a bejövő kommunikációt.

További beállítások – Lehetővé teszi a szabály tulajdonságainak testreszabását.

Kimenő megbízható kommunikáció

Példa a megbízható zónába irányuló kimenő kapcsolatra:
Egy helyi alkalmazás kapcsolatot próbál létesíteni a helyi hálózaton vagy a megbízható zónában lévő valamelyik hálózaton található másik számítógéppel.



Alkalmazás – Az az alkalmazás, amellyel egy távoli számítógép kapcsolatot kísérel meg létesíteni.

Gyártó – Az alkalmazás gyártója.

Megbízhatóság – Az alkalmazás megbízhatósága az ESET LiveGrid® technológiának köszönhetően..

Szolgáltatás – A számítógépen éppen futó szolgáltatás neve.

Távoli számítógép – Az a távoli számítógép, amely kapcsolatot kísérel meg létesíteni a számítógépen futó alkalmazással.

Helyi port – A kommunikációhoz használt port.

Mindig rákérdez – Ha egy szabályhoz alapértelmezés szerint **rákérdezés** van beállítva, a szabály aktiválásakor minden alkalommal megjelenik egy párbeszédpanel.

Megőrzés az alkalmazás kilépéséig – Az ESET Internet Security emlékezni fog a kiválasztott műveletre a rendszer következő újraindításáig.

Szabály létrehozása és végleges megőrzése – Ha a kommunikáció engedélyezése vagy letiltása előtt bejelöli ezt a választógombot, az ESET Internet Security emlékezni fog a műveletre, és azt használja, ha a távoli számítógép ismét megpróbál kapcsolatba lépni az alkalmazással.

Engedélyezés – Ezzel a beállítással engedélyezheti a bejövő kommunikációt.

Tiltás – Ezzel a beállítással letilthatja a bejövő kommunikációt.

További beállítások – Lehetővé teszi a szabály tulajdonságainak testreszabását.

Bejövő kommunikáció

Példa a bejövő internetes kommunikációra:
Egy távoli számítógép kommunikálni próbál a számítógépen futó egyik alkalmazással.

Alkalmazás – Az az alkalmazás, amellyel egy távoli számítógép kapcsolatot kísérel meg létesíteni.

Gyártó – Az alkalmazás gyártója.

Megbízhatóság – Az alkalmazás megbízhatósága az ESET LiveGrid® technológiának köszönhetően..

Szolgáltatás – A számítógépen éppen futó szolgáltatás neve.

Távoli számítógép – Az a távoli számítógép, amely kapcsolatot kísérel meg létesíteni a számítógépen futó alkalmazással.

Helyi port – A kommunikációhoz használt port.

Mindig rákérdez – Ha egy szabályhoz alapértelmezés szerint **rákérdezés** van beállítva, a szabály aktiválásakor minden alkalommal megjelenik egy párbeszédpanel.

Megőrzés az alkalmazás kilépéséig – Az ESET Internet Security emlékezni fog a kiválasztott műveletre a rendszer következő újraindításáig.

Szabály létrehozása és végleges megőrzése – Ha a kommunikáció engedélyezése vagy letiltása előtt bejelöli ezt a választógombot, az ESET Internet Security emlékezni fog a műveletre, és azt használja, ha a távoli számítógép ismét megpróbál kapcsolatba lépni az alkalmazással.

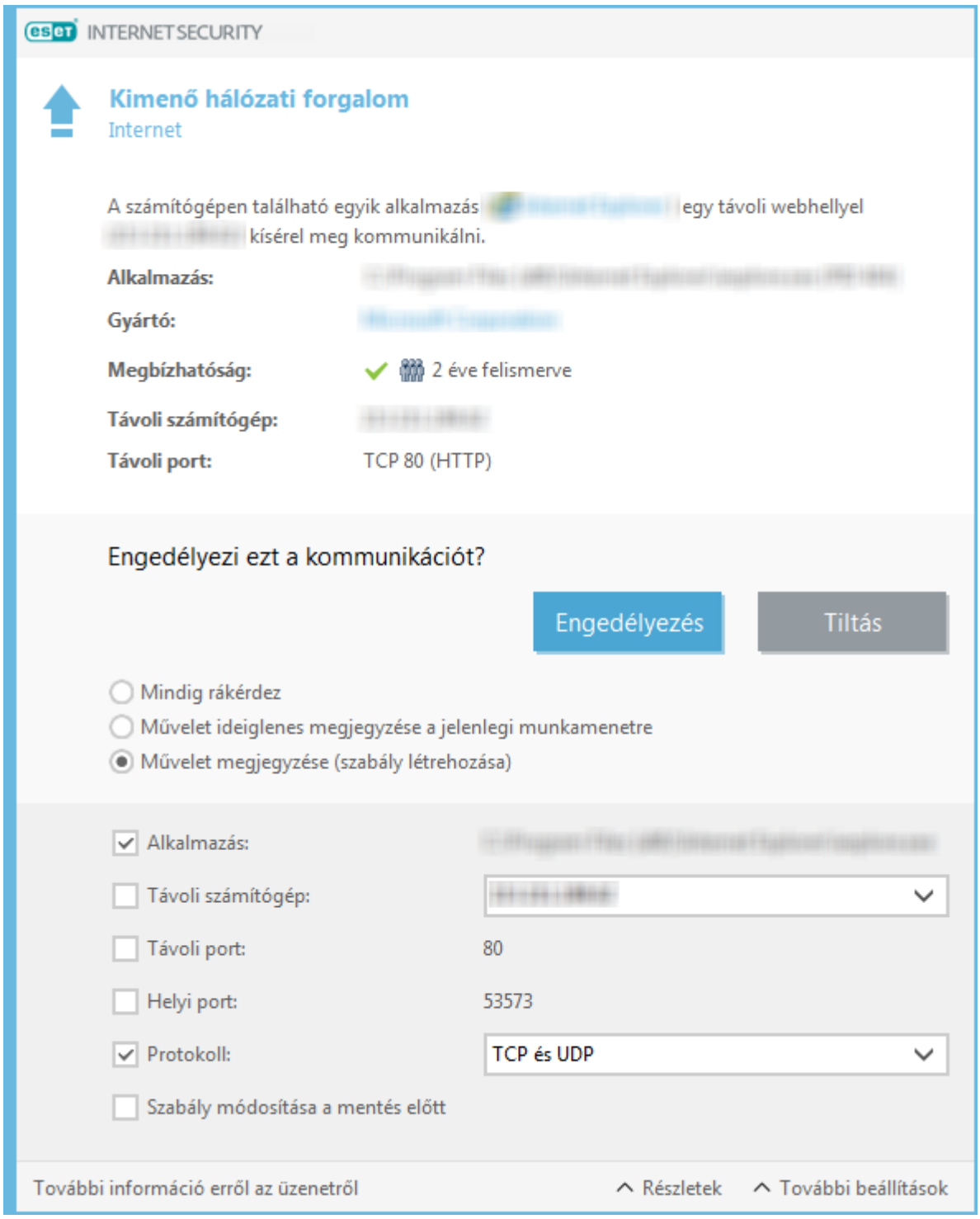
Engedélyezés – Ezzel a beállítással engedélyezheti a bejövő kommunikációt.

Tiltás – Ezzel a beállítással letilthatja a bejövő kommunikációt.

További beállítások – Lehetővé teszi a szabály tulajdonságainak testreszabását.

Kimenő kommunikáció

Példa a kimenő internetes kommunikációra:
Egy helyi alkalmazás internetkapcsolatot próbál létesíteni.



Alkalmazás – Az az alkalmazás, amellyel egy távoli számítógép kapcsolatot kísérel meg létesíteni.

Gyártó – Az alkalmazás gyártója.

Megbízhatóság – Az alkalmazás megbízhatósága az ESET LiveGrid® technológiának köszönhetően..

Szolgáltatás – A számítógépen éppen futó szolgáltatás neve.

Távoli számítógép – Az a távoli számítógép, amely kapcsolatot kísérel meg létesíteni a számítógépen futó alkalmazással.

Helyi port – A kommunikációhoz használt port.

Mindig rákérdez – Ha egy szabályhoz alapértelmezés szerint **rákérdezés** van beállítva, a szabály aktiválásakor minden alkalommal megjelenik egy párbeszédpanel.

Megőrzés az alkalmazás kilépéséig – Az ESET Internet Security emlékezni fog a kiválasztott műveletre a rendszer következő újraindításáig.

Szabály létrehozása és végleges megőrzése – Ha a kommunikáció engedélyezése vagy letiltása előtt bejelöli ezt a választógombot, az ESET Internet Security emlékezni fog a műveletre, és azt használja, ha a távoli számítógép ismét megpróbál kapcsolatba lépni az alkalmazással.

Engedélyezés – Ezzel a beállítással engedélyezheti a bejövő kommunikációt.

Tiltás – Ezzel a beállítással letilthatja a bejövő kommunikációt.

További beállítások – Lehetővé teszi a szabály tulajdonságainak testreszabását.

Kapcsolatok megjelenítésének beállításai

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

Állomásnevek feloldása – Ha bejelöli ezt az opciót, a hálózatcímek minden lehetséges esetben tartományneves formátumban (DNS-névként) jelennek meg az IP-címes formátum helyett.

Csak a TCP-kapcsolatok megjelenítése – A listában csak a TCP-protokollkészletet használó kapcsolatok jelennek meg.

Figyelő kapcsolatok 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 – Az opció bejelölése esetén a rendszer azokat a kapcsolatokat is megjeleníti, amelyekben a távoli oldal a helyi rendszer (a localhost tartománynévvel azonosított állomás).

Frissítési sebesség – Az aktív kapcsolatok frissítési gyakorisága.

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

Biztonsági eszközök

A **Biztonsági eszközök** beállítás lehetővé teszi a következő modulok beállítását:

- **Netbank- és tranzakcióvédelem** – A védelem egy újabb rétege a böngésző számára, amellyel megóvhatja pénzügyi adatait az online tranzakciók során. Az **Összes böngésző védelme** funkció engedélyezésével elindíthatja az összes támogatott webböngészőt biztonságos módban. További információkért tekintse meg a Netbank- és tranzakcióvédelem című részt.

- **Szülői felügyelet** – A Szülői felügyelet modul megvédi gyermekeit azáltal, hogy blokkolja a nem megfelelő vagy káros tartalmakat az interneten.

- **Anti-Theft** – Az Lopásvédelem engedélyezésével megvédheti számítógépét az elvesztése vagy ellopása esetén.

Netbank- és tranzakcióvédelem

A Netbank- és tranzakcióvédelem a védelem egy újabb rétege, amellyel megóvhatja pénzügyi adatait az online tranzakciók során.

A legtöbb esetben a Netbank- és tranzakcióvédelem biztonságos böngésző az éppen használt böngészőben nyílik meg, miután felkeresett egy ismert netbankos webhelyet.

Válasszon a biztonságos böngésző alábbi konfigurációs beállításai közül:

- **Összes böngésző védelme** – Ha engedélyezve van, az összes támogatott webböngésző biztonságos módban indul. Ez lehetővé teszi az interneten való böngészést, az internetes banki szolgáltatások elérését, valamint az online vásárlásokat és tranzakciókat egyetlen biztonságos böngészőablakban, átirányítás nélkül.

- **Webhely-átirányítás** (alapértelmezett) – A védett webhelyek listájából származó webhelyek és a belső internetes banki listák átirányítása a biztonságos böngészőbe. Kiválaszthatja, hogy melyik böngésző (szabványos vagy biztonságos) legyen megnyitva.

- Mindkét előző beállítás le van tiltva – A biztonságos böngésző eléréséhez az ESET Internet Security szolgáltatásban kattintson az **Eszközök** > **Netbank- és tranzakcióvédelem** elemre, vagy kattintson a **Netbank- és tranzakcióvédelem** asztali ikonra. A Windows rendszerben alapértelmezettként beállított böngésző ekkor elindul biztonságos módban.

A biztonságos böngésző viselkedésének konfigurálásához tekintse meg a Netbank- és tranzakcióvédelem speciális beállítása című részt. Az Összes böngésző védelme funkció engedélyezéséhez az ESET Internet Security szolgáltatásban kattintson a **Beállítások** > **Biztonsági eszközök** elemre, majd engedélyezze az **Összes böngésző védelme** csúszkát.

A HTTPS használatával titkosított kommunikáció szükséges a védett böngészéshez. A következő böngészők támogatják a Netbank- és tranzakcióvédelmet:

- Internet Explorer 8.0.0.0+

- Microsoft Edge 83.0.0.0+

- Google Chrome 64.0.0.0+

- Firefox 24.0.0.0+

A Netbank- és tranzakcióvédelem funkcióról az ESET alábbi tudásbáziscikkében talál további részleteket angol és néhány további nyelven:

- Hogyan használhatom az ESET Netbank- és tranzakcióvédelem modult?

- Az ESET Netbank- és tranzakcióvédelem engedélyezése vagy letiltása egy adott webhelyen

- A Netbank- és tranzakcióvédelem szüneteltetése vagy letiltása az ESET Windows otthoni termékekben
- ESET Netbank- és tranzakcióvédelem – gyakori hibák
- ESET-szójegyzék | Netbank- és tranzakcióvédelem

Netbank- és tranzakcióvédelem speciális beállítása

Ezek a beállítások a **További beállítások** (F5) > **Web és e-mail** > **Netbank- és tranzakcióvédelem** lapon találhatók.

Általános

A Netbank- és tranzakcióvédelem engedélyezése – A Biztonságos internetes banki ügyintézés engedélyezését követően aktiválódik a védett webhelyek listája, és szerkesztheti a Védett webhelyek listát.

Böngészővédelem

Összes böngésző védelme – A funkció engedélyezésével elindíthatja az összes támogatott webböngészőt biztonságos módban.

Bővítmények telepítési módja – A legördülő menüben kiválaszthatja, hogy mely ESET által védett bővítmények telepíthetők: A bővítmények telepítési módjának módosítása nincs hatással a korábban telepített böngészőbővítményekre:

- **Alapvető kiterjesztések** – Csak az adott böngészőgyártó által kifejlesztett legfontosabb bővítmények.
- **Minden bővítmény** – Az adott böngésző által támogatott összes bővítmény.

Webhely-átirányítás

Védett webhelyek átirányításának engedélyezése – Ha engedélyezve van, a védett webhelyek listáján és a belső internetes banki szolgáltatások listáján lévő webhelyeket átirányítja a rendszer a biztonságos böngészőbe.

Védett webhelyek – Azon webhelyek listája, amelyeknél kiválaszthatja, hogy melyik böngészőt (normál vagy biztonságos) nyitja meg. A böngésző keretében egy ESET embléma jelenik meg, jelezve a biztonságos böngészés bekapcsolt állapotát. A lista szerkesztéséhez tekintse meg a Védett webhelyek című részt.

Védett böngésző

Fejlett memóravédelem engedélyezése – Ha engedélyezve van, a biztonságos böngésző memóriája védve lesz attól, hogy más folyamatok megvizsgálhassák.

Billentyűzetvédelem engedélyezése – Ha aktiválja a funkciót, akkor a billentyűzettel a biztonságos böngészőben megadott információk rejtve lesznek a többi alkalmazás elől. Ezzel növelhető a billentyűzetfigyelők elleni védelmi szint.

Böngésző zöld kerete — Ha ez le van tiltva, a böngészőn belüli informatív értesítés és a böngésző körüli zöld keret rövid időre megjelenik a böngésző indításakor, majd eltűnik.

Védett webhelyek

Az ESET Internet Security beépített listát tartalmaz azokról az előre definiált webhelyekről, amelyek hatására védett böngésző nyílik meg. A termék konfigurációjában hozzáadhat egy webhelyet, vagy szerkesztheti a webhelyek listáját.

A **Védett webhelyek** lista a **További beállítások** (F5) > **Web és e-mail** > **Netbank- és tranzakcióvédelem** > **Általános** > **Védett webhelyek** > **Szerkesztés** útvonalon tekinthető meg és szerkeszthető. Az ablak a következőkből áll:

Oszlopok

Webhely – A védett webhely.

Védett böngésző – A védett böngészés közben a böngésző szegélyén egy ESET embléma jelenik meg.

Rákérdezés – Ha engedélyezve van, a böngészési lehetőségeket tartalmazó párbeszédpanel jelenik meg, amikor egy védett weboldalt látogat meg. Az ESET Internet Security megjegyezheti a választott műveletet, vagy manuálisan is kiválaszthatja, hogy miként szeretné folytatni.

Normál böngésző – Válassza ezt a lehetőséget, ha további védelem nélkül folytatja a banki tranzakciót.

Vezérlőelemek

Hozzáadás – Ezt a gombot használva adhat hozzá webhelyet az ismert webhelyek listájához.

Szerkesztés – Ez a gomb a kijelölt bejegyzések szerkesztését teszi lehetővé.

Törlés – Ezzel a gombbal a kijelölt bejegyzéseket távolíthatja el.

Importálás/Exportálás – Lehetővé teszi a védett webhelyek listájának exportálását és egy új eszközre való importálását.

Böngészőn belüli értesítés

A védett böngésző a böngészőn belüli értesítések és a böngészőkeret színe révén tájékoztatja az aktuális állapotáról.

A böngészőn belüli értesítések a jobb oldali lapon jelennek meg.



A böngészőn belüli értesítés kibontásához kattintson az ESET ikonra . Az értesítés minimalizálásához kattintson az értesítési szövegre. Az értesítés törléséhez kattintson a bezárásra szolgáló ikonra .

Böngészőn belüli értesítések

Értesítés típusa	Állapot
Tájékoztató értesítés és zöld böngészőkeret	A maximális védelem biztosított, és a böngészőn belüli értesítés alapértelmezés szerint minimális méretű. Bontsa ki a böngészőn belüli értesítést a konfigurációs beállítások megjelenítéséhez: • **A böngésző zöld keretének elrejtése** – A jelölőnégyzet bejelölésével elrejtheti a böngésző körüli zöld keretet, amikor törli az értesítést. A Netbank- és tranzakcióvédelem speciális beállítása képernyőn véglegesen letilthatja a böngészőn belüli informatív értesítést és a böngésző körüli zöld keretet. • **Beállítások** – Megnyitja a Biztonsági eszközök beállítást.
Figyelmeztetés és narancssárga böngészőkeret	A védett böngésző a figyelmét kéri egy nem kritikus problémához. A problémával vagy megoldással kapcsolatos további információkért kövesse a böngészőn belüli értesítés utasításait.
Biztonsági riasztás és piros böngészőkeret	A böngészőt nem védi az ESET netbank- és tranzakcióvédelem. Indítsa újra a böngészőt, hogy a védelem aktív legyen. A böngészőbe betöltött fájlokkal való ütközés elhárításához vegye fel a kapcsolatot az ESET műszaki terméktámogatással a Tudásbáziscikkünk utasításainak követésével.

Szülői felügyelet

A Szülői felügyelet modulban adhatja meg a szülői felügyeletre vonatkozó beállításokat, amelyek automatizált eszközökkel 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 weboldalak letiltását. Ezenkívül a szülők több mint 40 előre definiált webhely-kategória és több mint 140 alkategória elérését is megtilthatják.

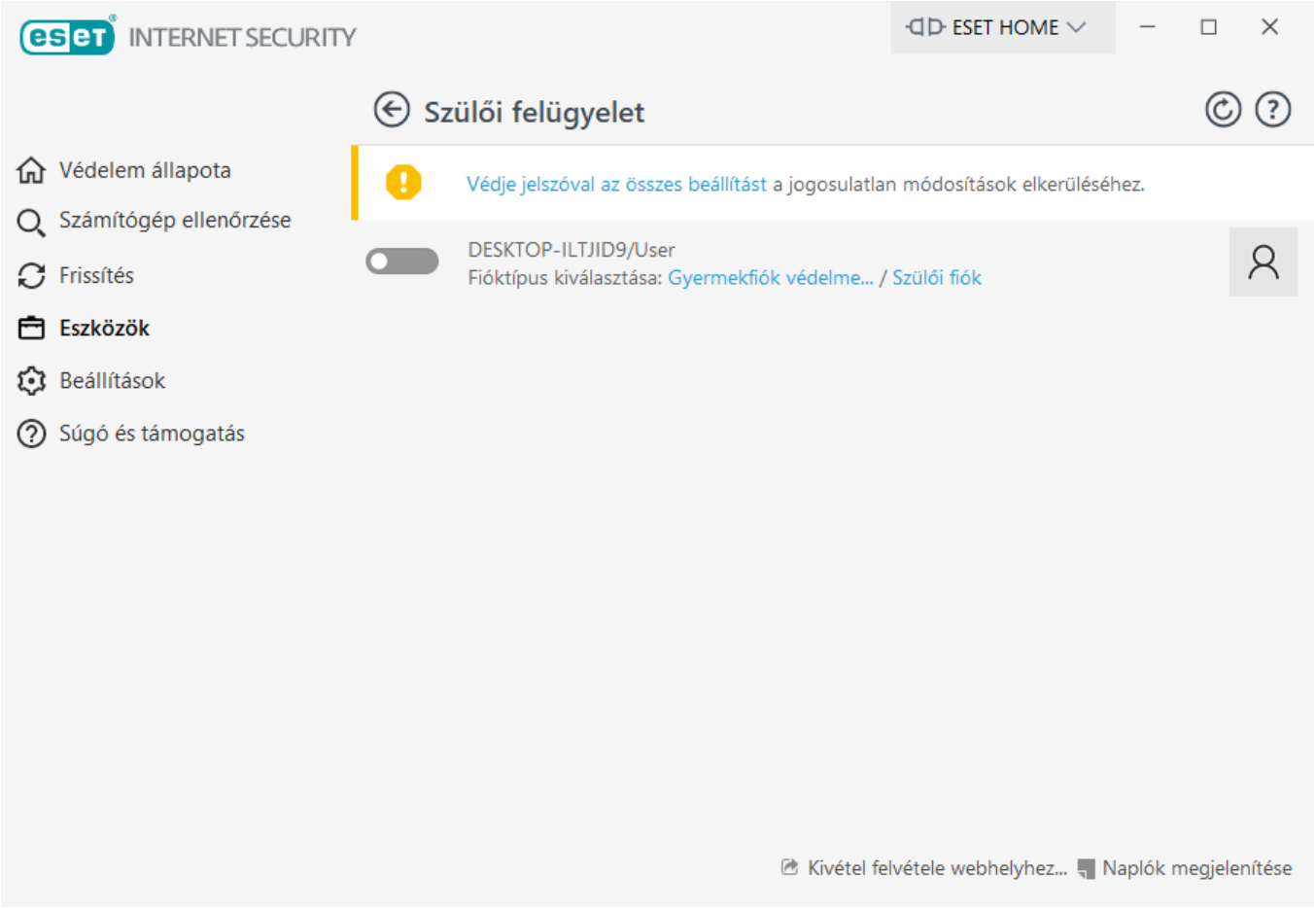
A szülői felügyelet az alábbi lépésekkel aktiválható egy adott felhasználói fiókhoz:

1. A szülői felügyelet alapértelmezés szerint le van tiltva az ESET Internet Security alkalmazásban. A szülői felügyelet két módon aktiválható:

   • Kattintson a  elemre a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** lehetőség mellett a program főablakában, és a szülői felügyelet állapotát módosítsa engedélyezettre.

   • Az F5 billentyűt lenyomva nyissa meg a **További beállítások** fastruktúrát, lépjen a **Web és e-mail** > **Szülői felügyelet** lapra, majd aktiválja **A szülői felügyelet engedélyezése** szöveg melletti csúszkát.

2. A program főablakában kattintson a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** elemre. Habár a **Szülői felügyelet** mellett az **Engedélyezve** felirat látható, a **Gyermekfiók védelme** vagy a **Szülői fiók** elemre kattintva konfigurálnia kell a szülői felügyeletet a kívánt fiókhoz. Ehhez kattintson a nyilat ábrázoló szimbólumra, majd a következő ablakban válassza ki a születésnapot a hozzáférés korlátozásához, és adja meg az adott kornak megfelelő, ajánlott weboldalakat. A program engedélyezi a szülői felügyeletet a megadott felhasználói fiókhoz. A fiók neve alatt található **Letiltott tartalmak és beállítások** hivatkozásra kattintva a Kategóriák lapon testre szabhatja az engedélyezni vagy letiltani kívánt kategóriákat. A kategóriákba nem sorolható egyéni weboldalak engedélyezéséhez vagy letiltásához kattintson a Kivételek fülre.



Ha az ESET Internet Security főablakában a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** lehetőségre kattint, láthatja, hogy a főablak az alábbi három részre van osztva:

Windows fiókok

Ha egy meglévő fiókhoz létrehozott egy szerepkört, az látható lesz itt. A fiókbeállítások Szülői felügyelet szakaszában kattintson a csúszkára, hogy zöld pipára váltson. Az aktív fiók neve található Letiltott tartalmak és beállítások hivatkozásra kattintva megtekintheti a fiókhoz engedélyezett weboldal-kategóriák listáját, valamint a letiltott és engedélyezett weboldalakat.

Új fiók létrehozásához (például egy gyermek számára) Windows 7 és Windows Vista rendszer esetén kövesse az alábbi lépésenkénti utasításokat:
1.Nyissa meg a **Felhasználói fiókok** eszközt: kattintson az asztal bal alsó szélén található **Start** gombra, majd a **Vezérlőpult**, végül a **Felhasználói fiókok** elemre.
2.Kattintson a **Felhasználói fiók kezelése** hivatkozásra. Ha a rendszer kéri, adja meg a rendszergazdai jelszót vagy a megerősítését.
3.Kattintson az **Új fiók létrehozása** hivatkozásra.
4.Írja be a felhasználói fiók nevét, jelölje ki az egyik fióktípust, majd kattintson a **Fiók létrehozása** gombra.
5.Nyissa meg újra a Szülői felügyelet ablaktáblát: az ESET Internet Security főablakában kattintson a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** elemre, majd a nyilat ábrázoló szimbólumra.

Az ablak alsó részén található elemek

Kivétel felvétele webhelyhez – Az adott webhely engedélyezhető vagy letiltható igény szerint külön az egyes szülői fiókokhoz.

Naplók megjelenítése – Itt tekintheti meg a szülői felügyeleti tevékenység részletes naplóját (letiltott oldalak, a letiltott oldalhoz tartozó fiók, kategória stb.). A **Szűrés** gombra kattintva a kiválasztott szempontok szerint szűrheti a naplót.

Szülői felügyelet

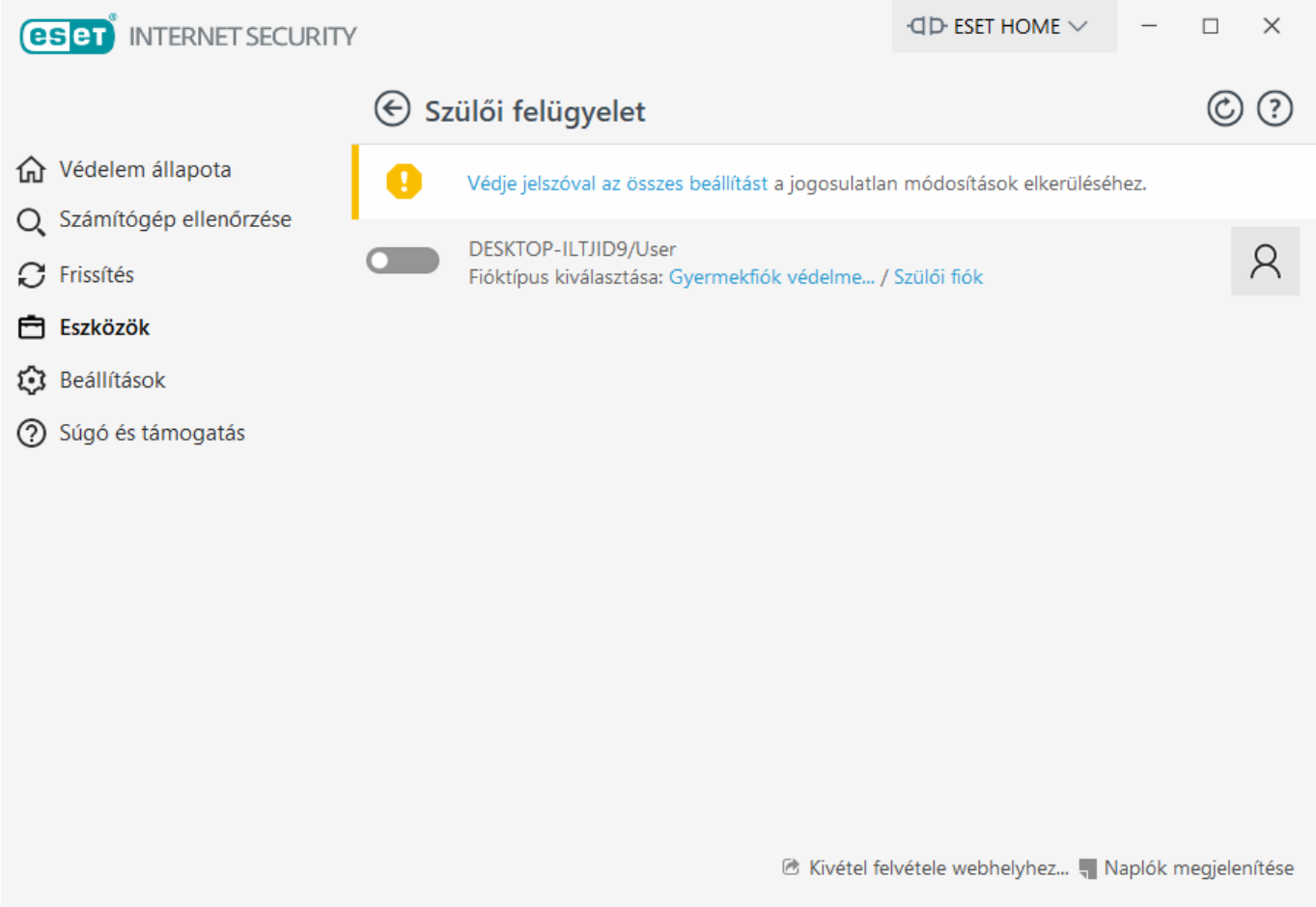
A Szülői felügyelet letiltása után megjelenik a **Szülői felügyelet letiltása** ablak. Itt megadhatja a védelem letiltásának időtartamát. A beállítás ezt követően **Felfüggesztve** vagy **Letiltva véglegesen** állapotra változik.

Fontos az ESET Internet Security beállításainak jelszavas védelme. A jelszót a Hozzáférési beállítások részben állíthatja be. Ha nincs beállítva jelszó, a következő figyelmeztetés jelenik meg: **Védje jelszóval az összes beállítást**. A Szülői felügyelet beállításcsoportban végzett módosítások csak a normál felhasználói fiókokra vonatkoznak. Mivel az adminisztrátorok (a Rendszergazdák csoport tagjai) minden korlátozást felülírhatnak, rájuk nincs hatással.

> A Szülői felügyelet megfelelő működéséhez a protokollszűrés, a HTTP-protokollszűrés és a tűzfal engedélyezése szükséges. Alapértelmezés szerint e funkciók mindegyike engedélyezve van.

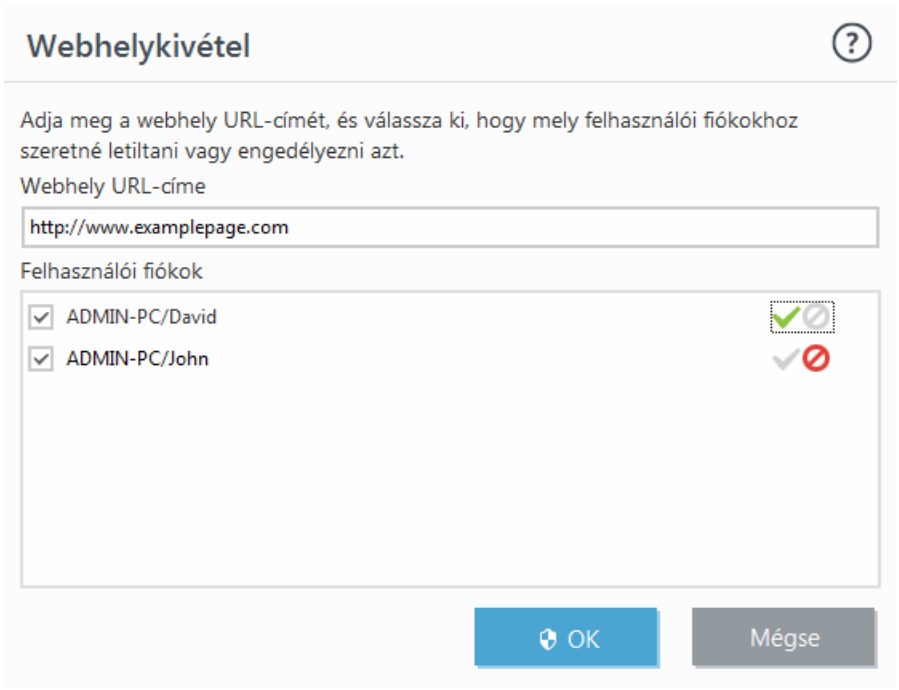
Webhelykivételek

Ha fel szeretne venni egy kivételt egy webhelyhez, válassza a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** lehetőséget, majd kattintson a **Kivétel felvétele webhelyhez** elemre.

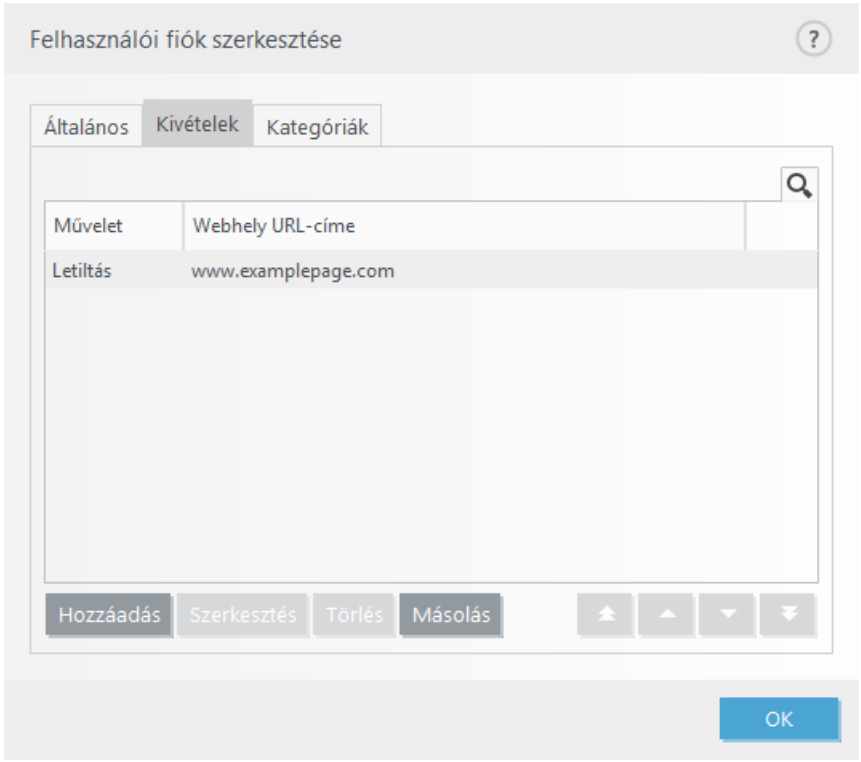


Írjon be egy URL-címet a **Webhely URL-címe** mezőbe, válassza ki a (engedélyezve) vagy a (letiltva)

lehetőséget az egyes felhasználói fiókokhoz, majd az **OK** gombra kattintva vegye fel a listára a kivételt.



Ha egy URL-címet törölni szeretne a listából, válassza a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** lehetőséget, majd kattintson a kívánt felhasználói fiók csoportjában a **Letiltott tartalmak és beállítások** elemre, majd a **Kivétel** fülre, a lapon jelölje ki a kivételt, és kattintson az **Eltávolítás** gombra.



Az URL-címlistában a speciális szimbólumok, nevezetesen a * (csillag) és a ? (kérdőjel) nem használhatók. A több felső szintű tartománnyal rendelkező weboldalcímeket például kézzel kell megadni (mintaoldal.com*examplepage.com*, *examplepage.sk*mintaoldal.hu stb.). Amikor felvesz egy tartományt a listára, a tartományban és az altartományokban található összes tartalom (például az al.mintaoldal.com*sub.examplepage.com*) letiltott vagy engedélyezett lesz a kiválasztott URL-alapú művelet alapján.

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

Felhasználói fiókok

Ezek a beállítások a **További beállítások** (F5) > **Web és e-mail** > **Szülői felügyelet** > **Felhasználói fiókok** > **Szerkesztés** lapon találhatók.

Ebben a szakaszban megtudhatja, hogy miként társíthatja a szülői felügyelet által használt Windows-fiókokat, hogy korlátozza bizonyos felhasználók hozzáférését a nem megfelelő vagy káros tartalmakhoz az interneten.

Oszlopok

Windows-fiók – A felhasználó neve.

Engedélyezve – Ha be van kapcsolva, a szülői felügyelet aktív az adott felhasználói fiókhoz.

Tartomány – A tartomány neve, amelyhez a felhasználó tartozik.

Születésnap – A fiókot használó felhasználó kora.

Vezérlőelemek

Hozzáadás – Megjeleníti A felhasználói fiókok használata párbeszédpanelt.

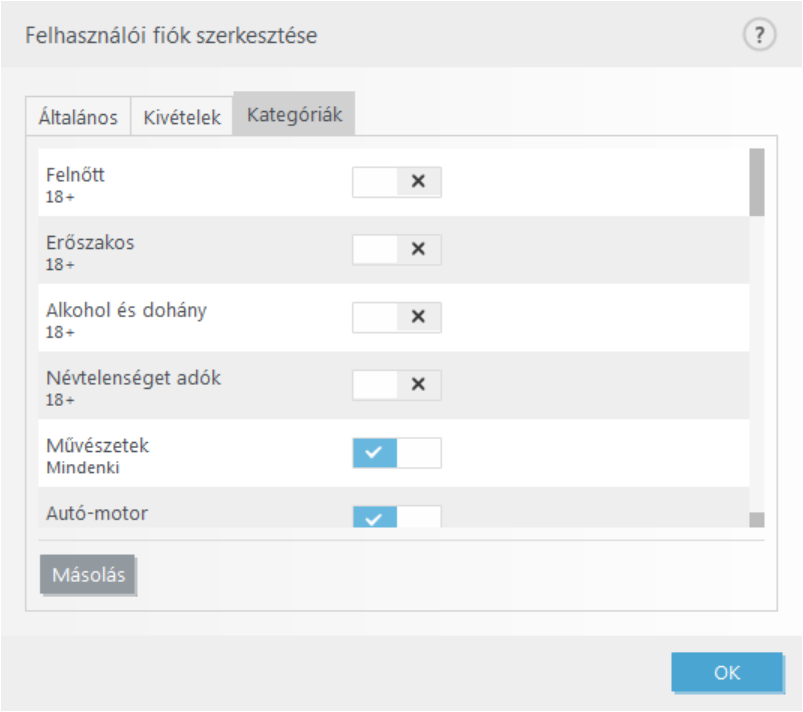
Szerkesztés – Erre kattintva szerkesztheti a kiválasztott fiókokat.

Törlés – Erre kattintva törölheti a kijelölt fiókot.

Frissítés – Ha hozzáadott egy felhasználói fiókot, az ESET Internet Security az ablak újbóli megnyitása nélkül frissítheti a felhasználói fiókok listáját.

Kategóriák

Az egyes kategóriák mellett látható **Engedélyezve** jelölőnégyzet bejelölésével engedélyezheti az adott kategóriát. Ha üresen hagyja a jelölőnégyzetet, a kategória nem lesz engedélyezve a fiókhoz.



Az alábbiakban a felhasználók által kevésbé ismert kategóriákra (csoportokra) talál példákat:

- **Egyéb** – Általában magán (helyi) IP-címek, például az intranet, 127.0.0.0/8, 192.168.0.0/16 stb. Ha 403-as vagy 404-es hibakódot kap, a webhely megegyezik ezzel a kategóriával is.
- **Nem feloldott** – Ebbe a kategóriába tartoznak azok a weboldalak, amelyek még nincsenek feloldva, mert a Szülői felügyelet adatbázismotorjához való csatlakozásakor hiba történt.
- **Nincs besorolva** – A Szülői felügyelet adatbázisában még nem szereplő ismeretlen weboldalak.
- **Dinamikus** – Weboldalak, amelyek más webhelyeken lévő oldalakra irányítják át a felhasználót.

A felhasználói fiókok használata

Az ablaknak három lapja van:

Általános

Kattintson az **Engedélyezve** szó melletti csúszkára az alább kiválasztott Windows-fiók szülői felügyeletének bekapcsolásához.

Először a **Kijelölés** gomb segítségével válasszon Windows-fiókot a számítógépről. A Szülői felügyelet beállításcsoportban végzett módosítások csak a normál Windows-fiókokra vonatkoznak. A rendszergazdai fiókok felülbírálhatják a korlátozásokat.

Amennyiben a fiókot egy szülő használja, válassza a **Szülői fiók** lehetőséget.

Adja meg a fiók tulajdonosának születési idejét a **Gyermek születésnapja** mezőben a hozzáférési szint megállapításához és az életkornak megfelelő weboldalakat engedélyező hozzáférési szabályok megadásához.

Naplózás részletessége

Az ESET Internet Security a fontos eseményeket egy naplófájlba menti, amely közvetlenül a fő menüből megtekinthető. Kattintson az **Eszközök** > **További eszközök** > **Naplófájlok** hivatkozásra, majd a **Napló** legördülő menüben válassza ki az **Szülői felügyelet** menüpontot.

- **Diagnosztikai** – A program pontos beállításához szükséges információk naplózása.
- **Tájékoztatás** – Tájékoztató jellegű üzenetek rögzítése, ideértve az engedélyezett és tiltott kivételekről szóló üzeneteket és a fent említett bejegyzéseket.
- **Figyelmeztetés** – Kritikus figyelmeztetések és figyelmeztető üzenetek rögzítése.
- **Nincs** – Nem rögzít naplókat.

Kivételek

Kivétel létrehozásával engedélyezheti vagy megtagadhatja a felhasználó a kivételek listáján nem szereplő webhelyekhez való hozzáférését. Ez akkor hasznos, ha az adott webhelyekhez való hozzáférés szabályozását részesíti előnyben a kategóriák használata helyett. Lehetősége van adott fiókhoz készített kivételek másolására más fiókokhoz. Ez olyankor jelent segítséget, ha hasonló korú gyermekek számára azonos szabályokat szeretne létrehozni.

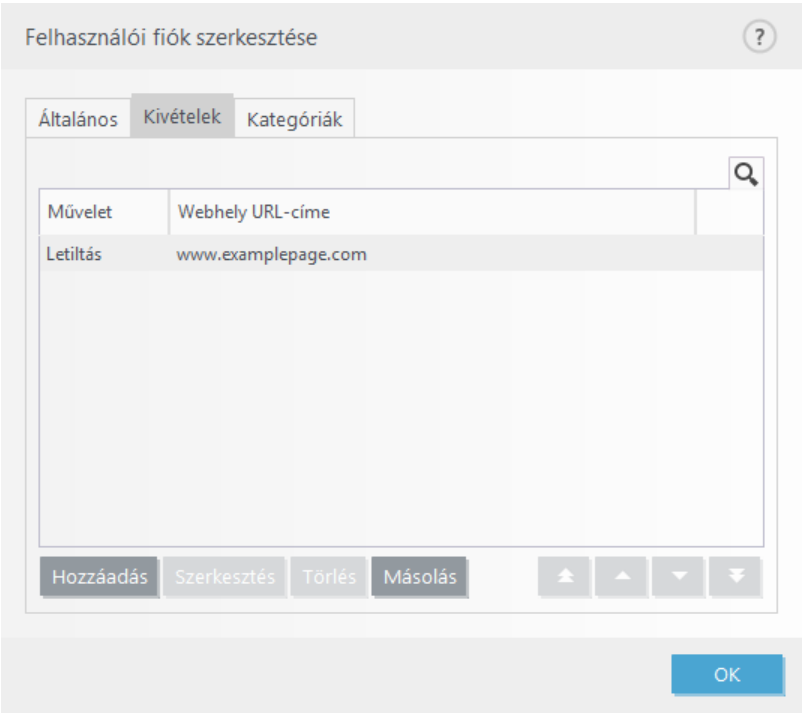
A **Hozzáadás** gombra kattintva újabb kivételt készíthet. Adja meg a **műveletet** (például **Letiltás**) a legördülő listában, írja be a **webhely URL-címét,** amelyre a kivétel vonatkozik majd kattintson az **OK** gombra. A kivétel bekerül a meglévő kivételek listájába, ahol látható az állapota.

Hozzáadás – Új kivétel létrehozása.

Szerkesztés – Itt szerkesztheti a kiválasztott kivétel **Webhely URL-címe** vagy **Művelet** paramétereit.

Törlés – Eltávolítható a kiválasztott kivétel.

Másolás – Válassza ki azt a felhasználót a legördülő listából, akinek a létrehozott kivételét át szeretné másolni.

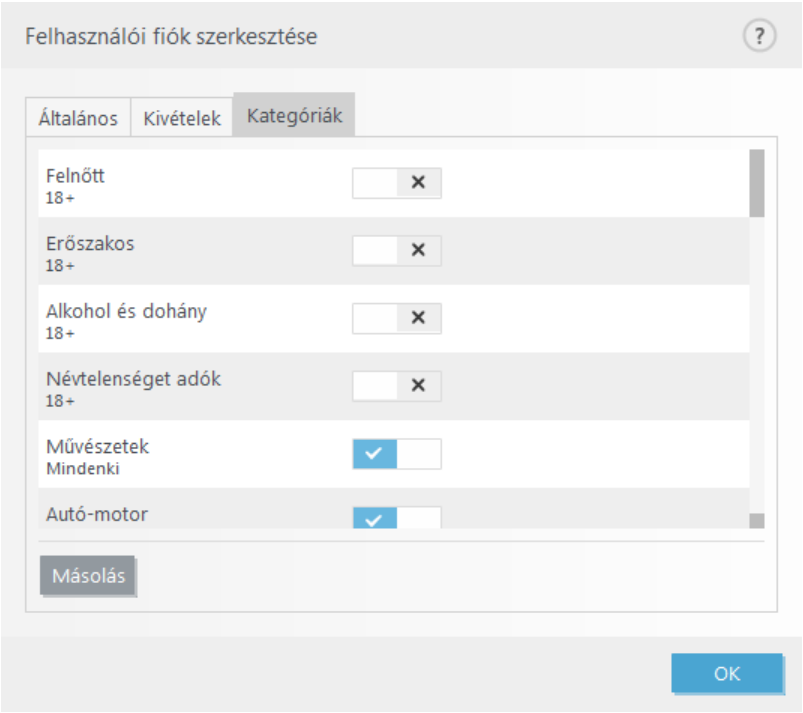


Az itt meghatározott kivételek elsőbbséget élveznek a kiválasztott fiók(ok) számára meghatározott kategóriákkal szemben. Ha például a **Hírek** kategória az adott fiók számára tiltott, de később egy engedélyezett híroldalt kivételként határoz meg, a fiók hozzáférhet a szóban forgó weboldalhoz. Az itt végzett módosításokat a Kivételek szakaszban láthatja.

Kategóriák

A **Kategóriák** lapon határozhatja meg azokat az általános webhelykategóriákat, amelyeket az egyes fiókok tekintetében engedélyezni vagy tiltani szeretne. Az egyes kategóriák mellett látható jelölőnégyzet bejelölésével engedélyezheti az adott kategóriát. Ha üresen hagyja a jelölőnégyzetet, a kategória nem lesz engedélyezve a fiókhoz.

Másolás – Lehetővé teszi a letiltott vagy engedélyezett kategóriák listájának másolását a meglévő, módosított fiókokból.



Kivétel másolása felhasználótól

Válassza ki azt a felhasználót a legördülő listából, akihez készített kivételt át szeretné másolni.

Kategóriák másolása fiókból

A jelölőnégyzet bejelölésekor a meglévő, módosított fiókokból másolhatja a letiltott vagy engedélyezett kategóriák listáját.

A szülői felügyelet engedélyezése

A **Szülői felügyelet engedélyezése** opció integrálja a Szülői felügyeletet az ESET Internet Security szolgáltatásba. Megjelenik a Szülői felügyelet rész a főablak **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** szakaszában.

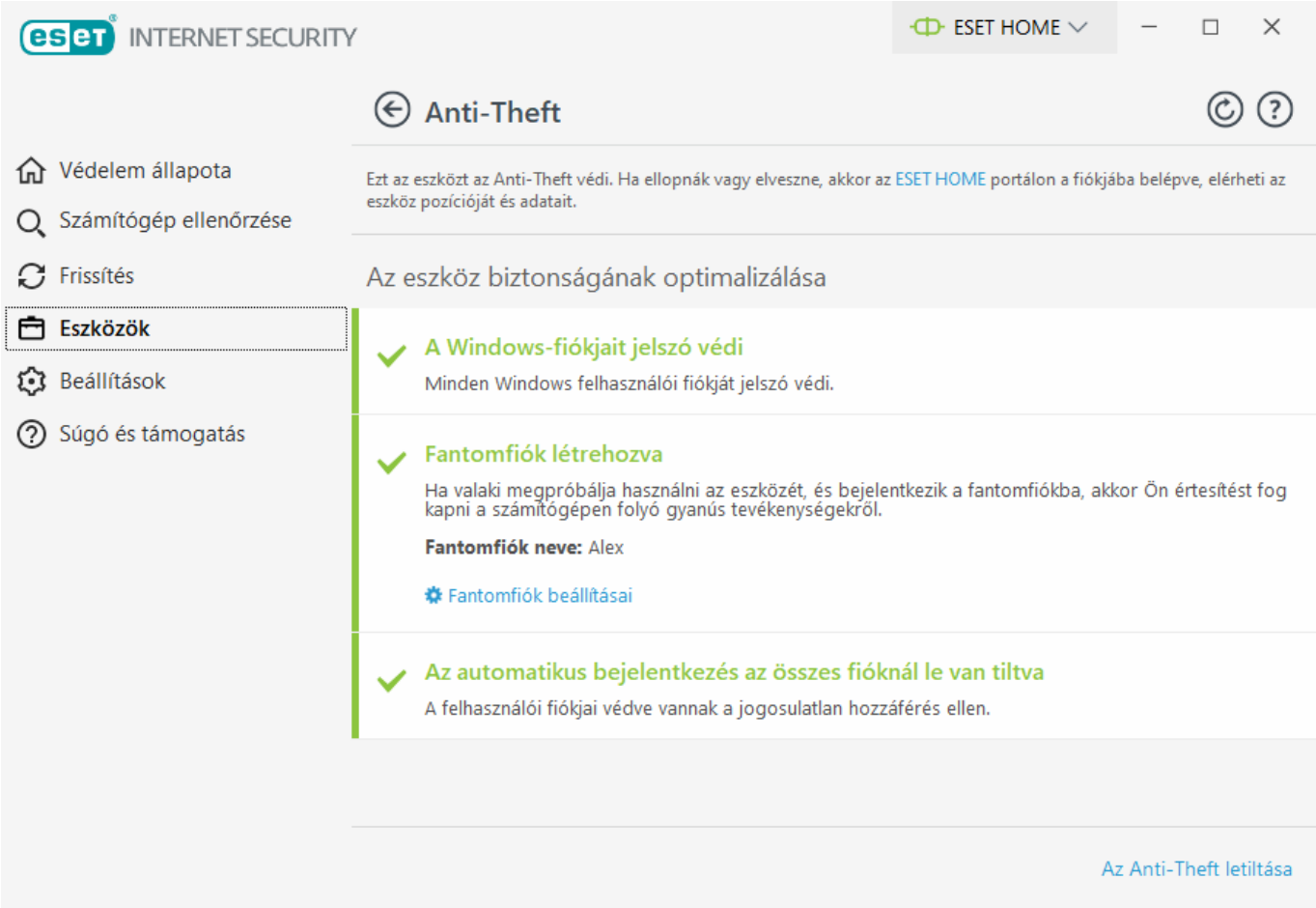
Lopásvédelem

Otthonunktól a munkahelyre vagy más nyilvános helyre történő mindennapos utazásaink során személyes eszközeink folyamatosan ki vannak téve a kockázatnak, hogy elveszítjük vagy ellopják őket. Az Lopásvédelem növeli a felhasználó biztonságát az eszköz elvesztése vagy ellopása esetén. Az Lopásvédelem lehetővé teszi az eszközhasználat figyelését és az eltűnt eszköz nyomon követését az IP-cím alapján történő helymeghatározással a ESET HOME szolgáltatásban, ami elősegíti az eszköz visszaszerzését és a személyes adatok védelmét.

Az Lopásvédelem korszerű technológiák – például a földrajzi IP-cím keresése, a webkamerával történő képrögzítés, a felhasználói fiók védelme és a készülék figyelése – használatával segíti Önt és a rendvédelmi szerveket a számítógép vagy a készülék helyének meghatározásában annak elvesztése vagy ellopása esetén. A ESET HOME szolgáltatásban megtekintheti, hogy milyen tevékenység zajlik a számítógépén vagy az eszközén.

A ESET HOME Lopásvédelem funkciójáról a ESET HOME online súgójában olvashat bővebben.

Az Lopásvédelem engedélyezése után optimalizálhatja az eszköz biztonságát a fő programablak > **Eszközök** > **Lopásvédelem** lapon.



Optimalizálási lehetőségek

Nincs fantomfiók létrehozva

Fantomfiók létrehozásával nagyobb eséllyel találhat meg egy elveszett vagy ellopott eszközt. Ha az eszközt eltűntnek jelöli, az Lopásvédelem blokkolja az aktív felhasználói fiókokhoz való hozzáférést a bizalmas adatok védelme érdekében. Bárki, aki megpróbálja használni az eszközt, csak a fantomfiókot használhatja majd. A

fantomfiók a vendégfiók egy formája, amely korlátozott engedélyekkel rendelkezik. Alapértelmezett rendszerfiókként lesz használatban addig, amíg az eszközt megtaláltként nem jelöli – ez megakadályozza, hogy bárki bejelentkezzen más felhasználói fiókokba vagy hozzáférjen a felhasználói adatokhoz.

> Amikor valaki bejelentkezik a fantomfiókba, amikor a számítógép normál állapotban van, e-mailben értesítést kap a számítógépen végzett gyanús tevékenységekről. Miután megkapta az e-mail-értesítést, eldöntheti, hogy eltűntnek jelöli-e a számítógépet.

Fantomfiók létrehozásához kattintson a **Fantomfiók létrehozása** elemre, írja be a **fantomfiók nevét** a szövegmezőbe, majd kattintson a **Létrehozás** gombra.

Miután létrejött a fantomfiók, a **Fantomfiók beállításai** elemre kattintva átnevezheti vagy törölheti a fiókot.

Windows-fiókok jelszavas védelme

Felhasználói fiókját nem védi jelszó. Ezt az optimalizálási figyelmeztetést akkor kapja meg, ha legalább egy felhasználói fiók nincs védve jelszóval. Ha jelszót hoz létre minden felhasználó számára (kivéve a **fantomfiókot**) a számítógépen, azzal megoldja a problémát.

A felhasználói fiók jelszavának létrehozásához kattintson a **Windows-fiókok kezelése** elemre, módosítsa a jelszót, vagy kövesse az alábbi instrukciókat:

1. Nyomja meg a CTRL+Alt+Delete billentyűkombinációt a billentyűzetet.
2. Kattintson a **Jelszó módosítása** elemre.
3. Hagyja üresen a **Régi jelszó** mezőt.
4. Írja be a jelszót az **Új jelszó** és a **Jelszó megerősítése** mezőbe, majd nyomja meg az **Enter** billentyűt.

Automatikus bejelentkezés Windows-fiókok esetén

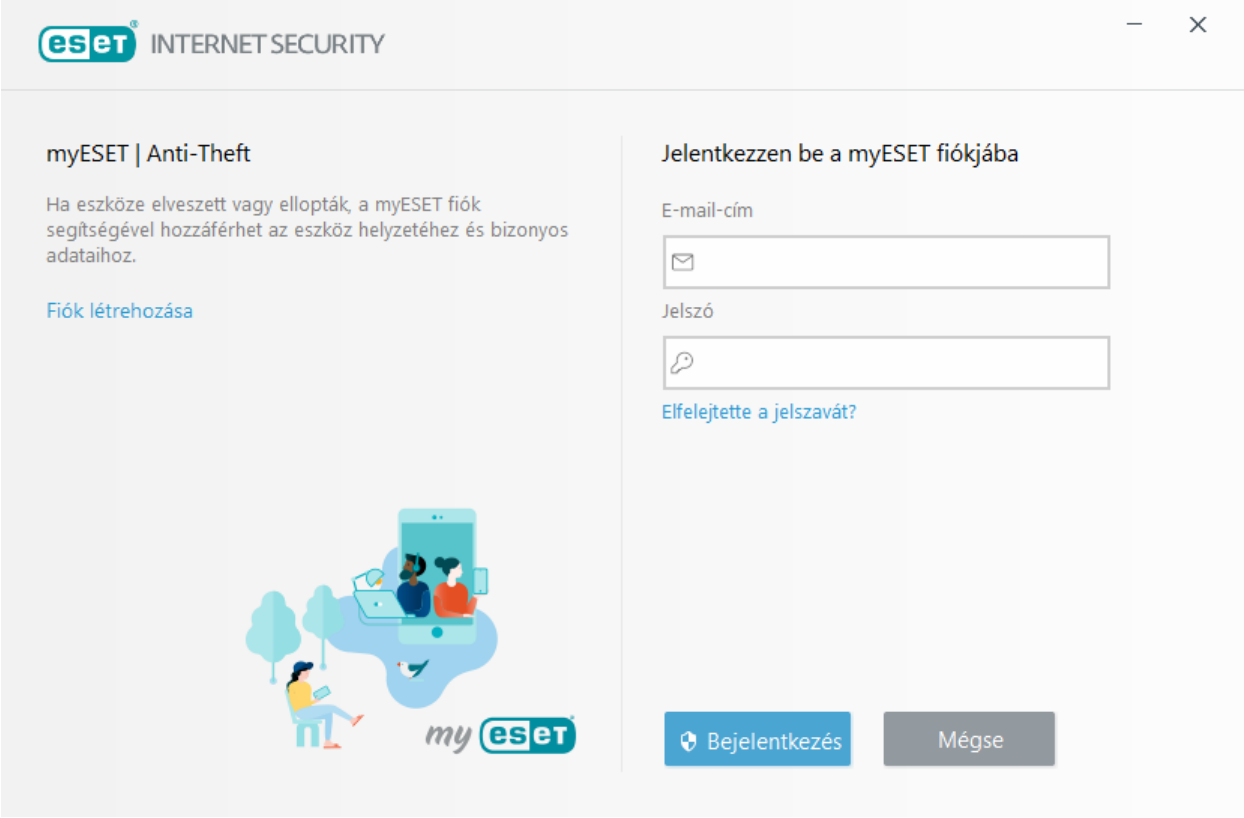
Felhasználói fiókjában engedélyezve van az automatikus bejelentkezés, ezért fiókja nem védett az illetéktelen hozzáférés ellen. Ezt az optimalizálási figyelmeztetést akkor kapja meg, ha legalább egy felhasználói fiókban engedélyezve van az automatikus bejelentkezés. Kattintson az **Automatikus bejelentkezés letiltása** elemre az optimalizálási probléma elhárításához.

Az automatikus bejelentkezés a fantomfióknál

Az automatikus bejelentkezés a **fantomfióknál** engedélyezve van. Ha az eszköz normál állapotban van, nem javasoljuk az automatikus bejelentkezés használatát, mert problémákat okozhat a valódi felhasználói fiókhoz való hozzáféréssel, vagy hamis riasztások jöhetnek létre a számítógép eltűnt állapotáról. Kattintson az **Automatikus bejelentkezés letiltása** elemre az optimalizálási probléma elhárításához.

Jelentkezzen be az ESET HOME-fiókjába.

Az Lopásvédelem engedélyezéséhez/letiltásához és eszköz helyének és adatainak ESET HOME szolgáltatásban való eléréséhez jelentkezzen be a ESET HOME-fiókjába.



A ESET HOME fiókjába való bejelentkezéshez számos módszer áll rendelkezésére:

- **A ESET HOME e-mail-cím és jelszó használata** – Írja be a ESET HOME-fiók létrehozásához használt **e-mail-címet** és **jelszót**, majd kattintson a **Bejelentkezés** gombra.

- **Google-fiók/AppleID**-fiók használata – Kattintson a **Folytatás a Google**-lal vagy a **Folytatás az Apple**-lel elemre, és jelentkezzen be a megfelelő fiókba. Sikeres bejelentkezés után a rendszer átirányítja a ESET HOME megerősítő weboldalra. A folytatáshoz váltson vissza az ESET-termékablakra. A Google-fiók/AppleID segítségével történő bejelentkezésről a ESET HOME online súgójában olvashat bővebben.

- **QR-kód beolvasása** – Kattintson a **QR-kód beolvasása** gombra a QR-kód megjelenítéséhez. Nyissa meg a ESET HOME mobilalkalmazást, és olvassa be a QR-kódot, vagy irányítsa a készülék kameráját a QR-kódra. További információkért tekintse meg a ESET HOME online súgóját.

Nem sikerült a bejelentkezés – gyakori hibák.

Ha nincs ESET HOME-fiókja, kattintson a **Fiók létrehozása** gombra a regisztrációhoz, vagy tekintse meg az instrukciókat a ESET HOME online súgóban.
Ha elfelejtette a jelszavát, kattintson az **Elfelejtettem a jelszavamat** szövegre, és kövesse a képernyőn látható lépéseket, vagy tekintse meg a ESET HOME online súgót.

Az Lopásvédelem nem támogatja a Microsoft Windows Home Server szoftvert.

Készüléknév beállítása

Az **Eszköz neve** mező jelzi a számítógép (eszköz) nevét, amely az összes ESET HOME szolgáltatásban azonosítóként látható lesz. Alapértelmezés szerint a számítógép számítógépneve lesz használatban. Írja be az eszköz nevét, vagy használja az alapértelmezettet, majd kattintson a **Folytatás** gombra.

Lopásvédelem engedélyezve/letiltva

Ez az ablak egy megerősítő üzenetet tartalmaz, amikor engedélyezi/letiltja az Lopásvédelem szolgáltatást:

- Engedélyezve – Az eszközét mostantól védi az Lopásvédelem, és a fiókja segítségével távolról is kezelheti a védelmét a ESET HOME portálon.
- Letiltva – Az Lopásvédelem le van tiltva ezen az eszközön, és az <%ESET_ANTTHEFT%> szolgáltatáshoz kapcsolódó összes adat törlődik a ESET HOME portálról.

Az új eszköz hozzáadása nem sikerült

Az Lopásvédelem aktiválásakor hiba történt.

A leggyakoribb forgatókönyvek a következők:

- Hiba történt a ESET HOME szolgáltatásba való bejelentkezéskor
- Nincs internetkapcsolat (vagy jelenleg nem működik az internet)

Ha nem tudja megoldani a problémát, forduljon az ESET műszaki terméktámogatásához.

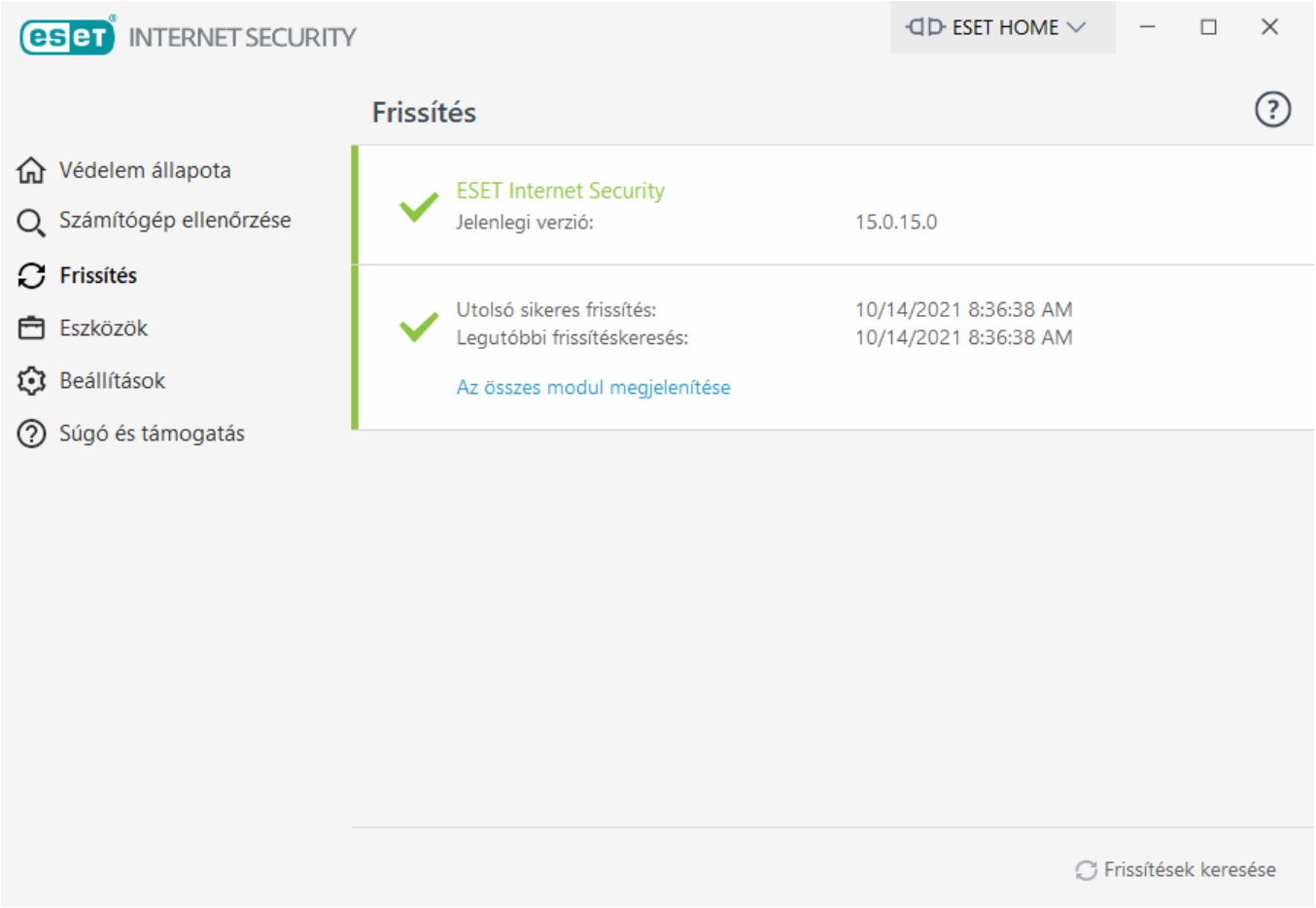
A program frissítése

Az ESET Internet Security rendszeres frissítésével biztosítható a leghatékonyabban a számítógép maximális védelme. A Frissítés modul biztosítja, hogy a programmodulok és a rendszerösszetevők mindig naprakészek legyenek.

A program főablakának **Frissítés** elemére kattintva megjelenítheti az aktuális frissítési állapotot, beleértve az utolsó sikeres frissítés dátumát és időpontját, valamint azt, hogy szükség van-e frissítésre.

Az automatikus frissítések mellett manuális frissítést indíthat a **Frissítések keresése** gombra kattintva. A kártevő kódok elleni maradéktalan védelem fontos része a programmodulok és a programösszetevők rendszeres frissítése. Ezért érdemes figyelmet fordítania a termékmodulok beállítására és működtetésére. A terméket a licenckulccsal kell aktiválni, hogy elérhetők legyenek a frissítések. Ha a telepítés során nem adta meg a licencadatokat, meg kell adnia a licenckulcsot a termék aktiválásához, hogy frissítéskor hozzáférjen az ESET frissítési szervereihez.

A licenckulcsot az ESET küldte el e-mailben az ESET Internet Security megvásárlása után.



Jelenlegi verzió – Megjeleníti a telepített aktuális szoftververzió számát.

Utolsó sikeres frissítés – Itt látható a legutóbbi sikeres frissítés dátuma. Ha nem látható friss dátum, lehetséges, hogy a termékmodulok elavultak.

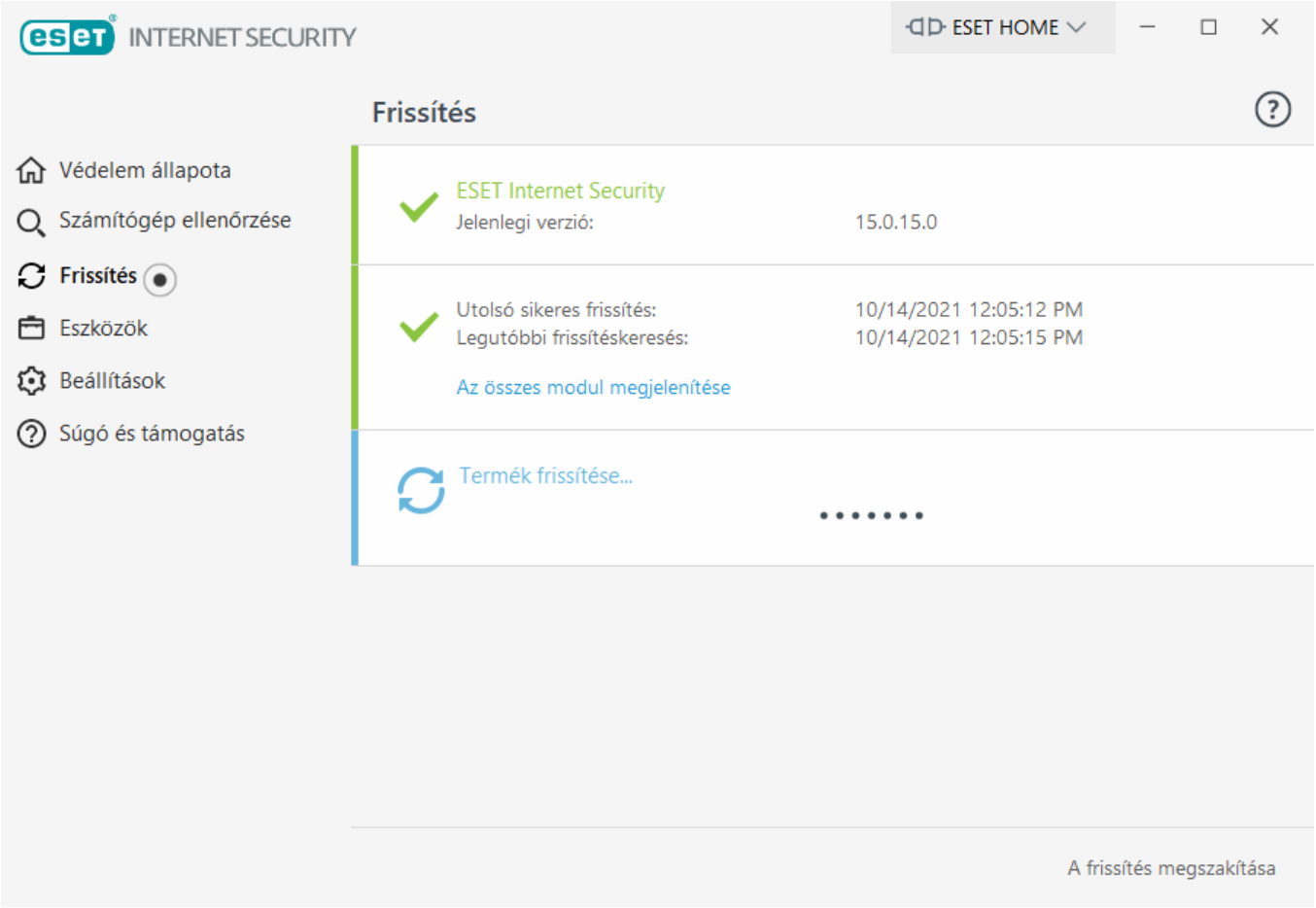
Utolsó sikeres frissítéskeresés – Itt látható a legutóbbi sikeres frissítéskeresés dátuma.

Az összes modul megjelenítése – Itt látható a telepített programmodulok listája.

A **Frissítések keresése** gombra kattintva beolvashatja az ESET Internet Security legújabb elérhető verzióját.

A frissítési folyamat

A **Frissítések keresése** gombra kattintást követően elindul a letöltés. Megjelenik a letöltési folyamatjelző sáv, illetve látható a letöltésből hátralévő idő. A frissítést **A frissítés megszakítása** gombra kattintva megszakíthatja.



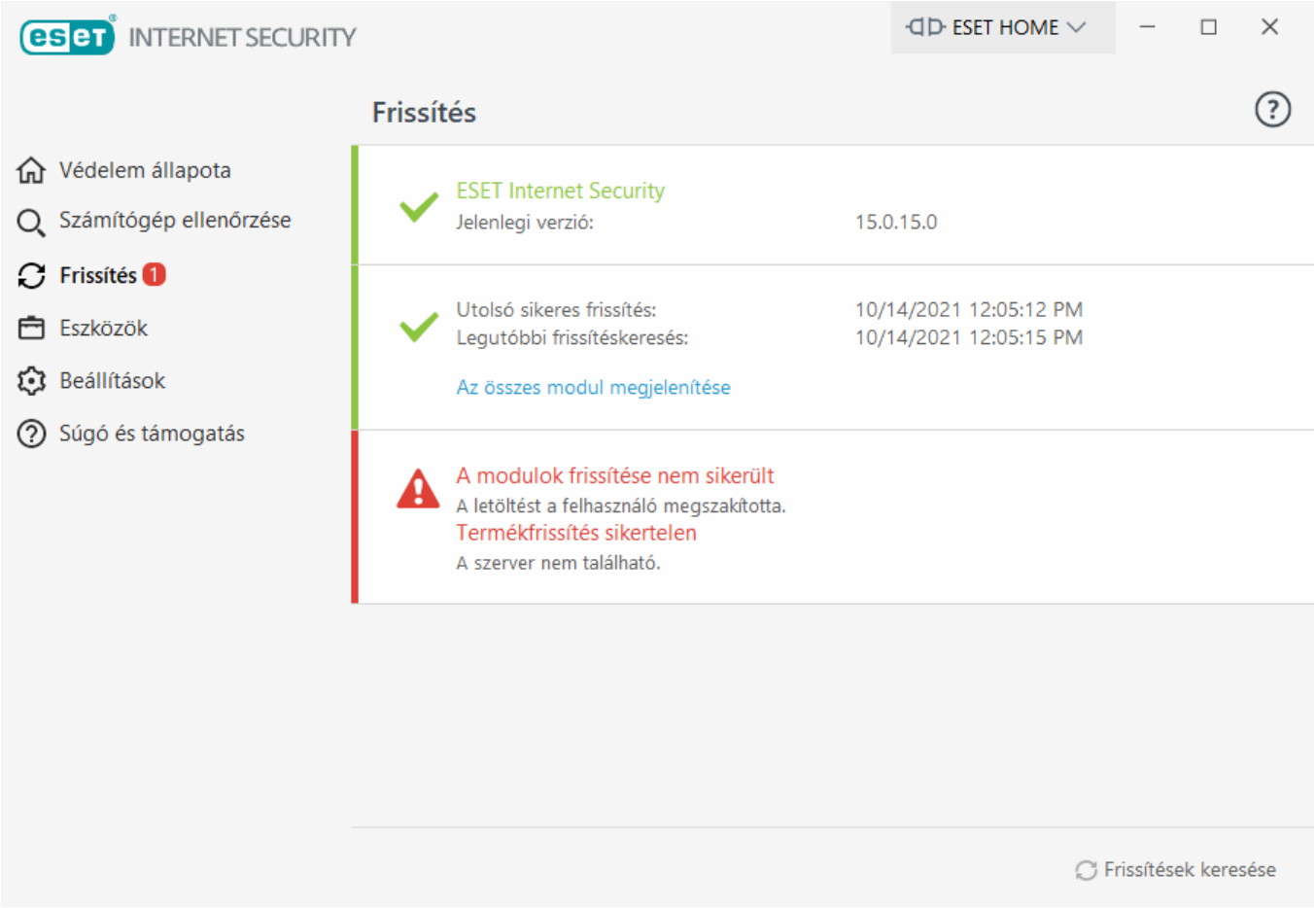
Normál körülmények között egy zöld pipa jelzi a **Frissítés** ablakban, hogy a program naprakész. Ha nem látható a zöld pipa, akkor a program elavult, és sokkal sérülékenyebb a fertőzésekkel szemben. Kérjük, minél hamarabb frissítse a programmodulokat.

Sikertelen frissítés

Ha sikertelen modulfrissítésről kap üzenetet, akkor azt a következők okozhatták:

1. **Érvénytelen licenc** – Az aktiváláshoz használt licenc érvénytelen vagy lejárt. A fő programablakban kattintson a **Súgó és támogatás** > **Licenc módosítása** elemre, és írjon be egy új licenckulcsot.

2. **A letöltést a felhasználó megszakította** – Ezt a nem megfelelő internetes kapcsolatbeállítások okozhatják. 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.



Azt javasoljuk, hogy indítsa újra a számítógépet, miután nem sikerült az ESET Internet Security frissítése egy újabb termékverzióra, hogy az összes programmodul megfelelően frissüljön. A rendszeres modulfrissítések után nem kell újraindítani a számítógépet.

További információk erről A „Modulok frissítése sikertelen” üzenet hibaelhárítása című fejezetben találhatók.

Frissítési beállítások

A frissítési beállítások az F5 billentyűvel megnyitható **További beállítások** fastruktúra **Frissítés** > **Általános** csoportjában érhetők el. Ebben a csoportban adhatja meg a frissítés forrásának beállításait, például a használatban lévő frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat.

Általános

Az aktuálisan használatban lévő frissítési profil (hacsak nincs megadva egy másik a **További beállítások** > **Tűzfal** > **Ismert hálózatok** lapon) az **Alapértelmezett frissítési profil kiválasztása** legördülő menüben látható.

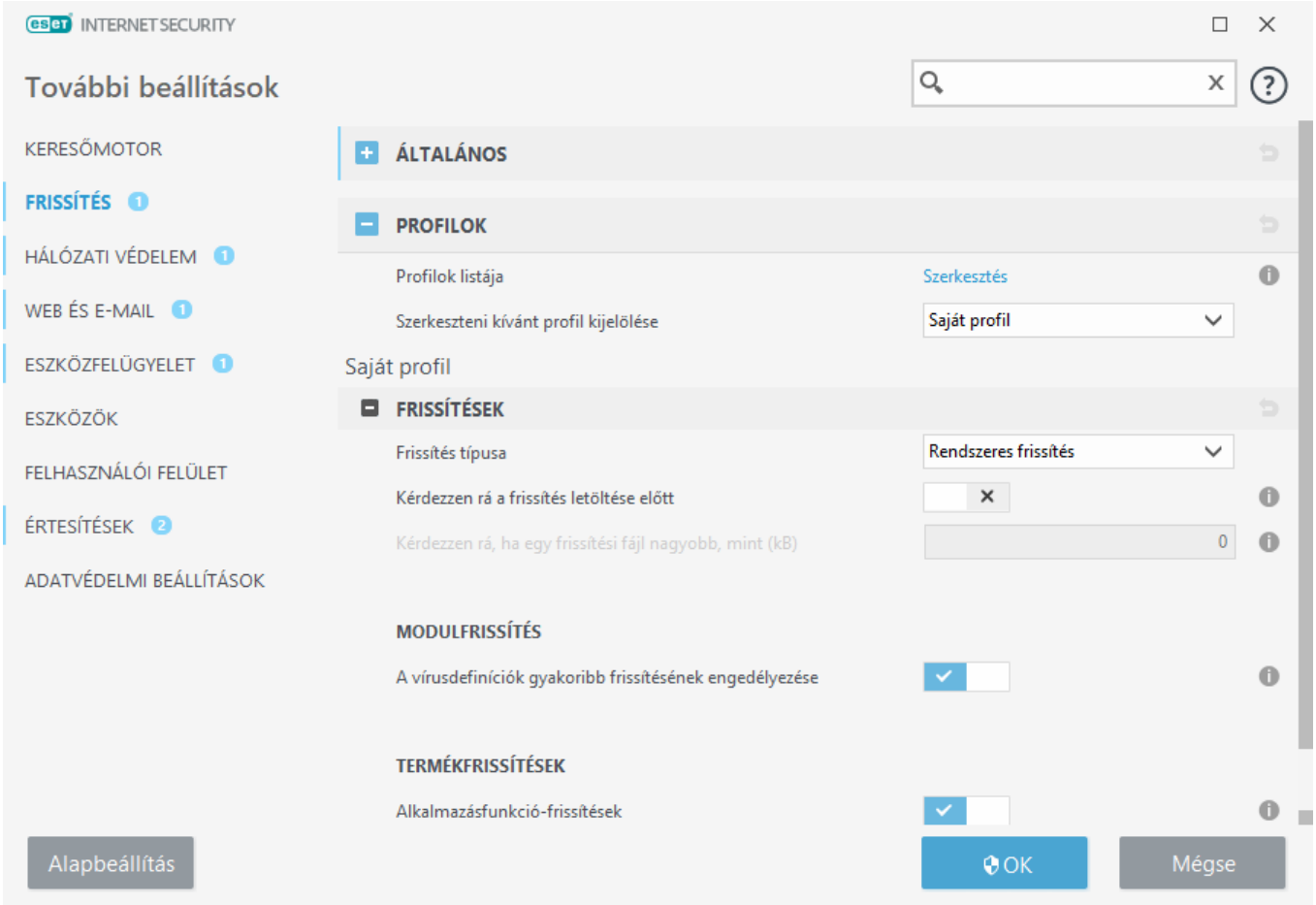
Ha új profilt szeretne hozzáadni, tekintse meg a Frissítési profilok című részt.

Automatikus profilváltás – Módosíthatja a profilt az adott hálózathoz.

Ha a keresőmotor vagy -modul frissítéseinek letöltése során problémát tapasztal, a **Kiürítés** gombra kattintva törölje az ideiglenes frissítési fájlokat/ürítse ki a gyorsítótárat.

Modul-visszaállítás

Ha a keresőmotor és/vagy a programmodulok egyik új frissítése feltehetően nem stabil, illetve sérült, visszaállhat az előző verzióra, és adott időszakra letilthatja a frissítéseket.



A program csak akkor tud frissíteni, ha minden frissítési paraméter pontosan be van állítva. Ha tűzfalat használ, engedélyezze az ESET-programnak az internettel való kommunikációt (azaz a HTTP-kommunikációt).

Profilok

Frissítési profilok többféle frissítési konfigurációhoz és feladathoz létrehozhatók. A frissítési profilok létrehozása különösen mobilt használók számára hasznos, akiknél az internetkapcsolat tulajdonságai gyakran változnak, és így létre kell hozniuk egy alternatív profilt.

A **Szerkeszteni kívánt profil kijelölése** legördülő listában az aktuálisan kiválasztott profil látható. Ez alapértelmezés szerint a **Saját profil** nevű profil. Új profil létrehozásához kattintson a **Szerkesztés** hivatkozásra a **Profilok listája** mellett, majd írja be a profil nevét a **Profil neve** mezőbe, és kattintson a **Hozzáadás** elemre.

Frissítések

A **Frissítés típusa** lista alapértelmezés szerinti **Rendszeres frissítés** beállítása biztosítja, hogy a program – a lehető legkisebb hálózati forgalom mellett – automatikusan letöltse a frissítési fájlokat az ESET szerveréről. A tesztelési mód (a **Tesztelési mód** választógomb) választásakor olyan frissítéseket használ, amelyek belső tesztelésen estek át, és hamarosan nyilvánosan is elérhetők lesznek. A tesztelési mód engedélyezése esetén hozzáférhet a legfrissebb felismerési módszerekhez és javításokhoz. A tesztelési mód veszélyeztetheti a rendszer stabilitását, ezért NEM SZABAD használni olyan szervereken és munkaállomásokon, ahol követelmény a maximális

rendelkezésre állás és stabilitás.

Kérdezzen rá a frissítés letöltése előtt – A program megjelenít egy értesítést, és megerősítheti, illetve elutasíthatja a frissítési fájlok letöltését.

Kérdezzen rá, ha egy frissítési fájl nagyobb, mint (kB) – A program megjelenít egy megerősítést kérő párbeszédpanelt, ha a frissítési fájl mérete nagyobb, mint a megadott érték. Ha a frissítési fájl 0 kB-ra van beállítva, a program mindig megjeleníti a megerősítést kérő párbeszédpanelt.

Sikeres frissítésről szóló értesítés letiltása – Ezzel az opcióval kikapcsolhatja 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.

Modulfrissítések

Vírusdefiníciók gyakrabban történő frissítésének engedélyezése – A program gyakrabban fogja frissíteni a vírusdefiníciókat. A funkció letiltása negatív hatással lehet az észlelési arányra.

Termékfrissítések

Alkalmazásfunkció-frissítések – Az ESET Internet Security új verzióinak automatikus telepítése.

Kapcsolati beállítások

Ha proxyszervert szeretne használni a frissítések letöltéséhez, tekintse meg a Kapcsolati beállítások című részt.

Frissítési fájlok visszaállítása

Ha a keresőmotor egyik frissítése vagy a programmodulok feltehetően nem stabilak, illetve sérültek, visszaállhat az előző verzióra, és átmenetileg letilthatja a frissítéseket. Másik lehetőségként engedélyezheti a korábban letiltott frissítéseket, ha bizonytalan időre elhalasztotta őket.

Az ESET Internet Security pillanatfelvételeket készít a keresőmotorról és a programmodulokról a visszaállítás funkcióhoz való használatra. A vírusdefiníciós adatbázis pillanatfelvételeinek létrehozásához hagyja engedélyezve a **Modulok pillanatképének létrehozása** funkciót. Ha a **Modulok pillanatképének létrehozása** funkció engedélyezve van, az első pillanatkép az első frissítés alkalmával jön létre. A következő 48 óra múlva jön létre. A **Helyben tárolt pillanatképek száma** mező meghatározza a keresőmotor pillanatképeinek tárolt számát.

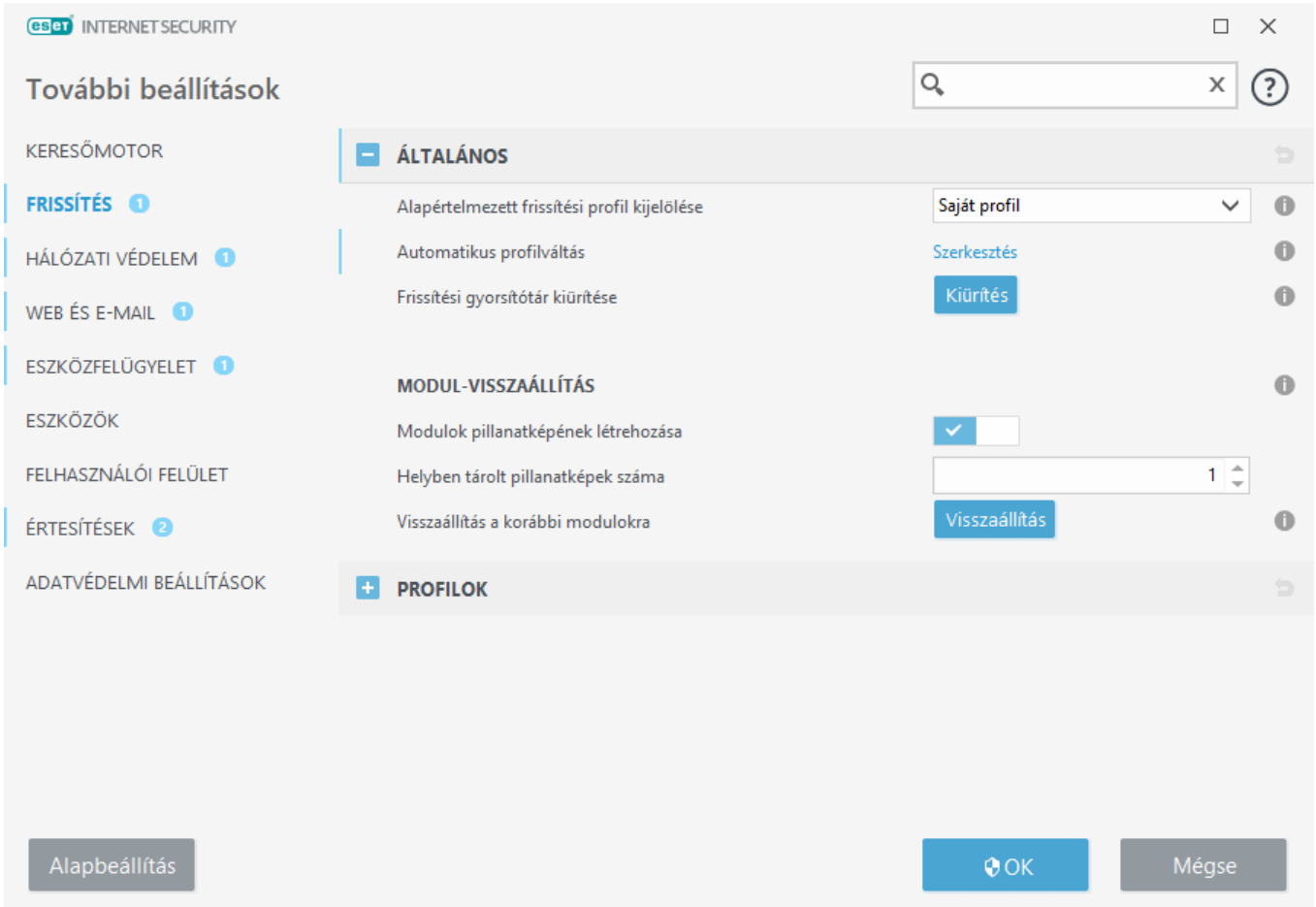
> Amikor elérte a pillanatképek maximális mennyiségét (például három), a legrégebbi pillanatképet 48 óránként új pillanatfelvétel váltja fel. Az ESET Internet Security visszaállítja a keresőmotor és a programmodulok frissítési verzióját a legrégebbi pillanatfelvételre.

Ha a **Visszaállítás** (**További beállítások** (F5) > **Frissítés** > **Alapbeállítások**) beállítást választja, az **Időtartam**legördülő listában jelöljön ki egy időtartamot, amely során a keresőmotor és a programmodulok frissítései szünetelnek.



A **Visszavonásig** beállítással határozatlan időre elhalaszthatja a szokásos frissítéseket, amíg kézzel vissza nem állítja a frissítési funkciót. Mivel biztonsági kockázatot jelent, az ESET nem javasolja ennek a beállításnak a használatát.

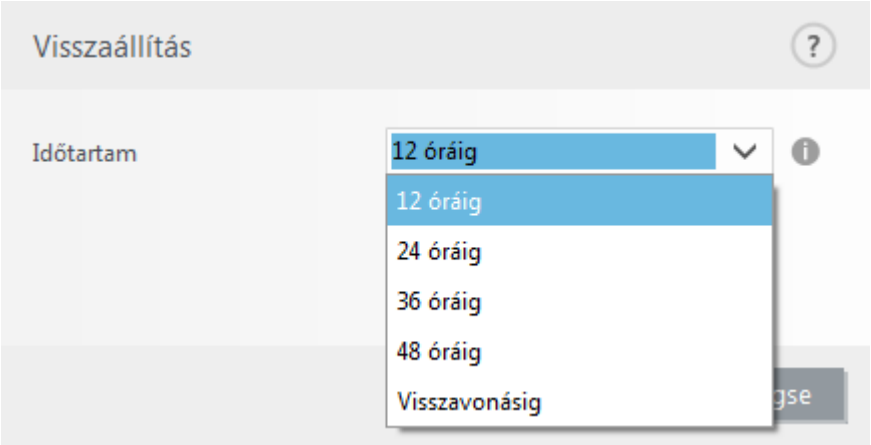
Ha végrehajt egy visszaállítást, a **Visszaállítás** gomb a **Frissítések engedélyezése** gombra vált. A **Frissítések felfüggesztése** legördülő listában kiválasztott időtartamra nem engedélyezettek a frissítések. A program a keresőmotor verzióját az elérhető legkorábbira minősíti vissza, és pillanatfelvételként tárolja a helyi számítógép fájlrendszerében.



Tételezzük fel, hogy a keresőmotor legújabb verziójának száma 22700. A 22698-as és a 22696-os verziót a keresőmotor pillanatképeként tárolja a rendszer. Vegye figyelembe, hogy a 22697-es nem érhető el. Ebben a példában leállították a számítógépet a 22697-es frissítés során, és egy újabb frissítés jelent meg a 22697-es letöltése előtt. Ha a **Helyben tárolt pillanatképek száma** mezőben a kettes szám van, és a **Visszaállítás** gombra kattintott, a keresőmotor (a programmodulokat is beleértve) a 22696-os számú verzióra áll vissza. Ez a folyamat kis időt igénybe vehet. A Frissítés képernyőn ellenőrizze, hogy a program visszaminősítette-e a keresőmotor verzióját.

Visszaállítási időintervallum

Ha a **Visszaállítás** (**További beállítások** (F5) > **Frissítés** > **Alapbeállítások**) beállítást választja, az **Időtartam**legördülő listában jelöljön ki egy időtartamot, amely során a keresőmotor és a programmodulok frissítései szünetelnek.



A **Visszavonásig** beállítással határozatlan időre elhalaszthatja a szokásos frissítéseket, amíg kézzel vissza nem állítja a frissítési funkciót. Mivel biztonsági kockázatot jelent, az ESET nem javasolja ennek a beállításnak a használatát.

Termékfrissítések

A **Termékfrissítések** szakasz lehetővé teszi az elérhetővé vált új funkciófrissítések automatikus telepítését.

Az alkalmazás funkciófrissítései révén új funkciók válnak elérhetővé, vagy módosulnak a korábbi verziókban is rendelkezésre álló funkciók. Automatikusan, felhasználói beavatkozás nélkül is végrehajtható, de a frissítésekről értesítés is kérhető. Miután telepítette az alkalmazás funkciófrissítését, szükség lehet a számítógép újraindítására.

Alkalmazásfunkció-frissítések – Ha ez engedélyezve van, az alkalmazásfunkció-frissítések automatikusan végbemennek.

Kapcsolati beállítások

Az egyes frissítési profilokhoz tartozó proxyszerver-beállítások megnyitásához az F5 billentyűt lenyomva nyissa meg a **További beállítások** párbeszédpanelt, kattintson a **Frissítés** ágra, majd a **Profilok** > **Frissítések** > **Kapcsolódási beállítások** elemre. Kattintson a **Proxy mód** legördülő menüre, és jelölje be az alábbi három választógomb egyikét:

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

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

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

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

- Az ESET Internet Security frissítéséhez egy, az **Eszközök** > **Proxyszerver** beállításhoz megadottól eltérő proxyszerver van használatban. Ebben a konfigurációban az új proxyval kapcsolatos információkat a **Proxyszerver** mezőbe a proxyszerver címét, a **Port** mezőbe a kommunikációs port számát (ez alapértelmezés szerint a 3128-as) beírva, illetve szükség esetén a **Felhasználónév** és a **Jelszó** mezőt kitöltve adhatja meg.

- A proxyszerver beállításai a globális beállítások között nem szerepelnek, az ESET Internet 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. Mert a program csak helyes beállításokkal tud csatlakozni a frissítési szerverekhez.

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

Közvetlen kapcsolat használata, ha nem érhető el proxy – Ha nem érhető el, a proxy ki lesz hagyva a frissítés során.

> Az ebben a szakaszban szereplő **Felhasználónév** és **Jelszó** mező a proxyszerverre vonatkozik. Ezeket a mezőket csak akkor töltse ki, ha a proxyszerver eléréséhez felhasználónév és jelszó szükséges. Ezeket a mezőket csak akkor kell kitölteni, ha az internet proxyszerveren keresztül történő eléréséhez felhasználónév és jelszó szükséges.

Frissítési feladatok létrehozása

A frissítések keresése és telepítése kézzel is elindítható, ha a főmenüben a **Frissítés** parancsot választja, majd a megjelenő elsődleges ablakban a **Frissítések keresése** gombra kattint.

A frissítések ütemezett feladatokként is futtathatók. Ütemezett feladat beállításához kattintson az **Eszközök** > **További eszközök** > **Feladatütemező** elemre. Az ESET Internet 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.

Párbeszédablak – Újraindítás szükséges

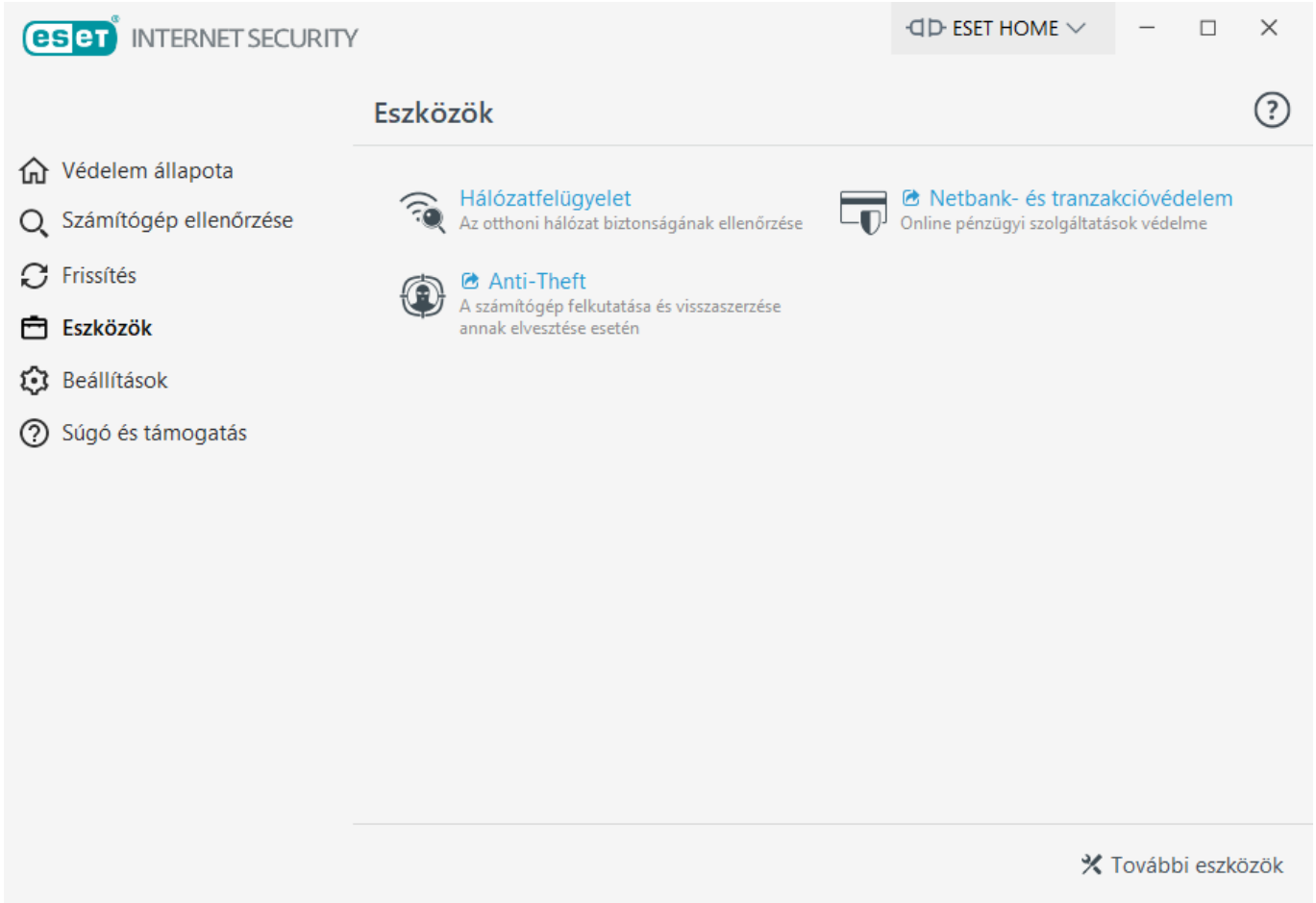
A számítógép újraindítására van szükség az ESET Internet Security új verzióra való frissítése után. Az ESET Internet Security új verziói továbbfejlesztett funkciókat tartalmaznak, és a programmodulok automatikus frissítésével nem megszüntethető problémákat orvosolnak.

Az ESET Internet Security új verziója automatikusan telepíthető a programfrissítési beállítások alapján, vagy manuálisan az előzőhöz képest egy újabb verzió letöltésével és telepítésével.

Kattintson az **Újraindítás most** gombra a számítógép újraindításához. Ha később szeretné újraindítani a számítógépet, kattintson az **Emlékeztetés később** szövegre. Később manuálisan újraindíthatja a számítógépet a fő programablak **Kezdőlap** szakaszából.

Eszközök

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



Hálózatfelügyelet – Csökkentheti a biztonsági problémák kockázatát, miközben egy hálózathoz csatlakozik. További információkért tekintse meg a Hálózatfelügyelet című részt.

**Netbank- és tranzakcióvédelem** – Az ESET Internet Security fokozott biztonságot nyújt az online banki tranzakciók vagy a fizetésre szolgáló webhelyek használata során a hitelkártyaszámok és más bizalmas adatok számára. Elindul egy biztonságos böngésző, amely biztosítja a banki tranzakciók fokozott védelmét.

**Lopásvédelem** – Meghatározza az eszköz helyét és segít a megkeresésében az elvesztése vagy az ellopása esetén.

A További eszközök hivatkozásra kattintva további eszközöket is talál, amelyekkel megvédheti számítógépét (például Karantén).

Hálózatfelügyelet

A Hálózatfelügyelet elősegíti a biztonsági rések – például nyitott portok vagy gyenge routerjelszó – beazonosítását a megbízható (otthoni vagy munkahelyi) hálózaton. A funkció egy könnyen elérhető listát is biztosít a csatlakoztatott, típus szerint csoportosított eszközökről (például nyomtató, útválasztó, mobileszköz stb.), így láthatja, hogy mi csatlakozik az otthoni hálózatához (például játékkonzol, IoT vagy más intelligens otthoni eszköz).

A Hálózatfelügyelet segítségével azonosíthatja a router biztonsági réseit, és növelheti a védelmi szintet a hálózatokhoz való csatlakozáskor.

A Hálózatfelügyelet nem konfigurálja újra a routert. Ön végezheti el a módosításokat a router egyedi felhasználói felületén. Az otthoni router sokszor rendkívül sérülékenyek a terjesztett szolgáltatásmegtagadásos (DDoS) támadások indítására használt káros szoftverekkel szemben. Ha a felhasználó nem módosította a router alapértelmezett jelszavát, a hackerek könnyen ki tudják találni, és így be tudnak jelentkezni a routerre. Ezután újrakonfigurálhatják a routert, illetve feltörhetik a hálózatot.

> ⚠ Javasoljuk, hogy erős jelszót adjon meg, amely elég hosszú, és számokat, szimbólumokat vagy nagybetűket tartalmaz. Ha nehezebben feltörhető jelszót szeretne megadni, használja különböző típusú karakterek kombinációját.

Ha a hálózat, amelyhez csatlakozik, megbízhatóként van konfigurálva, akkor megjelölheti a hálózatot „Saját hálózat” névvel. Kattintson a **Megjelölés „Saját hálózat” névvel** elemre, ha el szeretné látni a Saját hálózat címkével a hálózatot. A címke a hálózat mellett fog megjelenni az ESET Internet Security szolgáltatásban a könnyebb beazonosítás és a biztonság áttekintése érdekében. A **„Saját hálózat” jelölés törlése** elemre kattintva eltávolíthatja a címkét.

A hálózathoz csatlakoztatott összes eszköz listanézetben jelenik meg az alapvető információkkal együtt. A kívánt eszközre kattintva szerkesztheti az eszközt, illetve részletes információkat olvashat róla.

A **Hálózatok** legördülő menü lehetővé teszi az eszközök szűrését a következő feltételek alapján:

- Adott hálózathoz csatlakoztatott eszközök
- Az **összes hálózathoz** csatlakoztatott eszközök
- Nem kategorizált eszközök

A hálózathoz csatlakoztatott összes eszköz szonár nézetben való megjelenítéséhez kattintson a szonár ikonra . A kurzort egy eszköz ikonja fölé helyezve alapvető információkat jeleníthet meg, többek között a hálózat nevét és az utolsó megtekintés dátumát.

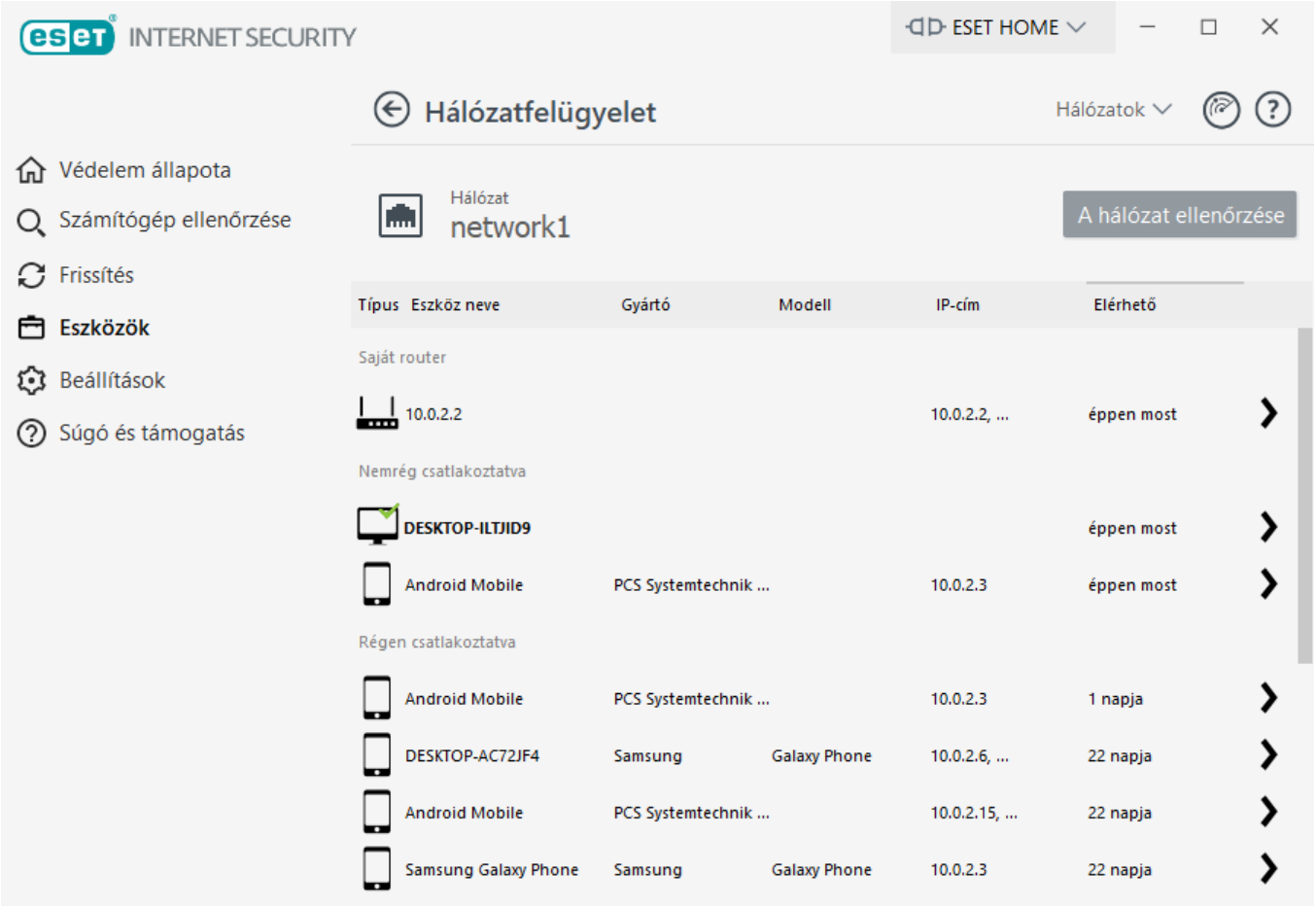
Az eszköz ikonjára kattintva szerkesztheti az eszközt, illetve részletes információkat olvashat róla. A legutóbb csatlakoztatott eszközök az routerhez közelebb jelennek meg, hogy könnyen észrevehetők legyenek.

Kattintson **A hálózat ellenőrzése** elemre, ha manuálisan szeretné ellenőrizni azt az routert, amelyhez éppen csatlakozik. **A hálózat ellenőrzése** elem csak a megbízható hálózatoknál érhető el. A hálózati beállítások áttekintéséhez vagy szerkesztéséhez tekintse át az Ismert hálózatok című részt.

Az alábbi ellenőrzési lehetőségek közül választhat:

- Minden ellenőrzése
- Csak a router ellenőrzése
- Csak az eszközök ellenőrzése

Hálózati ellenőrzést kizárólag megbízható hálózaton végezzen! Ha nem megbízható hálózaton hajtja végre, az veszélyt jelenthet.



Az ellenőrzés befejezésekor megjelenik egy értesítés a készülékre vonatkozó alapadatokra mutató hivatkozással, illetve lista- vagy szonárnézetben duplán a gyanús eszközre kattinthat. A legutóbb letiltott kommunikáció megjelenítéséhez kattintson a **Hibaelhárítás** elemre. További információk a tűzfal hibaelhárításáról.

A Hálózatfelügyelet modulban kétféle értesítés jelenik meg:

- **Új eszköz csatlakozik a hálózathoz** – Akkor jelenik meg értesítés, ha egy korábban nem látott eszköz csatlakozik a hálózathoz, miközben a felhasználó csatlakoztatva van.

• **Új hálózati eszköz található** – Ez akkor jelenik meg, ha ismét csatlakozik a megbízható hálózathoz, és jelen van egy korábban nem látott eszköz.

Mindkét értesítéstípus tájékoztatja arról, ha egy jogosulatlan eszköz megpróbál csatlakozni a hálózatához. Kattintson az **Eszköz adatainak megtekintése** elemre a részletek megjelenítéséhez.

Mit jelentenek az ikonok az eszközökön a Hálózatfelügyelet szolgáltatásban?

	A sárga csillagot ábrázoló ikon olyan eszközöket jelez, amelyek újak a hálózaton, illetve amelyeket az ESET első alkalommal észlel.
	A sárga figyelmeztető ikon azt jelzi, hogy a router biztonsági rést tartalmazhat. Kattintson az ikonra a termékben a problémával kapcsolatos további információkért.
	A piros figyelmeztető ikon azt jelzi, hogy a router biztonsági rést tartalmaz, és lehet, hogy fertőzött. Kattintson az ikonra a termékben a problémával kapcsolatos további információkért.
	A kék színű ikon akkor jelenhet meg, ha az ESET-termék további információkkal rendelkezik a router számára, viszont nincs szükség azonnali intézkedésekre, mert nem állnak fenn biztonsági kockázatok. Kattintson az ikonra további információkért.

Hálózati eszköz a Hálózatfelügyeletben

Ezen a részen található az eszközre vonatkozó részletes adatok, többek között az alábbiak:

- Eszköz neve
- Eszköz típusa
- Legutóbb elérhető
- Hálózat neve
- IP-cím
- MAC-cím
- Operációs rendszer

A ceruzát ábrázoló ikon jelzi, hogy módosíthatja az eszköz nevét vagy az eszköz típusát.

Eltávolítás az előzményekből – Az eszköz törlése az eszközök listájából. Ez az opció csak olyan eszközök esetében érhető el, amelyek jelenleg nem kapcsolódnak a hálózathoz.

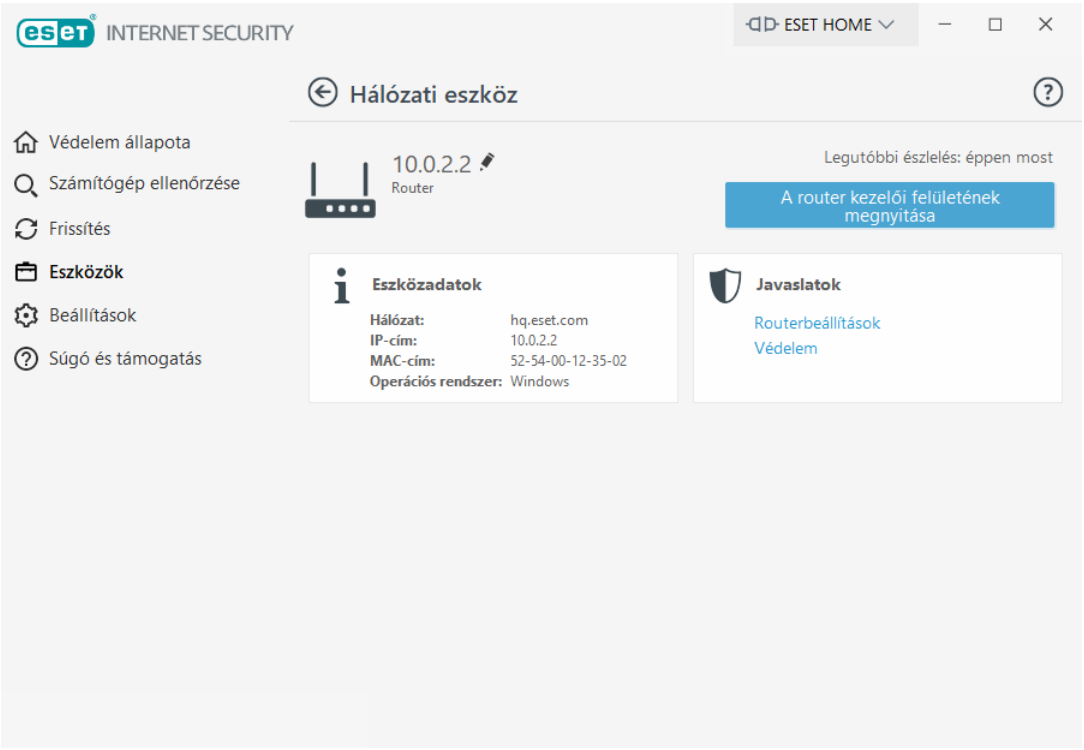
Mindegyik eszköz esetén a következő műveletek állnak rendelkezésre:

Router

Routerbeállítások – A router beállításai a webes felületen, a mobilalkalmazásban, illetve **A router kezelői felületének megnyitása** szövegre kattintva érhetők el. Ha internetszolgáltatója biztosítja a routert, akkor szükség lehet arra, hogy az internetszolgáltató segédanyagaiból vagy a router gyártójánál tájékozódjon a tapasztalt

biztonsági problémák elhárítási módjáról. Mindig kövesse a router felhasználói útmutatójában olvasható biztonsági óvintézkedéseket.

Védelem – A router és a hálózat informatikai biztonsági támadásoktól való megvédéséhez kövesse az alábbi egyszerű javaslatokat.

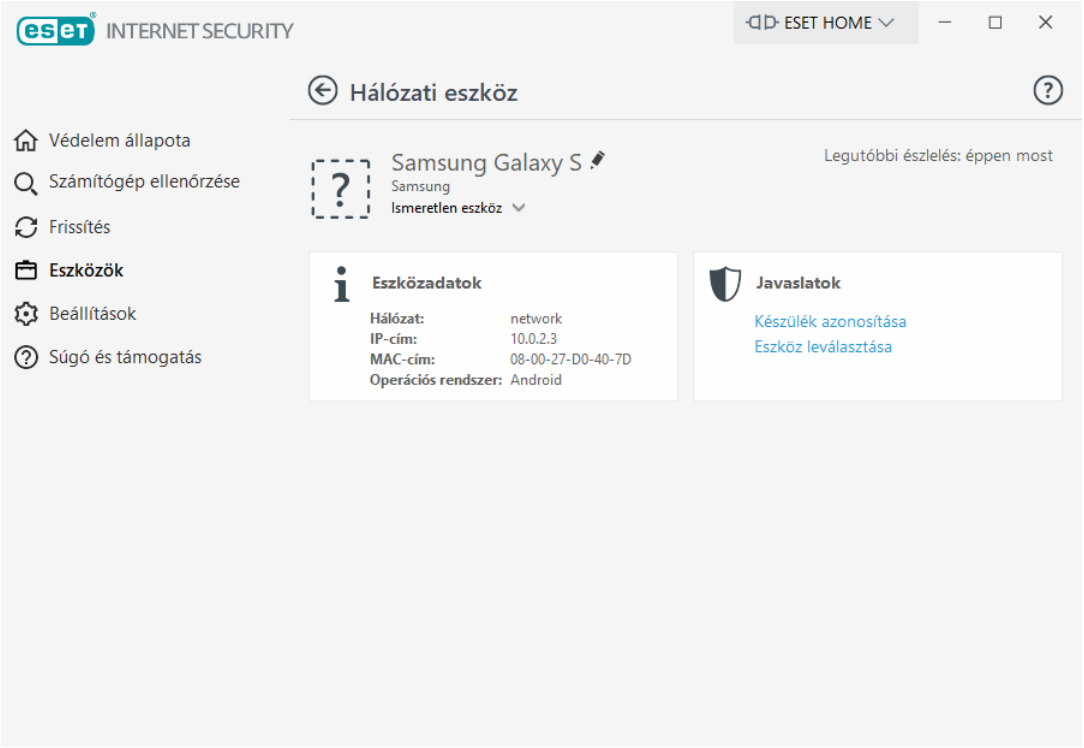


Hálózati eszköz

Készülék azonosítása – Ha nem biztos benne, hogy milyen eszköz csatlakozik a hálózatához, nézze meg a gyártó nevét az eszköz neve alatt. A gyártó neve segítséget nyújthat annak kiderítésében, hogy milyen eszközről van szó. Módosíthatja az eszköz nevét a későbbi problémák elkerülése érdekében.

Eszköz leválasztása – Ha nem biztos benne, hogy az egyik csatlakoztatott eszköz veszélyt jelent-e a hálózatra vagy az eszközökre nézve, a router beállításaiban módosítsa az eszköz hálózati hozzáférési beállítását, vagy módosítsa a hálózat jelszavát.

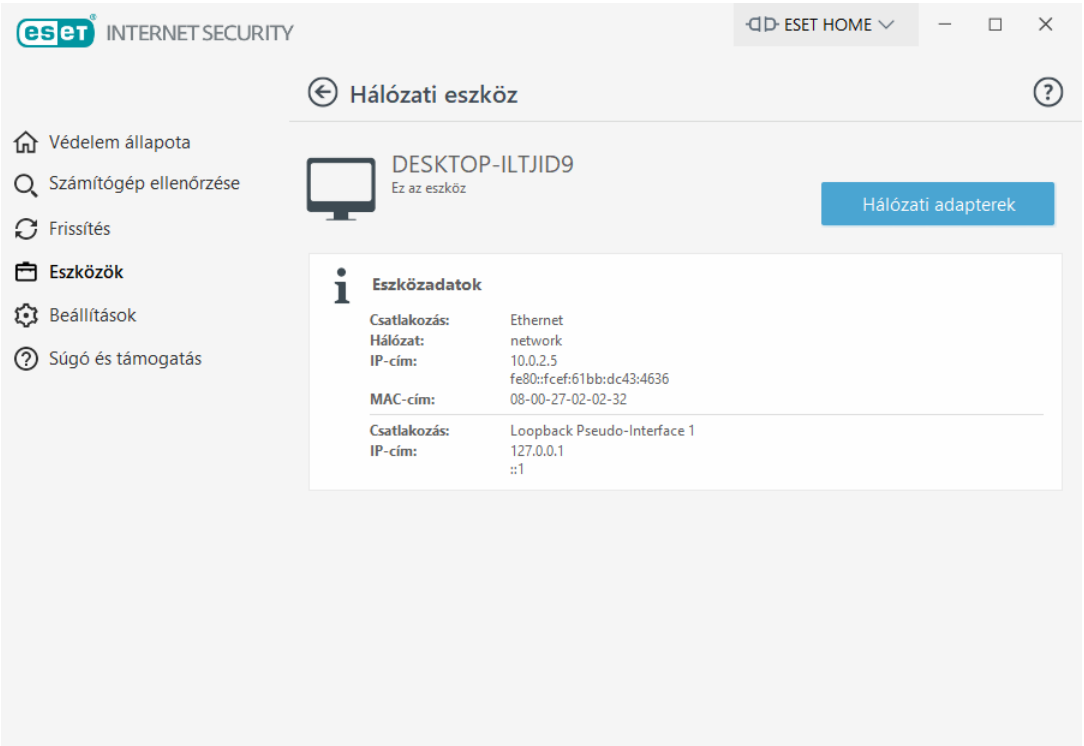
Védelem – Ha meg szeretné védeni az eszközét a támadásoktól és a kártevő szoftverektől, telepítsen informatikai biztonsági védelmet az eszközre, és tartsa naprakészen az operációs rendszert és a telepített szoftvereket. A biztonság fenntartása érdekében ne kapcsolódjon nem biztonságos Wi-Fi-hálózatokhoz.



Ez az eszköz

Ez az eszköz képviseli a számítógépét a hálózaton.

Hálózati adapterek – Itt a hálózati adapterekkel kapcsolatos információk találhatók.



Értesítések | Hálózatfelügyelet

Az alábbi értesítések jelenhetnek meg, amikor az ESET Internet Security valamilyen biztonsági rést fedez fel az útválasztóján. Minden értesítés tartalmaz egy rövid leírást, és megoldást vagy lépéseket biztosít, amelyeket elvégezve csökkentheti az útválasztó biztonsági résést. Ha nincs gyakorlata az útválasztó beállításában, azt javasoljuk, lépjen kapcsolatba az útválasztó gyártójával vagy az internetszolgáltatójával.

Lehetséges biztonsági rés található
Előfordulhat, hogy útválasztója olyan ismert biztonsági réseket tartalmaz, amelyek következtében könnyedén megtámadható és kihasználható lesz. Frissítse az útválasztó belső vezérlőprogramját.

Biztonsági rés található
Útválasztója olyan ismert biztonsági réseket tartalmaz, amelyek következtében könnyedén megtámadható és kihasználható lesz. Frissítse az útválasztó belső vezérlőprogramját.

A program kártevőt talált
Útválasztóját kártevő fertőzte meg. Indítsa újra az útválasztót, és ismételje meg az ellenőrzést.

Gyenge útválasztói jelszó
Útválasztóján gyenge a jelszó, és mások könnyedén kitalálhatják. Módosítja jelszavát az útválasztón.

Kártékony hálózati átirányítás
Internetes forgalmát valószínűleg kártékony webhelyekre irányították át. Ez azt jelentheti, hogy illetéktelenül hozzáfértek az útválasztójához. Módosítsa a DNS-szerver beállítását az útválasztón.

Nyílt hálózati szolgáltatások
Útválasztója olyan hálózati szolgáltatásokat futtat, amelyeket mások kihasználhatnak. Ezt az illetéktelenül elért útválasztó nem megfelelő konfigurációja okozhatja. Ellenőrizze az útválasztó konfigurációját.

Érzékeny nyílt hálózati szolgáltatások
Útválasztója olyan érzékeny hálózati szolgáltatásokat futtat, amelyeket mások kihasználhatnak. Ezt az illetéktelenül elért útválasztó nem megfelelő konfigurációja okozhatja. Ellenőrizze az útválasztó konfigurációját.

Elavult belső vezérlőprogram
Útválasztója belső vezérlőprogramja elavult, és biztonsági réseket tartalmazhat. Frissítse a belső vezérlőprogramot az útválasztón.

Kártékony útválasztó-beállítás
Az útválasztója által használt DNS-szerver kártékony, és előfordulhat, hogy veszélyes webhelyekre küldi. Ez azt jelentheti, hogy illetéktelenül hozzáfértek az útválasztójához. Módosítsa a DNS-szerver beállítását az útválasztón.

Hálózati szolgáltatások
Útválasztója szokásos hálózati szolgáltatásokat futtat. Ezekre a hálózatnak van szüksége, és valószínűleg biztonságosak. Ellenőrizze az útválasztó konfigurációját.

Az ESET Internet Security eszközei

Az **Eszközök** lapon található modulok segítik a program adminisztrációjának egyszerűsítését, és további lehetőségeket kínálnak a tapasztalt felhasználóknak. Ezek az eszközök csak akkor láthatók, ha a **További eszközök** elemre kattint a jobb alsó sarokban.

A lapon az alábbi eszközök láthatók:

 Naplófájlok

Biztonsági jelentés

Futó folyamatok (ha az ESET LiveGrid® engedélyezve van az ESET Internet Security alkalmazásban)

Hálózati kapcsolatok (ha a Tűzfal engedélyezve van az ESET Internet Security alkalmazásban)

ESET SysInspector

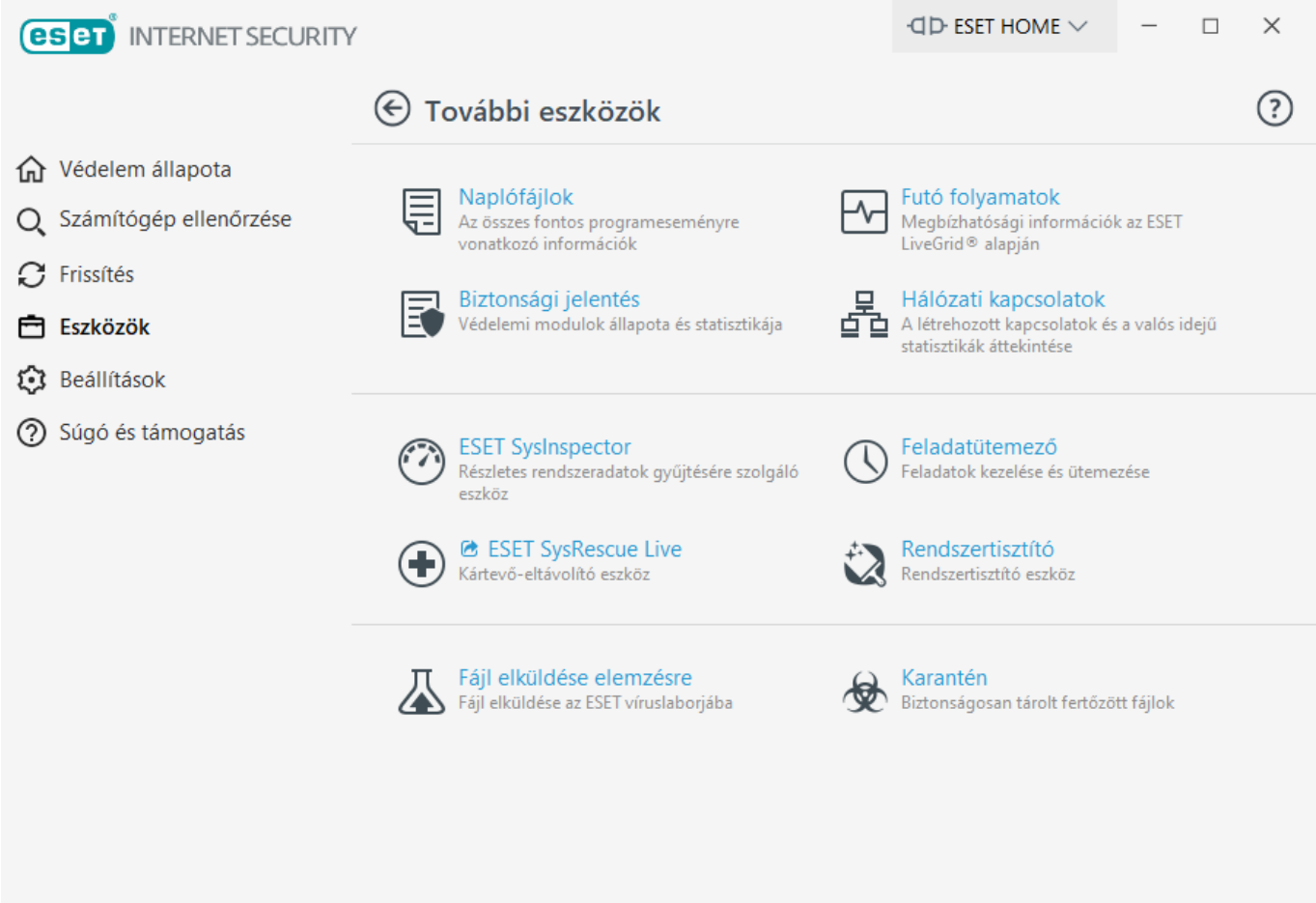
ESET SysRescue Live – Átirányítja az ESET SysRescue Live webhelyre, ahol letöltheti az ESET SysRescue Live .iso CD-/DVD-képet.

Feladatütemező

Rendszertisztító – A számítógép visszaállítása használható állapotba, miután megtisztította a kártevőtől.

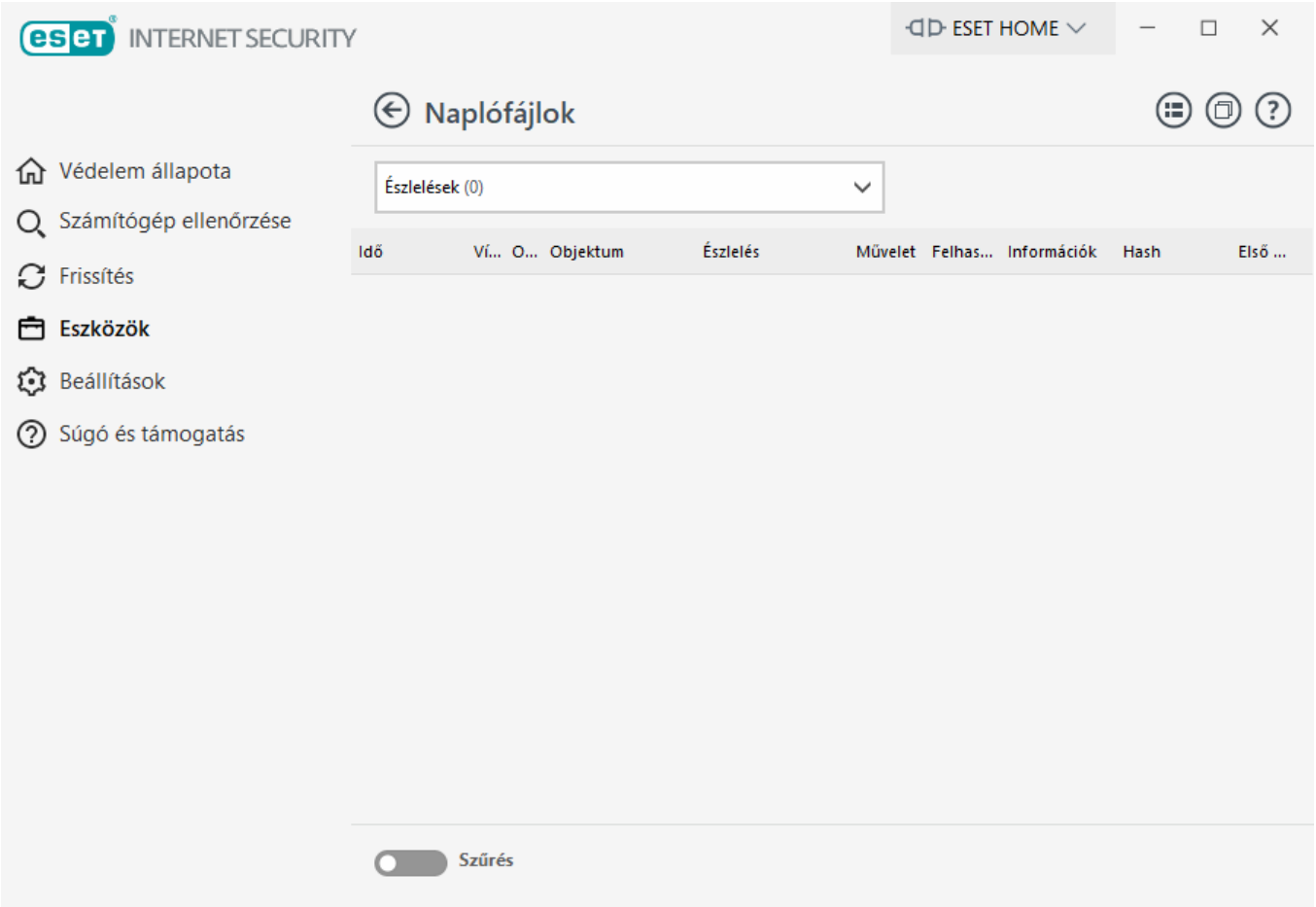
Minta elküldése elemzésre – A gyanús fájlok elküldése elemzésre az ESET víruslaborjába (az ESET LiveGrid® konfigurációjától függ, hogy erre van-e lehetőség).

Karantén



Naplófájlok

A Naplófájlok lap a fontos programeseményekről tájékoztatást, az észlelt kártevőkről áttekintést nyújt. A naplózás a rendszerelemzés, észlelés és hibaelhárítás alapvető részét képezi. 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 Internet Security-programkörnyezetből is megtekinthetők, de ugyanitt nyílik lehetőség a naplófájlok archiválására is.



A naplófájlok a fő programablakban az **Eszközök** > **További eszközök** > **Naplófájlok**. A **Napló** legördülő menüben válassza ki a kívánt naplótípust. A választható naplók az alábbiak:

- **Észlelések** – Ez a napló részletes információkat szolgáltat az ESET Internet Security által észlelt kártevőkről és fertőzésekről. A naplózott információk tartalmazzák az észlelés idejét, az ellenőrzés típusát, az objektum típusát, az objektum helyét, a kártevő nevét, a végrehajtott műveletet és annak a felhasználónak a nevét, aki a fertőzés észlelésének idején be volt jelentkezve, továbbá a kivonatot és az első előfordulást. A nem megtisztított fertőzések szövege vörös színű, a hátterük pedig halványpiros. Míg a megtisztított fertőzések szövege sárga színű, a hátterük pedig fehér színű. A nem megtisztított potenciálisan veszélyes és nem kívánt alkalmazások szövege sárga, a hátterük pedig fehér színű.

- **Események** – Az ESET Internet Security az általa 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 ellenőrzése** – Ezt a lehetőséget választva megjelenítheti az összes befejezett ellenőrzés eredményét. Minden sor egy-egy számítógép-ellenőrzésnek felel meg. Az egyes bejegyzésekre duplán

kattintva megjelenítheti az adott ellenőrzés részletes adatait.

• **Behatolásmegelőző rendszer** – A rögzítésre megjelölt adott behatolásmegelőzési szabályok bejegyzéseit tartalmazza. A protokoll megjeleníti a műveletet kiváltó alkalmazást, az eredményt (a szabály engedélyezett vagy letiltott volt-e) és a szabály nevét.

• **Hálózatvédelem** – A hálózatvédelmi napló megjeleníti a tűzfal, a Hálózati támadások elleni védelem (IDS) és a Botnet elleni védelem által észlelt összes távoli támadást. Valamint a számítógép ellen indított esetleges 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 hálózatvédelmi napló elemzésével időben felderítheti a rendszer ellen végrehajtott behatolási kísérleteket, és megakadályozhatja a számítógéphez való jogosulatlan hozzáférést. A hálózati támadásokról az IDS és további beállítások című fejezetben olvashat bővebben.

• **Szűrt webhelyek** – Ebben a listában láthatók a webhozzáférés-védelem vagy a szülői felügyelet által letiltott webhelyek. Ezekben a naplókban látható az idő, az URL-cím, a felhasználó és az adott webhellyel kapcsolatot létrehozó alkalmazás.

• **Levélszemétszűrő** – A levélszemétként megjelölt e-mail e-mailekhez tartozó bejegyzéseket tartalmazza.

• **Szülői felügyelet** – Megjeleníti a Szülői felügyelet által letiltott vagy engedélyezett weboldalakat. Az Egyezési típus és az Egyezési értékek oszlopban látható, hogy miként alkalmazta a szűrési szabályokat.

• **Eszközfelügyelet** – A számítógéphez csatlakoztatott cserélhető adathordozókra vagy eszközökre vonatkozó bejegyzéseket tartalmaz. A program csak a megfelelő eszközfelügyeleti szabállyal rendelkező eszközöket jegyzi fel a naplófájlba. Ha a szabály nem felel meg egy csatlakoztatott eszköznek, létrejön egy naplóbejegyzés az eszközhöz. Bizonyos adatok – többek között az eszköz típusa, a sorozatszám, a gyártó neve és az adathordozó mérete (ha van) – is láthatók.

• **Webkamera-védelem** – A Webkamera-védelem által letiltott alkalmazásokra vonatkozó bejegyzéseket tartalmazza.

Jelölje ki egy tetszőleges napló tartalmát, majd a **CTRL + C** billentyűkombinációval másolja a vágólapra. Több bejegyzést a **CTRL**, illetve a **SHIFT** billentyűt lenyomva tartva jelölhet ki.

Kattintson a  **Szűrés** ikonra a Napló szűrése ablak megnyitásához, ahol definiálhatja a szűrési feltételeket.

Kattintson a jobb gombbal egy adott rekordra a hozzá tartozó helyi menü megjelenítéséhez. A helyi menüben az alábbi parancsok találhatók:

• **Megjelenítés** – További részletes információkat jelenít meg egy új ablakban a kijelölt naplóról.

• **Azonos rekordok szűrése** – Ha aktiválja ezt a szűrőt, csak az azonos típusú bejegyzések jelennek meg (diagnosztika, figyelmeztetések stb.).

• **Szűrés** – Miután erre az opcióra kattintott, a Napló szűrése ablakban megadhatja az adott naplóbejegyzések szűrési feltételeit.

• **Szűrés engedélyezése** – Aktiválja a szűrőbeállításokat.

• **Szűrő letiltása** – Törli az összes szűrési beállítást (a fentiek szerint).

• **Másolás/Minden másolása** – Az ablakban lévő összes bejegyzésről másolja az információkat.

• **Törlés/Minden törlése** – Törli a kijelölt bejegyzéseket vagy az összes megjelenített bejegyzést. A művelet végrehajtásához rendszergazdai jogosultságokra van szükség.

• **Exportálás/Az összes exportálása** – A kijelölt rekordok vagy az összes rekord adatainak exportálása XML formátumban.

• **Keresés/Következő keresése/Előző keresése** – Miután erre az opcióra kattintott, a Napló szűrése ablakban megadhatja az adott naplóbejegyzések szűrési feltételeit.

• **Észlelt elem leírása** – Megnyitja az ESET Threat Encyclopedia programot, amely részletes információkat tartalmaz a rögzített beszivárgás veszélyeiről és tüneteiről.

• **Kivétel létrehozása** – Létrehozhat egy új észlelési kivételt egy varázsló segítségével (nem áll rendelkezésre kártevőkészlelések esetén).

Napló szűrése

Kattintson a **Szűrés** gombra az **Eszközök** > **További eszközök** > **Naplófájlok** lapon a szűrési feltételek megadásához.

A naplószűrési funkció segítségével könnyebben megtalálhatja a keresett információkat, különösen akkor, ha sok bejegyzés van. Lehetővé teszi az adott naplóbejegyzések megtalálását, ha például egy adott típusú eseményt, állapotot vagy időszakot keres. A naplóbejegyzések között különböző keresési feltételek megadásával szűrhet – csak a releváns bejegyzések fognak megjelenni (vagyis a keresési feltételeknek megfelelők) a Naplófájlok ablakban.

Írja be a keresett kulcsszót a **Szöveg keresése** mezőbe. A **Keresés oszlopokban** legördülő menüben finomíthatja a keresést. A **Bejegyzés-naplótípusok** legördülő menüben kiválaszthat egy vagy több bejegyzést. Megadhatja az **Időszakot**, amikortól meg szeretné jeleníteni a találatokat. További keresési feltételeket is használhat – ilyen például **A teljes szóval megegyező** és a **Kis- és nagybetű különbözik**.

Szöveg keresése

Írja be a karakterláncot (egy szót vagy egy szórészletet). Csak azok a bejegyzések jelennek meg, amelyek tartalmazzák a karakterláncot. A többi rekord kimarad.

Keresés oszlopokban

Válassza ki, hogy mely oszlopokat szeretné bevonni a keresésbe. Egy vagy több oszlopot választhat ki.

Bejegyzéstípusok

A legördülő listában a naplóbejegyzések típusai közül választhat:

• **Diagnosztikai** – Az alábbiak mellett a program pontos beállításához szükséges információk naplózása.

• **Tájékoztató** – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett bejegyzéseket).

• **Figyelmeztetések** – Kritikus figyelmeztetések és figyelmeztető üzenetek rögzítése.

• **Hibák** – A fájlletöltési és más kritikus hibák bejegyzése a naplóba.

- **Kritikus** – A program csak a kritikus (például a vírusvédelem indításával).

Időszak

A legördülő listában azt jelölheti ki, hogy mely időszak eseményei érdeklik.

- **Nincs megadva** (alapértelmezett) – Nem egy adott időszakban, hanem a teljes naplóban folyik a keresés.
- **Az elmúlt 24 óra**
- **Múlt hét**
- **Múlt hónap**
- **Időszak** – Megadhatja pontosan az időszakot (Ettől: és Eddig:), ha csak egy adott időszakban keletkezett bejegyzéseket szeretne kiszűrni.

A teljes szóval megegyező

A jelölőnégyzet bejelölése esetén a találatok közé csak azok a bejegyzések kerülnek be, melyekben a keresett kifejezés önálló szóként is előfordul.

Kis- és nagybetű különbözik

Akkor aktiválja ezt a funkciót, ha fontosnak tartja a nagy- és kisbetűk használatát szűrés közben. Miután megadta a szűrési/keresési feltételeket, kattintson az **OK** gombra a szűrt naplóbejegyzések megjelenítéséhez, vagy a **Keresés** elemre kattintva kezdje meg a keresést. A naplófájlok közötti keresés fentről lefelé megy végbe, az aktuális pozíciótól kezdve (ez a kiemelt bejegyzés). A keresés akkor leáll, ha megvan az első egyező bejegyzés. Az **F3** billentyű lenyomásával megkeresheti a következő bejegyzést, illetve a jobb gombbal kattintva és a **Keresés** lehetőséget kiválasztva finomíthatja a keresési feltételeket.

Naplózási konfiguráció

Az ESET Internet Security naplózási beállításai a program főablakában érhetők el. Kattintson a **Beállítások** > **További beállítások** > **Eszközök** > **Naplófájlok** elemre. 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:

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

- **Diagnosztikai** – A fentiek mellett a program pontos beállításához szükséges információk naplózása.
- **Tájékoztató** – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett bejegyzéseket).
- **Figyelmeztetések** – Kritikus figyelmeztetések és figyelmeztető üzenetek rögzítése.
- **Hibák** – A „Hiba a fájl letöltésekor” és más kritikus hibák bejegyzése a naplóba.
- **Kritikus** – A program csak a kritikus (például a vírusvédelem indításával,a tűzfallalás egyebekkel kapcsolatos) hibákat naplózza.

A Diagnosztikai részletességi szint választása esetén minden letiltott kapcsolatot feljegyez a rendszer.

A jelölőnégyzet bejelölésekor a rendszer automatikusan törli **Az ennél régebbi naplóbejegyzések törlése (nap)** mezőben megadott számú napnál régebbi naplóbejegyzéseket.

Naplófájlok automatikus optimalizálása – Az opció bejelölése esetén a naplófájlok töredezettségmentesítése automatikusan megtörténik, ha a százalékérték meghaladja a **Ha a fölösleges bejegyzések száma több mint (%)** mezőben megadott értéket.

Az **Optimalizálás** gombra kattintva elkezdheti a naplófájlok töredezettségmentesítését. 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.

A **Szöveges protokoll engedélyezése** beállítással engedélyezheti a naplók tárolását a naplófájloktól eltérő fájlformátumban:

- **Célkönyvtár** – A naplófájlok tárolására szolgáló könyvtár (csak szöveges/CSV-fájlokra vonatkozik). Az egyes naplószakaszokhoz saját, előre megadott nevű fájl tartozik (például a virlog.txt a naplófájlok **Észlelések** szakaszához, ha a naplók tárolásához egyszerű szöveges fájlformátumot használ).

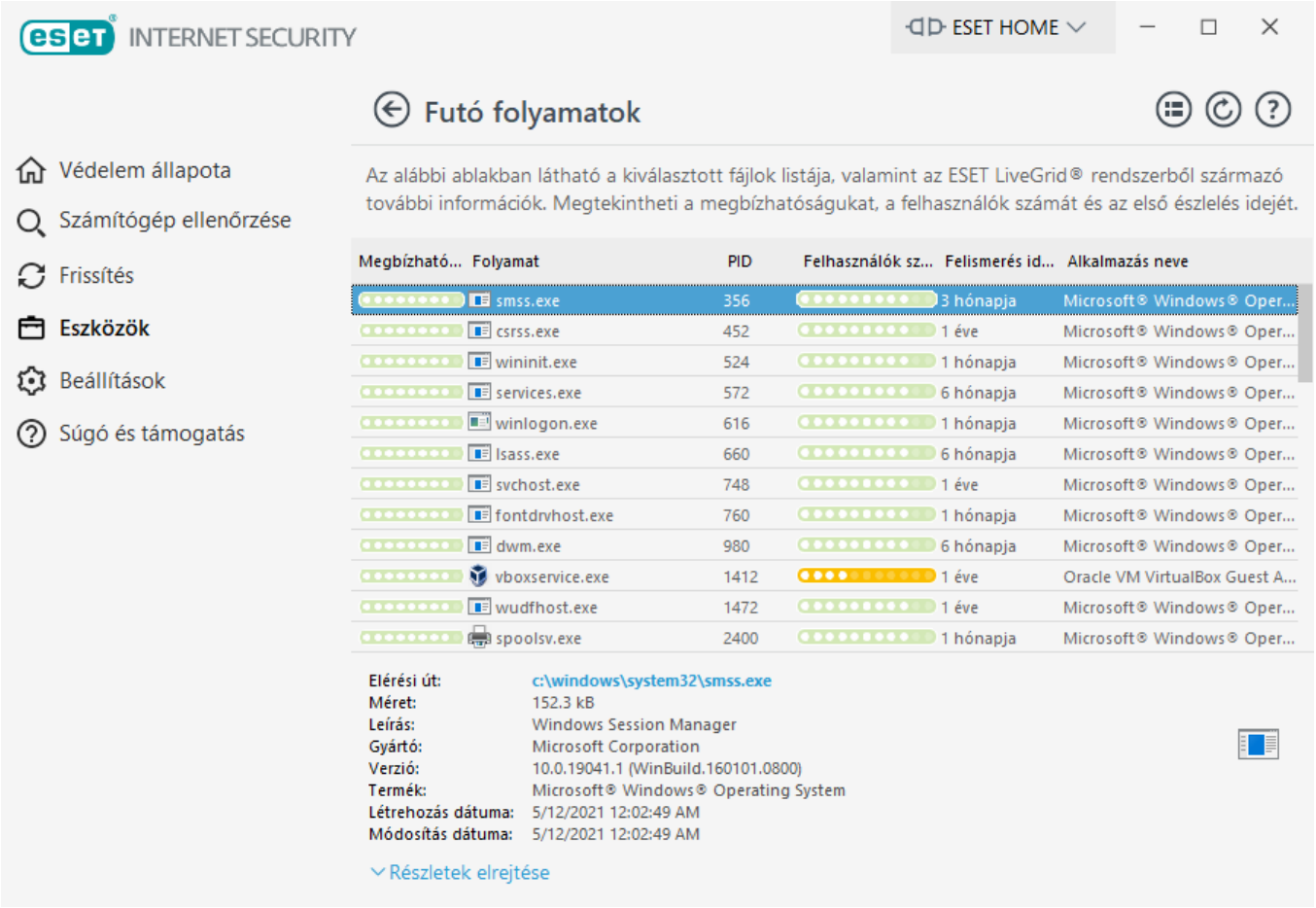
- **Típus** – Ha a **szöveges** fájlformátumot választja, a naplók tárolása szöveges fájlban történik, és az adatokat tabulátorok választják el egymástól. Ugyanez vonatkozik a vesszővel elválasztott **CSV** fájlformátumra is. Az **Esemény** típus kiválasztása esetén a naplók tárolása nem fájlban, hanem a Windows eseménynaplójában történik (amely a Vezérlőpult Eseménynapló eszközében tekinthető meg).

- **Az összes naplófájl törlése** hivatkozásra kattintva törölheti a **Típus** legördülő listában aktuálisan kijelölt összes tárolt naplót. Ezt követően a naplók sikeres törléséről tájékoztató értesítés jelenik meg.

A hibák gyorsabb elhárítása végett időnként lehetséges, hogy az ESET kérni fogja számítógépe naplóit. Az ESET Log Collector egyszerűvé teszi a szükséges információk összegyűjtését. Az ESET Log Collector részletes ismertetése az ESET tudásbáziscikkében található.

Futó folyamatok

A futó folyamatok megjelenítik a számítógépen futó programokat és folyamatokat. A megbízhatósági technológia révén az ESET azonnali és folyamatos tájékoztatást kap az új kártevőkről. Az ESET Internet Security részletes adatokat szolgáltat a futó folyamatokról, amelyek segítségével a ESET LiveGrid® technológia biztosítja a felhasználók védelmét.



Megbízhatóság – A legtöbb esetben az ESET Internet Security a ESET LiveGrid® 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 heurisztikus szabályok alapján az objektumok kockázati szintje az 1: Elfogadható (zöld) és a 9: Kockázatos (vörös) közé eshet.

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.

Az Elfogadható (zöld) jelzéssel ellátott ismert alkalmazások egészen biztosan nem fertőzöttek (engedélyezőlistán vannak), ezért a szűrésből kizártak.

PID – A folyamatazonosító paraméterként használható a különféle funkciómeghívásokban, például a folyamat prioritásának beállításakor.

Felhasználók száma – Egy adott alkalmazást használó felhasználók száma. Ezt az információt az ESET LiveGrid® technológia gyűjti.

Felismerés ideje – Az az időtartam, amióta az ESET LiveGrid® technológia észlelte az alkalmazást.

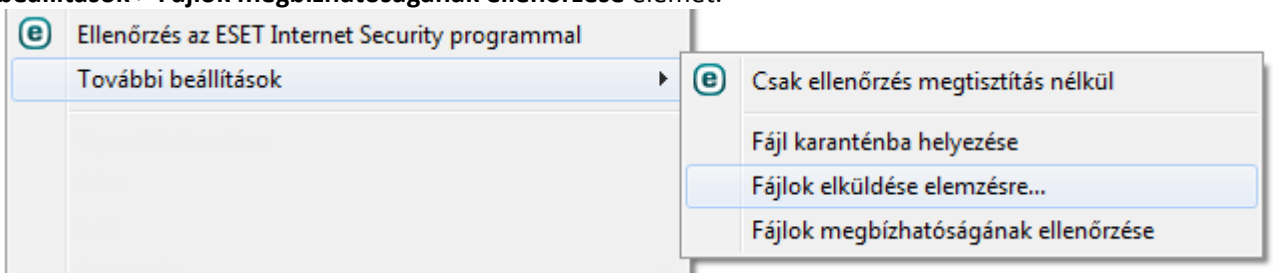
Az Ismeretlen (narancsszínű) jelöléssel ellátott alkalmazások nem feltétlenül kártevő szoftverek. Ezek rendszerint csak újabb alkalmazások. Ha kétségei vannak egy ilyen fájl biztonságosságát illetően, elküldheti a fájlt elemzésre az ESET víruslaborjába. Ha a fájl kártékony alkalmazás, bekerül a vírusdefiníciós adatbázis valamelyik későbbi frissítésébe.

Alkalmazás neve – Egy programnak vagy folyamatnak adott név.

Egy alkalmazásra kattintva megjelenítheti a következő adatokat az alkalmazásról:

- **Elérési út** – Egy alkalmazás helye a számítógépen.
- **Méret** – A fájl mérete kilobájtban (kB) vagy megabájtban (MB).
- **Leírás** – A fájl jellemzői az operációs rendszer leírása alapján.
- **Gyártó** – A gyártó vagy az alkalmazásfolyamat neve.
- **Verzió** – Az alkalmazás gyártójától származó információ.
- **Termék** – Az alkalmazás és/vagy a gyártó cég neve.
- **Létrehozás/Módosítás** – A létrehozás (módosítás) dátuma és időpontja.

Azoknak a fájloknak is ellenőrizheti a megbízhatóságát, amelyek nem futó programként/folyamatként viselkednek. Ehhez kattintson rájuk a jobb gombbal egy fájlkezelőben, majd válassza ki a **További beállítások** > **Fájlok megbízhatóságának ellenőrzése** elemet.



Biztonsági jelentés

Ez a funkció a következő kategóriák esetén ad áttekintést a statisztikai adatokról:

- **Letiltott weboldalak** – A letiltott weboldalak számát jeleníti meg (kéretlen alkalmazás letiltott URL-címe, adathalászat, feltört router, IP vagy tanúsítvány).
- **Észlelt fertőzött e-mail-objektumok** – Az észlelt fertőzött e-mail-objektumok számát jeleníti meg.
- **Letiltott szülői felügyelet alatt álló weboldalak** – A szülői felügyeletben letiltott weboldalak számát jeleníti meg.
- **Észlelt kéretlen alkalmazások** – A kéretlen alkalmazások számát jeleníti meg.
- **Észlelt levélszemét** – Az észlelt levélszemét számát jeleníti meg.
- **Webkamerához való hozzáférés letiltva** – Azt jeleníti meg, hogy hányszor volt szükség a webkamerához való hozzáférés letiltására.
- **Védett kapcsolatok az internetes banki szolgáltatásokhoz** – Azt jeleníti meg, hogy hányszor tiltotta meg a webhelyekhez való hozzáférést a Netbank- és tranzakcióvédelem funkció.
- **Ellenőrzött dokumentumok** – Az ellenőrzött dokumentumok számát jeleníti meg.
- **Ellenőrzött alkalmazások** – Az ellenőrzött végrehajtható objektumok számát jeleníti meg.

- **Egyéb ellenőrzött objektumok** – Az egyéb típusú ellenőrzött végrehajtható objektumok számát jeleníti meg.
- **Ellenőrzött weboldalobjektumok** – Az ellenőrzött weboldalobjektumok számát jeleníti meg.
- **Ellenőrzött e-mail-objektumok** – Az ellenőrzött e-mail-objektumok számának megjelenítése.

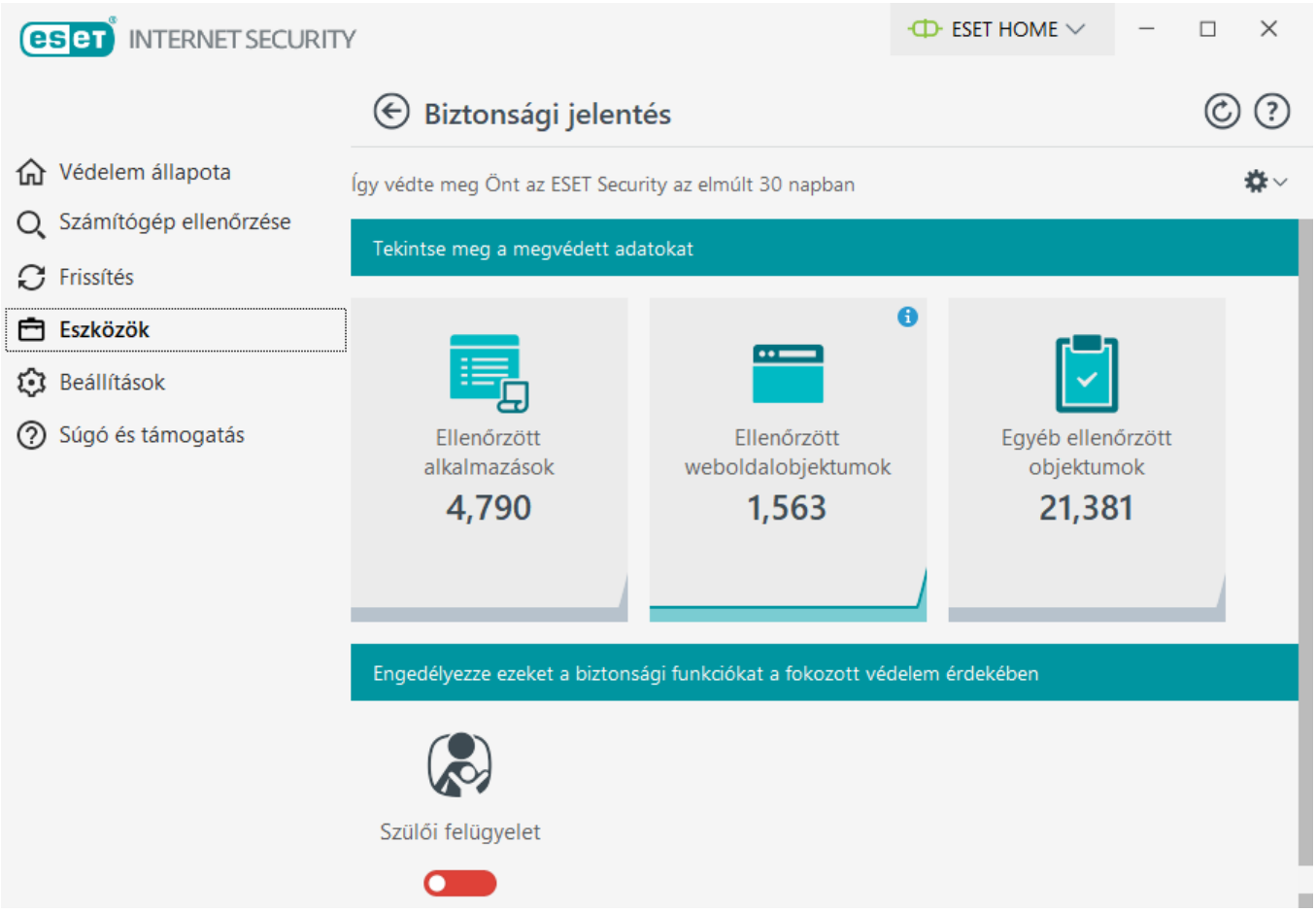
A kategóriák a legnagyobb számtól a legkisebbik rendeződnek. A nulla értékű kategóriák nem láthatók. A **Több mutatása** elemre kattintva megjeleníthetők a rejtett kategóriák.

A Biztonsági jelentés utolsó része a következő funkciók aktiválására ad lehetőséget:

- Szülői felügyelet
- Lopásvédelem

A kiválasztása után a funkció aktiváltként fog megjelenni a Biztonsági jelentésben.

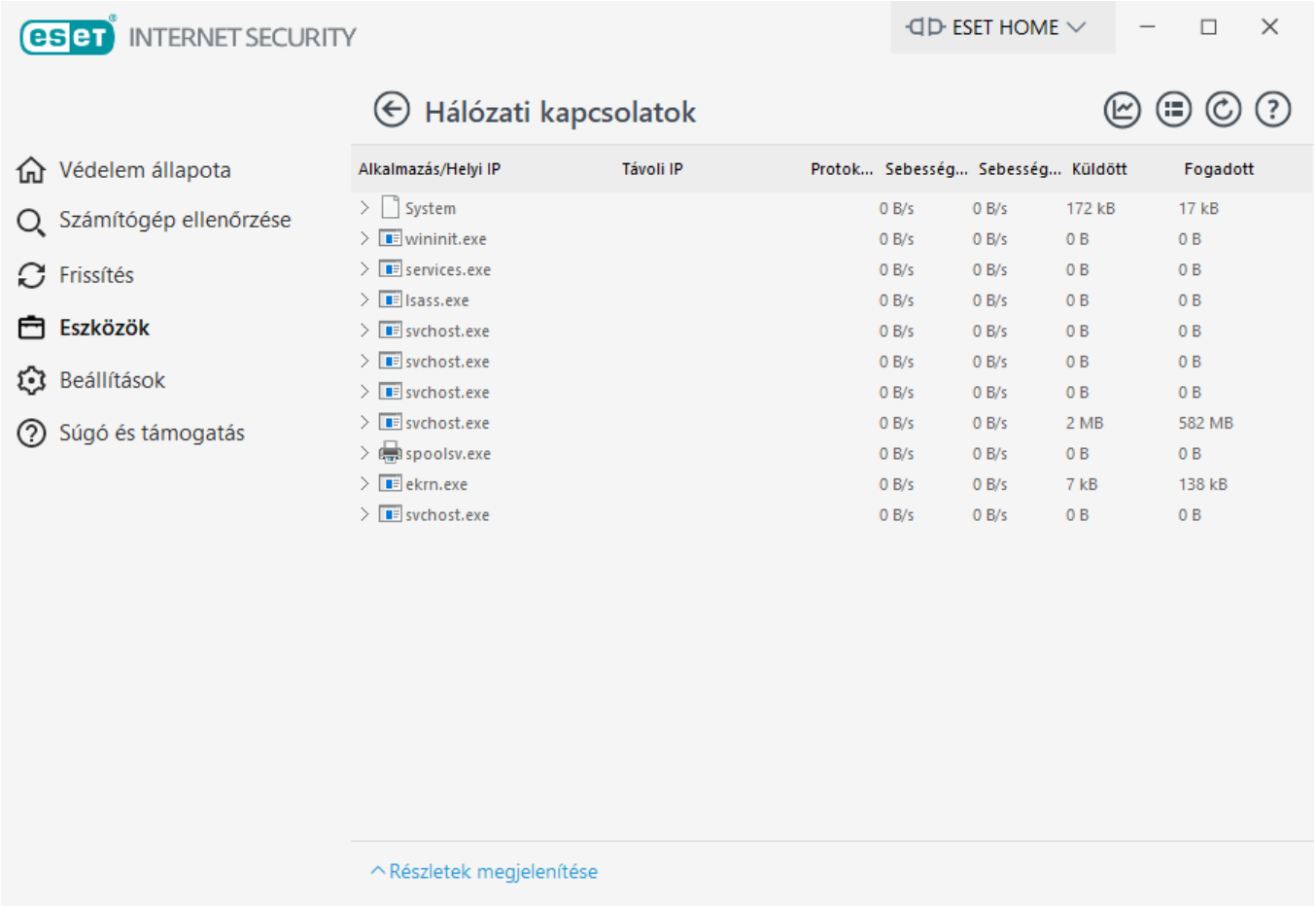
A jobb felső sarokban található fogaskerékre kattintva **engedélyezheti/letilthatja a biztonsági jelentésekről szóló értesítéseket**, vagy válassza ki, hogy az adatok az elmúlt 30 napból vagy a termék aktiválása óta jelenjenek meg. Ha az ESET Internet Security telepítése kevesebb, mint 30 napja történt meg, akkor csak a telepítés óta eltelt napok száma választható ki. Alapértelmezés szerint a 30 napos időszak van kiválasztva.



Az **Adatok visszaállítása** lehetőség kiválasztásakor törlődnek a statisztikai adatok és a Biztonsági jelentésben található adatok. A műveletet meg kell erősíteni, kivéve akkor, ha inaktiválja a **Rákérdezés a statisztika alaphelyzetbe állítása előtt** funkciót a **További beállítások** > **Értesítések** > **Interaktív riasztások** > **Megerősítési üzenetek** >**Szerkesztés** lapon.

Hálózati kapcsolatok

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



Kattintson a grafikont ábrázoló ikonra a Hálózati aktivitás ablak megnyitásához.

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

Oszlopok

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.

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

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

Állomásnevek feloldása – Ha bejelöli ezt az opciót, a hálózatcímek minden lehetséges esetben tartományneves formátumban (DNS-névként) jelennek meg az IP-címes formátum helyett.

Csak a TCP-kapcsolatok megjelenítése – A listában csak a TCP-protokollkészletet használó kapcsolatok jelennek meg.

Figyelő kapcsolatok 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 – Az opció bejelölése esetén a rendszer azokat a kapcsolatokat is megjeleníti, amelyekben a távoli oldal a helyi rendszer (a localhost tartománynévvel azonosított állomás).

Frissítési sebesség – Az aktív kapcsolatok frissítési gyakorisága.

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

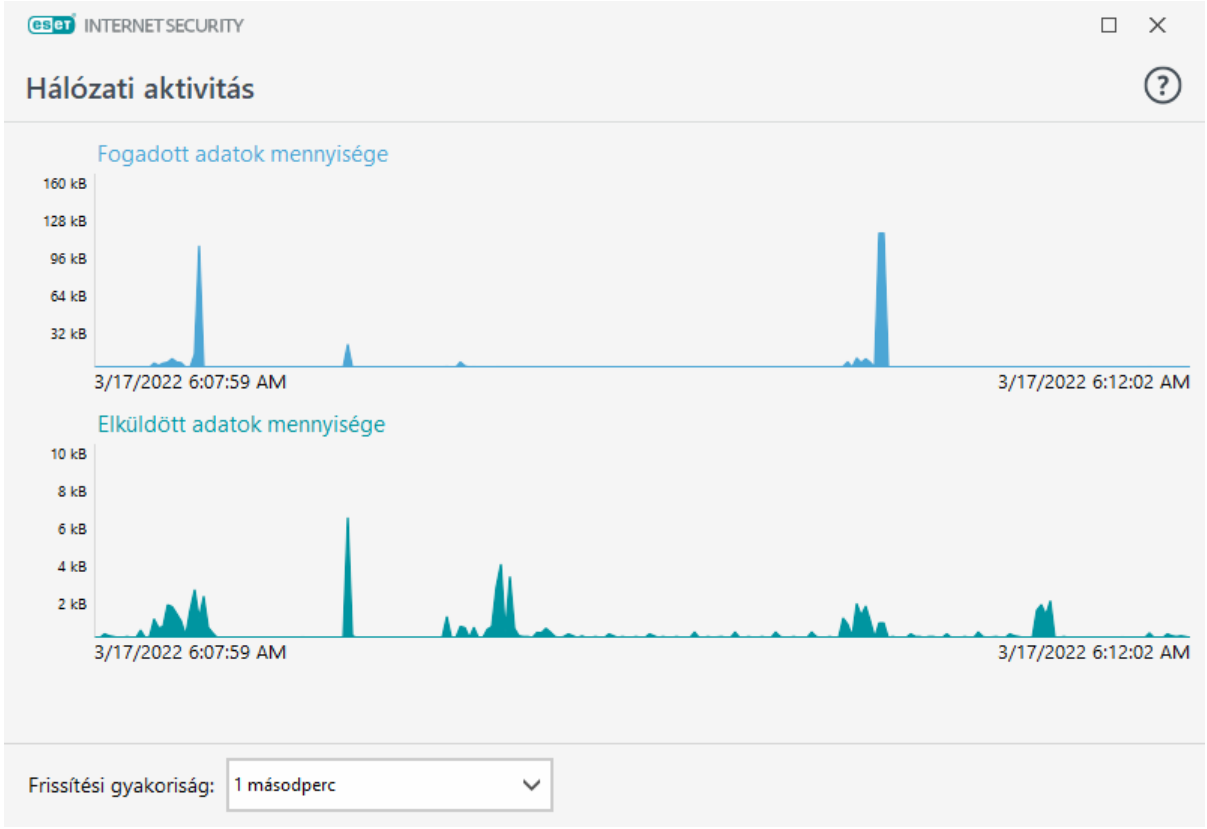
Az alábbi két beállítás csak akkor érhető el, ha nem egy aktív kapcsolatra, hanem egy alkalmazásra vagy egy folyamatra kattint:

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 beállítása és használata 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 beállítása és használata című témakörben található.

Hálózati aktivitás

Az aktuális **Hálózati aktivitás** grafikonos formában való megjelenítéséhez kattintson az **Eszközök** > **További eszközök** > **Hálózati kapcsolatok** elemre, majd kattintson a grafikont ábrázoló ikonra . A grafikon alján egy idősor található, amely valós időben, a kiválasztott időköz alapján rögzíti a hálózati aktivitást. Ha módosítani szeretné az időközt, jelölje ki az adott értéket a **Frissítési gyakoriság** legördülő menüben.



A választható lehetőségek az alábbiak:

- **1 másodperc** – A grafikon másodpercenként frissül, az idősor pedig az elmúlt 4 percet fedi le.
- **1 perc (az elmúlt 24 órában)** – A grafikon percenként frissül, az idősor pedig az elmúlt 24 órát fedi le.
- **1 óra (az elmúlt hónapban)** – A grafikon óránként frissül, az idősor pedig az elmúlt hónapot fedi le.

A grafikon függőleges tengelye a kapott és küldött adatok mennyiségét jeleníti meg. Ha az egér mutatóját a grafikon fölé viszi, megtekintheti az adott időpontban kapott és küldött adatok mennyiségét.

ESET SysInspector

Az ESET SysInspector egy alkalmazás, amely a számítógép részletes vizsgálatával adatokat gyűjt a rendszerösszetevőkről, például az 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. Az ESET SysInspector használatának megismeréséhez tekintse meg az ESET SysInspectoronline súgót.

Az ESET SysInspector ablaka a következő információkat jeleníti meg a naplókról:

- **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:

- **Megjelenítés** – Megnyitja a kijelölt naplót az ESET SysInspector szolgáltatásban. A jobb gombbal kattinthat egy adott naplófájlra, és a helyi menüben választhatja a **Megjelenítés** parancsot.
- **Összehasonlítás** – Két meglévő napló összehasonlítása.
- **Létrehozás** – Új napló létrehozása. Várjon, amíg az ESET SysInspector létrejön (**Létrehozva** állapot), mielőtt megpróbálná megnyitni a naplót.
- **Törlés** – A kijelölt naplók eltávolítása a listából.

Ha legalább egy naplófájlt kijelöl, a helyi menüben az alábbi parancsok érhetők el:

- **Megjelenítés** – Megnyitja a kiválasztott naplót az ESET SysInspector alkalmazásban (ugyanezt az eredményt érheti el a naplóra duplán kattintva).
- **Összehasonlítás** – Két meglévő napló összehasonlítása.
- **Létrehozás** – Új napló létrehozása. Várjon, amíg az ESET SysInspector létrejön (**Létrehozva** állapot), mielőtt megpróbálná megnyitni a naplót.
- **Törlés** – A kijelölt naplók eltávolítása a listából.
- **Minden törlése** – Az összes napló törlése.
- **Exportálás** – A napló exportálása .xml vagy tömörített .xml fájlba. Az exportált napló a C:\ProgramData\ESET\ESET Security\SysInspector mappába kerül.

Feladatütemező

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

A Feladatütemező az ESET Internet Security fő programablakából érhető el az **Eszközök** > **További eszközök** > **Feladatütemező** elemre kattintva. A **Feladatütemező** valamennyi ütemezett feladat és beállított tulajdonságainak (például előre definiált dátum, időpont és ellenőrzési profil) összesített listáját tartalmazza.

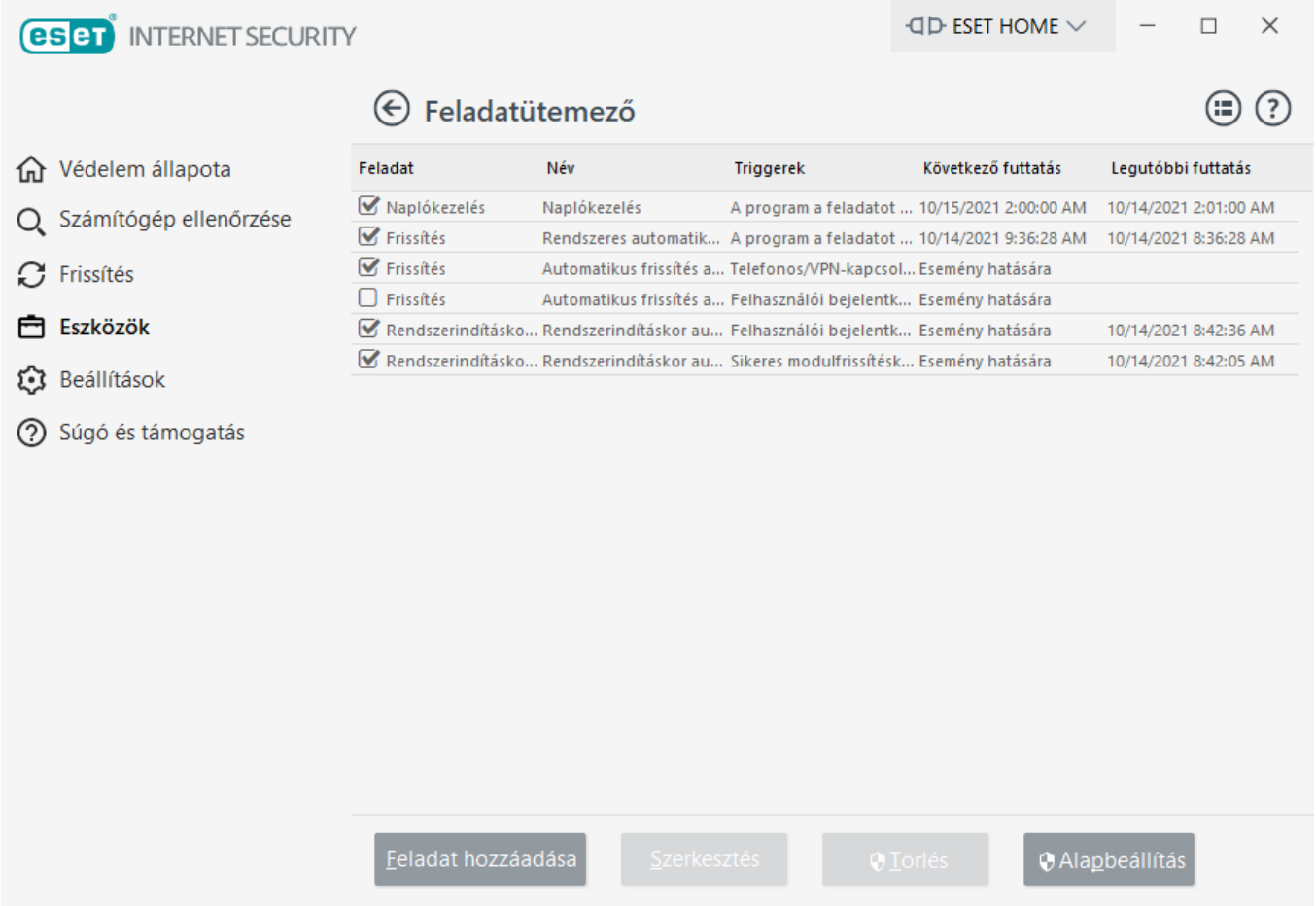
A feladatütemező a következő feladatok időzített végrehajtására alkalmas: modulok frissítése, ellenőrzési feladatok, rendszerindításkor automatikusan futtatott fájlok ellenőrzése és naplókezelés. A Feladatütemező főablakából közvetlenül hozzáadhat vagy törölhet feladatokat. (Kattintson az ablak alján lévő **Feladat hozzáadása** vagy **Törlés** gombra.) Az **Alapértelmezett** elemre kattintva alapértelmezettre állíthatja a beütemezett feladatokat, és törölheti az összes módosítást. 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**
- **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** (a felhasználó bejelentkezése után)
- **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** (a keresőmotor sikeres frissítésekor)

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



Új feladat hozzáadása

1. Kattintson az ablak alján található **Feladat hozzáadása** gombra.
2. Írja be a feladat nevét.
3. Jelölje ki a szükséges feladatot a legördülő listában:
   - **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. 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.

- **Kézi indítású számítógép-ellenőrzés** – Számítógép-ellenőrzés végrehajtása, amelynek során a számítógépen található fájlokat és mappákat vizsgálja meg a program.

- **Frissítés** – Frissítési feladat ütemezése a modulok frissítésére.

4. Kattintson az **Engedélyezve** szó melletti csúszkára, ha aktiválni szeretné a feladatot (ezt később az ütemezett feladatok listájában található jelölőnégyzet bejelölésével/jelölésének törlésével teheti meg), kattintson a **Tovább** gombra, és válasszon egyet az alábbi időzítési beállítások közül:

- **Egyszer** – A feladat az előre meghatározott napon és időben lesz végrehajtva.

- **Ismétlődően** – A feladat a meghatározott időközönként lesz végrehajtva.

- **Naponta** – A feladat minden nap a meghatározott időpontban fog futni.

- **Hetente** – A feladat a kijelölt napokon és időpontban fog futni.

- **Esemény hatására** – A feladat egy meghatározott eseményt követően lesz végrehajtva.

5. Válassza a **Feladat kihagyása akkumulátorról történő futtatáskor** lehetőséget, ha minimalizálni szeretné a rendszererőforrásokat, miközben a laptop akkumulátorról működik. A rendszer a feladatot a **Feladat végrehajtása** mezőkben megadott dátumon és időpontban fogja futtatni. Meghatározhatja, hogy mikor fusson a feladat, ha az előre meghatározott időben nem lehetett azt futtatni (például ki volt kapcsolva a számítógép). Választható lehetőségek:

- **A következő ütemezett időpontban**

- **Amint lehetséges**

- **Azonnal, ha a legutóbbi futtatás óta eltelt idő túllépi a megadott értéket (óra)** – A feladat első kihagyott futtatása óta eltelt időt jelöli. Ha elmúlik ez az időtartam, a feladat azonnal elindul. Állítsa be az időt az alábbi léptető segítségével.

Az ütemezett feladat áttekintéséhez kattintson a jobb gombbal, és válassza a **Feladat részleteinek megjelenítése** parancsot.



Ütemezett ellenőrzés beállításai

Ebben az ablakban adhat meg további beállításokat az ütemezett számítógép-ellenőrzési feladatokhoz.

Ha megtisztítás nélkül szeretne ellenőrzést futtatni, kattintson a **További beállítások** elemre, majd válassza ki a **Csak ellenőrzés megtisztítás nélkül** lehetőséget. Az ellenőrzési előzményeket a program az ellenőrzési naplóba menti.

Ha aktív a **Kivételek mellőzése** beállítás, akkor az olyan kiterjesztésű fájlok, amelyek korábban ki lettek hagyva az ellenőrzésből, most kivétel nélkül ellenőrizve lesznek.

A legördülő menüben megadhatja, hogy az ellenőrzés befejezését követően milyen műveletet végezzen el automatikusan a program:

- **Nincs művelet** – Az ellenőrzés befejezését követően nincs végrehajtandó művelet.
- **Leállítás** – A számítógép kikapcsolása egy ellenőrzés befejezését követően.
- **Újraindítás** – Az összes program bezárása és a számítógép újraindítása egy ellenőrzés befejezését követően.
- **Újraindítás szükség esetén** – A számítógép csak akkor indul újra, ha erre szükség van az észlelt kártevők megtisztításához.
- **Újraindítás kényszerítése** – Az összes nyitott program bezárásának kényszerítése a felhasználói interakcióra való várakozás nélkül és a számítógép újraindítása az ellenőrzés befejezése után.
- **Szükség esetén az újraindítás kényszerítése** – A számítógép csak akkor indul újra, ha erre szükség van az észlelt kártevők megtisztításához.
- **Alvó állapot** – A munkamenet mentése és a számítógép alacsony energiájú állapotba állítása, hogy gyorsan folytathassa a munkát.
- **Hibernálás** – Mindent, ami a RAM-on fut, áthelyez egy adott fájlba a merevlemezen. A számítógép kikapcsol, de a legközelebbi indításakor az előző állapotot állítja vissza.

Az **Alvás** vagy **Hibernálás** művelet elérhetősége a számítógép operációs rendszerének Bekapcsolás és alvó állapot beállításaitól, illetve a számítógép/laptop funkcióitól függ. Vegye figyelembe, hogy az alvó állapotú számítógép továbbra is egy működő számítógép. Az alapfunkciók akkor is futnak és elektromos áramot használnak, amikor a számítógép csökkentett energiával működik. Az akkumulátor üzemidejének meghosszabbításához (például az irodán kívüli utazás esetén) javasoljuk, hogy használja a Hibernálás lehetőséget.

Az ellenőrzés nem szakítható meg lehetőséget kiválasztva megakadályozhatja, hogy a nem jogosult felhasználók leállítsák az ellenőrzés után végzett műveleteket.

Válassza **A felhasználó felfüggesztheti az ellenőrzést ennyi időre (perc)** beállítást, ha engedélyezni szeretné, hogy a korlátozott felhasználó szüneteltesse a számítógép ellenőrzését a megadott időszakra.

Lásd még: Az ellenőrzés folyamata.

Ütemezett feladat áttekintése

Ez a párbeszédpanel részletes információkat jelenít meg a kijelölt ütemezett feladatról, amikor duplán egy egyéni feladatra kattint, illetve amikor a jobb gombbal egy egyéni feladatra kattint, majd a **Feladat részleteinek megjelenítése** parancsot választja.

Feladat részletei

Írja be a **feladat nevét**, válassza ki a **feladattípust**, majd kattintson a **Tovább** gombra:

- **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. 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.
- **Kézi indítású számítógép-ellenőrzés** – Számítógép-ellenőrzés végrehajtása, amelynek során a számítógépen található fájlokat és mappákat vizsgálja meg a program.
- **Frissítés** – Frissítési feladat ütemezése a modulok frissítésére.

Feladat időzítése

A feladat a meghatározott időközönként lesz végrehajtva. Válasszon az alábbi 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 mindennap 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 eseményt követően lesz végrehajtva.

Feladat kihagyása akkumulátorról történő futtatáskor – A feladat végrehajtása nem kezdődik meg, ha az ütemezett időpontban a számítógép akkumulátorról működik. Ez a szünetmentes tápegységről működő számítógépekre is vonatkozik.

Feladat időzítése – Egyszer

Feladat végrehajtása – A megadott feladat futtatására csak egyszer, a megadott napon és időpontban kerül sor.

Feladat időzítése – Naponta

A feladat mindennap a meghatározott időpontban fog futni.

Feladat időzítése – Hetente

A feladat minden héten többször fog futni a kiválasztott napokon és időpontban.

Feladat időzítése – Esemény hatására

A feladat a következő esetekben lesz végrehajtva:

- **Minden számítógép-indításkor**
- **Minden nap az első számítógép-indításkor**
- **A telefonos internet/VPN-kapcsolat létrejöttekor**
- **Sikeres modulfrissítéskor**
- **Sikeres termékfrissítéskor**
- **Felhasználói bejelentkezéskor**
- **Fertőzés észlelésekor**

Ha eseményhez köti egy feladat végrehajtását, akkor megadhat egy minimális időszakot a feladat két végrehajtása között. Ha például egy nap sokszor jelentkezik be a számítógépre, akkor válasszon 24 órás időszakot. Így a feladat egy napon csak az első bejelentkezéskor lesz végrehajtva, legközelebb pedig a következő napon.

Kihagyott feladat

A program kihagyja a feladatot, ha a számítógép akkumulátorról működik vagy ki van kapcsolva. A beállítások egyikét választva adja meg, hogy a kihagyott feladatnak mikor kell futnia, majd kattintson a **Tovább** gombra:

- **A következő ütemezett időpontban** – A feladat akkor fog futni, ha a számítógép be van kapcsolva a következő ütemezett időpontban.
- **Amint lehetséges** – A feladat akkor fog futni, amikor a számítógép be van kapcsolva.
- **Azonnal, ha az utolsó ütemezett futtatás óta eltelt idő meghaladja az alábbi értéket (órában)** – A feladat első kihagyott futtatása óta eltelt időt jelöli. Ha elmúlik ez az időtartam, a feladat azonnal elindul.

Azonnal, ha az utolsó ütemezett futtatás óta eltelt idő meghaladja az alábbi értéket (órában) – példák

Egy példafeladat úgy van beállítva, hogy óránként ismételten fusson. Az **Azonnal, ha az utolsó ütemezett futtatás óta eltelt idő meghaladja az alábbi értéket (órában)** beállítás ki van választva, és a túllépési idő két órára van állítva. A feladat 13:00 órakor fut, és amikor befejeződött, a számítógép alvó állapotba lép:

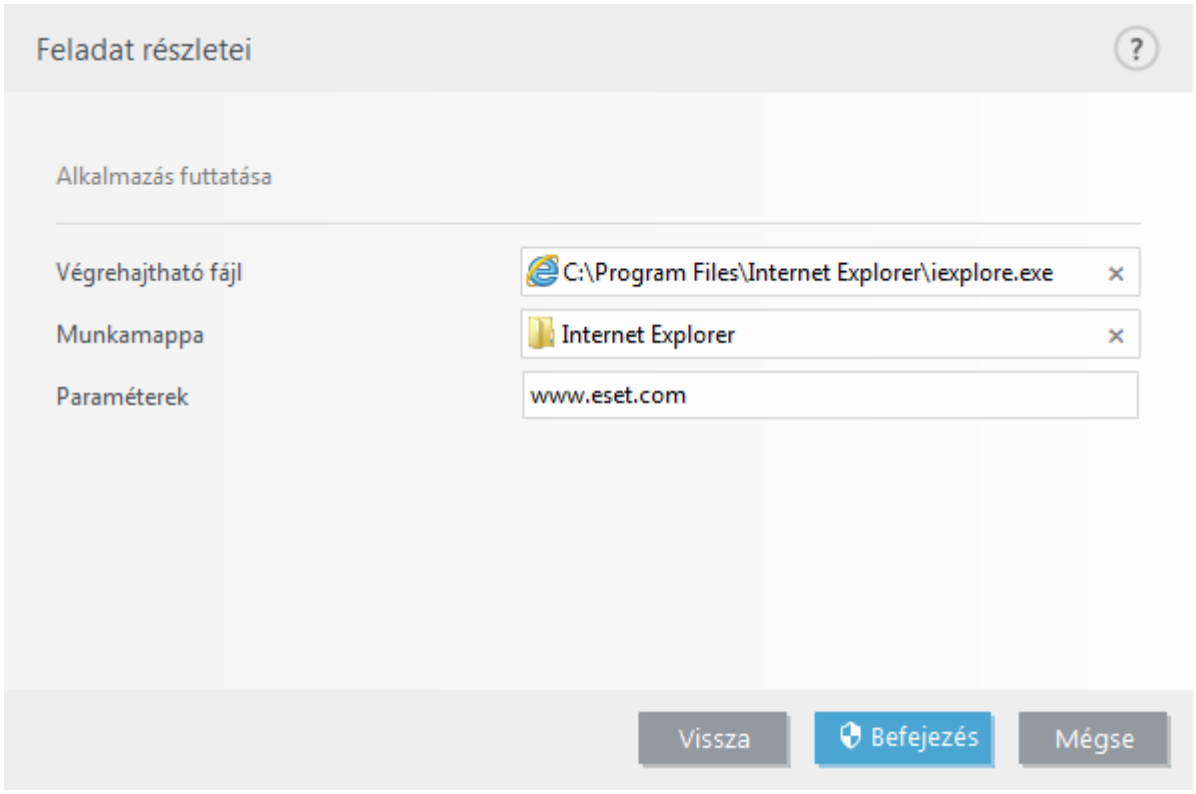
- A számítógép 15:30 órakor felébred. A feladat első kihagyott futtatása 14:00 órakor volt. Csak 1,5 óra telt el 14:00 óra óta, így a feladat 16:00 órakor fog futni.
- A számítógép 16:30 órakor felébred. A feladat első kihagyott futtatása 14:00 órakor volt. Két és fél óra telt el 14:00 óra óta, így a feladat azonnal elindul.

Feladat részletei – Frissítés

Ha a programot két frissítési szerverről szeretné frissíteni, akkor két különböző frissítési profilt kell létrehozni. Ha az első nem tudja letölteni a frissítési fájlokat, a program automatikusan átvált az alternatív szerverre. Ez használható például hordozható számítógépekhez, amelyek frissítése általában helyi hálózati frissítési szerverről történik, tulajdonosaik azonban gyakran más hálózatokat használva kapcsolódnak az internethez. Így ha az első profil sikertelen, a második automatikusan letölti a frissítési fájlokat az ESET frissítési szervereiről.

Feladat részletei – Alkalmazás futtatása

Ezzel a feladattal egy külső alkalmazás végrehajtásának ütemezése adható meg.



Alkalmazás – Ebben a mezőben adhatja meg a futtatandó programot teljes elérési útjával. A mező melletti **Tallózás** gombra kattintva ki is jelölheti a fájlt.

Munkamappa – Ebben a mezőben az alkalmazás által használt mappa adható meg. Az **Alkalmazás** mezőben megadott program által létrehozott ideiglenes fájlok ebben a mappában fognak létrejönni.

Paraméterek – A választott program parancssori paraméterei (nem kötelező megadni).

A feladat alkalmazásához kattintson a **Befejezés** gombra.

Rendszertisztító

A Rendszertisztító eszközzel használható állapotba állíthatja vissza a számítógépet, miután megtisztította a kártevőtől. A kártevők képesek letiltani a rendszersegédprogramokat, például a beállításszerkesztőt, a feladatkezelőt, a Windows-frissítéseket. A rendszertisztítóval egy kattintással visszaállíthatók az alapértelmezett értékek és beállítások egy adott rendszer esetén.

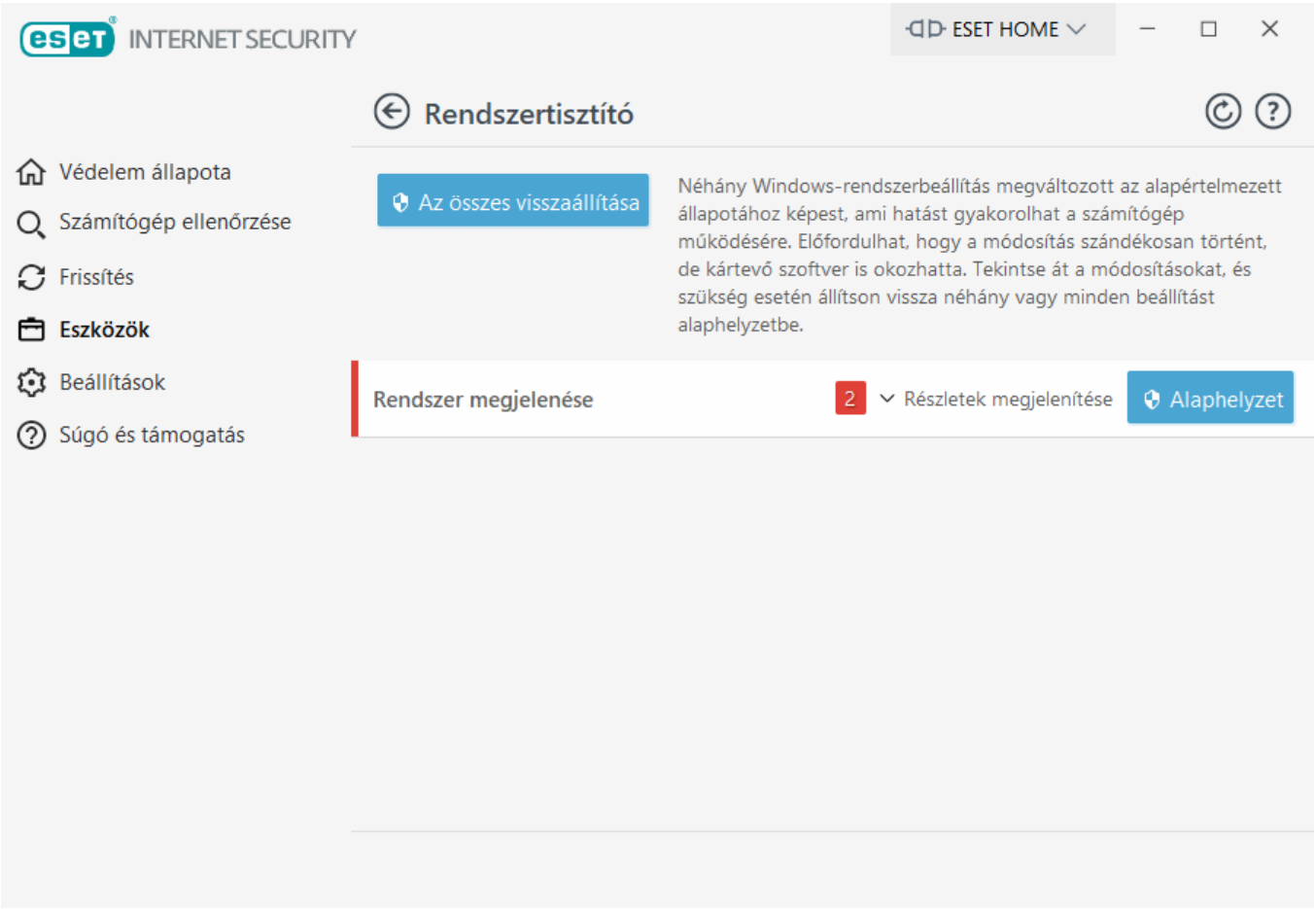
A rendszertisztító öt beállításkategória szerint jelzi a problémákat:

- **Biztonsági beállítások**: ha úgy módosultak a beállítások, hogy az veszélyezteti a számítógépet, például a Windows Update módosítása miatt.
- **Rendszerbeállítások**: a számítógép működését, többek között a fájltársításokat módosító beállítások.
- **Rendszer megjelenése**: a rendszer megjelenését, többek között az asztal háttérképét módosító beállítások.
- **Letiltott funkciók**: letiltható fontos funkciók és alkalmazások.
- **Windows Rendszer-visszaállítás**: a rendszer korábbi állapotának visszaállítására szolgáló Windows Rendszer-visszaállítás funkció beállításai.

Rendszertisztítás kérhető:

- amikor a rendszer kártevőt talál;
- amikor a felhasználó az **Alaphelyzet** gombra kattint.

Áttekintheti a módosításokat, és szükség esetén visszaállíthatja a beállításokat.



A Rendszertisztítóban csak rendszergazdai jogosultsággal rendelkező felhasználók hajthatnak végre műveleteket.

ESET SysRescue Live

Az ESET SysRescue Live egy ingyenes segédprogram, amellyel rendszerindításra alkalmas biztonsági CD/DVD-lemez, illetve USB-meghajtó hozható létre. A biztonsági adathordozóról fertőzött számítógépet indíthat, és így megkeresheti a kártevőt, és megtisztíthatja a fertőzött fájlokat.

Az ESET SysRescue Live fő előnye abban rejlik, hogy az operációs rendszertől függetlenül fut, de közvetlen hozzáféréssel rendelkezik a lemezhez és a fájlrendszerhez. Ennek köszönhetően eltávolíthatók a normál működési feltételek mellett (például az operációs rendszer futásakor) nem törölhető kártevők.

- Az ESET SysRescue Live online súgója

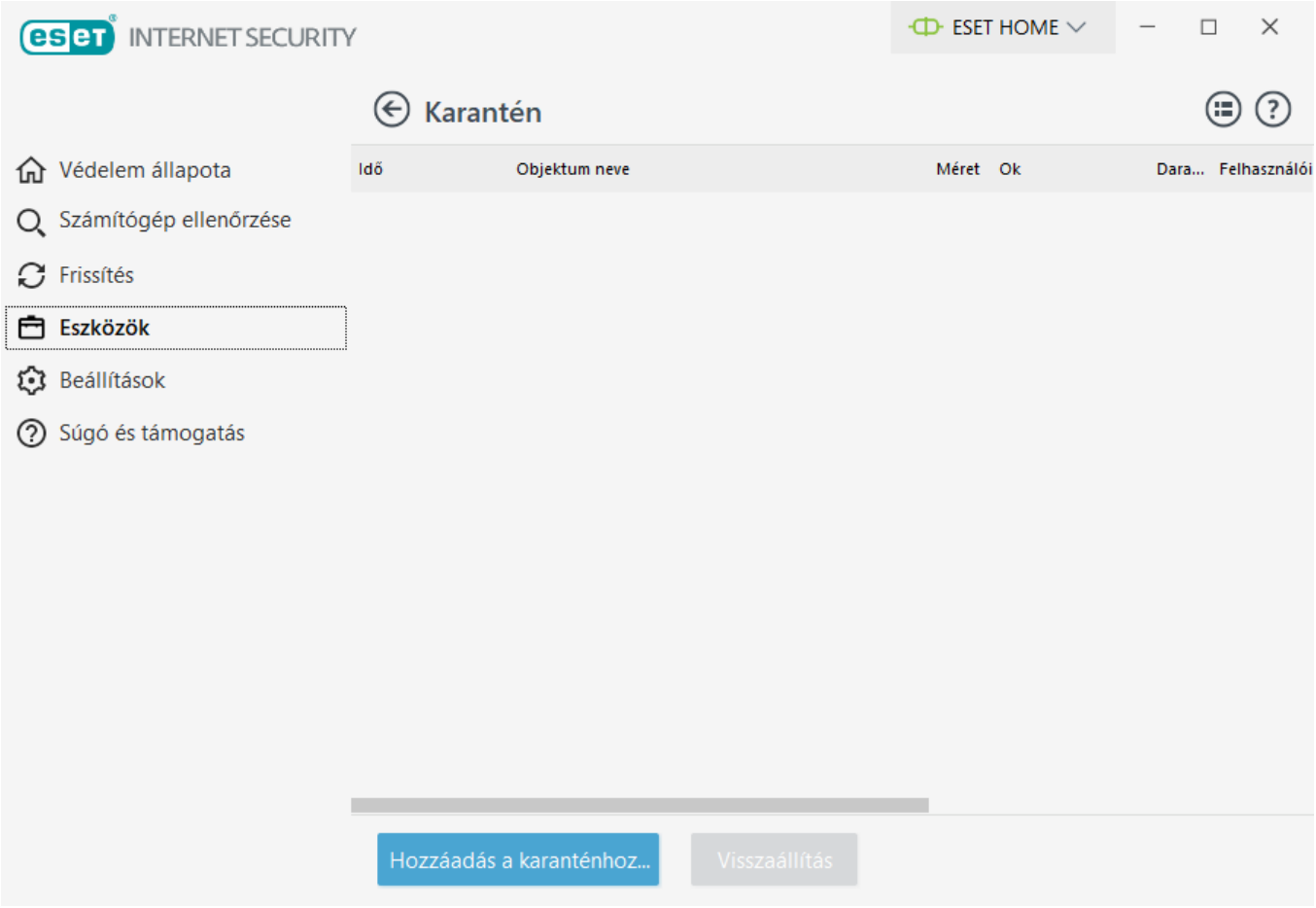
Karantén

A karantén fő funkciója a jelentett objektumok (például kártevő, fertőzött fájlok vagy kéretlen alkalmazások) biztonságos tárolása.

A karantén az ESET Internet Security fő programablakából érhető el az **Eszközök** > **További eszközök** > **Karantén** elemre kattintva.

A karanténmappában lévő fájlokat egy táblázat jeleníti meg, amelyben a következők láthatók:

- a karantén dátuma és időpontja,
- a fájl eredeti helyére vezető útvonal,
- a mérete bájtban,
- ok (például felhasználó által hozzáadott objektum),
- észlelések száma (például egy fájl dupla észlelése, vagy ha több fertőzést tartalmazó archívum).



Fájlok karanténba helyezése

Az ESET Internet Security automatikusan karanténba helyezi a fájlokat (ha nem tiltotta le ezt a funkciót a riasztási ablakban).

További fájlokat akkor kell karanténba helyezni, ha:

a.nem tisztíthatók meg,

b.ha a törlésük nem biztonságos vagy tanácsos,

c.ha tévesen észlelte őket az ESET Internet Security,

d.ha egy fájl viselkedése gyanús, a víruskereső azonban nem észleli.

A fájlok karanténba helyezésére több lehetőség is van:

a.A húzás funkcióval manuálisan helyezheti karanténba a fájlt: kattintson a fájlra, vigye az egérmutatót a megjelölt területre, miközben nyomva tartja az egér gombját, majd engedje fel. Ezután az alkalmazás az előtérbe kerül.

b.Kattintson a jobb gombbal a fájlra > kattintson a **További beállítások** > **Fájl karanténba helyezése** elemre.

c.Kattintson a **Hozzáadás a karanténhoz** gombra a **Karantén** ablakban.

d.A művelet a helyi menüből is végrehajtható: kattintson a jobb gombbal a **Karantén** ablakra, majd válassza ki a **Karantén** lehetőséget.

Visszaállítás a karanténból

A karanténba helyezett fájlok vissza is állíthatók az eredeti helyükre:

- Erre használja a **Visszaállítás** funkciót, amely a helyi menüből érhető el, azután hogy jobb gombbal az adott fájlra kattintott a Karanténban.

- Ha a fájl kéretlen alkalmazásként van megjelölve, akkor kiválasztható a **Visszaállítás és kizárás az ellenőrzésből** lehetőség. Lásd a Kivételek című részt is.

- A helyi menüben megtalálható a **Visszaállítás megadott helyre** menüpont is, mellyel a törlés helyétől különböző mappába is visszaállíthatók a fájlok.

- A visszaállítási funkció nem áll rendelkezésre bizonyos esetekben, például írásvédett hálózati megosztáson található fájlok esetén.

Törlés a karanténból

Kattintson a jobb gombbal egy adott elemen, és válassza a **Törlés a karanténból** parancsot, vagy jelölje ki a törlendő elemet, és a billentyűzeten nyomja le a **Delete** billentyűt. Kijelölhet és egyszerre törölhet több elemet is. A törölt elemek véglegesen törlődnek az eszközről és a karanténból.

Fájl elküldése a karanténból

Ha karanténba helyezett 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 helyezte, küldje el a fájlt az ESET kutatólaborjába. A fájl elküldéséhez kattintson a jobb gombbal a fájlra, majd kattintson a **Elemzésre küldés** menüpontra a helyi menüben.

Észlelt elem leírása

Kattintson a jobb gombbal a kívánt elemre, majd az **Észlelt elem leírása** szövegre kattintva nyissa meg az ESET Threat Encyclopedia programot, amely részletes információkat tartalmaz a rögzített beszivárgás veszélyeiről és tüneteiről.

Ábrákkal ellátott útmutató
Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
- Karanténba helyezett fájl visszaállítása az ESET Internet Security alkalmazásban
- Karanténba helyezett fájl törlése az ESET Internet Security alkalmazásban
- Az ESET-termékem észlelésről értesített – mit tegyek?

A karanténba helyezés sikertelen

Okok, amelyek miatt bizonyos fájlok nem helyezhetők a karanténba:

- **Nincs olvasási jogosultsága** – ezt azt jelenti, hogy nem tekintheti meg a fájl tartalmát.
- **Nincs írási jogosultsága** – ezt azt jelenti, hogy nem módosíthatja a fájl tartalmát, azaz nem adhat hozzá új tartalmat, illetve nem törölheti a meglévő tartalmat.
- **Túl nagy a fájl, amelyet a karanténba próbál helyezni** – csökkenteni kell a fájl méretét.

Amikor „A karanténba helyezés sikertelen” hibaüzenet jelenik meg, kattintson a **További információk** elemre. Megjelenik a Karantén hibalista ablak, ahol látható a fájl neve és az az ok, amiért nem lehet karanténba helyezni a fájlt.

Proxyszerver

Nagy méretű LAN-hálózatokon a számítógép és az internet közötti kommunikáció egy proxyszerveren keresztül folyhat. E készülék használata meg kell adni az alábbi beállításokat. Különben előfordulhat, hogy a program nem frissül majd. Az ESET Internet 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 Internet Security összes globális proxyszerver-beállítását meghatározza. Az itt található paramétereket fogja használja az internetkapcsolatot igénylő összes modul.

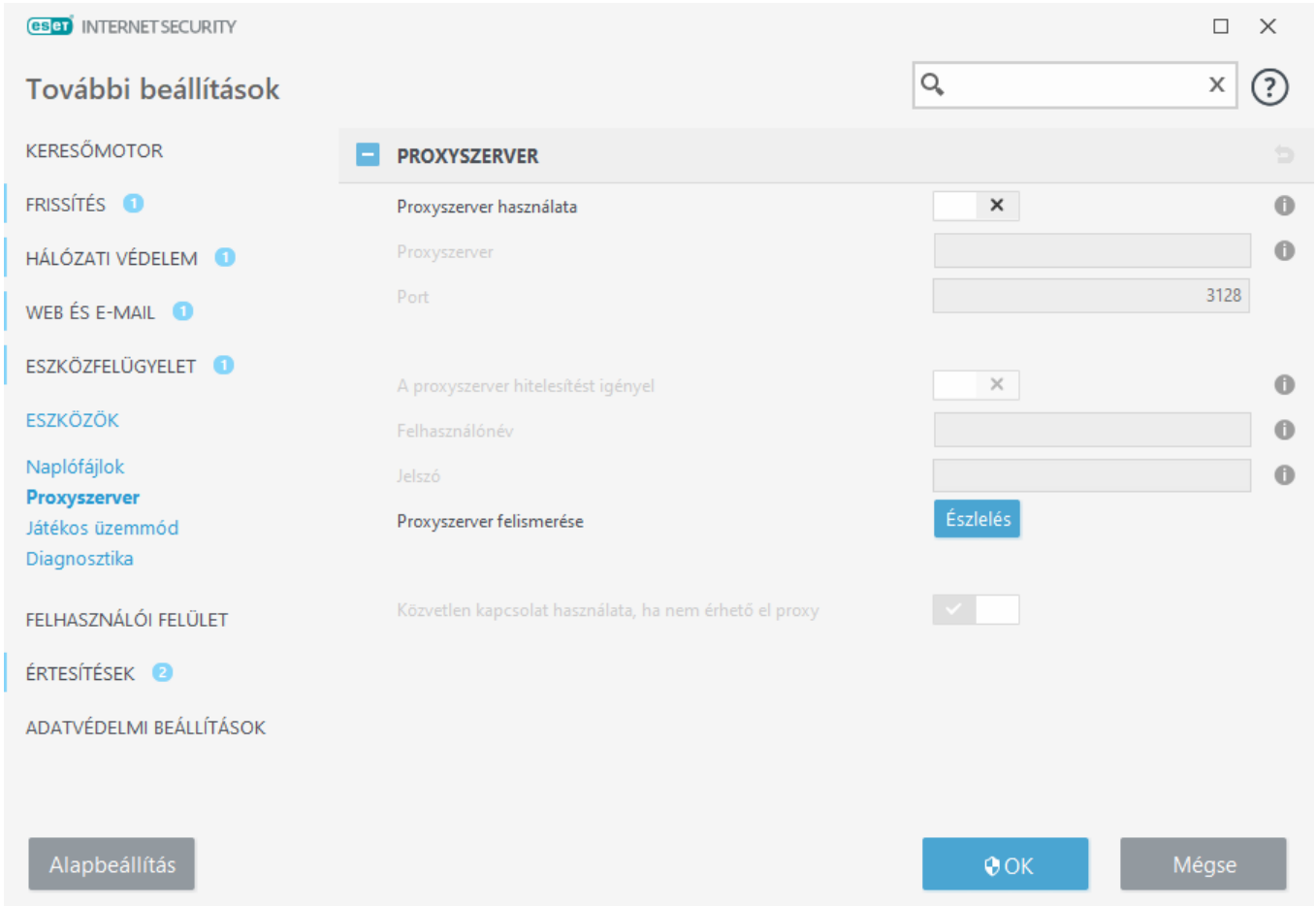
A proxyszerver ehhez a szinthez tartozó beállításainak megadásához válassza a **Proxyszerver használata** opciót, majd írja be a proxyszerver címét a **Proxyszerver** mezőbe, a portszámot pedig a **Port** mezőbe.

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

Felhasználónevét és jelszavát manuálisan kell megadnia a **Proxyszerver** beállításai között.

Közvetlen kapcsolat használata, ha nem érhető el proxy – Ha az ESET Internet Security proxy használatára van konfigurálva, és a proxy nem érhető el, az ESET Internet Security kihagyja a proxyt, és közvetlenül az ESET-szerverekkel kommunikál.

A proxyszerver-beállítások létrehozhatók a további frissítési beállításokban is (a **További beállítások** > **Frissítés** > **Profilok** > **Frissítések** > **Kapcsolódási beállítások** lapon válassza ki a **Kapcsolódás proxyszerveren keresztül** menüpontot a **Proxy mód** legördülő menüben). Ez a beállítás adott frissítési profilra vonatkozik és laptopok esetén javasolt, mivel azok a vírusdefiníciós adatbázis frissítéseit gyakran távoli helyekről kapják. Erről a beállításról a További frissítési beállítások című témakörben talál további információt.



Minta kiválasztása elemzésre

Ha gyanús fájlt talál a számítógépen, vagy gyanús webhellyel találkozik az interneten, elküldheti az ESET kutatólaborjába elemzésre (az ESET LiveGrid® konfigurációjától függ, hogy erre van-e lehetőség).

Mielőtt leadna mintákat az ESET-nek

Ne küldjön be mintát, ha az nem felel meg legalább egy feltételnek a következők közül:

- Az ESET-termék egyáltalán nem észleli a mintát
- A program tévesen kártevőként észlelte a mintát
- Nem fogadjuk el a személyes fájlokat (amelyek esetén azt szeretné, hogy vizsgálja meg őket az ESET) mintaként (az ESET kutatólaborja nem hajt végre egyéni ellenőrzést a felhasználók számára)
- A levél tárgysorában jelezze röviden a problémát, a levélben pedig adjon meg minél több információt a fájlról (például mellékeljen képernyőfotót vagy annak a webhelynek a címét, ahonnan letöltötte).

A következő módszerekkel küldheti el a mintát (fájlt vagy webhelyet) az ESET-nek elemzésre:

1. A termékben található, minták leadására szolgáló űrlap használata: az **Eszközök** > > **További eszközök** > **Minta elküldése elemzésre** lapon található. A beküldött minta maximális mérete 256 MB.

2. A fájlt e-mailben is elküldheti. Ha inkább ezt a megoldást választja, tömörítse a fájlt WinRAR/WinZIP tömörítővel, lássa el az „infected” jelszóval a tömörített fájlt, majd küldje el a samples@eset.com címre.

3. Levélszemét, tévesen levélszemétnek észlelt elemek, illetve a Szülői felügyelet modul által helytelenül kategorizált webhelyek bejelentéséhez ez az ESET-tudásbáziscikk nyújt segítséget.

A **Minta kiválasztása elemzésre** nevű űrlapon válassza ki a megfelelő leírást **A minta elküldésének oka** legördülő menüben:

- Gyanús fájl
- Gyanús webhely (valamilyen kártevővel fertőzött webhely),
- Tévesen jelentett webhely
- Tévesen jelentett fájl (fertőzöttként észlelt, de nem fertőzött fájl)
- Egyéb

Fájl/Webhely – A beküldeni kívánt fájl vagy webhely elérési útja.

E-mail cím – A megadott e-mail-címet a program a gyanús fájlokkal együtt küldi el az ESET-nek. Ezen a címen az ESET kapcsolatba is léphet a felhasználóval, ha az elemzéshez további adatokra van szükség. Az e-mail cím megadása nem kötelező. Válassza ki az **Elküldés névtelenül** lehetőséget, ha nem szeretné megadni.

> **Előfordulhat, hogy az ESET nem ad választ**
> Az ESET csak akkor válaszol, ha további információkra van szüksége. Szervereink fájlok tízezreit fogadják nap mint nap, így nem tudunk válaszolni minden egyes üzenetre.
> Ha a minta valóban egy kártékony alkalmazás vagy webhely, bekerül a vírusdefiníciós adatbázis valamelyik későbbi ESET-frissítésébe.

Minta kiválasztása elemzésre – Gyanús fájl

Kártevőfertőzés észlelt jelei és tünetei – Adja meg a gyanús fájl számítógépen észlelt viselkedésének leírását.

Fájl eredete (URL-cím vagy gyártó) – Adja meg a fájl eredetét (forrását), és azt is, hogy hogyan talált rá.

Megjegyzések és további információk – Itt olyan kiegészítő információt, illetve leírást adhat meg, amely segítheti a gyanús fájl azonosításának feldolgozását.

> A **Kártevőfertőzés észlelt jelei és tünetei** első paraméter megadása kötelező, a további információk pedig jelentős segítséget nyújthatnak laboratóriumainknak a minták azonosításában és feldolgozásában.

Minta kiválasztása elemzésre – Gyanús webhely

Válasszon legalább egy okot a **Mi a probléma a webhellyel?** legördülő menüben:

- **Fertőzött** – Különféle módokon terjesztett vírusokat vagy más kártevőket tartalmazó webhely.
- **Adathalászat** – Gyakran bizalmas adatok, többek között bankszámlaszámok, PIN kódok vagy más adatok megszerzésére irányul. Erről a támadástípusról további információt a szószedetben olvashat.
- **Csalás** – Csalás vagy félrevezetés céljából, főleg gyors profitszerzés érdekében készült webhely.
- Válassza az **Egyéb** lehetőséget, ha a fenti beállítások egyike sem felel meg az elküldendő webhelynek.

Megjegyzések és további információk – Itt olyan kiegészítő információt, illetve leírást adhat meg, amely segítheti a gyanús webhely elemzését.

Minta kiválasztása elemzésre – Tévesen jelentett fájl

Kérjük, küldje el a fertőzöttként észlelt, de nem fertőzött fájlokat, hogy továbbfejleszthessük a vírus- és kémprogramvédelmi motorunkat, hogy a segítségével biztosíthassuk a felhasználók védelmét. Téves riasztások (TR) olyankor fordulhatnak elő, ha egy fájl mintája megegyezik a keresőmotorban tárolt minták valamelyikével.

Alkalmazás neve és verziója – Adja meg a program nevét és verzióját (például a számát, alternatív nevét vagy kódnevét).

Fájl eredete (URL-cím vagy gyártó) – Adja meg a fájl eredetét (forrását), és azt is, hogyan talált rá.

Alkalmazás célja – Az alkalmazás általános ismertetése, típusa (például böngésző, médialejátszó stb.), illetve funkcióinak összefoglalása.

Megjegyzések és további információk – Itt olyan kiegészítő információt, illetve leírást adhat meg, amely segítheti a gyanús fájl feldolgozását.

> Az első három paramétert a jogszerű alkalmazások azonosítása, illetve a kártékony kódoktól való megkülönböztetése érdekében feltétlenül meg kell adni. Minden további információ jelentős segítséget nyújthat laboratóriumainknak a minták azonosításában és feldolgozásában.

Minta kiválasztása elemzésre – Tévesen jelentett webhely

Kérjük, küldje el azoknak a webhelyeknek a címét, amelyekről azt észlelte, hogy fertőzöttek, csalásra vagy adathalászatra készültek, de nem azok. Téves riasztások (TR) olyankor fordulhatnak elő, ha egy fájl mintája megegyezik a keresőmotorban tárolt minták valamelyikével. Kérjük, adja meg ezt a webhelyet, hogy továbbfejleszthessük vírus- és kémprogramvédelmi motorunkat, és a segítségével biztosíthassuk a felhasználók védelmét.

Megjegyzések és további információk – Itt olyan kiegészítő információt, illetve leírást adhat meg, amely segítheti a gyanús webhely feldolgozását.

Minta kiválasztása elemzésre – Egyéb

Ezt az űrlapot akkor használja, ha a fájl nem tartozik sem a **Gyanús fájl**, sem a **Téves riasztás** kategóriába.

A fájl elküldésének oka – Itt részletes leírást és a fájl elküldésének az okát adhatja meg.

Microsoft Windows® frissítés

A Windows frissítés 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 Internet 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.

Párbeszédablak – Rendszerfrissítések

Ha rendelkezésre állnak frissítések az operációs rendszerhez, az ESET Internet Security kezdőablaka megjeleníti az értesítést. A **További információ** gombra kattintva nyissa meg az Operációsrendszer-frissítések ablakot.

Az Operációsrendszer-frissítések ablakban látható a letöltéshez és telepítéshez elérhető frissítések listája. A frissítés típusa a frissítés neve mellett látható.

Egy tetszőleges frissítésre duplán kattintva megjelenítheti a további információkat tartalmazó Frissítési információk ablakot.

Kattintson az **Operációsrendszer-frissítés futtatása** gombra az operációsrendszer-frissítések letöltéséhez és telepítéséhez.

Frissítési információk

Információk a Windows frissítéseiről. A frissítés neve és száma, ezt követően a prioritása és a frissítés által megoldott probléma leírása az ablak tetején látható.

Felhasználói felület

A grafikus felhasználói felület (GUI) viselkedésének konfigurálásához a program főablakában kattintson a **Beállítások** > **További beállítások** (F5) > **Felhasználói felület** elemre.

A Felhasználói felület elemei További beállítások képernyőn módosíthatja a program vizuális megjelenését és a használt hatásokat.

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

> A rendszerértesítések, az észlelési figyelmeztetések és alkalmazásállapotok viselkedésének konfigurálásáról az Értesítések című részben tájékozódhat.

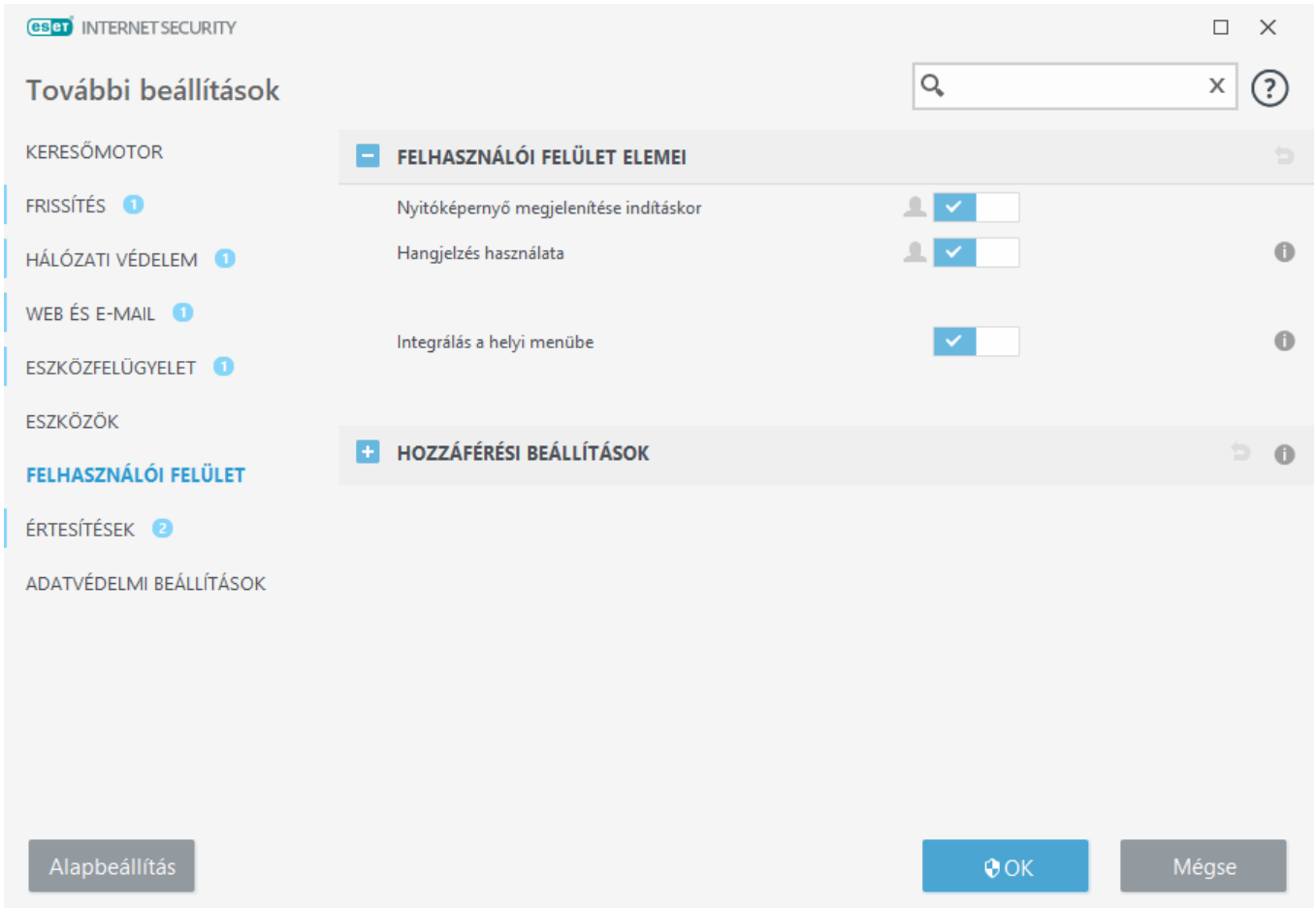
Felhasználói felület elemei

Az ESET Internet Security felhasználói felületének beállításai lehetővé teszik, hogy a felhasználó a saját igényei szerint alakítsa ki munkakörnyezetét. Ezek a beállítások a **További beállítások** (F5) > **Felhasználói felület** > **Felhasználói felület elemei** csomópontban érhetők el.

Az ESET Internet Security nyitóképernyőjének letiltásához törölje a **Nyitóképernyő megjelenítése indításkor** jelölőnégyzet bejelölését.

Hangjelzés használata – Az ESET Internet Security hanggal jelzi az ellenőrzések során bekövetkező fontos eseményeket, például egy kártevő felismerését vagy az ellenőrzés befejezését.

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



Hozzáférési beállítások

Az ESET Internet Security beállításai biztonsági házirendje lényeges részét képezik. A jogosulatlan módosítások veszélyeztethetik a rendszer stabilitását és védelmét. A jogosulatlan módosítások elkerülése érdekében az ESET Internet Security beállításai paraméterei és eltávolítása jelszóval védhető.

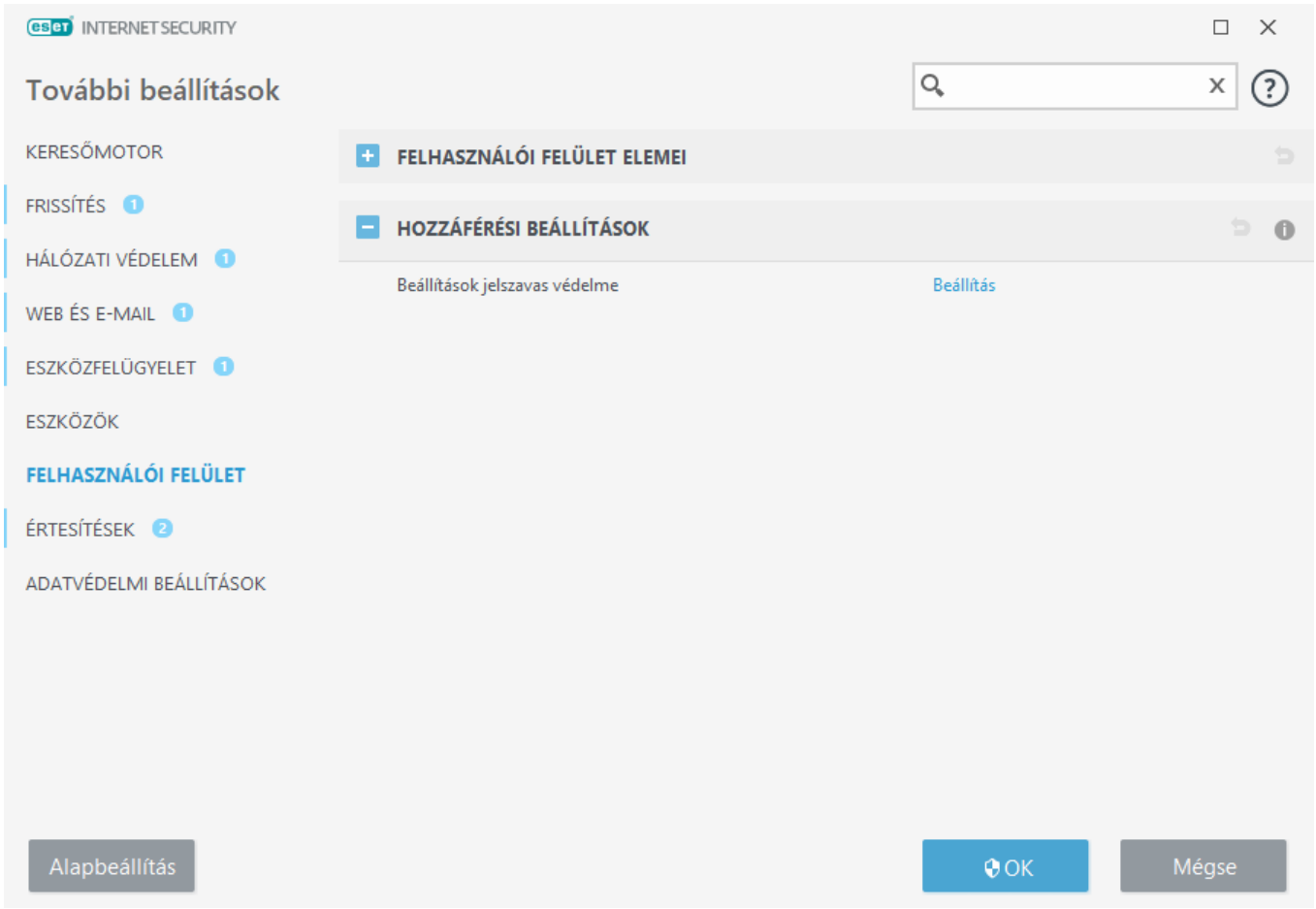
Az ESET Internet Security beállítási paramétereinek és eltávolításának védelmére szolgáló jelszó megadásához kattintson a **Beállítás** elemre a **Beállítások jelszavas védelme** felirat mellett.

Amikor használni szeretné a védett További beállítások funkciót, megjelenik a jelszó beírására szolgáló ablak. Ha elfelejti vagy elveszíti a jelszót, kattintson lent a **Jelszó visszaállítása** elemre, majd adja meg a licenc regisztrálásához használt e-mail-címet. Az ESET ekkor küld Önnek e-mailt, amelyben megtalálható az ellenőrző kód és a jelszó visszaállításának útmutatója.

- A További beállítások feloldása

A jelszó módosításához kattintson a **Jelszó módosítása** elemre a **Beállítások jelszavas védelme** felirat mellett.

A jelszó eltávolításához kattintson az **Eltávolítás** elemre a **Beállítások jelszavas védelme** felirat mellett.



Jelszó a További beállításokhoz

Ha az ESET Internet Security további beállításait szeretné megvédeni a jogosulatlan módosítások ellen, adjon meg egy új jelszót.

Ha módosítani szeretné a meglévő jelszót:

1. Írja be a régi jelszót a **Régi jelszó** mezőbe.
2. Adja meg az új jelszót az **Új jelszó** és a **Jelszó megerősítése** mezőben.
3. Kattintson az **OK** gombra.

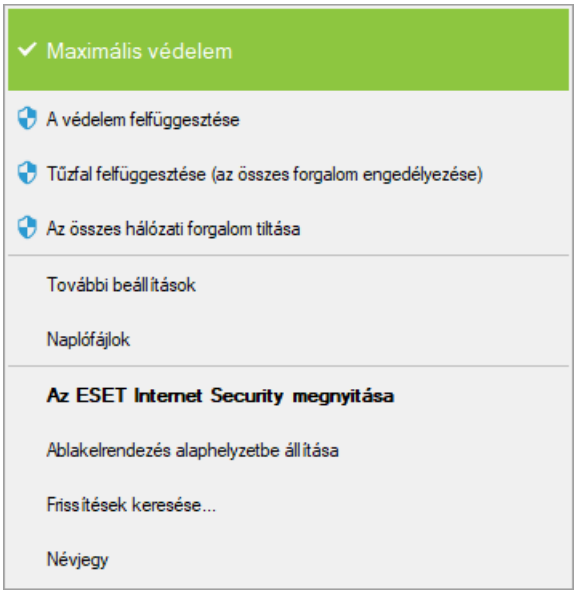
A jelszóra mindig szükség lesz az ESET Internet Security módosításakor.

Ha elfelejti a jelszavát, a „Jelszó visszaállítása” módszer segítségével ismét hozzáférhet a további beállításokhoz.

Az elveszett ESET-licenckulcs, a licenc lejárati dátumának vagy egyéb licencinformációk visszaszerzéséhez ESET Internet Security olvassa el ezt a tudásbáziscikkünket.

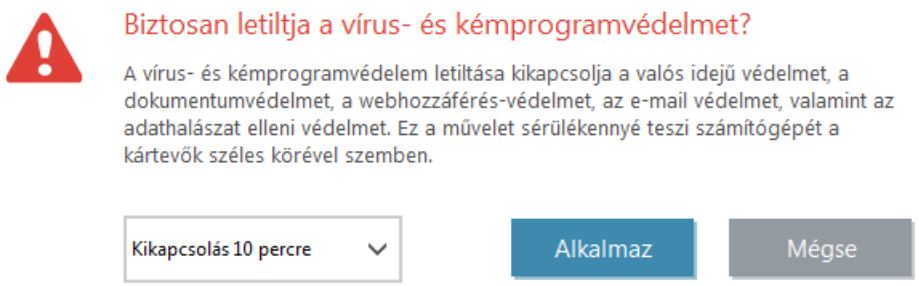
A rendszer tálcaikonja

A legfontosabb beállítási lehetőségek és funkciók a rendszertálca ikonjára a jobb gombbal kattintva érhetők el.



A védelem ideiglenes kikapcsolása – Megjeleníti a fájlok, a webes tevékenységek és az elektronikus levelezés felügyeletén keresztül a rendszert a kártékony rendszertámadásoktól védő Keresőmotor funkciót letiltó megerősítési párbeszédpanelt.

Az **Időpont** legördülő listában adhatja meg, hogy milyen időtartamra szeretné letiltani a védelmet.



Tűzfal felfüggesztése (az összes forgalom engedélyezése) – A tűzfal inaktív állapotba kapcsolása. További információt a Hálózat című témakörben talál.

Minden forgalom tiltása – Az összes hálózati forgalom tiltása. Az újbóli engedélyezéshez kattintson **Az összes hálózati forgalom tiltásának megszüntetése** elemre.

További beállítások – Ezt a lehetőséget választva megnyithatja a **További beállítások** fát. A párbeszédpanel másképp is megnyitható, például az F5 billentyű lenyomásával, illetve a **Beállítások** > **További beállítások** lehetőségre kattintva.

Naplófájlok – A naplófájlok tájékoztatást nyújtanak a programban bekövetkezett fontos eseményekről, illetve az észlelt veszélyekről.

Az ESET Internet Security megnyitása – Megnyílik az ESET Internet Security fő programablaka a tálcaikonról.

Ablakelrendezés alaphelyzetbe állítása – Az ESET Internet Security ablakának visszaállítása az eredeti méretére és eredeti pozíciójába a képernyőn.

Frissítések keresése – Elindítja a keresőmotor (korábbi nevén vírusdefiníciós adatbázis) frissítését, és így biztosítja a kártékony kódok elleni védelmi szintet.

Névjegy – Rendszerinformációk megjelenítése, köztük az ESET Internet Security telepített verziójának számával és

a telepített programmodulok adataival. Itt megtalálható a licenc lejárati dátuma, valamint az operációs rendszerre és a rendszererőforrásokra vonatkozó információk.

Képernyőolvasók támogatása

Az ESET Internet Security képernyőolvasókkal együtt is használható, így látássérült ESET-felhasználók is egyszerűen navigálhatnak a termékben, illetve konfigurálhatnak beállításokat. A következő képernyőolvasók használhatók: (JAWS, NVDA, Narrator).

Annak biztosításához, hogy a képernyőolvasó szoftver megfelelően el tudja érni az ESET Internet Security grafikus felhasználói felületét, kövesse a tudásbáziscikkünkben ismertetett instrukciókat.

Súgó és támogatás

Az ESET Internet Security súgója hibaelhárítási eszközöket és támogatási információkat tartalmaz, amelyek segítséget nyújtanak a felmerülő problémák megoldásában.

-licenc

- **Licenc hibaelhárítása** – Erre a hivatkozásra kattintva megoldást találhat a licencmódosítással kapcsolatos problémákra.

- **Licenc módosítása** – Kattintson ide az aktiválási ablak elindításához és a licenc aktiválásához. Ha az eszköze kapcsolódik a ESET HOME szolgáltatáshoz, válasszon ki egy licencet a ESET HOME-fiókjából, vagy adjon meg egy újat.

Telepített termék

- **Újdonságok** – Ide kattintva megnyithatja az új és továbbfejlesztett funkciókat ismertető információs ablakot.

- **Az ESET Internet Security névjegye** – Információkat jelenít meg az ESET Internet Security példányáról.

- **Termékkel kapcsolatos hibák elhárítása** – Erre a hivatkozásra kattintva megoldást találhat a leggyakrabban előforduló problémákra.

- **Termékváltás** – Erre kattintva megnézheti, hogy az ESET Internet Security átváltható-e egy másik terméktípusra a jelenlegi licenccel.

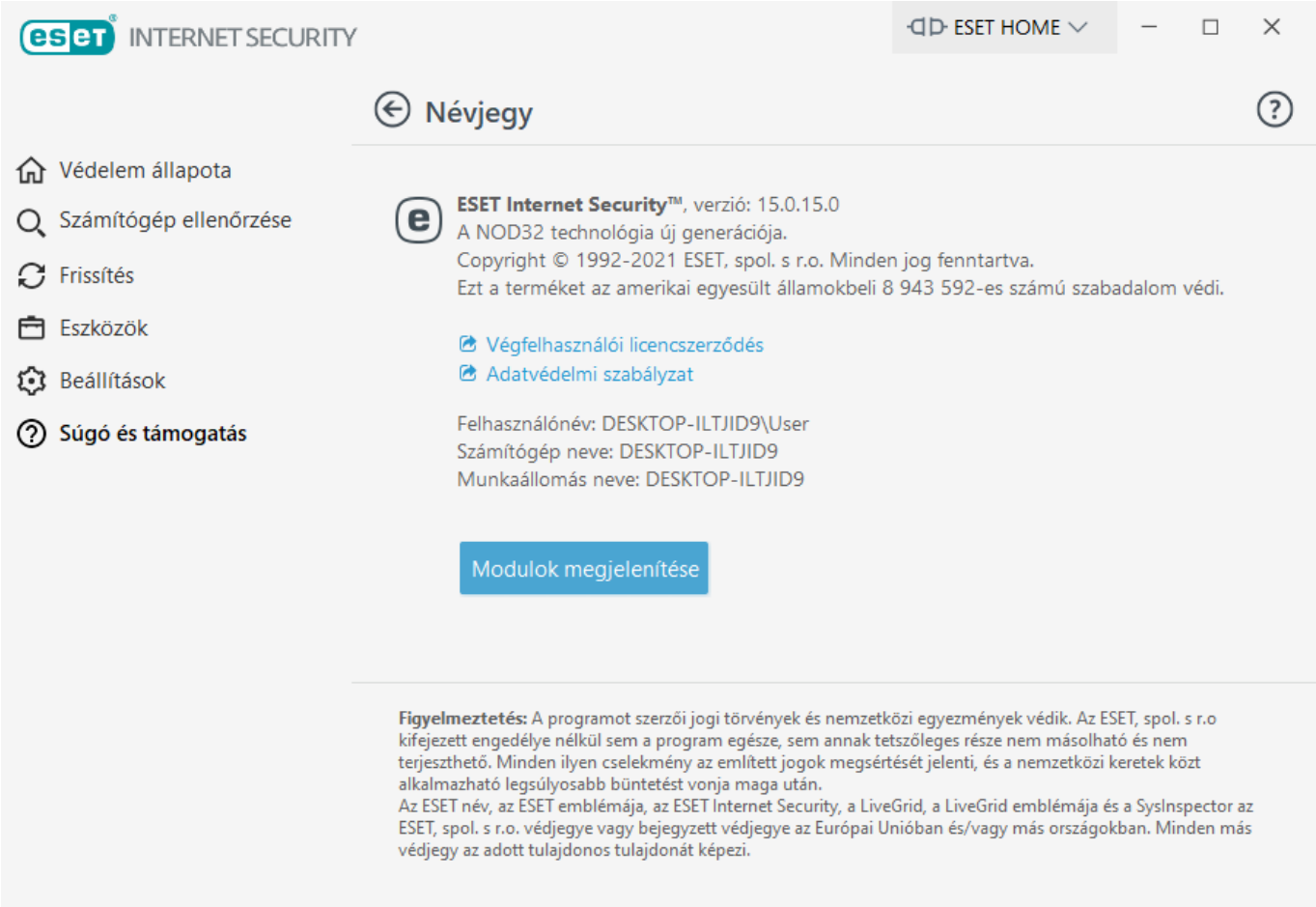
Súgóoldal – Kattintson erre a hivatkozásra az ESET Internet Security súgójának megnyitásához.

Műszaki terméktámogatás

Tudásbázis – Az ESET tudásbázisában (angol nyelven) találhatók a leggyakoribb kérdésekre adott válaszok, valamint a különböző problémákra ajánlott megoldások. Az ESET műszaki szakemberei által rendszeresen frissített tudásbázis a különböző problémák megoldásának leghatékonyabb eszköze.

Az ESET Internet Security névjegye

Az ablakban az ESET Internet Security telepített verziójának és a számítógép adatait tekintheti meg.



Kattintson a **Modulok megjelenítése** elemre a betöltött programmodulokra vonatkozó információk megtekintéséhez.

- A **Másolás** elemre kattintva a vágólapra másolhatja a modulok adatait. Ez a hibakereséshez, illetve a terméktámogatási szolgálattal folytatott kommunikáció során lehet hasznos.
- A Modulok ablakban kattintson a **Keresőmotor** elemre az ESET Vírusradar megnyitásához, amely tartalmazza az ESET Keresőmotor egyes verzióira vonatkozó információkat.

ESET Hírek

Ebben az ablakban az ESET Internet Security rendszeresen tájékoztatja az ESET híreiről.

A terméken belüli üzenetküldés arra való, hogy a felhasználókat tájékoztassa az ESET híreiről és más információiról. A marketingüzenetek küldéséhez a felhasználó beleegyezése szükséges. Alapértelmezés szerint ezért a rendszer nem küld marketingüzeneteket a felhasználónak (kérdőjel látható). A funkció engedélyezésével hozzájárul ahhoz, hogy az ESET marketingüzeneteket küldjön Önnek. Ha nem szeretne marketinges anyagokat kapni az ESET-től, tiltsa le a **Marketingüzenetek megjelenítése** funkciót.

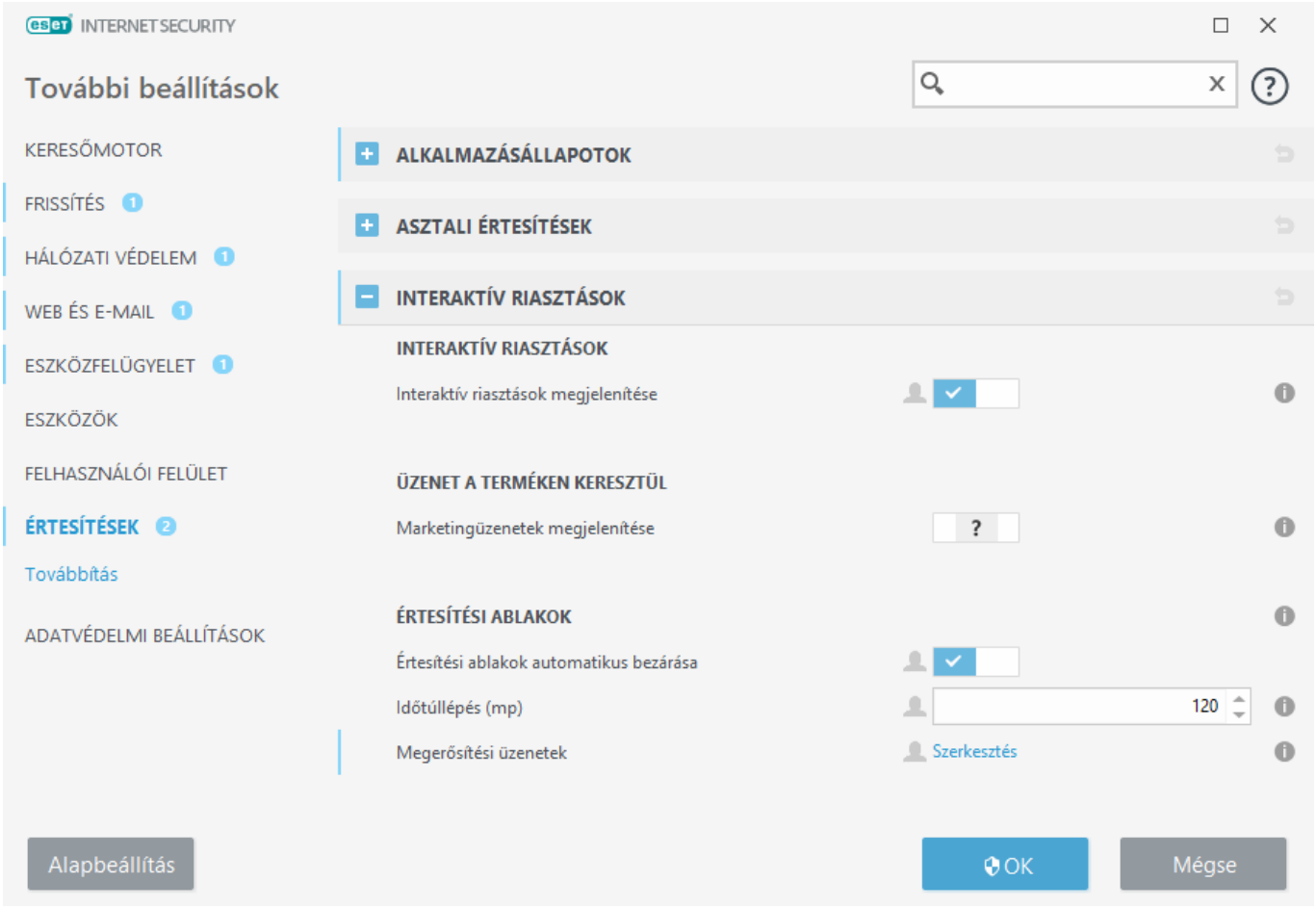
A marketingüzenetek felugró ablakban történő fogadásának engedélyezéséhez vagy letiltásához kövesse az alábbi instrukciókat.

1. Nyissa meg az ESET-termék fő ablakát.

2. Nyomja le az **F5** billentyűt a **További beállítások** párbeszédpanel megnyitásához.

3. Kattintson az **Értesítések** > **Interaktív riasztások** elemre.

4. Módosítsa a **Marketingüzenetek megjelenítése** beállítást.



Rendszer-konfigurációs adatok küldése

A lehető leggyorsabb és legpontosabb segítségnyújtáshoz az ESET számára meg kell adnia az ESET Internet Security konfigurációját, a részletes rendszer-információkat, a futó folyamatokra vonatkozó adatokat (az ESET SysInspector naplófájlját), valamint a beállításértékeket. Az ESET ezeket az adatokat kizárólag az Ön, mint ügyfél számára nyújtott technikai segítségnyújtás céljából használja fel.

A webes űrlap elküldésekor a rendszer-konfigurációs adatokat is elküldi az ESET számára. Válassza ki a **Mindig küldje el ezeket az információt** beállítást, ha szeretné menteni a műveletet ehhez a folyamathoz. Ha adatok küldése nélkül szeretné elküldeni az űrlapot, a **Ne legyen adatküldés** elemre kattintva az online támogatási űrlapot használva felveheti a kapcsolatot az ESET műszaki támogatási szolgálatával.

Ez a beállítás megadható a **További beállítások** > **Eszközök** > **Diagnosztika** > Műszaki támogatási szolgálat lapon is.

> Ha úgy dönt, hogy elküldi a rendszeradatokat, ki kell töltenie és el kell küldenie a webes űrlapot, ellenkező esetben nem jön létre a jegye, és elvesznek a rendszeradatai.

Műszaki terméktámogatás

A fő programablakban kattintson a **Súgó és támogatás** > **Műszaki terméktámogatás** elemre.

Kapcsolatfelvétel a műszaki terméktámogatással

Terméktámogatási kérelem – Ha nem talál megoldást a problémájára, az ESET webhelyén megtalálható űrlapon keresztül gyorsan kapcsolatba léphet az ESET műszaki támogatási szolgálatával. A beállítások alapján megjelenik a rendszerkonfigurációs adatok elküldése ablak a webes űrlap kitöltése előtt.

Információk összegyűjtése a terméktámogatás számára

Részletek a műszaki támogatási szolgálat számára – Amikor a rendszer kéri, az adatokat (például a licenc adatait, a terméknevet, a termékverziót, az operációs rendszert és a számítógép adatait) kimásolhatja és elküldheti az ESET műszaki támogatási szolgálatának.

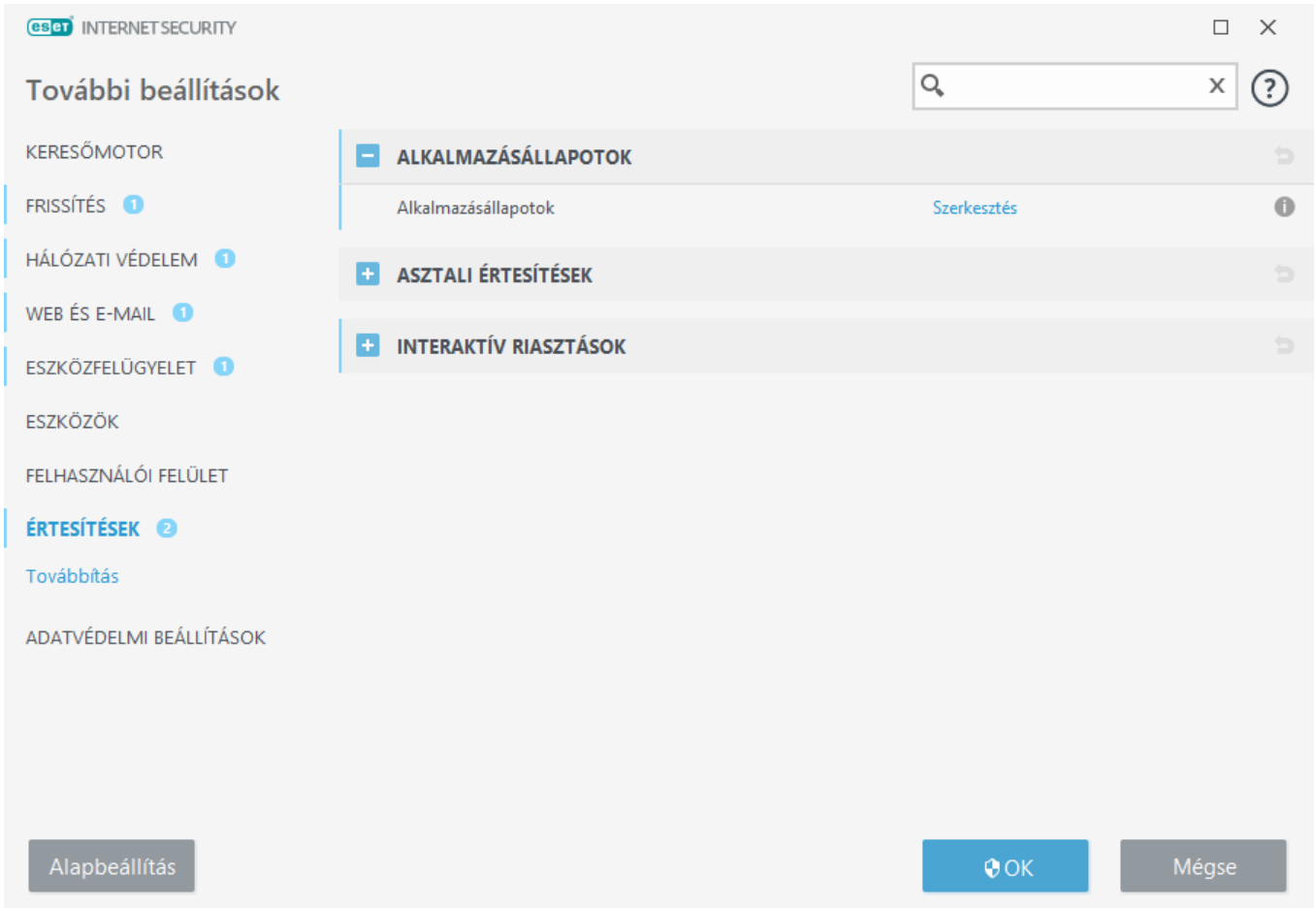
ESET Log Collector – Az ESET tudásbázisának cikkére mutató hivatkozások, amelyekkel letöltheti az ESET Log Collector alkalmazást. Az alkalmazás automatikusan összegyűjti a számítógépről az információkat és a naplókat, hogy segítségükkel gyorsabban megoldhassa a problémákat. További információkat az ESET Log Collector online felhasználói útmutatójában talál.

A **Részletes naplózás** elemre kattintva speciális naplókat hozhat létre mindegyik rendelkezésre álló funkcióhoz, hogy a fejlesztők diagnosztizálhassák és kijavíthassák a problémákat. A naplók minimális részletessége **Diagnosztika** szintre van beállítva. Két óra elteltével a speciális naplózás automatikusan leáll, ha nem állítja le hamarabb a **Speciális naplózás leállítása** elemre kattintva. Az összes napló létrehozása után megjelenik az értesítési ablak, ahonnan közvetlenül megnyithatja a naplókat tartalmazó Diagnosztika mappát.

Értesítések

Az ESET Internet Security-értesítések kezeléséhez nyissa meg a **További beállítások** (F5) > **Értesítések** lapot. A következő típusú értesítéseket konfigurálhatja:

- Alkalmazásállapotok – A program főablakának kezdő szakaszában megjelenő értesítések.
- Asztali értesítések – Kis előugró ablakok a rendszertálca mellett.
- Interaktív figyelmeztetések – Riasztási ablakok és értesítési ablakok, amelyek felhasználói interakciót igényelnek.
- Továbbítás (E-mail-értesítések) – Az e-mail-értesítések a megadott e-mail-címre érkeznek.



Alkalmazásállapotok

Alkalmazásállapotok – Kattintson a **Szerkesztés** gombra annak kiválasztásához, hogy mely alkalmazásállapotok jelenjenek meg a program főablakának kezdő szakaszában.

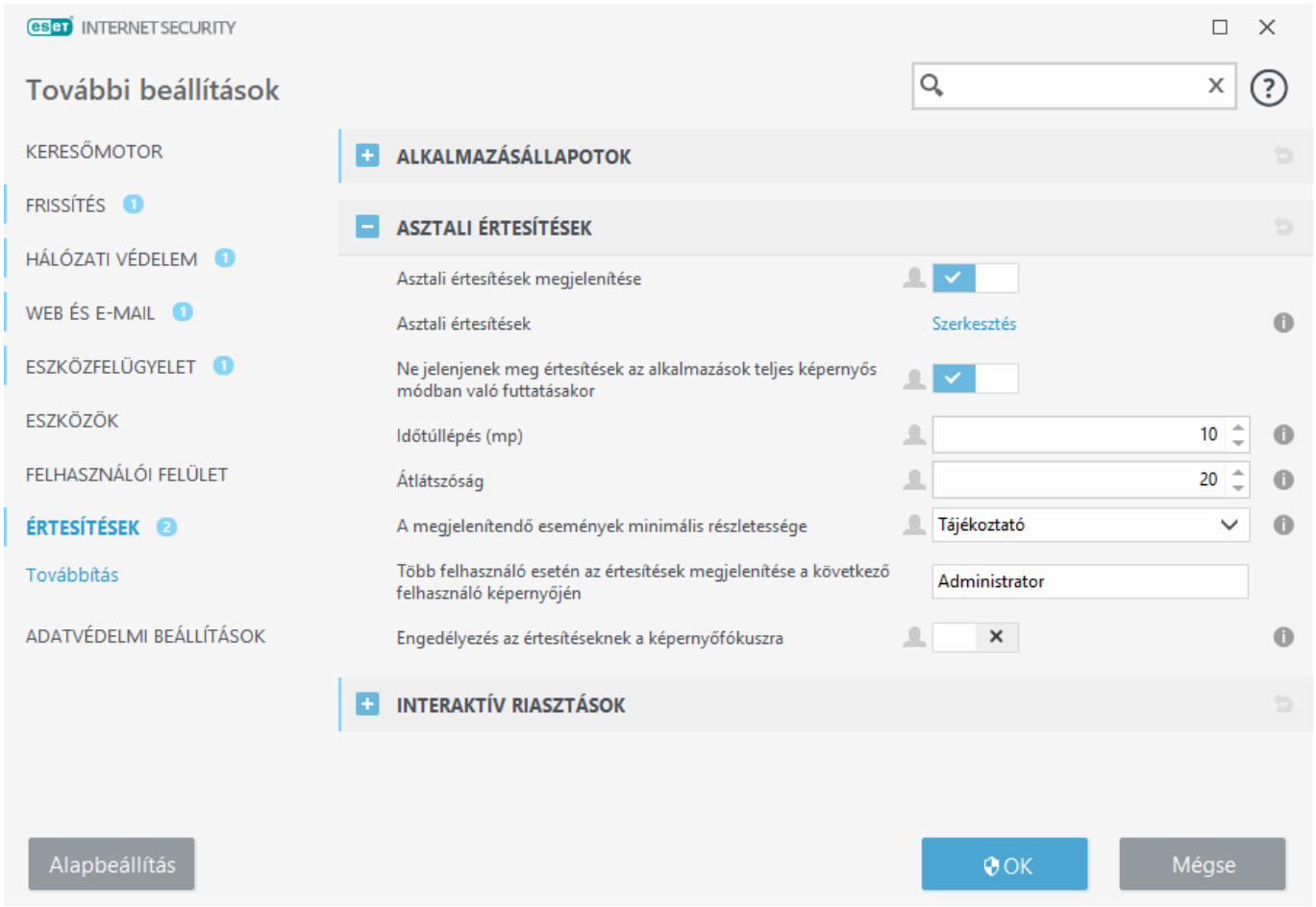
Párbeszédablak – Alkalmazásállapotok

Ezen a párbeszédpanelen megadhatja, hogy mely alkalmazásállapotok jelenjenek meg. Erre például a vírus- és kémprogramvédelem szüneteltetése vagy a Játékos üzemmód engedélyezése esetén lehet szükség.

Akkor is megjelenik alkalmazásállapot, ha a termék nincs aktiválva, vagy ha lejárt a licenc.

Asztali értesítések

Az asztali értesítések egy kis előugró ablakban jelennek meg a rendszertálca mellett. Az alapértelmezett beállítás 10 másodperc, amelynek letelte után lassan eltűnnek az értesítések. Az értesítések tájékoztatnak a sikeres termékfrissítésről, új eszköz csatlakoztatásakor, a víruskeresések befejezéséről és új kártevők észlelésekor.



Értesítések megjelenítése az asztalon – Azt javasoljuk, hogy hagyja engedélyezve ezt a beállítást, így a termék értesíteni tudja, ha új esemény történik.

Asztali értesítések – Kattintson a **Szerkesztés** elemre a kívánt asztali értesítések engedélyezéséhez vagy letiltásához.

Ne jelenjenek meg értesítések az alkalmazások teljes képernyős módban való futtatásakor – Az összes nem interaktív értesítés letiltása az alkalmazások teljes képernyős módban történő futtatásakor.

Időtúllépés (mp) – Az értesítés megjelenítési időtartamának beállítása. Az értéknek 3–30 másodperc között kell lennie.

Átlátszóság – Az értesítések átláthatóságának százalékos beállítása. A támogatott tartomány 0 (nincs átlátszóság) és 80 (nagyon magas átlátszóság) között van.

A megjelenítendő események minimális részletessége – Beállítható, hogy milyen súlyossági szinttől kezdve jelenjenek meg az értesítések. A legördülő listában válasszon egy beállítást:

- **Diagnosztikai** – A fentiek mellett a program pontos beállításához szükséges információk megjelenítése.
- **Tájékoztató** – Tájékoztató jellegű üzenetek megjelenítése, például szokatlan hálózati események és sikeres frissítésekről szóló üzenetek, valamint a fent említett bejegyzések.
- **Figyelmeztetések** – Figyelmeztető üzenetek és kritikus hibák megjelenítése (például az Anti-Stealth nem fut megfelelően, vagy nem sikerült a frissítés).
- **Hibák** – Hibák (például a dokumentumvédelem sikertelen indítása) és más kritikus hibák megjelenítése.

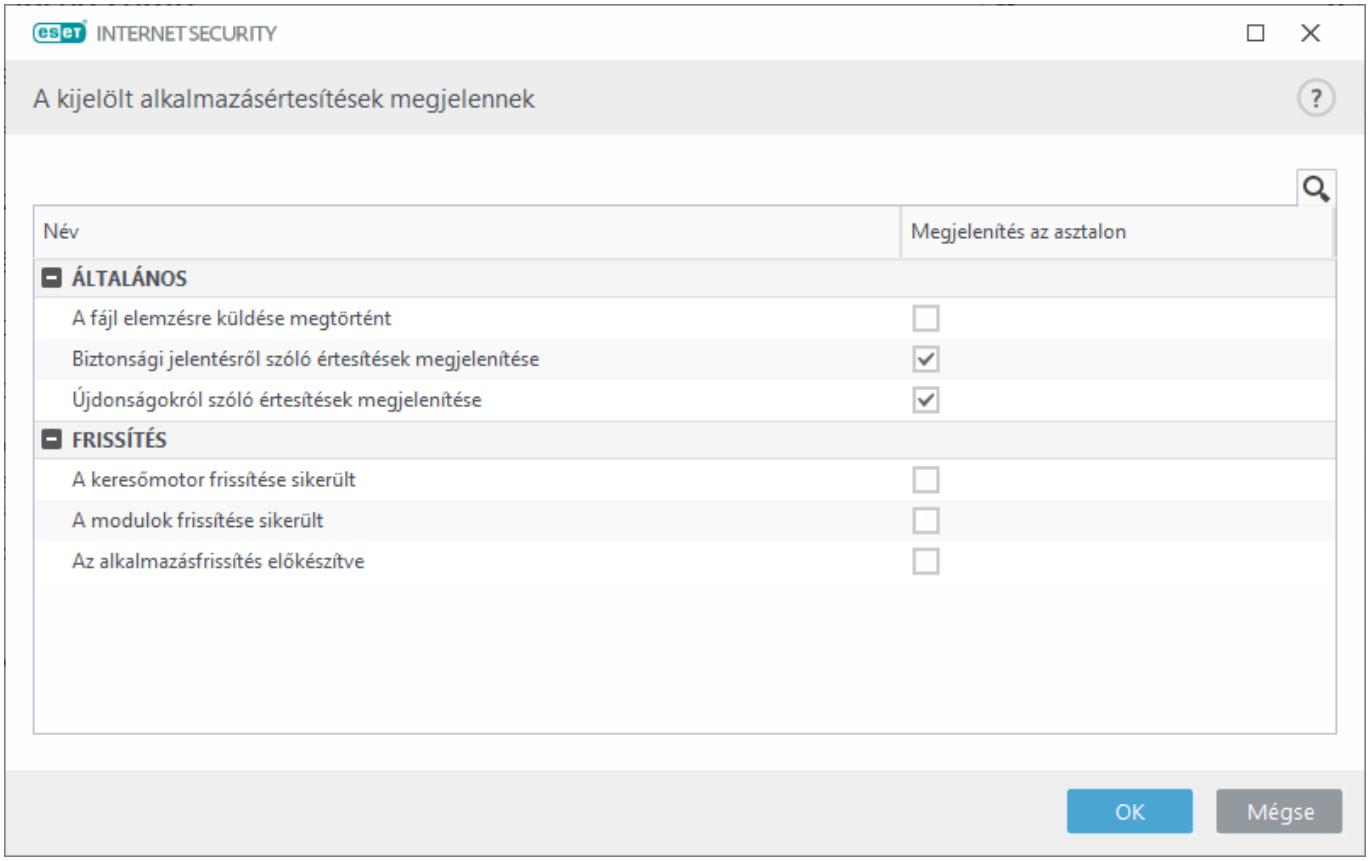
- **Kritikus** – Csak a kritikus (például a vírusvédelem indításával vagy a fertőzött rendszerrel kapcsolatos) hibák megjelenítése.

Több felhasználó esetén az értesítések megjelenítése a következő felhasználó képernyőjén – A kiválasztott fiók asztali értesítéseket fogadhat. Ha például nem használ rendszergazdai fiókot, írja be a teljes fióknevet, és asztali értesítések fog kapni az adott fiókkal kapcsolatban. Csak egy felhasználói fiók kaphat asztali értesítéseket.

Engedélyezés az értesítéseknek a képernyőfókuszra – Képernyőfókusz engedélyezése az értesítéseknek, és az **ALT + Tab** menüben érhetők el.

Asztali értesítések listája

Ha módosítani szeretné az asztali értesítések láthatóságát (amelyek a képernyő jobb alsó sarkában jelennek meg), nyissa meg a **További beállítások** (F5) > **Értesítések** > **Asztali értesítések** lapra. Kattintson a **Szerkesztés** gombra az **Asztali értesítések** felirat mellett, majd jelölje be a megfelelő **Megjelenítés** jelölőnégyzetet.



Általános

Biztonsági jelentésről szóló értesítések megjelenítése – Értesítést kap, ha új Biztonsági jelentés jött létre.

Újdonságokról szóló értesítések megjelenítése – Értesítések a legújabb termékverzió összes új és továbbfejlesztett funkciójáról.

A fájl elemzésre küldése megtörtént – Értesítést kap minden alkalommal, amikor az ESET Internet Security egy fájlt elküld elemzésre.

Frissítés

Az alkalmazásfrissítés előkészítve – Értesítést kap, ha elő van készítve egy frissítés az ESET Internet Security új verziójához.

A keresőmotor frissítése sikerült – Értesítést kap, amikor a termék frissíti a keresőmotor-modulokat.

A modulok frissítése sikerült. – Értesítést kap, ha a termék frissíti a program összetevőit.

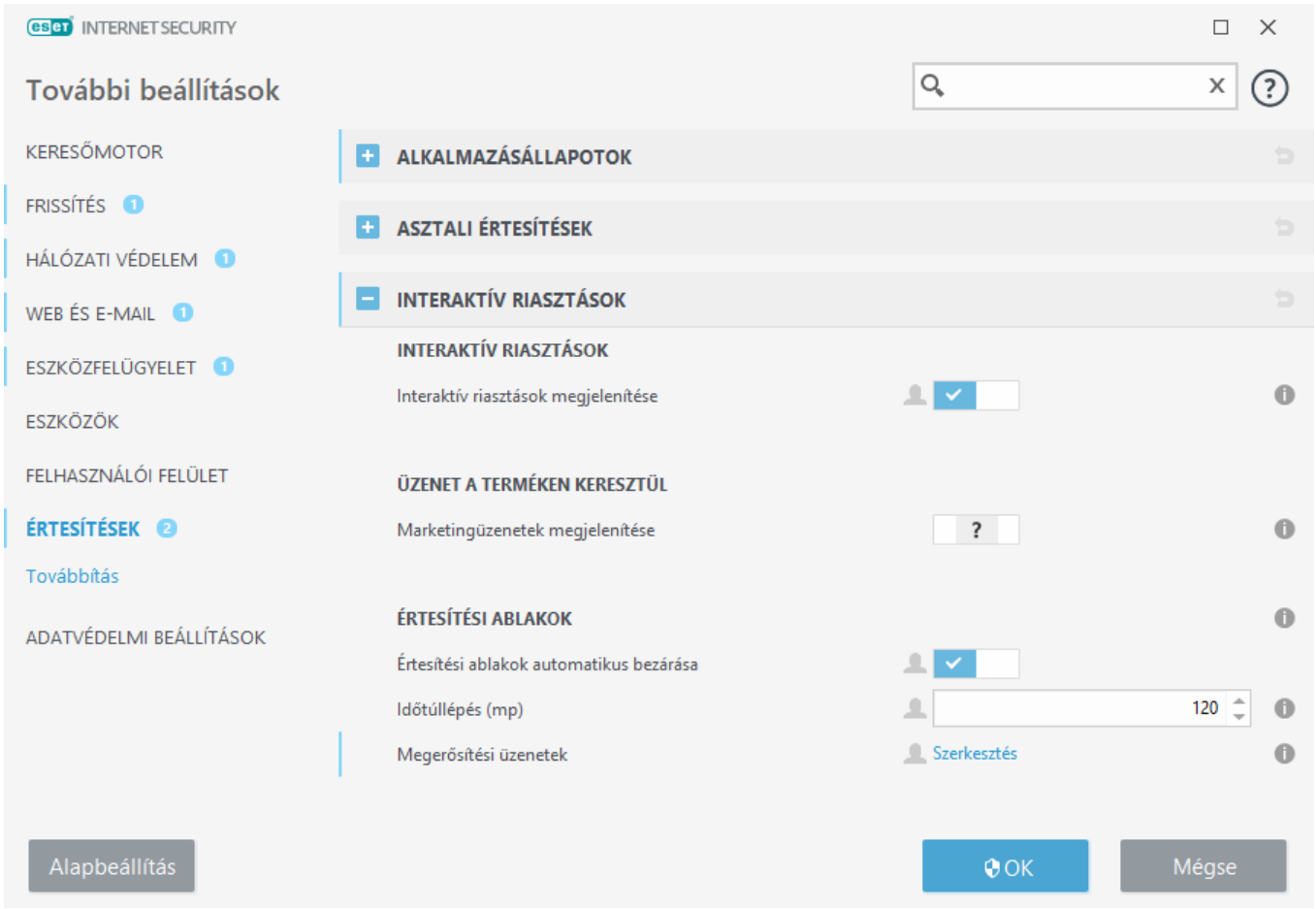
Ha az asztali értesítések általános beállításait szeretné megadni, például azt, hogy mennyi ideig jelenjenek meg az üzenetek, illetve a megjelenő események minimális részletességét, lépjen az Asztali értesítések szakaszhoz a **További beállítások** (F5) > **Értesítések** lapon.

Interaktív riasztások

Gyakori riasztásokról és értesítésekről keres információkat?

- A program kártevőt talált
- A cím letiltva
- A licenc nincs aktiválva
- Váltás egy több funkcióval rendelkező termékre
- Váltás egy kevesebb funkcióval rendelkező termékre
- Frissítés elérhető
- A frissítési adatok nem egységesek
- A „Modulok frissítése sikertelen” üzenet hibaelhárítása
- Modulfrissítési hibák elhárítása
- Hálózati kártevő letiltva
- A webhely tanúsítványát visszavonták

A **További beállítások** (F5) > **Értesítések** lapon található **Interaktív riasztások** szakaszban beállítható, hogy az értesítési ablakokat és az interaktív riasztásokat hogyan kezelje az ESET Internet Security, amikor a felhasználónak kell döntést hoznia (például potenciális adathalász webhelyek esetén).



Interaktív riasztások

Ha törli az **Interaktív riasztások megjelenítése** jelölőnégyzet bejelölését, nem fognak megjelenni riasztási ablakok és böngészős párbeszédpanelek – mindez azonban csak az események szűk körére alkalmazható beállítás. Az ESET azt javasolja, hogy a jelölőnégyzetet hagyja bejelölve.

Üzenet a terméken keresztül

A terméken belüli üzenetküldés arra való, hogy a felhasználókat tájékoztassa az ESET híreiről és más információiról. A marketingüzenetek küldéséhez a felhasználó beleegyezése szükséges. Alapértelmezés szerint ezért a rendszer nem küld marketingüzeneteket a felhasználónak (kérdőjel látható). A funkció engedélyezésével hozzájárul ahhoz, hogy az ESET marketingüzeneteket küldjön Önnek. Ha nem szeretne marketinges anyagokat kapni az ESET-től, tiltsa le a **Marketingüzenetek megjelenítése** funkciót.

Értesítési ablakok

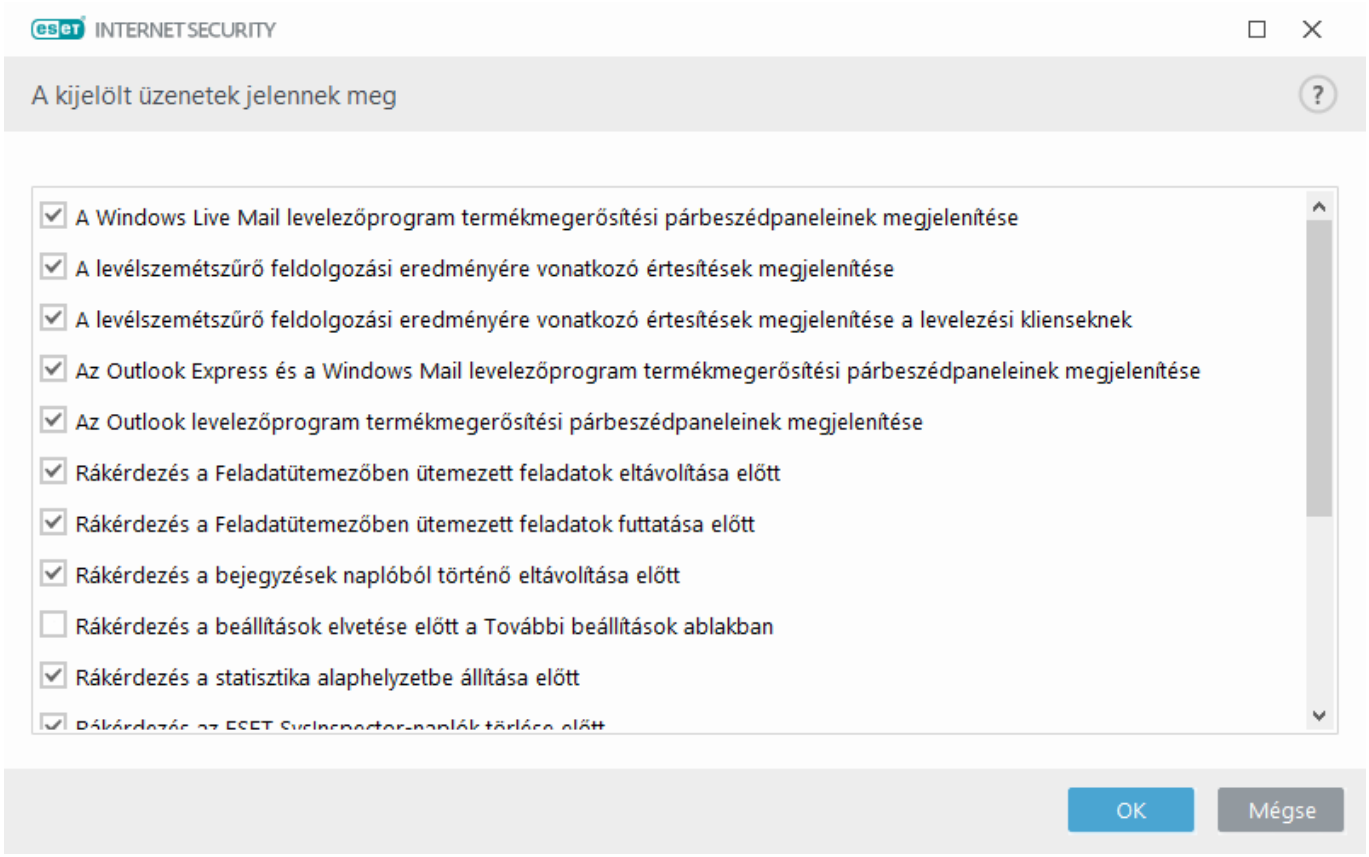
Az értesítési ablakok adott időtartam utáni automatikus bezárásához jelölje be az **Értesítési ablakok automatikus bezárása** jelölőnégyzetet. Ha a felhasználó nem zárja be az ablakokat, akkor ezt a megadott időtartam elteltével a program automatikusan megteszi.

Időtúllépés (mp) – A riasztás megjelenítési időtartamának beállítása. Az értéknek 10–999 másodperc között kell lennie.

Megerősítési üzenetek – Kattintson a **Szerkesztés** gombra az olyan megerősítési üzenetek megtekintéséhez, amelyek megjelenítését engedélyezheti és letilthatja.

Megerősítési üzenetek

A megerősítési üzenetek beállításához lépjen a **További beállítások** (F5) > **Értesítések** > **Interaktív értesítések** lapra, majd kattintson a **Szerkesztés** elemre a **Megerősítési üzenetek** szöveg mellett.



Ezen a párbeszédpanelen az ESET Internet Security által a műveletek végrehajtása előtt megjelenített megerősítési üzeneteket találja. Az egyes üzenetek melletti jelölőnégyzetek bejelölésével vagy jelölésük törlésével engedélyezheti vagy letilthatja az üzeneteket.

További információk a megerősítő üzenetekkel kapcsolatos funkciókról:

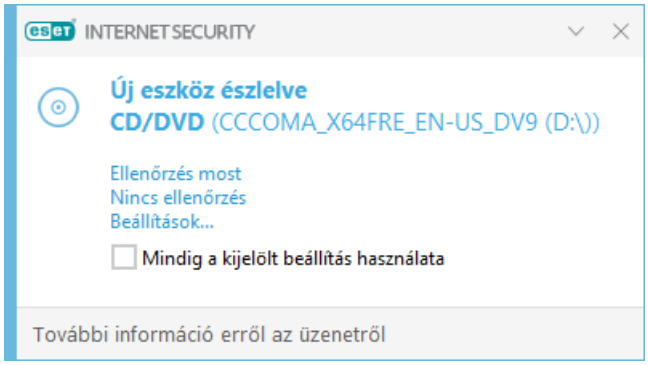
- Rákérdezés az ESET SysInspector-naplók törlése előtt
- Rákérdezés az összes ESET SysInspector-napló törlése előtt
- Rákérdezés az objektumok karanténból való törlése előtt
- Rákérdezés a beállítások elvetése előtt a További beállítások ablakban
- Rákérdezés egy riasztási ablakban, mielőtt mellőzné a megtisztítást az összes észlelt kártevő esetén
- Rákérdezés a bejegyzések naplóból történő eltávolítása előtt
- Rákérdezés a Feladatütemezőben ütemezett feladatok eltávolítása előtt
- Rákérdezés az összes naplóbejegyzés törlése előtt
- Rákérdezés a statisztika alaphelyzetbe állítása előtt

- Rákérdezés az objektumok karanténból való visszaállítása előtt
- Rákérdezés az objektumok karanténból való visszaállítása és ellenőrzésből történő kizárása előtt
- Rákérdezés a Feladatütemezőben ütemezett feladatok futtatása előtt
- A levélszemétszűrő feldolgozási eredményére vonatkozó értesítések megjelenítése
- A levélszemétszűrő feldolgozási eredményére vonatkozó értesítések megjelenítése a levelezési klienseknek
- Az Outlook Express és a Windows Mail levelezőprogram termékmegerősítési párbeszédpaneleinek megjelenítése
- A Windows Live Mail levelezőprogram termékmegerősítési párbeszédpaneleinek megjelenítése
- Az Outlook levelezőprogram termékmegerősítési párbeszédpaneleinek megjelenítése

Cserélhető adathordozók

Az ESET Internet Security lehetővé teszi a cserélhető adathordozók (CD, DVD, USB stb) automatikus ellenőrzését a számítógépbe való behelyezésük után. Ez különösen hasznos lehet akkor, ha a számítógép rendszergazdája meg kívánja akadályozni, hogy a felhasználók kéretlen tartalmú cserélhető adathordozót helyezzenek a számítógépbe.

Az alábbi párbeszédpanel jelenik meg, ha cserélhető adathordozót helyeznek be, és az **Ellenőrzési beállítások megjelenítése** funkció be van állítva az ESET Internet Security szolgáltatásban:



A párbeszédpanel beállításai:

- **Ellenőrzés most** – Erre a hivatkozásra kattintva elindíthatja a cserélhető adathordozó ellenőrzését.
- **Nincs ellenőrzés** – A cserélhető adathordozó nem lesz ellenőrizve.
- **Beállítások** – Megnyílik a **További beállítások** szakasz.
- **Mindig a kijelölt beállítás használata** – A jelölőnégyzet bejelölése esetén ugyanazt a műveletet végzi el a program, amikor legközelebb cserélhető adathordozót helyez be.

Az ESET Internet Security tartalmazza ezenkívül az Eszközfelügyelet funkciót, amely lehetővé teszi külső eszközök adott számítógépen való használatának szabályozását. Az eszközfelügyeletről további tudnivalókat olvashat az Eszközfelügyelet című szakaszban.

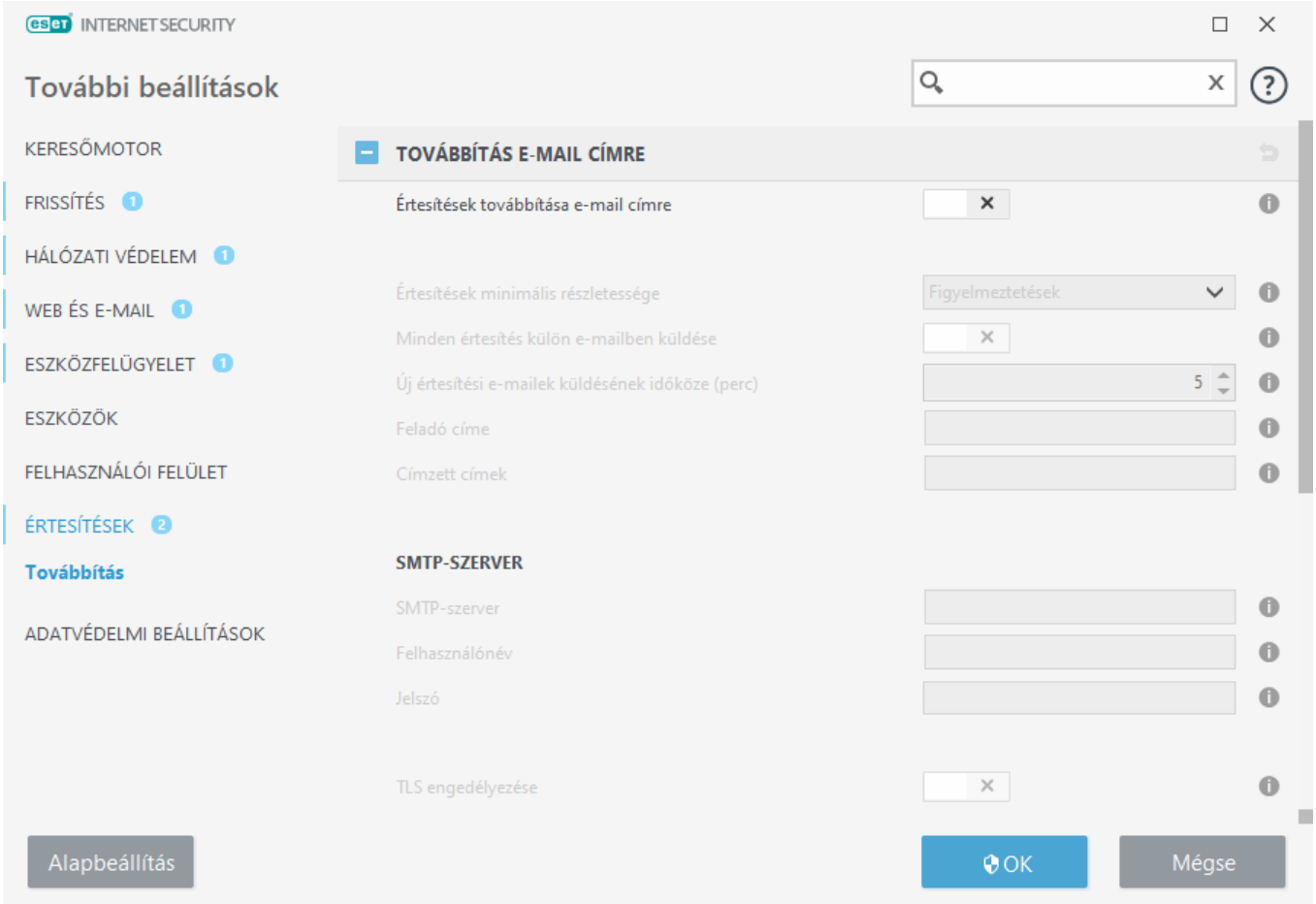
A cserélhető adathordozók ellenőrzésére vonatkozó beállítások kezeléséhez nyissa meg a További beállítások (**F5**) > **Keresőmotor** > **Kártevő-ellenőrzések** > **Cserélhető adathordozók** ablakot.

A cserélhető adathordozó behelyezése után szükséges művelet – Válassza ki a cserélhető adathordozó (CD/DVD/USB) számítógépbe történő behelyezését követően végrehajtandó alapértelmezett műveletet. Válassza ki, hogy milyen művelet menjen végbe, miután cserélhető adathordozót helyeztek a számítógépbe:

- **Nincs ellenőrzés** – Nincs művelet, és az **Új eszköz található** ablak nem nyílik meg.
- **Eszköz automatikus ellenőrzése** – A behelyezett cserélhető adathordozó eszköz ellenőrzése.
- **Ellenőrzési beállítások megjelenítése** – Megnyitja a **Cserélhető adathordozók** csoportot.

Továbbítás

Az ESET Internet Security automatikusan értesítő e-maileket tud küldeni a kiválasztott részletességi szintű esemény előfordulása esetén. Nyissa meg a **További beállítások** (F5) > **Értesítések** > **Továbbítása** lapot, és engedélyezze az **Értesítések továbbítása e-mail címre** beállítást az e-mail-értesítések aktiválásához.



Az **Értesítések minimális részletessége** legördülő menüben kiválaszthatja a küldendő értesítések kezdő részletességi szintjét.

- **Diagnosztikai** – A fentiek mellett a program pontos beállításához szükséges információk naplózása.

• **Tájékoztató** – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a szokatlan hálózati eseményekről és a sikeres frissítésekről szóló üzeneteket, valamint a fent említett bejegyzéseket).

• **Figyelmeztetések** – Kritikus hibák és figyelmeztető üzenetek rögzítése (az Anti-Stealth nem fut megfelelően, vagy nem sikerült a frissítés).

• **Hibák** – A dokumentumvédelem sikertelen indításával kapcsolatos és más kritikus hibák bejegyzése.

• **Kritikus** – Csak a kritikus (például a vírusvédelem indításával vagy talált kártevővel kapcsolatos) hibák naplózása.

Minden értesítés külön e-mailben küldése – Ha engedélyezi ezt az opciót, a címzett minden értesítés esetén új e-mailt kap. Ennek következtében rövid időn belül sok e-mailre lehet számítani.

Új értesítési e-mailek küldésének időköze (perc) – Percekben megadott időköz, amely után a program új értesítéseket küld az e-mail-címre. Ha azonnal el szeretné küldeni az értesítéseket, állítsa az időközt 0 értékre.

Feladó címe – Megadhatja a feladó címét, amely az értesítő e-mailek fejlécében jelenik meg.

Címzett címe – Megadhatja a címzett címét, amely az értesítő e-mailek fejlécében jelenik meg. Több érték is támogatott. Használjon pontosvesszőt elválasztóként.

SMTP szerver

SMTP-szerver – Az értesítések küldéséhez használt SMTP-szerver (például smtp.provider.com:587, az előre definiált port a 25-ös).

> A TLS-titkosítású SMTP-szervereket nem támogatja az ESET Internet Security.

Felhasználónév és **jelszó** – Ha az SMTP-szerver hitelesítést igényel, írja be ezekbe a mezőkbe az SMTP-szerver eléréséhez szükséges felhasználónevet és jelszót.

TLS engedélyezése – TLS titkosítást használó biztonsági figyelmeztetések és értesítek küldése.

SMTP-kapcsolat tesztelése – A rendszer egy teszt e-mailt küld a címzett e-mail-címére. Ki kell tölteni az SMTP-szerver, Felhasználónév, Jelszó, Feladó címe és Címzett címek mezőt.

Üzenetformátum

A program és a távoli felhasználó vagy rendszergazda közötti kommunikáció e-mailek vagy (a Windows üzenetküldő szolgáltatásával továbbított) helyi hálózati üzenetek formájában történik. Az **Alapértelmezett üzenetformátum használata** beállítás a riasztások és értesítések esetén a legtöbb helyzethez megfelelő. De bizonyos esetekben előfordulhat, hogy módosítania kell az eseményüzenetek formátumát.

Értesítések formátuma – A távoli számítógépeken megjelenített értesítések formátuma.

Riasztások formátuma – A riasztások és értesítések előre megadott alapértelmezett formátumúak. Az ESET azt javasolja, hogy hagyja őket változatlanul. Néhány esetben azonban előfordulhat (ha például automatizált e-mail feldolgozó rendszert használ), hogy módosítania kell az üzenet formátumát.

Karakterkészlet – A Windows területi beállításai (például windows-1250, Unicode (UTF-8), ACSII 7-bit vagy japán

(ISO-2022-JP)) alapján az e-maileket ANSI-karakterkódolássá alakítja át. Ennek eredményeképpen az "á" karakter "a" karakterre változik, egy ismeretlen szimbólum pedig a "?" karakterre.

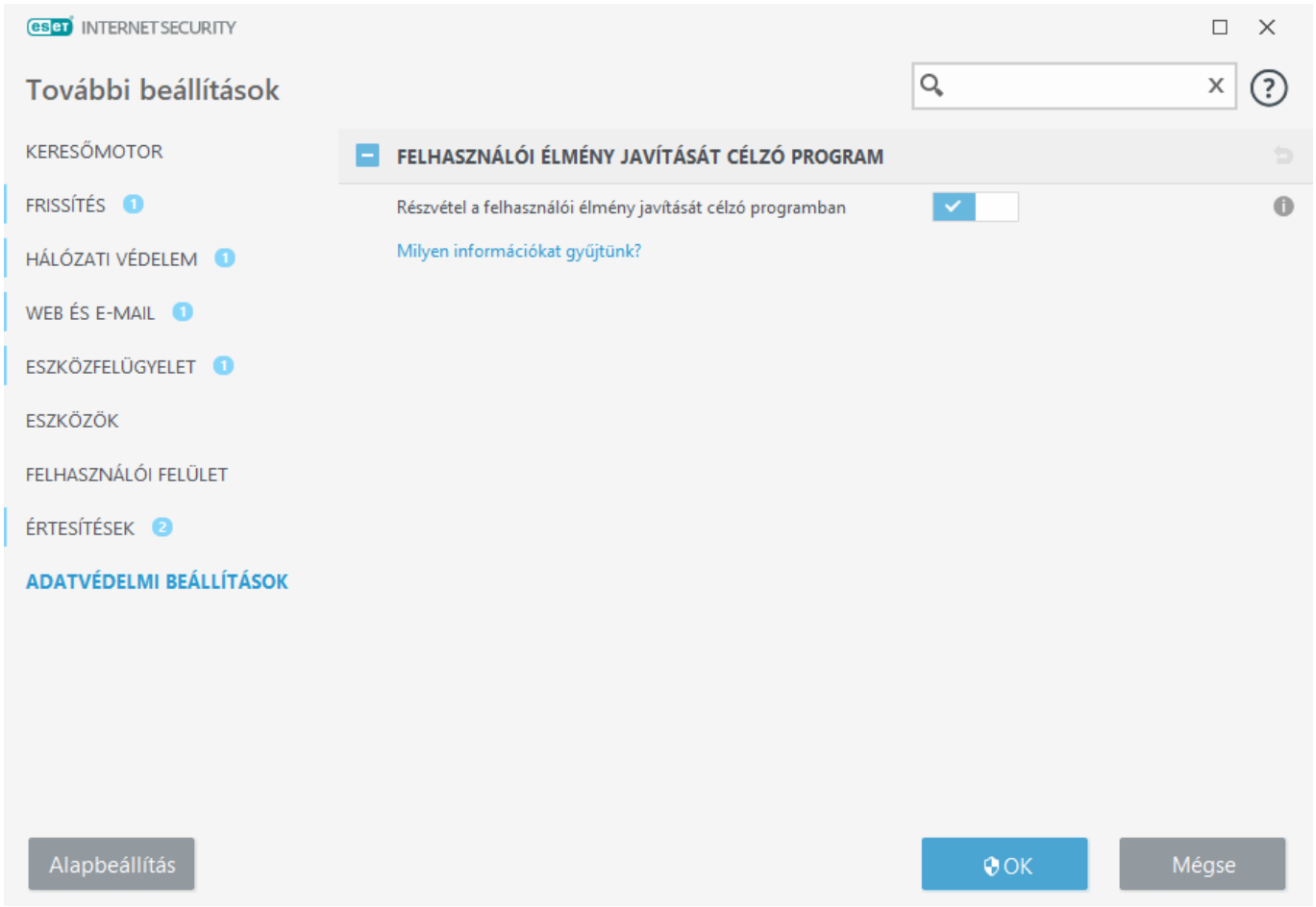
Idézett nyomtatható karakteres kódolás használata – A program az e-mail forrását Quoted-printable (QP), idézőjeles nyomtatható) formátumba kódolja, amely ASCII karaktereket használ, és az e-mailekben 8 bites formátumban tud helyesen továbbítani speciális nemzeti karaktereket (áéíóú).

- **%TimeStamp%** – Az esemény dátuma és időpontja
- **%Scanner%** – Az érintett modul
- **%ComputerName%** – A riasztást megjelenítő számítógép neve
- **%ProgramName%** – A riasztást létrehozó program
- **%InfectedObject%** – A fertőzött fájl, üzenet stb. neve.
- **%VirusName%** – A fertőzés azonosítása
- **%Action%** – Művelet fertőzés esetén
- **%ErrorDescription%** – Nem vírussal kapcsolatos esemény leírása

Az **%InfectedObject%** és a **%VirusName%** kulcsszó csak riasztásokban fordul elő, míg az **%ErrorDescription%** eseményekre vonatkozó üzenetekben használatos.

Adatvédelmi beállítások

A program főablakában kattintson a **Beállítások** > **További beállítások** (F5) > **Adatvédelmi beállítások** elemre.



Felhasználói élmény javítását célzó program

A **Részvétel a felhasználói élmény javítását célzó programban** szöveg melletti csúszka engedélyezésével csatlakozhat a Felhasználói élmény javítását célzó programhoz. Ha csatlakozik, névtelen információkat fog biztosítani az ESET számára a ESET-termékek használatáról. A begyűjtött adatok segítségével fokozni tudjuk a felhasználói élményt, és nem osztjuk meg az adatokat harmadik féllel. Milyen információkat gyűjtünk?

Profilok

A profilkezelőt az ESET Internet Security programban két helyen használhatja: a **Kézi indítású számítógép-ellenőrzés** és a **Frissítés** csoportban.

Számítógép ellenőrzése

Négy előre megadott ellenőrzési profilt biztosít az ESET Internet Security:

- **Optimalizált ellenőrzés** – Ez az alapértelmezett speciális ellenőrzési ellenőrzésprofil. Az intelligens ellenőrzési profil az Intelligens optimalizálási technológiát alkalmazza, amely kizárja azokat a fájlokat, amelyeket egy korábbi ellenőrzés tisztának talált, és amelyek az ellenőrzés óta nem módosultak. Ez gyorsabb ellenőrzést tesz lehetővé, ami minimális hatással van a rendszer biztonságára.

- **Helyi menüből indított ellenőrzés** – A helyi menüből elindíthatja bármely fájl kézi indítású ellenőrzését. A Helyi menü ellenőrzési profil lehetővé teszi egy ellenőrzési konfiguráció meghatározását, amely akkor fog érvényesülni, amikor ilyen módon indít ellenőrzést.

• **Mindenre kiterjedő ellenőrzés** – A részletes ellenőrzési profil alapértelmezés szerint nem használja az Intelligens optimalizálást, így egyetlen fájl sincs kizárva az ellenőrzésből a profil használatakor.

• **Számítógép ellenőrzése** – Ez a szabványos számítógépes ellenőrzés során használt alapértelmezett profil.

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

Új profil létrehozásához nyissa meg a További beállítások ablakot (az F5 billentyű lenyomásával), és kattintson a **Keresőmotor** > **Kártevőellenőrzések** > **Kézi indítású számítógép-ellenőrzés** > **Profilok listája** elemre. A **Profilkezelő** ablakban látható a meglévő ellenőrzési profilokat tartalmazó **Kiválasztott profil** legördülő lista, valamit a profilok létrehozására szolgáló lehetőség is. Ha segítségre van szüksége az igényeinek megfelelő ellenőrzési profil létrehozásával kapcsolatban, olvassa el az ellenőrzési beállítások egyes paramétereinek a leírását A ThreatSense keresőmotor beállításai című részben.

Tegyük fel, hogy saját ellenőrzési profilt szeretne létrehozni, és **A számítógép ellenőrzése** konfiguráció részben megfelel az elképzeléseinek, nem kívánja azonban a futtatás közbeni tömörítőket vagy a veszélyes alkalmazásokat ellenőrizni, emellett **Mindig kezelje a fertőzést** szeretne alkalmazni. Írja be az új profil nevét a **Profilkezelő** ablakban, és kattintson a **Hozzáadás** gombra. Jelölje ki az új profilt a **Kiválasztott profil** legördülő menüben, és adja meg a fennmaradó paraméterek beállításait úgy, hogy megfeleljenek a követelményeknek, majd kattintson az **OK** gombra az új profil mentéséhez.

Frissítés

A Frissítési profilszerkesztővel a felhasználók új frissítési profilokat hozhatnak létre. Csak akkor hozzon létre és használjon egyéni profilokat (az alapértelmezett **saját profilon** kívül), ha több frissítési szerverről kell frissítenie a programnak.

Példa lehet erre egy olyan hordozható számítógép, amely általában egy helyi szerverhez (tükörszerverhez) kapcsolódik a helyi hálózaton, de a hálózatról leválasztva (például üzleti úton) közvetlenül az ESET frissítési szervereiről tölti le a frissítéseket. Az egyikkel a helyi szerverhez, a másikkal az ESET szervereihez kapcsolódhat. Miután beállította ezeket a profilokat, nyissa meg az **Eszközök** > **Feladatütemező** ablakot, és módosítsa a frissítési feladat paramétereit. Az egyik profilt jelölje ki elsődlegesnek, a másikat másodlagosnak.

Frissítési profil – Ez az aktuálisan használt frissítési profil. Ha meg szeretné változtatni, válasszon egy másik profilt a legördülő listából.

Profilok listája – Új frissítési profilokat hozhat létre, illetve eltávolíthatja a meglévőket.

Billentyűparancsok

Az alábbi billentyűparancsok segítik a jobb navigálást az ESET Internet Security szolgáltatásban:

Billentyűparancsok	Művelet
F1	a súgólapok megnyitása
F5	a További beállítások ablak megnyitása
Fel/Le nyíl	navigáció a legördülő menüpontokban
TAB	ugrás a következő GUI elemre az ablakban

Billentyűparancsok	Művelet
Shift+TAB	ugrás az előző GUI elemre az ablakban
ESC	az aktív párbeszédpanel bezárása
Ctrl+U	az ESET-licenccel és a számítógéppel kapcsolatos adatok megjelenítése (a terméktámogatási szolgáltatás számára)
Ctrl+R	a termékablak visszaállítása az eredeti méretére és pozíciójába
ALT + Balra nyíl	visszalépés
ALT + Jobbra nyíl	előrelépés
ALT+Home	ugrás a kezdőlapra

Az előre és hátra egérgombokat is használhatja a navigációhoz.

Diagnosztika

A diagnosztika az ESET folyamatainak (például ekrn) alkalmazás-összeomlási képeit biztosítja. Ha egy alkalmazás összeomlik, a program létrehoz egy memóriaképet. Ez elősegíti, hogy a fejlesztők fel tudják deríteni és el tudják hárítani a problémákat az ESET Internet Security alkalmazásban.

Nyissa meg a **Memóriakép típusa** legördülő menüt, és válasszon az alábbi három beállítás közül:

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

Célkönyvtár – Az összeomlás során készült memóriaképet tároló könyvtár.

Diagnosztikai mappa megnyitása – A **Megnyitás** parancsra kattintva megnyithatja a könyvtárt a *Windows Intéző* egy új ablakában.

Diagnosztikai memóriakép létrehozása – Kattintson a **Létrehozás** gombra diagnosztikai memóriaképfájlok létrehozásához a **Célkönyvtár** mappában.

Részletes naplózás

Speciális naplózás engedélyezése a marketingüzenetekben – A terméken belüli marketingüzenetekkel kapcsolatos összes esemény rögzítése.

Levélszemétszűrő motor speciális naplózásának engedélyezése – A levélszemétszűrés során előforduló összes esemény rögzítése. Ez segít a fejlesztőknek az ESET levélszemétszűrő motorjával kapcsolatos problémák felismerésében és javításában.

Lopásvédelmi motor speciális naplózásának engedélyezése – A Lopásvédelemben történő összes esemény rögzítése diagnosztizálás és problémamegoldás céljából.

A Netbank- és tranzakcióvédelem részletes naplózásának engedélyezése – Az összes esemény rögzítése, amely a Netbank- és tranzakcióvédelemben történik.

A számítógépes víruskereső részletes naplózásának engedélyezése – Rögzíthető az összes olyan esemény, amely akkor lép fel, amikor a Számítógép ellenőrzése.

Eszközfelügyelet speciális naplózásának engedélyezése – Az Eszközfelügyelet modulban előforduló összes esemény rögzítése. Ez segíteni tud a fejlesztőknek az Eszközfelügyelet modullal kapcsolatos problémák felismerésében és javításában.

A Direct Cloud részletes naplózásának engedélyezése – Az ESET LiveGrid® modulban előforduló összes esemény rögzítése. Ez segíthet a fejlesztőknek az ESET LiveGrid® modullal kapcsolatos problémák felismerésében és javításában.

A Dokumentumvédelem speciális naplózásának engedélyezése – A Dokumentumvédelemben előforduló összes esemény rögzítése, amivel lehetővé válik a problémák diagnosztizálása és elhárítása.

A E-mail-védelem speciális naplózásának engedélyezése – Az E-mail-védelemben és a levelezőprogramos beépülő modulban előforduló összes esemény rögzítése, amivel lehetővé válik a problémák diagnosztizálása és elhárítása.

Kernel részletes naplózásának engedélyezése – Az ESET-kernelben (ekrn) fellépő összes esemény rögzítése.

Licencelés speciális naplózásának engedélyezése – A termék ESET aktiválási szervereivel vagy az ESET License Manager-szerverekkel folytatott kommunikációjának rögzítése.

Memóriakövetés engedélyezése – Rögzíthet minden eseményt, ami segítséget nyújt a fejlesztőknek a memóriavesztés elemzésében.

A hálózati védelem speciális naplózásának engedélyezése – A tűzfalon átmenő összes hálózati adat rögzítése PCAP formátumban, hogy a fejlesztők diagnosztizálhassák és javíthassák a tűzfallal kapcsolatos problémákat.

Operációs rendszer speciális naplózásának engedélyezése – További információk rögzítése az operációs rendszerről, például a futó folyamatok, a processzoraktivitás és a lemezműveletek. A fejlesztők ezáltal meg tudják vizsgálni és el tudják hárítani az operációs rendszeren futó ESET-termékkel kapcsolatos problémákat.

Szülői felügyelet speciális naplózásának engedélyezése – A Szülői felügyelet modulban előforduló összes esemény rögzítése. Ez segíthet a fejlesztőknek a Szülői felügyelet modullal kapcsolatos problémák felismerésében és javításában.

A protokollszűrés speciális naplózásának engedélyezése – A protokollszűrési modulon átmenő összes adat rögzítése PCAP formátumban, így a fejlesztők diagnosztizálni és javítani tudják és a protokollszűréssel kapcsolatos problémákat.

A push üzenetküldés részletes naplózásának engedélyezése – A push üzenetküldés során előforduló összes esemény rögzítése.

A valós idejű fájlrendszervédelem részletes naplózásának engedélyezése – Az összes olyan esemény rögzítése, amely akkor lép fel, amikor a Valós idejű fájlrendszervédelem fájlokat és mappákat ellenőriz.

Frissítési motor speciális naplózásának engedélyezése – Rögzíti a frissítési folyamat során előforduló összes eseményt. Ez segíti a fejlesztőket a Frissítési motorral kapcsolatos hibák felismerésében és javításában.

A naplófájlok a következő helyen találhatók: *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Műszaki terméktámogatás

Ha kapcsolatba lép az ESET műszaki terméktámogatással az ESET Internet Security segítségével, elküldhet rendszer-konfigurációs adatokat. Az adatok automatikus küldéséhez válassza ki a **Mindig küldje el** lehetőséget a **Rendszerkonfigurációs adatok küldése** legördülő menüben vagy a **Rákérdezés a küldés előtt** lehetőséget, ha azt szeretné, hogy a rendszer jóváhagyást kérjen az adatok küldése előtt.

Beállítások importálása és exportálása

Az ESET Internet Security .xml testre szabott .xml konfigurációs fájlját a **Beállítások** menüből importálhatja, illetve exportálhatja.

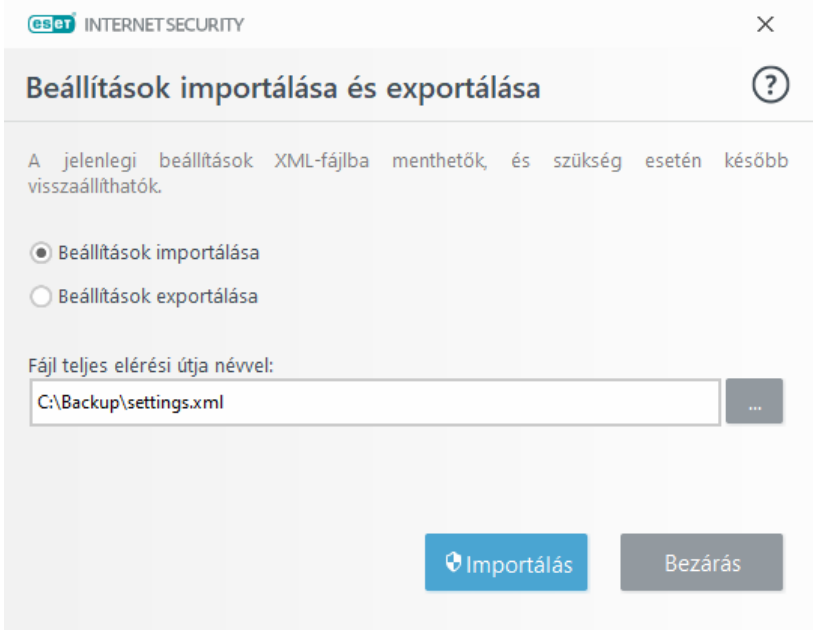
> **Ábrákkal ellátott útmutató**
> Tekintse meg az ESET konfigurációs beállításainak importálása és exportálása .xml fájl használatával című témakörben az angol és számos más nyelven elérhető illusztrált instrukciókat.

Mindkét művelet hasznos abban az esetben, ha az ESET Internet Security aktuális konfigurációjáról későbbi felhasználás céljából biztonsági másolatot szeretne készíteni. A beállítások exportálása akkor is kényelmes, ha több rendszeren szeretné használni a preferált konfigurációt. A beállítások átviteléhez importálhat egy .xml fájlt.

Konfiguráció importálásához a fő programablakban válassza ki a **Beállítások** > **Beállítások importálása és exportálása** lehetőséget, és jelölje be a **Beállítások importálása** választógombot. Írja be a konfigurációs fájl nevét, vagy a **...** gombra kattintva keresse meg az importálandó konfigurációs fájlt.

Konfiguráció exportálásához a fő programablakban kattintson a **Beállítások** > **Importálási/exportálási beállítások** elemre. Válassza ki a **Beállítások exportálása** lehetőséget, és írja be a fájl teljes elérési útját és a nevét. A **...** gombra kattintva keresse meg a számítógépen található helyet a konfigurációs fájl mentéséhez.

> Ha nem rendelkezik megfelelő jogosultsággal az exportált fájl adott könyvtárba írásához, a beállítások exportálásakor hiba léphet fel.



Az összes beállítás visszaállítása ezen a részen

A kanyarodó nyílra kattintva állítsa vissza az összes beállítást az aktuális szakaszban az ESET által meghatározott alapértelmezett beállításokra.

Vegye figyelembe, hogy a **Visszaállítás alapbeállításra** elemre való kattintás után minden korábban elvégzett módosítás elvész.

Táblázatok tartalmának visszaállítása – Ha engedélyezve van, elvesznek a kézzel vagy automatikusan hozzáadott szabályok, feladatok vagy profilok.

Tekintse meg a következőt is: Beállítások importálása és exportálása.

Visszaállítás az alapbeállításokra

A **További beállításokban** (F5) található **Alapbeállítás** elemre kattintva visszaállíthatja az összes programbeállítást minden modul esetén. Az az állapot áll vissza, amely egy új telepítést követően fennállna.

Tekintse meg a következőt is: Beállítások importálása és exportálása.

Hiba a konfiguráció mentésekor

Ez a hibaüzenet jelzi, hogy a beállítások mentése egy hiba következtében nem volt megfelelő.

Ez általában azt jelenti, hogy a felhasználó, aki megpróbálta módosítani a programparamétereket:

- nem rendelkezik megfelelő hozzáférési jogokkal, illetve a konfigurációs fájlok és a rendszer beállításjegyzékének módosításához szükséges jogosultsággal.
  > A szükséges módosítások elvégzéséhez a rendszergazdának kell bejelentkeznie.

- nemrég aktiválta Tanuló módot a Behatolásmegelőző rendszerben (HIPS) vagy a Tűzfalban, és megpróbált módosításokat eszközölni a További beállításokban.
  > A konfiguráció mentéséhez és a konfigurációs ütközés elkerüléséhez zárja be a További beállításokat mentés nélkül, és próbálja meg ismét végrehajtani a módosításokat.

A második legáltalánosabb ok az, hogy a program már nem működik megfelelően, vagyis sérült, és ezért újra kell telepíteni.

Parancssori víruskereső

Az ESET Internet Security vírusvédelmi modulja a parancssor használatával is elindítható – akár manuálisan az „ecls” paranccsal, akár egy .bat kiterjesztésű kötegfájllal.

Az ESET parancssoros ellenőrzőjének használata:

```
ecls [OPTIONS..] FILES..
```

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
/unsafe	veszélyes alkalmazások keresése
/no-unsafe	veszélyes alkalmazások keresésének mellőzése (alapbeállítás)
/unwanted	kéretlen alkalmazások ellenőrzése
/no-unwanted	kéretlen alkalmazások ellenőrzésének mellőzése (alapbeállítás)
/suspicious	gyanús alkalmazások keresése (alapbeállítás)
/no-suspicious	gyanús alkalmazások keresésének mellőzése
/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-exclude=KITERJESZTÉSEK	a kettősponttal elválasztott FÁJLKITERJESZTÉSEK kizárása az ellenőrzésből
/clean-mode=MÓD	megtisztítási MÓD használata a fertőzött objektumokhoz A választható lehetőségek az alábbiak: • `none` (alap) – Nem történik automatikus tisztítás. • `standard` – Az ecls.exe megkísérli automatikusan megtisztítani vagy törölni a fertőzött fájlokat. • `strict` (teljes) – Az ecls.exe megkísérli felhasználói beavatkozás kérése nélkül, automatikusan megtisztítani vagy törölni a fertőzött fájlokat (nem kell jóváhagynia a fájlok törlését). • `rigorous` (alapos) – Az ecls.exe a tisztítás megkísérlése nélkül törli a fájlokat, függetlenül attól, hogy milyen fájlról van szó. • `delete` (törlés) – Az ecls.exe a tisztítás megkísérlése nélkül törli a fájlokat, a fontos fájlokat, például a Windows rendszerfájljait azonban meghagyja.
/quarantine	a fertőzött fájlok karanténba másolása (kiegészíti a megtisztítás során végrehajtott műveletet)
/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

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

ESET CMD

Ez a funkció engedélyezi speciális ecmd parancsok használatát. És lehetővé teszi beállítások exportálását és importálását parancssor (ecmd.exe) használatával. Mostanáig a beállításokat csak a felhasználói felület segítségével lehetett exportálni és importálni. A ESET Internet Security-konfiguráció .xml.*xml* fájlba exportálható.

Az ESET CMD engedélyezése esetén két hitelesítési mód lehetséges:

- **Nincs** – nincs hitelesítés. Nem javasoljuk ennek a módszernek a használatát, mivel ez lehetővé teszi bármilyen aláíratlan konfiguráció importálását, ami lehetséges kockázatot jelent.

- **További beállítások jelszava** – jelszóra van szükség, ha .xml fájlból szeretne importálni egy konfigurációt. A fájlt alá kell írni (az .xml konfigurációs fájl aláírásáról lent olvashat). Meg kell adni a Hozzáférési beállításokban megadott jelszót egy új konfiguráció importálása előtt. Ha nincsenek hozzáférési beállítások engedélyezve, a jelszó nem egyezik meg, vagy az .xml konfigurációs fájl nincs aláírva, a rendszer nem importálja a konfigurációt.

Az ESET CMD engedélyezését követően parancssor használatával importálhat és exportálhat ESET Internet Security-konfigurációkat. Ezt végezheti manuálisan, illetve automatizálási célból létrehozhat egy parancsfájlt.

Speciális ecmd parancsok használatához rendszergazdai jogosultságokkal kell futtatnia őket, vagy a **Futtatás rendszergazdaként** paranccsal meg kell nyitnia a Windows parancssori ablakát (cmd). Ellenkező esetben a következő hibaüzenet jelenik meg: **Error executing command**. Konfiguráció exportálásakor célmappának is lennie kell. Az exportálási parancs továbbra is működik, ha az ESET CMD funkció ki van kapcsolva.

Beállítások exportálása parancs:
```
ecmd /getcfg c:\config\settings.xml
```

Beállítások importálása parancs:
```
ecmd /setcfg c:\config\settings.xml
```

A speciális ecmd-parancsok csak helyileg futtathatók.

.*xml* konfigurációs fájl aláírása:

1. Töltse le az XmlSignTool végrehajtható fájlt.

2. Nyissa meg a Windows parancssori ablakát (cmd) a **Futtatás rendszergazdaként** paranccsal.

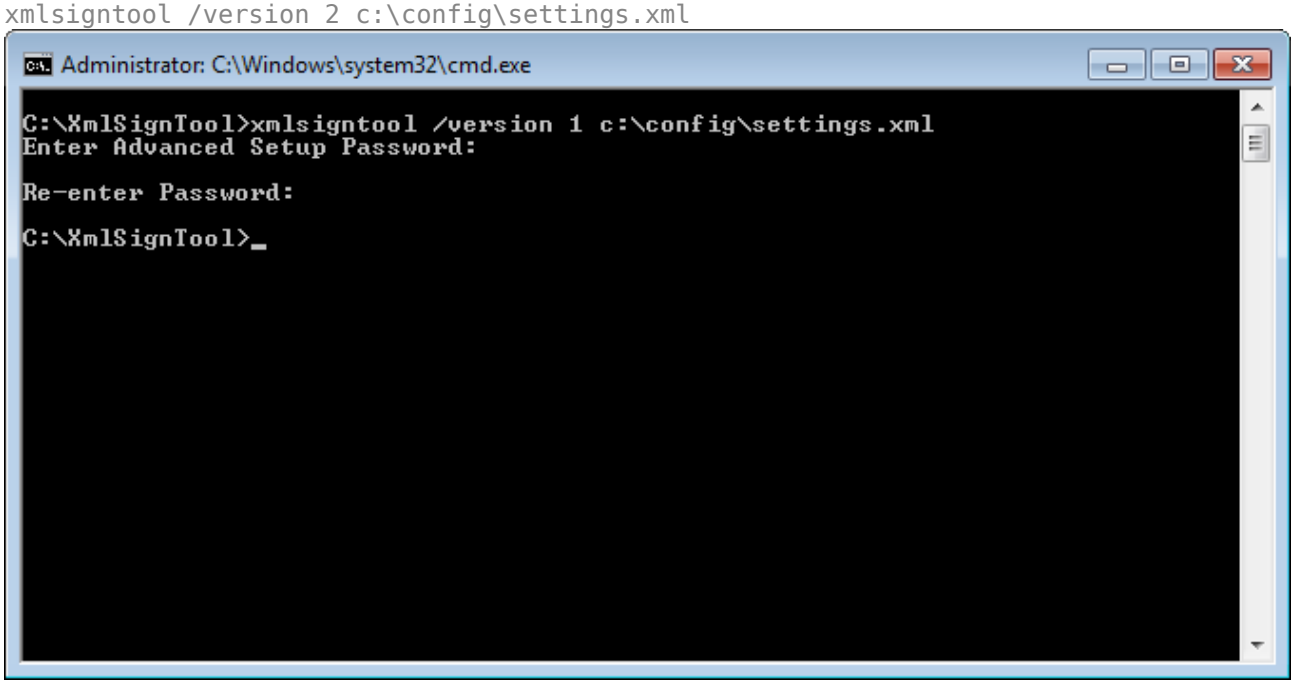
3. Lépjen oda, ahová az `xmlsigntool.exe` fájlt mentette.

4. Az *.xml* konfigurációs fájl aláírásához hajtson végre egy parancsot. Használat: `xmlsigntool /version 1|2 <xml_file_path>`

A `/version` paraméter értéke az ESET Internet Security verziójától függ. Az ESET Internet Security 11.1-esnél korábbi verziója esetén a következőt használja: `/version 1`. Az ESET Internet Security aktuális verziója esetén a következőt használja: `/version 2`.

5. Az XmlSignTool kérésére adja meg, majd újból adja meg a [további beállítások jelszavát](). Az *.xml* konfigurációs fájl most már alá van írva, és használható importáláshoz a ESET Internet Security másik példányán az ESET CMD funkció beállítások jelszava hitelesítési módjának használatával.

Exportált konfigurációs fájl aláírási parancs:
`xmlsigntool /version 2 c:\config\settings.xml`



Ha a [Hozzáférési beállítások]() jelszava módosul, és importálni szeretne egy olyan konfigurációt, amelyet korábban egy régi jelszóval írtak alá, akkor ismét alá kell írnia az *.xml* konfigurációs fájlt az aktuális jelszóval. Így egy régebbi konfigurációs fájlt használhat anélkül, hogy az importálás előtt exportálnia kellene egy másik olyan gépre, amelyen fut az ESET Internet Security.

Nem javasoljuk az ESET CMD engedélyezését hitelesítés nélkül, mivel ez lehetővé teszi nem aláírt konfigurációk importálását. A **További beállítások** > **Felhasználói felület** > **Hozzáférési beállítások** részen adja meg a jelszót, így megakadályozhatja, hogy a felhasználók jogosultság nélkül módosításokat végezhessenek.

Üresjárat idején történő ellenőrzés

Az üresjárat idején történő ellenőrzés beállításai a **További beállítások** ablakban adhatók meg, amely a **Keresőmotor** > **Kártevőellenőrzések** > **Üresjárat idején történő ellenőrzés** > **Üresjárat idején történő ellenőrzés** csoportban nyitható meg. Ezek a beállítások eseményindítót adnak meg az [üresjárat idején történő ellenőrzéshez]() az alábbi esetekben:

- **Kikapcsolt képernyő vagy képernyőkímélő**
- **Számítógép zárolása**
- **Felhasználó kijelentkezése**

Az üresjárat idején történő ellenőrzés eseményindítóinak engedélyezéséhez vagy letiltásához használhatja az egyes állapotok csúszkáit.

Gyakori kérdések

Az alábbiakban megtalál néhányat a leggyakrabban feltett kérdések és tapasztalt problémák közül. Az adott probléma megoldási módjának megtekintéséhez kattintson a megfelelő témakör címére:

- Az ESET Internet Security frissítése
- Vírus eltávolítása a számítógépről
- Kommunikáció engedélyezése adott alkalmazás számára
- Szülői felügyelet engedélyezése egy fiókhoz
- Új feladat létrehozása a feladatütemezőben
- Ellenőrzési feladat ütemezése (heti)
- A következő hiba elhárítása: „A Netbank- és tranzakcióvédelem átirányítása nem sikerült a kért weboldalra”
- A További beállítások feloldása
- Hogyan hárítható el a termékdeaktiválási probléma a ESET HOME portálról?

Ha a tapasztalt problémát nem találja a fenti listában, próbálja megkeresni az ESET Internet Security online súgójában.

Ha az ESET Internet Security online súgójában sem talál megoldást a problémára vagy a kérdésére, keresse fel a rendszeresen frissített online ESET-tudásbázisunkat. A legnépszerűbb tudásbáziscikkeinkre mutató hivatkozásokat az alábbiakban találja:

- Hogyan újíthatom meg a licencemet?
- Aktiválási hibába futottam a program telepítésének végén. Mit jelent ez?
- A Windows ESET otthoni szoftver aktiválása felhasználónévvel, jelszóval vagy licenckulccsal
- Az ESET otthoni szoftver eltávolítása vagy újratelepítése
- Értesítést kaptam arról, hogy az ESET telepítése idő előtt befejeződött
- Mi a teendő a licenc megújítása után? (otthoni felhasználók esetén)
- Mi történik, ha módosítom az e-mail címem?
- ESET-termékem átvitele új számítógépre vagy eszközre
- A Windows indítása csökkentett módban vagy hálózati funkciókat is futtató csökkentett módban
- Annak megakadályozása, hogy le legyen tiltva egy biztonságos webhely

- Engedélyezze a hozzáférést a képernyőolvasó-szoftvernek az ESET GUI-hoz

Szükség esetén kérdésével vagy problémájával forduljon a műszaki támogatási szolgálatunkhoz.

Az ESET Internet Security frissítése

Az ESET Internet Security kézzel vagy automatikusan frissíthető. A frissítés indításához kattintson **Frissítés** elemre a program főablakában, majd kattintson a **Frissítések keresése** elemre.

Az alapértelmezett telepítés beállításai egy óránként végrehajtandó automatikus frissítési feladatot adnak meg. Ha módosítani szeretné az időtartamot, lépjen az **Eszközök** > **Feladatütemező** lapra.

Vírus eltávolítása a számítógépről

Ha a számítógép fertőzés jeleit mutatja, például lassabb vagy gyakran lefagy, ajánlott az alábbiakat elvégezni:

1. A program főablakában kattintson a **Számítógép ellenőrzése** lehetőségre.

2. A rendszer ellenőrzéséhez kattintson **Optimalizált ellenőrzés** hivatkozásra.

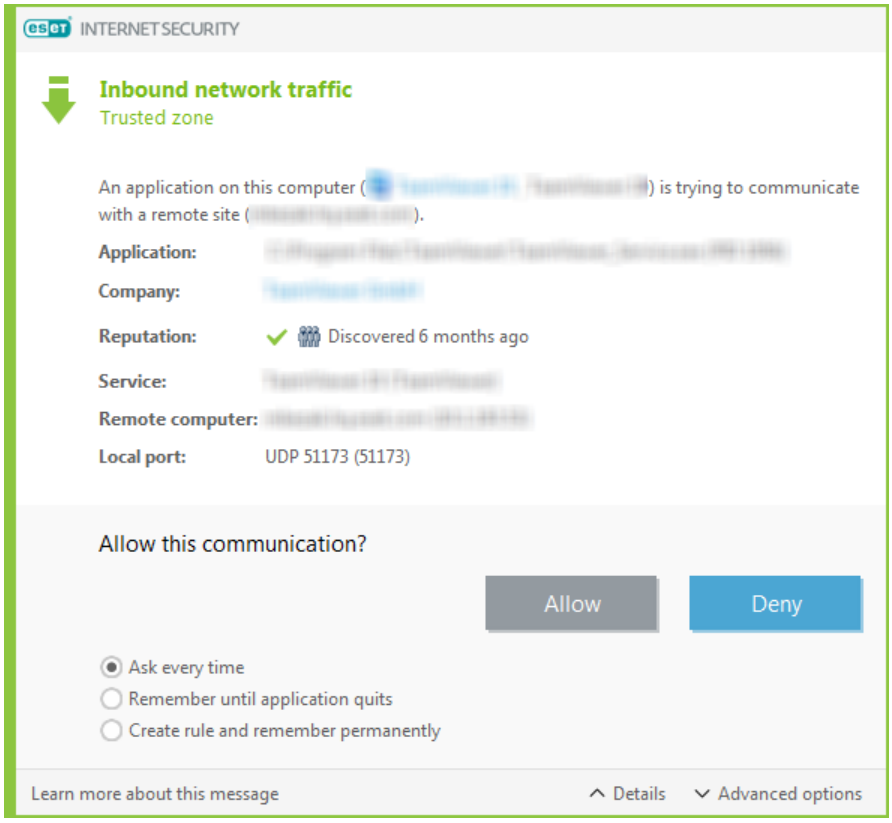
3. Az ellenőrzés befejeztével tekintse át az ellenőrzött, fertőzött és megtisztított fájlok számát tartalmazó naplót.

4. Ha csak a lemez egy részét szeretné ellenőrizni, válassza az **Egyéni ellenőrzés** lehetőséget, és adja meg az ellenőrizni kívánt célterületeket.

További információt a rendszeresen frissített ESET-tudásbáziscikk tartalmaz.

Kommunikáció engedélyezése adott alkalmazás számára

Ha interaktív módban a program új kapcsolatot észlel, és nincs szabályegyezés, akkor felajánlja a kapcsolat engedélyezését vagy tiltását. Ha azt szeretné, hogy az ESET Internet Security minden alkalommal ugyanazt a műveletet hajtsa végre, amikor egy adott alkalmazás kapcsolatot próbál meg létrehozni, jelölje be a **Művelet megjegyzése (szabály létrehozása)** jelölőnégyzetet.



Mielőtt az ESET Internet Security észlelné az alkalmazásokat, új tűzfalszabályokat hozhat létre az alkalmazásokhoz a Tűzfal beállítási ablakban. Nyissa meg a fő programablakot > **Beállítások** > **Hálózati védelem** > Kattintson a ⚙ ikonra a **Tűzfal** > **Konfigurálás** > **Speciális** > **Szabályok** > **Szerkesztés** gomb mellett.

Kattintson a **Hozzáadás** gombra az **Általános** lapon, írja be a szabály nevét, irányát és kommunikációs protokollját. Ebben az ablakban megadhatja a szabály alkalmazásakor végrehajtandó műveletet is.

A **Helyi** lapon adja meg az alkalmazás elérési útját és a helyi kommunikációs portot. A **Távoli** lapon adhatja meg a távoli címet és portot (ha van ilyen). Az újonnan létrehozott szabályt a program azonnal alkalmazza, ha a kérdéses alkalmazás újra kommunikálni kezd.

Szülői felügyelet engedélyezése egy fiókhoz

A szülői felügyelet az alábbi lépésekkel aktiválható egy adott felhasználói fiókhoz:

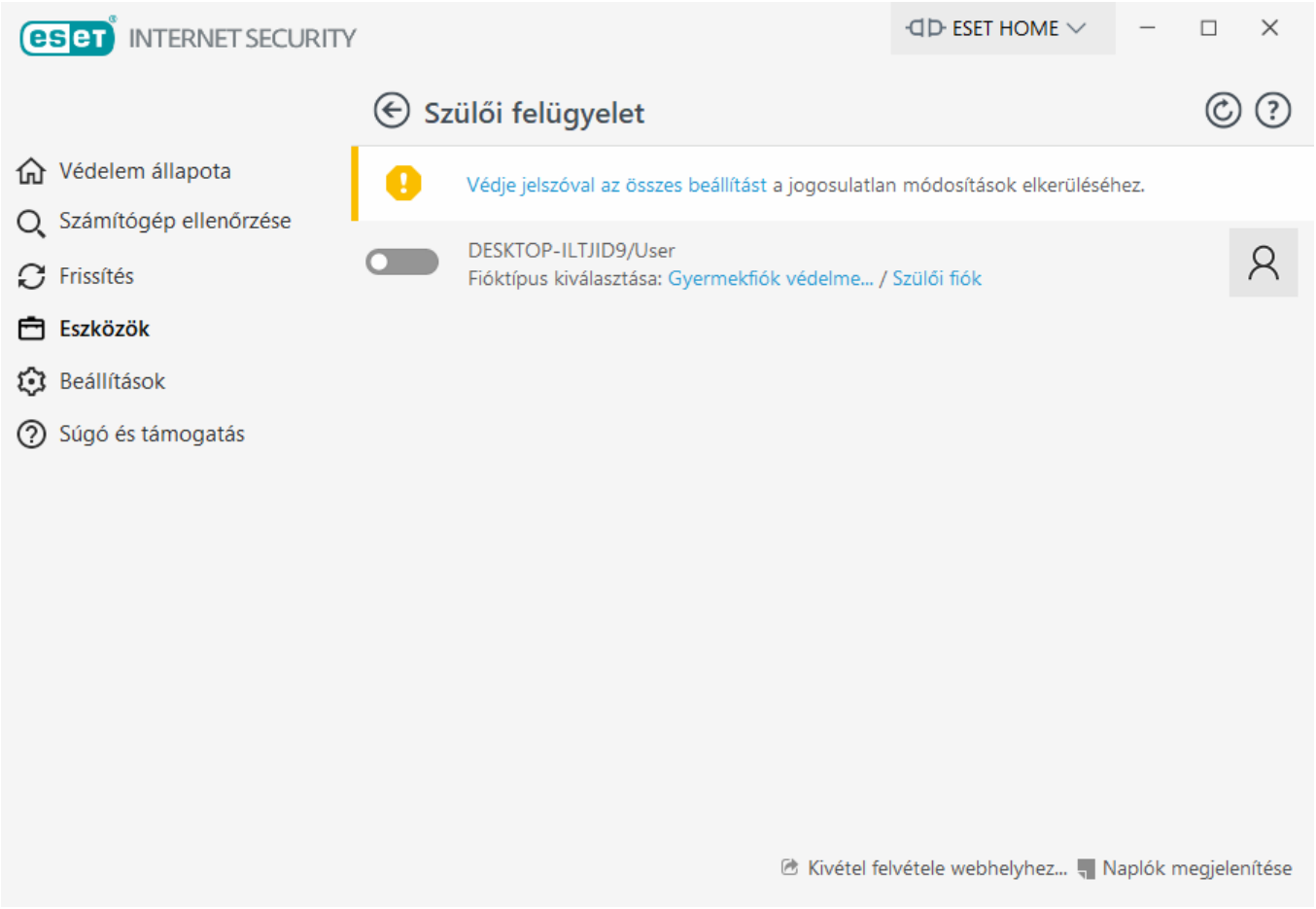
1. A szülői felügyelet alapértelmezés szerint le van tiltva az ESET Internet Security alkalmazásban. A szülői felügyelet két módon aktiválható:

   • Kattintson a ⬭ elemre a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** lehetőség mellett a program főablakában, és a szülői felügyelet állapotát módosítsa engedélyezettre.

   • Az F5 billentyűt lenyomva nyissa meg a **További beállítások** fastruktúrát, lépjen a **Web és e-mail** > **Szülői felügyelet** lapra, majd aktiválja **A szülői felügyelet engedélyezése** szöveg melletti csúszkát.

2. A program főablakában kattintson a **Beállítások** > **Biztonsági eszközök** > **Szülői felügyelet** elemre. Habár a **Szülői felügyelet** mellett az **Engedélyezve** felirat látható, a **Gyermekfiók védelme** vagy a **Szülői fiók** elemre kattintva konfigurálnia kell a szülői felügyeletet a kívánt fiókhoz. Ehhez kattintson a nyilat ábrázoló szimbólumra, majd a következő ablakban válassza ki a születésnapot a hozzáférés korlátozásához, és adja meg az adott kornak megfelelő, ajánlott weboldalakat. A program engedélyezi a szülői felügyeletet a megadott

felhasználói fiókhoz. A fiók neve alatt található **Letiltott tartalmak és beállítások** hivatkozásra kattintva a Kategóriák lapon testre szabhatja az engedélyezni vagy letiltani kívánt kategóriákat. A kategóriákba nem sorolható egyéni weboldalak engedélyezéséhez vagy letiltásához kattintson a Kivételek fülre.



Új feladat létrehozása a feladatütemezőben

Ha új feladatot szeretne létrehozni az **Eszközök** > **További eszközök** > **Feladatütemező** eszközben, kattintson a **Hozzáadás** gombra, vagy kattintson a jobb gombbal, és a helyi menüben válassza a **Hozzáadás** parancsot. 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. 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.

- **Kézi indítású számítógép-ellenőrzés** – Számítógép-ellenőrzés végrehajtása, amelynek során a számítógépen található fájlokat és mappákat vizsgálja meg a program.

- **Frissítés** – Frissítési feladat ütemezése a modulok frissítésére.

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. Írja be a feladat nevét a **Feladat neve** mezőbe, és kattintson a **Tovább** gombra. Adja meg a feladat gyakoriságát. A választható lehetőségek az alábbiak: **Egyszer**, **Ismétlődően**, **Naponta**, **Hetente** és **Esemény hatására**. Válassza a **Feladat kihagyása akkumulátorról történő futtatáskor** lehetőséget, ha minimalizálni szeretné a rendszererőforrásokat, miközben a laptop akkumulátorról működik. A rendszer a feladatot a **Feladat végrehajtása** mezőkben megadott dátumon és időpontban fogja futtatni. Ezután meghatározhatja, hogy milyen műveletet hajtson végre a rendszer akkor, ha a feladat nem hajtható végre vagy nem fejezhető be az ütemezett időpontban. A választható lehetőségek az alábbiak:

- **A következő ütemezett időpontban**
- **Amint lehetséges**
- **Azonnal, ha a legutóbbi futtatás óta eltelt idő túllépi a megadott értéket** (az időköz az **Utolsó futtatás óta eltelt idő (óra)** görgetődobozban adható meg)

A következő lépésben a szoftver megjeleníti az aktuális ütemezett feladat teljes összegzését. Ha befejezte a módosításokat, kattintson a **Befejezés** gombra.

Megjelenik egy párbeszédpanel, amelyen kiválaszthatók az ütemezett feladathoz használandó profilok. Itt megadhatja az elsődleges és a másodlagos profilt. A másodlagos profil akkor használatos, ha a feladat nem hajtható végre az elsődleges profillal. A megerősítéshez kattintson a **Befejezés** gombra. Ezzel a program felveszi az új ütemezett feladatot a jelenleg ütemezett feladatok listájára.

Heti számítógép-ellenőrzés ütemezése

Ha rendszeres feladatot szeretne ütemezni, nyissa meg a program főablakát, és kattintson az **Eszközök** > **További eszközök** > **Feladatütemező** gombra. Az alábbi rövid útmutató bemutatja, hogy miként ütemezhet egy olyan ismétlődő feladatot, amely hetente ellenőrzi a helyi lemezeket. Részletesebb utasításokat a vonatkozó tudásbáziscikkben talál.

Ellenőrzési feladat ütemezéséhez:

1. Kattintson a **Hozzáadás** gombra a Feladatütemező főképernyőjén.

2. Adja meg a feladat nevét, majd válassza ki a **Kézi indítású számítógép-ellenőrzés** menüpontot a **Feladattípus** legördülő menüből.

3. A feladat gyakoriságának válassza ki a **Heti** lehetőséget.

4. Állítsa be a feladat végrehajtásának napját és időpontját.

5. Válassza a **Hajtsa végre a feladatot az első adandó alkalommal** lehetőséget a feladat későbbi végrehajtásához, ha az ütemezett feladat valamilyen okból nem fut (például mert a számítógépet kikapcsolták).

6. Tekintse át az ütemezett feladat összegzését, és kattintson a **Befejezés** gombra.

7. A **Célterületek** legördülő listában válassza a **Helyi meghajtók** elemet.

8. A feladat alkalmazásához kattintson a **Befejezés** gombra.

A következő hiba elhárítása: „A Netbank- és tranzakcióvédelem átirányítása nem sikerült a kért weboldalra”

> **Az Összes böngésző védelme funkció használata a webhely-átirányítás helyett**
> Alapértelmezés szerint a Netbank- és tranzakcióvédelem által védett böngésző az aktuálisan használt böngészőben indul el egy ismert netbankos webhely meglátogatása után. A webhely-átirányítás helyett az Összes böngésző védelme funkciót is használhatja az összes támogatott webböngésző biztonságos módban való elindításához. Ez lehetővé teszi az interneten való böngészést, az internetes banki szolgáltatások elérését, valamint az online tranzakciókat átirányítás nélkül, egyetlen biztonságos böngészőablakban.
> Az Összes böngésző védelme funkció használatához nyissa meg a fő programablakot, lépjen a **Beállítások** > **Biztonsági eszközök** lapra, majd engedélyezze az **Összes böngésző védelme** melletti csúszkát.

A webhely-átirányítási hiba elhárításához kövesse az alábbi lépéseket:

> **Az egyes műveletek végrehajtása után ellenőrizze, hogy működik-e a Netbank- és tranzakcióvédelem**
> Ha a böngészőablak továbbra sem működik, hajtsa végre a következő műveleteket addig, amíg ismét nem működik.

1. Indítsa újra a számítógépet.

2. Gondoskodjon arról, hogy a Windows operációs rendszer és az ESET Internet Security legújabb verzióját használja: Az ESET Windows otthoni termékek frissítése a legújabb verzióra.

3. Előfordulhat, hogy külső gyártású biztonsági szoftver, VPN vagy tűzfal okoz problémát. Ideiglenesen tiltsa le vagy távolítsa el a szoftvert.

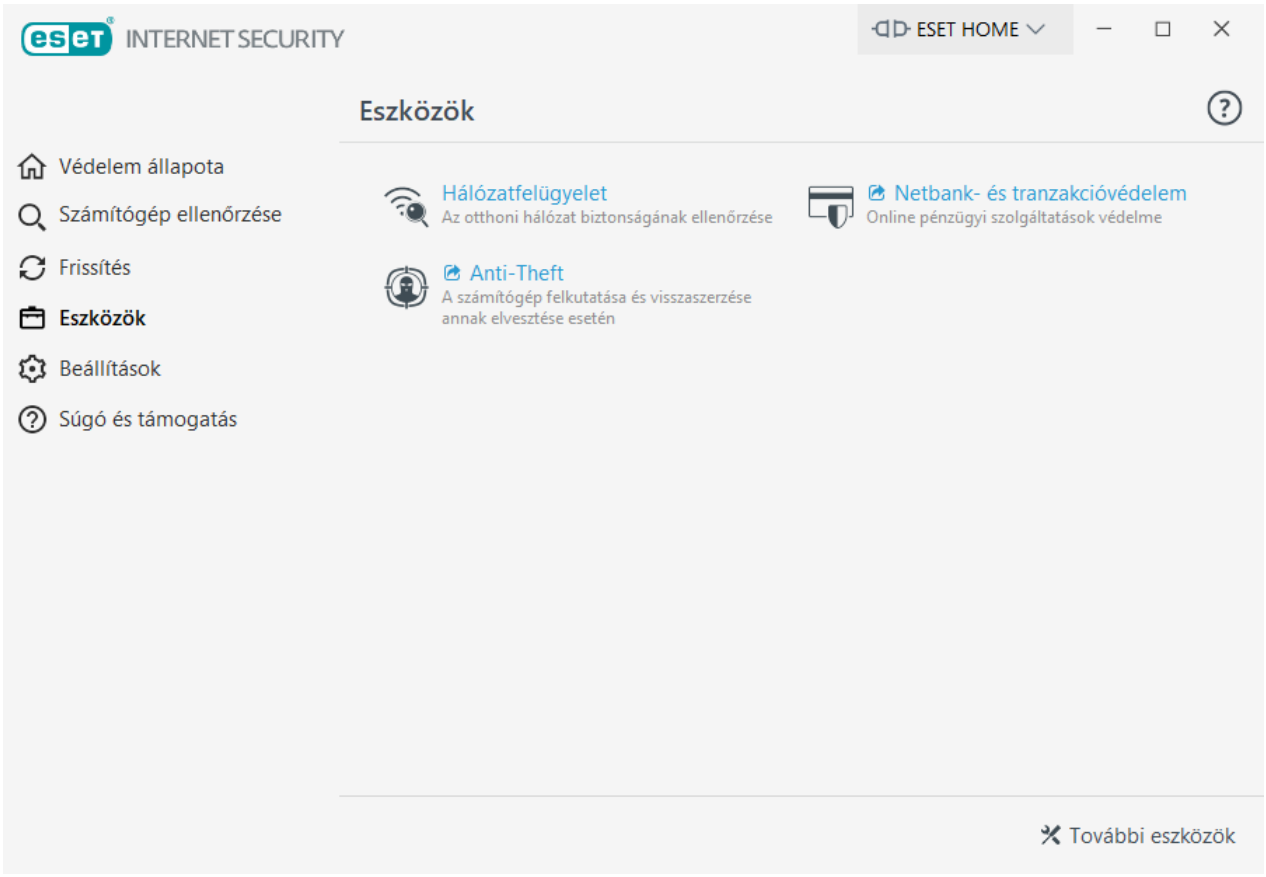
4. Tiltsa le az összes külső gyártású böngészőbővítményt.

5. Ürítse ki a böngésző gyorsítótárát. Hogyan üríthető ki a Firefox gyorsítótára vagy a Google Chrome gyorsítótára a böngészőmben?

6. Győződjön meg arról, hogy az alapértelmezett böngészője nincs kizárva a **További beállítások** > **Web és e-mail** > **Protokollszűrés** > **Kizárt alkalmazások listában**. A További beállítások megnyitása.

7. Ha nem frissítette az ESET-terméket az előző lépésekben, távolítsa el, majd telepítse újra az ESET-terméket ismét. A telepítés után indítsa újra a számítógépet.

8. Ha a probléma továbbra is fennáll, engedélyezheti az Összes böngésző védelme funkciót, vagy hozzáférhet a biztonságos böngészőhöz a fő programablak > **Eszközök** > **Netbank- és tranzakcióvédelem** lapról.



A Netbank- és tranzakcióvédelem a védelem egy újabb rétege, amellyel megóvhatja pénzügyi adatait az online tranzakciók során.

A legtöbb esetben a Netbank- és tranzakcióvédelem biztonságos böngésző az éppen használt böngészőben nyílik meg, miután felkeresett egy ismert netbankos webhelyet.

Válasszon a biztonságos böngésző alábbi konfigurációs beállításai közül:

- **Összes böngésző védelme** – Ha engedélyezve van, az összes támogatott webböngésző biztonságos módban indul. Ez lehetővé teszi az interneten való böngészést, az internetes banki szolgáltatások elérését, valamint az online vásárlásokat és tranzakciókat egyetlen biztonságos böngészőablakban, átirányítás nélkül.

- **Webhely-átirányítás** (alapértelmezett) – A védett webhelyek listájából származó webhelyek és a belső internetes banki listák átirányítása a biztonságos böngészőbe. Kiválaszthatja, hogy melyik böngésző (szabványos vagy biztonságos) legyen megnyitva.

- Mindkét előző beállítás le van tiltva – A biztonságos böngésző eléréséhez az ESET Internet Security szolgáltatásban kattintson az **Eszközök** > **Netbank- és tranzakcióvédelem** elemre, vagy kattintson a **Netbank- és tranzakcióvédelem** asztali ikonra. A Windows rendszerben alapértelmezettként beállított böngésző ekkor elindul biztonságos módban.

A biztonságos böngésző viselkedésének konfigurálásához tekintse meg a Netbank- és tranzakcióvédelem speciális beállítása című részt. Az Összes böngésző védelme funkció engedélyezéséhez az ESET Internet Security szolgáltatásban kattintson a **Beállítások** > **Biztonsági eszközök** elemre, majd engedélyezze az **Összes böngésző védelme** csúszkát.

A HTTPS használatával titkosított kommunikáció szükséges a védett böngészéshez. A következő böngészők

támogatják a Netbank- és tranzakcióvédelmet:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

A Netbank- és tranzakcióvédelem funkcióról az ESET alábbi tudásbáziscikkében talál további részleteket angol és néhány további nyelven:

- Hogyan használhatom az ESET Netbank- és tranzakcióvédelem modult?
- Az ESET Netbank- és tranzakcióvédelem engedélyezése vagy letiltása egy adott webhelyen
- A Netbank- és tranzakcióvédelem szüneteltetése vagy letiltása az ESET Windows otthoni termékekben
- ESET Netbank- és tranzakcióvédelem – gyakori hibák
- ESET-szójegyzék | Netbank- és tranzakcióvédelem

Ha nem oldódott meg a probléma, küldjön e-mailt az ESET műszaki támogatási szolgálatának.

A jelszóval védett További beállítások feloldása

Amikor használni szeretné a védett További beállítások funkciót, megjelenik a jelszó beírására szolgáló ablak. Ha elfelejti vagy elveszíti a jelszót, kattintson a **Jelszó visszaállítása** elemre, majd adja meg a licenc regisztrálásához használt e-mail-címet. Az ESET ekkor küld Önnek e-mailben egy ellenőrző kódot. Adja meg az ellenőrző kódot, majd írja be és erősítse meg a jelszót. Az ellenőrző kód hét napig érvényes.

Jelszó visszaállítása ESET HOME-fiókján keresztül – Akkor használja ezt a lehetőséget, ha az aktiváláshoz használt licenc a ESET HOME-fiókjához van társítva. Írja be a ESET HOME-fiókjába való bejelentkezéshez használt e-mail-címet.

Ha nem emlékszik az e-mail-címre, vagy nem tudja visszaállítani a jelszót, kattintson a **Kapcsolatfelvétel a műszaki terméktámogatással** szövegre. Ekkor a rendszer átirányítja az ESET webhelyére, ahol kapcsolatba léphet Műszaki terméktámogatási szolgálatunkkal.

Kód generálása a Műszaki támogatási szolgálat számára – Itt generálhat egy kódot a Műszaki támogatási szolgálat számára. Másolja be a Műszaki támogatási szolgálat által biztosított kódot, majd kattintson a **Rendelkezem ellenőrző kóddal** elemre. Adja meg az ellenőrző kódot, majd írja be és erősítse meg a jelszót. Az ellenőrző kód hét napig érvényes.

További információkért tekintse meg a következőt: A beállítási jelszó feloldása az ESET Windows otthoni termékekben.

Hogyan hárítható el a termékdeaktiválási probléma a ESET HOME portálról?

A licenc nincs aktiválva

Ez a hibaüzenet akkor jelenik meg, ha a licenctulajdonos deaktiválja az ESET Internet Security szolgáltatást a ESET HOME portálról, vagy a ESET HOME-fiókjával megosztott licenc már nincs megosztva. A probléma elhárítása:

- Kattintson az **Aktiválás** elemre, és az egyik aktiválási módszerrel aktiválja az ESET Internet Securityszolgáltatást.
- Vegye fel a kapcsolatot a licenc tulajdonosával, és értesítse, hogy az ESET Internet Security szolgáltatást deaktiválta a licenctulajdonos, vagy a licenc már nincs megosztva Önnel. A tulajdonos a ESET HOME szolgáltatásban elháríthatja a problémát.

A termék inaktiválva, az eszköz leválasztva

Ez a hibaüzenet azután jelenik meg, hogy eltávolított egy eszközt a ESET HOME-fiókból. A probléma elhárítása:

- Kattintson az **Aktiválás** elemre, és az egyik aktiválási módszerrel aktiválja az ESET Internet Securityszolgáltatást.
- Vegye fel a kapcsolatot a licenc tulajdonosával, és értesítse, hogy az ESET Internet Security deaktiválódott, és az eszköz le lett választva a ESET HOME portálról.
- Ha Ön a licenc tulajdonosa, és nem tud ezekről a módosításokról, tekintse át a ESET HOME Tevékenységnaplóját. Ha gyanús tevékenységet észlel, módosítsa a ESET HOME-fiók jelszavát, és lépjen kapcsolatba az ESET műszaki terméktámogatásával.

A termék inaktiválva, az eszköz leválasztva

Ez a hibaüzenet azután jelenik meg, hogy eltávolított egy eszközt a ESET HOME-fiókból. A probléma elhárítása:

- Kattintson az **Aktiválás** elemre, és az egyik aktiválási módszerrel aktiválja az ESET Internet Securityszolgáltatást.
- Vegye fel a kapcsolatot a licenc tulajdonosával, és értesítse, hogy az ESET Internet Security deaktiválódott, és az eszköz le lett választva a ESET HOME portálról.
- Ha Ön a licenc tulajdonosa, és nem tud ezekről a módosításokról, tekintse át a ESET HOME Tevékenységnaplóját. Ha gyanús tevékenységet észlel, módosítsa a ESET HOME-fiók jelszavát, és lépjen kapcsolatba az ESET műszaki terméktámogatásával.

A licenc nincs aktiválva

Ez a hibaüzenet akkor jelenik meg, ha a licenctulajdonos deaktiválja az ESET Internet Security szolgáltatást a ESET HOME portálról, vagy a ESET HOME-fiókjával megosztott licenc már nincs megosztva. A probléma elhárítása:

• Kattintson az **Aktiválás** elemre, és az egyik aktiválási módszerrel aktiválja az ESET Internet Securityszolgáltatást.

• Vegye fel a kapcsolatot a licenc tulajdonosával, és értesítse, hogy az ESET Internet Security szolgáltatást deaktiválta a licenctulajdonos, vagy a licenc már nincs megosztva Önnel. A tulajdonos a ESET HOME szolgáltatásban elháríthatja a problémát.

Felhasználói élmény javítását célzó program

Ha részt vesz az ügyfélélmény javítása programban, névtelen információkat biztosít az ESET-nek a termékeink használatáról. Az adatfeldolgozással kapcsolatban az Adatvédelmi nyilatkozatban talál további információt.

Az Ön hozzájárulása

A programban való részvétel önkéntes és beleegyezésen alapul. A csatlakozás után nincs további teendője. Bármikor visszavonhatja a beleegyezését a termékbeállítások módosításával. Ezzel meggátolja az Öntől származó további névtelen adatok feldolgozását.

Bármikor visszavonhatja a beleegyezését a termékbeállítások módosításával:

- A Felhasználói élmény javítását célzó program beállításainak módosítása az ESET Windows otthoni termékekben

Milyen típusú információkat gyűjtünk?

A termék használatával kapcsolatos adatok

Ezek az információk arra vonatkoznak, hogyan használják a termékeinket. Segítségükkel meg tudjuk állapítani, hogy a felhasználók mely funkciókat használják a leggyakrabban, milyen beállításokat módosítanak, és mennyi időt töltenek a termék használatával.

Az eszközökkel kapcsolatos adatok

Ezeknek az információknak a begyűjtésével meg tudjuk állapítani, hogy hol és milyen eszközökön használják a termékeinket. Ilyen információ például az eszközmodell, az ország, valamint az operációs rendszer neve és verziója.

Hibadiagnosztikai adatok

A hibákkal és az összeomlásokkal kapcsolatos információkat is begyűjtjük, például azt, hogy milyen hiba történt, és milyen műveletek vezettek a hibához.

Miért gyűjtünk ilyen információkat?

Ezeket a névtelen információkat arra használjuk fel, hogy felhasználóinknak, köztük Önnek, még jobb termékeket bocsáthassunk a rendelkezésére. Segítenek abban, hogy termékeink modernek, könnyen használhatók és lehetőleg hibamentesek legyenek.

Ki felügyeli ezeket az információkat?

Az ESET, spol. s r.o. a program keretében begyűjtött adatok kizárólagos kezelője. Nem osztjuk meg külső felekkel az adatokat.

Végfelhasználói licencszerződés

Hatályos 2021. október 19-től.

FONTOS: Kérjük, hogy a letöltés, telepítés, másolás vagy használat előtt olvassa el figyelmesen a termék használatára vonatkozó alábbi feltételeket. **A SZOFTVER LETÖLTÉSÉVEL, TELEPÍTÉSÉVEL, MÁSOLÁSÁVAL VAGY HASZNÁLATÁVAL ÖN ELFOGADJA EZEKET A FELTÉTELEKET, ÉS TUDOMÁSUL VESZI AZ ADATVÉDELMI SZABÁLYZATOT.**

Végfelhasználói licencszerződés

Jelen végfelhasználói licencszerződés („a Szerződés”) alapján, amely egyfelől az ESET, spol. s r. o. (székhelye: Einsteinova 24, 85101 Bratislava, Slovak Republic; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B; cégjegyzékszám: 31333532; („ESET” vagy „a Gyártó”), másfelől Ön mint természetes vagy jogi személy („Ön” vagy „a Végfelhasználó”) között jött létre, Ön jogosult a jelen Szerződés 1. pontjában meghatározott szoftver használatára. A jelen Szerződés 1. pontjában meghatározott Szoftver az alábbiakban megadott feltételeknek megfelelően adathordozón tárolható, e-mailben küldhető, az internetről vagy a Gyártó szervereiről letölthető, illetve más forrásokból beszerezhető.

JELEN SZERZŐDÉS VÉGFELHASZNÁLÓI JOGOSULTSÁGOKRA VONATKOZIK, ÉS NEM ÉRTÉKESÍTÉSI SZERZŐDÉS. Az értékesítési csomagban található szoftvermásolat és a fizikai adathordozó, valamint a jelen Szerződés alapján a Végfelhasználó által készíthető bármely másolat továbbra is a Gyártó tulajdonát képezi.

Ha az „Elfogadom” vagy egyéb, jóváhagyásra szolgáló gombra kattint a Szoftver telepítése, letöltése, másolása vagy használata közben, illetve bármilyen alkalmazásáruházból való telepítésekor, azzal elfogadja a jelen Szerződés feltételeit és jóváhagyja az Adatvédelmi szabályzatot. Ha nem ért egyet a Szerződés és vagy az Adatvédelmi szabályzatot bármely rendelkezésével, azonnal kattintson a megszakításra szolgáló gombra, szakítsa meg a letöltést vagy a telepítést, illetve semmisítse meg vagy küldje vissza a Szoftvert, a telepítési adathordozót, valamint a kapcsolódó dokumentációt és a vásárlási számlát a Gyártónak vagy abba az üzletbe, ahol a Szoftvert beszerezte.

ÖN ELFOGADJA, HOGY A SZOFTVER HASZNÁLATÁVAL KIFEJEZI, HOGY A JELEN SZERZŐDÉST ELOLVASTA, MEGÉRTETTE, ÉS RENDELKEZÉSEIT ÖNMAGÁRA NÉZVE KÖTELEZŐ ÉRVÉNYŰNEK ISMERTE EL.

1. **Szoftver**. A jelen Szerződésben a „Szoftver” kifejezés a következőt jelenti: (i) a jelen Szerződéshez mellékelt számítógépes program és annak összes komponense; (ii) a lemezek, CD-ROM-ok, DVD-k, e-mailek és mellékleteik vagy más adathordozók tartalma, amelyhez a jelen Szerződés tartozik, beleértve az adathordozón nyújtott vagy e-mailben küldött, illetve interneten letölthető Szoftver tárgykódját; (iii) minden kapcsolódó írásbeli használati utasítás vagy a Szoftverhez tartozó egyéb dokumentáció, beleértve többek között a szoftver bármilyen leírását, specifikációját, tulajdonságainak vagy működésének ismertetését, a működési környezet leírását, amelyben a Szoftvert használják, a Szoftver telepítési vagy használati útmutatóit, a Szoftver megfelelő használatára vonatkozó bármilyen leírást („Dokumentáció”); (iv) a Szoftver másolatai, lehetséges hibáinak javításai, kiegészítései, bővítményei, módosított verziói, összetevőinek frissítései (ha vannak), amelyekhez a Gyártó a jelen Szerződés 3. pontja szerint Önnek használati engedélyt adott. A Szoftver kizárólag végrehajtható tárgykód formájában szerezhető be.

2. **Telepítés, Számítógép és Licenckulcs**. Az adathordozón biztosított, e-mailben küldött vagy az internetről, illetve a Gyártó szervereiről letöltött vagy más forrásból megszerzett Szoftvert telepíteni kell. A Szoftvert megfelelően konfigurált számítógépre kell telepíteni, amely legalább a Dokumentációban közölt követelményeknek megfelel. A telepítési módszer leírása a Dokumentációban található. A Szoftvert futtató Számítógépre nem telepíthető olyan számítógépes program vagy hardver, amely kedvezőtlen hatással lehet a Szoftverre. A Számítógép olyan hardver – korlátozás nélkül ideértve a személyi számítógépeket, laptopokat, munkaállomásokat, tenyérszámítógépeket, okostelefonokat, kézi elektronikus készülékeket, illetve egyéb elektronikus eszközöket –, amelyre a Szoftver készült, és amelyre telepíteni fogják, illetve amelyen használni fogják a Szoftvert. A Licenckulcs szimbólumok, betűk, számok, illetve speciális jelek egyedi sorozata, amelyet a Végfelhasználó kap annak érdekében, hogy legálisan használhassa a Szoftvert vagy annak egy adott verzióját, illetve kiterjeszthesse a Licencet a jelen Szerződéssel összhangban.

3. **Licenc**. Amennyiben Ön elfogadja a jelen Szerződés rendelkezéseit, az érvényességi időn belül megfizeti a licencdíjat, és megfelel az itt előírt összes feltételnek, a Gyártó az alábbi jogokat (a továbbiakban „a Licenc”) biztosítja az Ön számára: a) Telepítés és használat:

a) **Telepítés és használat.** Nem kizárólagos és nem átruházható jogot szerez a Gyártótól arra, hogy a Szoftvert egy számítógép merevlemezére vagy más tartós adattárolásra alkalmas adathordozóra telepítse, a Szoftvert számítógépes rendszerek memóriájába telepítse, és ott tárolja, valamint megjelenítse azt.

b) **A licencek számának kikötése.** A Szoftver használatára vonatkozó jogosultságot a Végfelhasználók száma határozza meg. Egy Végfelhasználónak kell tekinteni a következőt: (i) a Szoftver telepítése egyetlen számítógépre, vagy (ii) ha a licenc terjedelme az e-mail postafiókok számához kötött, a Végfelhasználó egy olyan számítógép-használót jelent, aki levelezőprogramon (Mail User Agent, levelezési felhasználói ügynök, „Levelezőprogram”) keresztül fogad e-mailt. Ha egy Levelezőprogram e-mailt fogad, majd azt automatikusan továbbítja több felhasználónak, akkor a Végfelhasználók számának meghatározása az alapján történik, hogy ténylegesen hány felhasználó kapja meg a továbbítással az e-mailt. Ha a levelezési szerver levelezési kapuként működik, a Végfelhasználók száma megegyezik azon levelezésiszerver-használók számával, akiknek a kapu szolgáltatást nyújt. Csak egy számítógépre szükséges licencet szerezni, ha meghatározatlan számú e-mail-cím (alias) van átirányítva egy felhasználónak, és csak egyetlen felhasználó fogadja őket, továbbá a kliens nem továbbítja automatikusan az üzeneteket nagyszámú felhasználóhoz. A Licenc egyidejűleg csak egy számítógépen használható. A Végfelhasználó csak abban a mértékben jogosult megadni a Licenckulcsot a Szoftvernek, amennyi joga van használni a Szoftvert a Gyártó által adott Licencek száma alapján. A Licenckulcs bizalmas jellegű, Ön nem oszthatja meg harmadik féllel, illetve nem engedélyezheti a Licenckulcs használatát harmadik félnek, kivéve akkor, ha a jelen Szerződés vagy a Gyártó ezt megengedi. Ha a Licenckulcs illetéktelenekhez kerül, haladéktalanul értesítse a Gyártót.

c) **Otthoni/üzleti változat.** A Szoftver Otthoni verziója kizárólag privát, illetve nem kereskedelmi környezetben használható otthoni és családi használatra. A Szoftver Üzleti verzióját kereskedelmi környezetben való használatra lehet beszerezni, valamint a Szoftver levelezési szervereken, levelezési átjárókon vagy internetes átjárókon való használatához.

d) **A licenc érvényességi időszaka.** A Szoftver használatára vonatkozó jogosultság korlátozott időtartamra szól.

e) **Számítógép-gyártói (OEM-) szoftver.** A számítógép-gyártói (OEM) besorolású szoftver használata arra a számítógépre van korlátozva, amelyen beszerezte. amellyel megvásárolta azt, és másik számítógépre nem vihető át.

f) **Kereskedelmi forgalomba nem hozható termék és próbaverzió.** A „kereskedelmi forgalomba nem hozhatóként” minősített Szoftver és a próbaverzió nem lehet díjköteles, és kizárólag a Szoftver funkcióinak ellenőrzésére és tesztelésére, valamint szemléltetési célra használható.

g) **A licenc lejárata.** A Licenc az érvényességi időszak végén automatikusan lejár. Ha Ön nem teljesíti a jelen

Szerződés bármely rendelkezését, a Gyártónak jogában áll felmondani a Szerződést bármely jogosultság vagy az ilyen esetekben a Gyártó számára elérhető jogorvoslati lehetőség megsértése nélkül. A Licenc felmondása esetén a Szoftvert, illetve az összes biztonsági másolatot haladéktalanul törölnie kell, meg kell semmisítenie, vagy a saját költségén vissza kell küldenie az ESET címére vagy abba az üzletbe, ahol a Szoftvert beszerezte. A Licenc lejárata esetén a Gyártónak szintjén jogában áll felmondania a Végfelhasználó jogosultságát a Szoftver olyan funkcióinak használatára, amelyek a Gyártó vagy harmadik felek szervereihez való kapcsolódást igényelnek.

4. **Adatgyűjtésre és internetkapcsolatra vonatkozó követelmények.** A Szoftver megfelelő működtetéséhez, valamint az Adatvédelmi szabályzatnak megfelelő adatgyűjtés céljából internetkapcsolat szükséges, és rendszeres időközönként csatlakoznia kell a Gyártó vagy a harmadik fél szervereihez. Az internetkapcsolatra és az adatgyűjtésre a Szoftver alábbi funkcióihoz van szükség:

a) **A Szoftver frissítései.** A Gyártó jogosult, de nem köteles időnként kiadni frissítéseket („Frissítések”) a Szoftverhez. Ez a funkció a Szoftver általános beállításai között engedélyezve van, és a Frissítések ezért automatikusan települnek, kivéve ha a Végfelhasználó letiltotta a Frissítések automatikus telepítését. A frissítések biztosításához szükség van a Licenc eredetiségének ellenőrzésére, ideértve a Számítógépre vonatkozó információkat és/vagy annak ellenőrzését, hogy megfelel-e az Adatvédelmi szabályzatnak az a platform, amelyre a Szoftver telepítve van.

A Frissítések biztosítására az Életciklus végéről szóló szabályzat („EOL szabályzat”) vonatkozik, amely a https://go.eset.com/eol_home weboldalon érhető el. Nem biztosítunk Frissítéseket, miután a Szoftver vagy bármely funkciója elérte az EOL szabályzatban meghatározott Életciklus végét.

b) **Kártevők és információk továbbítása a Gyártónak.** A Szoftver olyan funkciókat tartalmaz, amelyek mintákat gyűjtenek a vírusokról és egyéb kártékony számítógépes programokról, a gyanús, problémás, kéretlen vagy veszélyes objektumokról, többek között fájlokról, URL-címekről, IP-csomagokról vagy Ethernet-keretekről („Kártevők”), majd a mintákat elküldik a Gyártónak, beleértve, de nem kizárólag a telepítési folyamatra, arra a számítógépre és/vagy platformra vonatkozó adatokkal, amelyen a Szoftver telepítve van, valamint a szoftver működésével és funkcióival („Adatok”) együtt. Ezek az Adatok és Kártevők magukban foglalhatják a Végfelhasználóval vagy a Szoftvert futtató számítógép más felhasználóival kapcsolatos adatokat (beleértve a véletlenszerűen vagy nem szándékosan megszerzett személyes adatokat is), valamint a kártevők által érintett fájlokat a kapcsolódó metaadatokkal együtt.

Az információkat és a kártevőket a szoftver következő funkciói gyűjthetik:

i. A LiveGrid megbízhatósági rendszer végzi a kártevőkkel kapcsolatos egyirányú kivonatok gyűjtését és elküldését a Gyártónak. Ez a funkció a Szoftver általános beállításai között engedélyezhető.

ii. A LiveGrid visszajelzési rendszer hajtja végre a kártevők gyűjtését és elküldését a Gyártónak a kapcsolódó metaadatokkal és információkkal együtt. Ezt a funkciót a Végfelhasználó aktiválja a Szoftver telepítése során.

A Gyártó a kapott Adatokat és Kártevőket kizárólag a Kártevők elemzésére és tanulmányozására, a Szoftver fejlesztésére, valamint a Licenc eredetiségének ellenőrzésére használja, és megfelelő intézkedésekkel biztosítja a kapott Adatok és Kártevők bizalmas kezelését. A Szoftver fent említett funkciójának aktiválásával Ön hozzájárul ahhoz, hogy a Gyártó összegyűjtsön és feldolgozzon Kártevőket és Adatokat az Adatvédelmi szabályzatot és a vonatkozó jogszabályokat betartva. Ez a funkció bármikor kikapcsolható.

A jelen Szerződés értelmében szükség van az olyan adatok gyűjtésére, feldolgozására és tárolására, amelyek lehetővé teszik a Gyártónak az Ön beazonosítását az Adatvédelmi szabályzatnak megfelelő módon. Ön elfogadja, hogy a Gyártó saját eszközeinek segítségével ellenőrizheti, hogy Ön a jelen Szerződés előírásainak megfelelően használja-e a Szoftvert. Ön elfogadja azt is, hogy a jelen Szerződés értelmében szükség van az Ön adatainak átvitelére a Szoftver és a Gyártó számítógépes rendszerei, illetve a Gyártó forgalmazói és támogatási hálózatának részét képező üzleti partnerei által működtetett számítógépes rendszerek között folyó kommunikáció során a

Szoftver működésének biztosításához, a Szoftver használatához szükséges engedélyezés, valamint a Gyártó jogainak védelme érdekében.

A Szerződés megkötését követően a Gyártó, illetve a Gyártó forgalmazói és támogatási hálózatának részét képező üzleti partnerei jogosult az Önt azonosító alapvető adatok átadására, feldolgozására és tárolására számlázási célból, a jelen Szerződés végrehajtása érdekében, valamint azért, hogy az értesítések továbbíthatók legyenek az Ön Számítógépére.

Az adatvédelemről, a személyes adatok védelméről és az Önt mint adatalanyt megillető jogokról az Adatvédelmi szabályzat tartalmaz részletes információkat, amely a Gyártó webhelyén található, és közvetlenül a telepítési eljárás során érhető el. A szoftver súgójában is talál erről információkat.

5. **A Végfelhasználó jogainak gyakorlása**. Ön a Végfelhasználó jogait kizárólag személyesen vagy alkalmazottjai útján gyakorolhatja. Végfelhasználóként a Szoftvert csak a saját tevékenységének biztosítására és csak azon Számítógépek vagy számítógépes rendszerek védelmére használhatja fel, amelyekre vonatkozóan a Licencet megszerezte.

6. **A jogok korlátozása.** A Szoftvert nem másolhatja, nem terjesztheti, nem nyerheti ki az összetevőit, és nem készíthet belőle semmilyen származtatott tartalmat. A Szoftver használatakor az alábbi korlátozásokat kell betartania:

a) Biztonsági másolatként készíthet a Szoftverről egy másolatot tartós adattárolásra alkalmas adathordozón, feltéve, hogy a biztonsági másolatot később más számítógépen nem telepíti vagy nem használja. A Szoftver bármilyen, ettől eltérő módon történő másolása a jelen Szerződés megszegését jelenti.

b) Ön a jelen Szerződésben kifejezetten megengedett eseteken kívül nem jogosult a szoftvert és annak másolatait használni, módosítani, lefordítani, többszörözni és a használati jogát átruházni.

c) Ön a Szoftvert nem értékesítheti, használatát nem adhatja tovább, nem adhatja sem bérbe, sem kölcsön más személynek, illetve nem veheti bérbe más személytől, és nem használhatja kereskedelmi szolgáltatások nyújtásához.

d) Ön a Szoftvert nem jogosult visszafordítani, visszafejteni, vagy egyéb módon megkísérelni a Szoftver forráskódjának megszerzését, azon eseteket kivéve, melyek körében az e rendelkezés által előírt korlátozást a törvény kifejezetten tiltja.

e) Ön elfogadja, hogy a Szoftvert kizárólag olyan módon használja fel, amely megfelel az alkalmazandó jogszabályok előírásainak, amelyek alapján a Szoftvert használja, ideértve kivétel nélkül a szerzői jogról szóló törvényben és az egyéb szellemi alkotásokra vonatkozó jogszabályokban található korlátozásokat is.

f) Elfogadja, hogy a Szoftvert és annak funkcióit csak úgy használhatja, hogy azzal más Végfelhasználókat nem korlátoz e szolgáltatások elérésében. A Gyártó fenntartja magának a jogot az egyes Végfelhasználóknak nyújtott szolgáltatások hatókörének korlátozására annak érdekében, hogy a szolgáltatások használatát a lehető legnagyobb számú Végfelhasználó számára biztosíthassa. A szolgáltatások hatókörének korlátozása azt is magában foglalja, hogy a Gyártó teljes mértékben megakadályozhatja a Szoftver bármely funkciójának használatát, és törölheti a Szoftver egy adott funkciójával kapcsolatos Adatokat és információkat a Gyártó vagy harmadik fél által üzemeltetett szerverekről.

g) Ön beleegyezik abba, hogy nem folytat semmiféle olyan tevékenységet a Licenckulccsal kapcsolatban, amely megszegné a jelen Szerződés feltételeit, illetve amelynek következtében olyan személy kapná meg a Licenckulcsot, aki nem jogosult a Szoftver használatára. Ilyen tevékenység például a használt vagy nem használt Licenckulcs bármilyen formában való átadása, engedély nélküli másolása, megkettőzött vagy generált Licenkulcsok továbbadása, illetve a Szoftver használata olyan Licenkulccsal, amely nem a Gyártótól származik.

7. **Szerzői jogok**. A Szoftver és minden jogosultság, beleértve korlátozás nélkül a benne foglalt jogcímeket és szellemi tulajdonjogot, az ESET és/vagy a Licencet adó partnerei tulajdonát képezik. E jogokat a vonatkozó nemzetközi egyezmények rendelkezései és a használat helye szerinti ország alkalmazandó nemzeti jogszabályai védik. A Szoftver szerkezete, felépítése és kódja az ESET és/vagy a Licencet adó partnerei üzleti titkának és bizalmas információinak minősül. A 6(a) pontban foglalt esetet kivéve tilos a Szoftver másolása. A jelen Szerződés szerint másolt példányoknak is minden esetben tartalmazniuk kell a Szoftverrel megegyező szerzői jogokra és egyéb jogcímekre vonatkozó értesítéseket. Ha visszafordítja, visszafejti, vagy egyéb módon megkísérli a Szoftver forráskódjának megszerzését a jelen Szerződés rendelkezéseinek megszegésével, az úgy tekintendő, hogy az ezúton szerzett összes információ létrejöttének pillanatában automatikusan és visszavonhatatlanul a Gyártóra átruházza azt, a Gyártónak a jelen Szerződés megsértésével kapcsolatos jogaival együtt.

8. **Fenntartott jogok**. A Gyártó fenntartja magának a Szoftverre vonatkozó összes jogot, azokat kivéve, amelyeket Ön a Szoftver Végfelhasználójaként a jelen Szerződés keretei között gyakorolhat.

9. **Többnyelvű verzió, több adathordozón biztosított szoftver, több másolat**. Ha a Szoftver több platformot vagy nyelvet támogat, vagy ha Ön több példánnyal rendelkezik, a Szoftvert csak annyi számítógéprendszeren és azokkal a verziókkal használhatja, amelyekre a Licencet megszerezte. Ön nem jogosult a Szoftver nem használt verzióit vagy példányait értékesíteni, bérbe adni, haszonbérbe adni vagy a használatát továbbadni, kölcsönadni, illetve más személyre átruházni.

10. **A Szerződés hatálybalépése és megszűnése.** A jelen Szerződés attól a dátumtól érvényes, amikor Ön elfogadja a Szerződés feltételeit. Ön a Szerződést bármikor megszüntetheti a Szoftver, az összes biztonsági másolat és a gyártótól vagy üzleti partnereitől kapott kapcsolódó anyag végleges törlésével, megsemmisítésével vagy a saját költségen történő visszaküldésével. A Szoftver és bármely funkciójának használatára vonatkozó jog az EOL szabályzat hatálya alá tartozhat. Miután a Szoftver vagy bármely funkciója eléri az EOL szabályzatban meghatározott Életciklus végét, megszűnik a Szoftver használatára vonatkozó joga. A Szerződés megszűnésének módjától függetlenül a 7., 8., 11., 13., 19. és 21. pontban foglalt rendelkezések korlátlan ideig érvényben maradnak.

11. **VÉGFELHASZNÁLÓI JOGNYILATKOZATOK**. VÉGFELHASZNÁLÓKÉNT ÖN TUDOMÁSUL VESZI, HOGY A SZOFTVERT ANNAK „ADOTT ÁLLAPOTÁBAN”, MINDENFÉLE KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁS NÉLKÜL KAPJA, AZZAL, HOGY AZ ALKALMAZANDÓ JOGSZABÁLYOK ÁLTAL MEGENGEDETT MÉRTÉKIG SEM A GYÁRTÓ, A LICENCET ADÓ PARTNEREI VAGY LEÁNYVÁLLALATAI, SEM A SZERZŐI JOGOK JOGOSULTJAI NEM VÁLLALNAK KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁST, KÜLÖNÖSKÉPPEN, DE NEM KIZÁRÓLAGOSAN ADÁSVÉTELHEZ KAPCSOLÓDÓ JÓTÁLLÁST, MEGHATÁROZOTT CÉLRA VALÓ ALKALMASSÁGOT, VALAMINT ARRA VONATKOZÓ JOGSZAVATOSSÁGOT, HOGY A SZOFTVER NEM SÉRTI HARMADIK SZEMÉLYEK SZABADALMI, SZERZŐI, VÉDJEGYRE VONATKOZÓ VAGY EGYÉB JOGAIT. SEM A GYÁRTÓ, SEM MÁS FÉL NEM VÁLLAL JÓTÁLLÁST AZÉRT, HOGY A SZOFTVERBEN TALÁLHATÓ FUNKCIÓK MEGFELELNEK AZ ÖN ELVÁRÁSAINAK, ILLETVE HOGY A SZOFTVER MŰKÖDÉSE ZAVARTALAN ÉS HIBAMENTES LESZ. A KÍVÁNT EREDMÉNY MEGVALÓSÍTÁSÁRA ALKALMAS SZOFTVER KIVÁLASZTÁSA, TELEPÍTÉSE ÉS HASZNÁLATA, ILLETVE A SZOFTVERREL ÖN ÁLTAL ELÉRT EREDMÉNY TELJES MÉRTÉKBEN AZ ÖN FELELŐSSÉGE ÉS KOCKÁZATA.

12. **További kötelezettségvállalás kizárása**. A jelen Szerződés a benne kifejezetten felsoroltakon kívül a Gyártóra és a Licencet adó partnereire nem ró további kötelezettségeket.

13. **KORLÁTOZOTT FELELŐSSÉGVÁLLALÁS**. AZ ALKALMAZANDÓ JOGSZABÁLYOK ÁLTAL MEGENGEDETT MÉRTÉKIG A GYÁRTÓ, ILLETVE ALKALMAZOTTAI ÉS LICENCET ADÓ PARTNEREI SEMMILYEN ESETBEN SEM FELELŐSEK BÁRMIFÉLE BEVÉTEL- VAGY NYERESÉGKIESÉSÉRT, MEGHIÚSULT ÉRTÉKESÍTÉSI LEHETŐSÉGÉRT, ADATVESZTÉSÉRT, HELYETTESÍTŐ TERMÉKEK VAGY SZOLGÁLTATÁSOK BESZERZÉSÉBŐL FAKADÓ KÖLTSÉGEKÉRT, TULAJDONBAN BEKÖVETKEZETT VAGY SZEMÉLYT ÉRINTŐ KÁRÉRT, ÜZLETI FORGALOM KIESÉSÉÉRT, ÜZLETI INFORMÁCIÓ ELVESZTÉSÉRT VAGY BÁRMIFÉLE SPECIÁLIS, KÖZVETLEN, KÖZVETETT, ESETI, GAZDASÁGI, FEDEZETI, BÜNTETŐJOGI VAGY KÖVETKEZMÉNYKÁRÉRT, FÜGGETLENÜL A KÁROKOZÁS MIKÉNTJÉTŐL, ÉS ATTÓL, HOGY AZ SZERZŐDÉSBŐL,

SZÁNDÉKOS KÁROKOZÁSBÓL, GONDATLANSÁGBÓL, VAGY MÁS, FELELŐSSÉGET MEGALAPOZÓ TÉNYBŐL ERED, HA EZEK A SZOFTVER TELEPÍTÉSÉNEK, A HASZNÁLATÁNAK VAGY HASZNÁLHATATLANSÁGÁNAK OKÁN MERÜLTEK FEL, MÉG ABBAN AZ ESETBEN IS, HA A GYÁRTÓT VAGY A LICENCET ADÓ PARTNEREIT, ILLETVE LEÁNYVÁLLALATAIT ELŐZŐLEG ÉRTESÍTETTÉK AZ ILYEN KÁR BEKÖVETKEZTÉNEK LEHETŐSÉGÉRŐL. MIVEL EGYES ORSZÁGOK ÉS JOGSZABÁLYOK NEM TESZIK LEHETŐVÉ A FELELŐSSÉG KIZÁRÁSÁT, A KORLÁTOZÁSÁT VISZONT IGEN, A GYÁRTÓ, ANNAK ALKALMAZOTTAI ÉS A LICENCET ADÓ PARTNEREI, ILLETVE LEÁNYVÁLLALATAI FELELŐSSÉGE A LICENCÉRT FIZETETT DÍJ MÉRTÉKÉRE KORLÁTOZÓDIK.

14. A jelen Szerződés egyetlen rendelkezése sem érinti annak a félnek a jogait, aki a jogszabályok értelmében fogyasztónak minősül.

15. **Terméktámogatás**. Az ESET vagy az ESET által meghatalmazott harmadik felek jótállás vagy jognyilatkozatok nélkül, saját döntésüknek megfelelően terméktámogatást nyújtanak. Nem biztosítunk terméktámogatást, miután a Szoftver vagy bármely funkciója elérte az EOL szabályzatban meghatározott Életciklus végét. A terméktámogatás előkészületeként a Végfelhasználónak biztonsági másolatot kell készítenie az összes meglévő adatról, szoftverről és a program összetevőiről. Az ESET vagy/és az ESET által meghatalmazott harmadik felek nem vállalnak felelősséget az adatok, a tulajdon, a szoftver vagy a hardver terméktámogatás következtében keletkező sérüléséért vagy elvesztéséért, illetve a veszteség miatt. Az ESET vagy/és az ESET által meghatalmazott harmadik felek fenntartják a jogot, hogy eldönthessék, miszerint a probléma megoldása túllépi-e a terméktámogatás hatáskörét. Az ESET fenntartja a jogot, hogy saját hatáskörében elutasítsa, felfüggessze vagy befejezze a terméktámogatás nyújtását. Technikai terméktámogatás céljából szükség lehet Licencadatokra, Adatokra és egyéb adatokra az Adatvédelmi szabályzatnak megfelelően.

16. **A licenc átadása.** A szoftver egyik számítógéprendszerről átvihető egy másikra, feltéve ha az nem ellentétes a Szerződés feltételeivel. Ha nem ütközik a Szerződés feltételeivel, a Végfelhasználó csak a Gyártó jóváhagyásával jogosult véglegesen átadni a Licencet és a jelen Szerződésből fakadó minden jogosultságot másik Végfelhasználónak azzal a feltétellel, hogy (i) az eredeti Végfelhasználó nem tartja meg a Szoftver egyetlen másolatát sem; (ii) a jogosultságok átadása közvetlen, vagyis az eredeti Végfelhasználóról az új Végfelhasználóra történik; (iii) az új Végfelhasználónak vállalnia kell a jelen Szerződés szerint az eredeti Végfelhasználót érintő minden jogosultságot és kötelezettséget; (iv) az eredeti Végfelhasználónak át kell adnia az új Végfelhasználó részére a Szoftver eredetiségének ellenőrzését lehetővé tevő összes dokumentációt a 17. pontban leírtak szerint.

17. **A Szoftver eredetiségének ellenőrzése.** A Végfelhasználó a Szoftver használatára vonatkozó jogosultságát az alábbi módok valamelyikén igazolhatja: (i) a Gyártó vagy a Gyártó által kinevezett harmadik fél által kibocsátott licenctanúsítvánnyal; (ii) írásbeli licencszerződéssel, amennyiben készült ilyen szerződés; (iii) a Gyártó által e-mailben küldött licencadatokkal (felhasználónév és jelszó). A Szoftver eredetiségének ellenőrzése céljából szükség lehet Licencadatokra és a Végfelhasználó személyazonosítására alkalmas adatokra az Adatvédelmi szabályzatnak megfelelően.

18. **Licencek adása hatóságok és az Amerikai Egyesült Államok kormánya számára.** A Szoftver a jelen Szerződésben rögzített licencjogosultságokkal és korlátozásokkal biztosítható a hatóságok, többek között az Amerika Egyesült Államok kormánya számára.

19. **A kereskedelmi felügyeleti törvények betartása**.

a) Ön vállalja, hogy nem fogja közvetve vagy közvetlenül exportálni, újraexportálni, továbbítani vagy más módon elérhetővé tenni a Szoftvert, nem fogja semmilyen módon használni, illetve nem vesz részt olyan tevékenységben, amelynek következtében az ESET vagy holdingtársaságai, leányvállalatai és holdingtársaságainak leányvállalatai, valamint a holdingtársaságai által irányított jogalanyok („Társult vállalatok”) megsértenének kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük. Kereskedelmi felügyeleti törvénynek minősül

i. minden olyan törvény, amely szabályozást, korlátozást, illetve licencelési követelményeket szab meg áruk,

szoftverek, technológiai termékek, illetve szolgáltatások exportálásának, újraexportálásának vagy továbbításának vonatkozásában, és amelyet az Amerikai Egyesült Államok, Szingapúr, az Egyesült Királyság, az Európai Unió vagy bármely tagállama, illetve bármely olyan ország kormányzata, állami vagy szabályozó hatósága rendelt vagy fogadott el, ahol a Szerződés értelmében kötelezettségeket kell végrehajtani, illetve ahol az ESET vagy bármely társult vállalata be van jegyezve vagy működik, valamint

ii. minden olyan gazdasági, pénzügyi, kereskedelmi vagy egyéb jellegű szankció, korlátozás, embargó, importálási vagy exportálási tilalom, tiltás források vagy eszközök továbbításának vagy szolgáltatások nyújtásának vonatkozásában, illetve ezekkel egyenértékű intézkedés, amelyet az Amerikai Egyesült Államok, Szingapúr, az Egyesült Királyság, az Európai Unió vagy bármely tagállama, illetve bármely olyan ország kormányzata, állami vagy szabályozó hatósága rendelt vagy fogadott el, ahol a Szerződés értelmében kötelezettségeket kell végrehajtani, illetve ahol az ESET vagy bármely társult vállalata be van jegyezve vagy működik.

(a fenti i. és ii. pontban említett jogi aktusok együttesen „Kereskedelmi szabályozási törvények").

b) Az ESET jogában áll azonnali hatállyal felfüggeszteni vagy felmondani a jelen Feltételek szerinti kötelezettségeit abban az esetben, ha:

i. Az ESET – észszerű feltételezés révén – megállapítja, hogy a Felhasználó megsértette vagy nagy valószínűséggel megsértette a Szerződés 19 a) cikkelyét; illetve

ii. a Végfelhasználó, illetve a Szoftver kereskedelmi felügyeleti törvények hatálya alá esik, és ennek eredményeképpen az ESET – észszerű feltételezés révén – megállapítja, hogy a Szerződés szerinti kötelezettségeinek további teljesítése következtében az ESET vagy Társult vállalatai megsérthetnek kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük.

c) A Szerződés egyik rendelkezése sem azzal a szándékkal jött létre és nem értelmezhető úgy, hogy bármely felet ráveszi vagy kötelezi a vonatkozó kereskedelmi felügyeleti törvényekkel össze nem egyeztethető vagy azok értelmében büntetendő vagy tiltott cselekedek végrehajtására vagy bizonyos cselekedek mellőzésére (illetve arra, hogy beleegyezzenek ilyen cselekedek végrehajtásába vagy bizonyos cselekedek mellőzésébe).

20. **Értesítések**. Minden értesítést, a visszaküldendő Szoftvert és Dokumentációt a következő címre kell küldeni: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Az ESET fenntartja a jogot arra, hogy értesítse Önt a jelen Szerződés, az Adatvédelmi szabályzat, az EOL szabályzat és a Dokumentáció bármilyen módosításáról a Szerződés 22. cikkelye szerint. Az ESET küldhet Önnek e-maileket, alkalmazáson belüli értesítéseket a Szoftveren keresztül, illetve közzétehetünk közleményeket a webhelyünkön. Ön beleegyezik abba, hogy elektronikus formában jogi tájékoztatást fog kapni az ESET-től, beleértve a Feltételek, a Különleges feltételek vagy az Adatvédelmi irányelvek módosításával kapcsolatos értesítéseket, olyan szerződéses ajánlatokat/jóváhagyásokat vagy meghívásokat, amelyeket kezelnie kell, értesítéseket és egyéb jogi közleményeket. Az ilyen elektronikus kommunikációt írásban átvettnek kell tekinteni, kivéve akkor, ha a vonatkozó jogszabályok más kommunikációs formát írnak elő.

21. **Alkalmazandó jog**. A jelen Szerződésre a Szlovák Köztársaság törvénye az irányadó, és a szerződés a szerint értelmezendő. A Végfelhasználó és a Gyártó ezennel megállapodnak abban, hogy az alkalmazandó jog és az ENSZ által elfogadott „Nemzetközi árukereskedelmi szerződésekről szóló egyezmény" ütközése esetén az ütköző rendelkezések nem alkalmazhatók. A Gyártóval fennálló, illetve a Szoftver használatával kapcsolatos minden jogvita vagy követelés tekintetében Ön kifejezetten aláveti magát a Pozsonyi I. sz. Kerületi Bíróság kizárólagos joghatóságának, továbbá kifejezetten aláveti magát a nevezett bíróság illetékességének az ilyen jogviták rendezésében.

22. **Általános rendelkezések**. Amennyiben a jelen Szerződés bármely rendelkezése érvénytelen vagy kikényszeríthetetlen, az nem érinti a Szerződés többi részének érvényességét. A többi rendelkezés továbbra is érvényes és végrehajtható marad az itt lefektetett feltételek szerint. A jelen Szerződés angol nyelven íródott.

Amennyiben a Szerződésről bármilyen fordítás készül kényelmi okokból vagy bármely más célból, illetve bármilyen ellentmondás van a jelen Szerződés különböző nyelvi változatai között, az angol változat az irányadó.

Az ESET fenntartja a jogot arra, hogy bármikor módosítsa a Szoftvert és felülvizsgálja a jelen Feltételek pontjait, a függelékeket, a mellékeleteket, az Adatvédelmi szabályzatot, az EOL szabályzatot és a dokumentációt, illetve azok bármely részét a releváns dokumentum frissítésével (i) a Szoftver vagy az ESET megváltozott üzleti eljárásainak megfelelően, (ii) törvényi, szabályozási vagy biztonsági okokból vagy (iii) a visszaélések vagy károk megakadályozása érdekében. A Szerződés módosításáról Ön minden esetben értesítést fog kapni e-mailben, alkalmazáson belüli értesítés útján vagy egyéb elektronikus úton. Ha nem ért egyet a Szerződés javasolt módosításaival, a 10. cikkely szerint felmondhatja a módosításról szóló értesítés kézhezvételétől számított 30 napon belül. Hacsak nem mondja fel a Szerződést ezen határidőn belül, a javasolt változtatások elfogadottnak tekinthetők és kötelezővé válnak Önre nézve attól a naptól kezdve, amikor az értesítést kézhez kapta a változásról.

Az Ön és a Gyártó között létrejött jelen Szerződés jelenti a Szoftverre vonatkozó teljes szerződést, és hatályon kívül helyezi a Szoftverre vonatkozóan tett minden korábbi jognyilatkozatot, megállapodást, kötelezettségvállalást, kommunikációt vagy hirdetést.

SZERZŐDÉSHEZ CSATOLT FÜGGELÉK

Hálózaton keresztül csatlakozó eszközök biztonsági szempontból való felmérése. Kiegészítő rendelkezések vonatkoznak a Hálózaton keresztül csatlakozó eszközök biztonsági szempontból való felmérése című részhez a következők szerint:

A Szoftver tartalmaz egy olyan funkciót, amely ellenőrzi a Végfelhasználó helyi hálózatának biztonságát és a helyi hálózaton található eszközök biztonságát. Ehhez szükség van a helyi hálózat nevére és a helyi hálózaton található eszközökkel kapcsolatos adatokra, így például az állapotukra, típusukra, nevükre, IP-címükre és MAC-címükre és a licencelési adatokra. A routerek vezeték nélküli biztonsági típusára és vezeték nélküli titkosítási típusára is szükség van. Előfordulhat, hogy a funkció arról is információkat, nyújt, hogy rendelkezésre áll-e biztonsági szoftver a helyi hálózaton található eszközök védelméhez.

Az adatokkal való visszaélés elleni védelem. Kiegészítő rendelkezések vonatkoznak az Adatokkal való visszaélés elleni védelem című részre a következők szerint:

A Szoftver egyik funkciója megakadályozza az ellopott Számítógépen lévő fontos adatok elvesztését, illetve a velük való visszaélést. Ez a funkció ki van kapcsolva a Szoftver alapértelmezett beállításaiban. Az aktiváláshoz létre kell hozni egy ESET HOME-fiókot, amelyen keresztül a funkció aktiválja az adatgyűjtést a számítógép ellopása esetén. Ha engedélyezi a funkciót, akkor a Gyártó megkapja az ellopott Számítógéppel kapcsolatos adatokat, amelyek magukban foglalhatják a Számítógép hálózati helyét, a Számítógép képernyőjén megjelenő tartalmat, a Számítógép konfigurációját és a Számítógéphez csatlakoztatott kamera által rögzített adatokat (a továbbiakban „Adatok”). A Végfelhasználó jogosult arra, hogy a funkció által megszerzett és a ESET HOME-fiók által biztosított Adatokat kizárólag a számítógép ellopásából adódó hátrányos helyzet megszüntetése céljából felhasználja. Kizárólag a funkció rendeltetési céljából a Gyártó feldolgozhatja az Adatokat az Adatvédelmi szabályzatnak megfelelően és a vonatkozó jogszabályokkal összhangban. A Gyártónak engedélyeznie kell a Végfelhasználónak az Adatokhoz való hozzáférést annyi időre, amennyi szükséges annak a célnak az eléréséhez, amely miatt végbement az Adatok megszerzése. Ez az időtartam nem lépheti túl az Adatvédelmi szabályzatban rögzített megőrzési időtartamot. Az adatokkal való visszaélés elleni védelem kizárólag olyan számítógépek és fiókok esetében vehető igénybe, amelyekhez a Végfelhasználó jogszerű hozzáféréssel rendelkezik. A Gyártó minden illegális használatot a megfelelő hatóságok tudomására hoz. A Gyártó eleget tesz a vonatkozó törvényi előírásoknak, és visszaélés esetén minden segítséget megad az igazságszolgáltatási szerveknek. Ön tudomásul veszi és elfogadja, hogy felelősséggel tartozik a ESET HOME-fiók eléréséhez szükséges jelszó biztonságáért, és hogy nem adja át a jelszót harmadik félnek. A Végfelhasználó felelős minden olyan jogosult vagy jogosulatlan műveletért, amely az adatokkal való visszaélés elleni védelmet biztosító szolgáltatással vagy a ESET HOME-fiókkal kapcsolatos. A ESET HOME-

fiókkal való bárminemű visszaélésről azonnal értesítenie kell a Gyártót. Az Adatokkal való visszaélés elleni védelemre vonatkozó kiegészítő rendelkezések kizárólag az ESET Internet Security és az ESET Smart Security Premium végfelhasználóira vonatkoznak.

ESET Secure Data. Kiegészítő rendelkezések vonatkoznak az ESET Secure Data szoftverre a következők szerint:

1. Definíciók. Az ESET Secure Data szoftverre vonatkozó kiegészítő rendelkezésekben a következő kifejezések a következőket jelentik:

a) „Információk” a szoftverrel titkosított vagy visszafejtett bármilyen információ vagy adat;

b) „Termékek” az ESET Secure Data szoftver és a dokumentáció;

c) „ESET Secure Data” az elektronikus adatok titkosításához és visszafejtéséhez használt szoftver(ek);

A többes számra utaló minden hivatkozás magában foglalja az egyes számot, és a férfinemre történő minden hivatkozás a nőneműt és a semleges neműt, és fordítva. A pontosan nem definiált szavakat a Szerződés általi definícióknak megfelelően kell használni.

2. További Végfelhasználói jognyilatkozat. Ön tudomásul veszi és elfogadja az alábbiakat:

a) az Ön felelőssége az Adatok védelme, karbantartása és biztonsági mentése;

b) az ESET Secure Data telepítése előtt minden információról és adatról (korlátozás nélkül beleértve minden kritikus információt és adatot) teljes biztonsági másolatot kell készítenie;

c) meg kell őriznie az ESET Secure Data beállításához és használatához szükséges jelszavak és egyéb információk biztonságos rekordját, emellett biztonsági másolatot kell készítenie az összes titkosítási kulcsról, licenckódról, fontos fájlról és a különféle tárolási adathordozóhoz létrehozott egyéb adatról;

d) a Termékek használatáért Ön felel. A Gyártó nem tehető felelőssé az Információk vagy egyéb adatok jogosulatlan vagy téves titkosításából vagy visszafejtéséből eredő bármilyen veszteségért, kárért vagy sérülésért, bárhogyan és bárhol történik az Információk vagy egyéb adatok tárolása;

e) míg a Gyártó minden ésszerű lépéssel biztosítja az ESET Secure Data sértetlenségét és biztonságát, a Termékeket (vagy egyetlen Terméket) sem szabad használni olyan területen, amely veszély esetén a működést automatikusan kikapcsoló biztonsági szinttől függ, illetve potenciálisan kockázatos vagy veszélyes, korlátozás nélkül beleértve a nukleáris létesítményeket, repülőgép-irányítást, vezérlési vagy kommunikációs rendszereket, fegyver- és védelmi rendszereket, valamint az emberi szervezet életműködését támogató és figyelő rendszereket;

f) a Végfelhasználói felelőssége annak biztosítása, hogy a termékek által nyújtott biztonság és titkosítás szintje megfeleljen az Ön követelményeinek;

g) Ön felel a Termékek (vagy bármelyik Termék) használatáért, korlátozás nélkül ideértve annak biztosítását, hogy az ilyen használat összhangban legyen a Szlovák Köztársaság vagy más olyan ország, régió vagy állam vonatkozó jogszabályaival vagy rendelkezéseivel, ahol a Termékeket használják. A Termékek használata előtt győződjön meg arról, hogy az nem sérti egyetlen kormány (a Szlovák Köztársaságban vagy máshol) embargóját sem;

h) Az ESET Secure Data időről időre a Gyártó szervereihez kapcsolódhat a licencadatok, elérhető javítások, szervizcsomagok és egyéb frissítések keresése céljából, amelyekkel javítható, karbantartható, módosítható vagy továbbfejleszthető az ESET Secure Data működése. Előfordulhat, hogy a szoftver a működésével kapcsolatos általános rendszerinformációkat küld az Adatvédelmi szabályzatnak megfelelően.

i) A Gyártó nem tehető felelőssé semmilyen veszteségért, kárért, költségért vagy követelését, amely jelszavak,

beállítási adatok, titkosítási kulcsok, licencaktiválási kódok és a szoftver használata során létrehozott vagy tárolt egyéb adat elvesztése, ellopása, jogtalan használata, sérülése, károsodása vagy megsemmisítése következtében lép fel.

A ESET Secure Data szoftverre vonatkozó kiegészítő rendelkezések kizárólag az ESET Smart Security Premium végfelhasználóira alkalmazhatók.

Password Manager Szoftver. Kiegészítő rendelkezések vonatkoznak a Password Manager szoftverre a következők szerint:

1. További Végfelhasználói jognyilatkozat. Ön tudomásul veszi és elfogadja az alábbiakat:

a) használhatja a Password Manager szoftvert olyan létfontosságú alkalmazás működtetéséhez, amely esetén az emberi élet vagy tulajdon forog kockán. Ön tudomásul veszi, hogy a Password Manager nem ilyen célokra készült, és hogy ilyen esetben a hiba halálhoz, személyi sérüléshez vagy a tulajdonban, illetve környezetben keletkezett súlyos károkhoz vezethet, amelyekért a Gyártó nem vállal felelősséget.

A PASSWORD MANAGER SZOFTVER KIVITELE, RENDELTETÉSE VAGY LICENCELÉSE NEM OLYAN VESZÉLYES KÖRNYEZETBEN VALÓ HASZNÁLATRA SZOLGÁL, AHOL VESZÉLY ESETÉN AUTOMATIKUSAN KIKAPCSOLÓ VEZÉRLŐK SZÜKSÉGESEK, BELEÉRTVE KORLÁTOZÁS NÉLKÜL A NUKLEÁRIS LÉTESÍTMÉNYEK, REPÜLŐGÉP-IRÁNYÍTÁS VAGY KOMMUNIKÁCIÓS RENDSZEREK, LÉGIFORGALMI IRÁNYÍTÁS, VALAMINT AZ EMBERI SZERVEZET ÉLETMŰKÖDÉSÉT TÁMOGATÓ RENDSZEREK VAGY FEGYVERRENDSZEREK TERVEZÉSÉT, ÖSSZEÁLLÍTÁSÁT, KARBANTARTÁSÁT VAGY MŰKÖDTETÉSÉT. A GYÁRTÓ KIFEJEZETTEN ELHÁRÍTJA AZ ILYEN CÉLOKRA VALÓ ALKALMASSÁGRA VONATKOZÓ MINDEN KIFEJEZETT VAGY FELTÉTELEZETT GARANCIÁT.

b) használhatja a Password Manager szoftvert olyan módon, amely sérti a jelen szerződést, illetve a Szlovák Köztársaság vagy saját joghatóságának törvényeit. Ön kifejezetten nem használhatja a Password Manager szoftvert illegális tevékenység végzéséhez vagy támogatásához, beleértve a kártékony, illetve bármilyen illegális tevékenységhez használható tartalom vagy bármely harmadik fél törvényét vagy jogait (beleértve a szellemi tulajdonjogokat) valamilyen módon megsértő tartalom feltöltését, korlátozás nélkül ideértve a Tárhelyen lévő fiókokhoz, illetve bármely fiókhoz és a Password Manager szoftver vagy a Tárhely más felhasználói adataihoz való hozzáférési kísérleteket (a Password Manager szoftver jelen kiegészítő rendelkezéseiben a „Tárhely” a Gyártó vagy a Gyártótól eltérő harmadik fél és a felhasználó által kezelt adattárhelyre utal, a szinkronizálás és a felhasználói adatok biztonsági mentésének engedélyezése céljából). Ha megszegi ezen kikötések bármelyikét, a Gyártónak jogában áll azonnal felmondani a jelen szerződést és Önre hárítani mindenféle szükséges jogorvoslat költségeit, valamint a szükséges lépéseket megtéve a visszatérítés lehetősége nélkül megakadályozni, hogy tovább használhassa a Password Manager szoftvert.

2. KORLÁTOZOTT FELELŐSSÉGVÁLLALÁS. A PASSWORD MANAGER SZOFTVERT ANNAK „ADOTT ÁLLAPOTÁBAN” BIZTOSÍTJUK. MINDENFÉLE KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁS NÉLKÜL KAPJA. A SZOFTVERT SAJÁT KOCKÁZATÁRA HASZNÁLJA. A GYÁRTÓ NEM VÁLLAL FELELŐSSÉGET AZ ADATVESZTÉSÉT, KÁROKÉRT, A SZOLGÁLTATÁS RENDELKEZÉSRE ÁLLÁSÁNAK KORLÁTOZÁSÁÉRT, BELEÉRTVE A PASSWORD MANAGER SZOFTVER ÁLTAL ADATSZINKRONIZÁLÁS ÉS BIZTONSÁGI MENTÉS CÉLJÁBÓL KÜLSŐ TÁRHELYRE KÜLDÖTT BÁRMILYEN ADATOT. AZ ADATOKNAK A PASSWORD MANAGER SZOFTVERREL TÖRTÉNŐ TITKOSÍTÁSA NEM JELENTI A GYÁRTÓNAK AZ ADATOK BIZTONSÁGÁVAL KAPCSOLATOS FELELŐSSÉGÉT. ÖN KIFFEJEZETTEN HOZZÁJÁRUL, HOGY A PASSWORD MANAGER SZOFTVER HASZNÁLATÁVAL BEOLVASOTT, HASZNÁLT, TITKOSÍTOTT, TÁROLT, SZINKRONIZÁLT VAGY ELKÜLDÖTT ADATOK HARMADIK FELEK SZERVEREIN TÁROLHATÓK LEGYENEK (KIZÁRÓLAG A PASSWORD MANAGER SZOFTVER OLYAN HASZNÁLATÁRA VONATKOZIK, AHOL A SZINKRONIZÁLÁSI ÉS BIZTONSÁGI MENTÉSI SZOLGÁLTATÁSOK ENGEDÉLYEZVE VANNAK). HA A GYÁRTÓ SAJÁT BELÁTÁSA SZERINT ÚGY DÖNT, HOGY HARMADIK FÉL TÁRHELYÉT, WEBHELYÉT, WEBES PORTÁLJÁT, SZERVERÉT VAGY SZOLGÁLTATÁSÁT HASZNÁLJA, A GYÁRTÓ NEM FELELŐS AZ ADOTT HARMADIK FÉL SZOLGÁLTATÁSÁNAK MINŐSÉGÉÉRT, BIZTONSÁGÁÉRT VAGY RENDELKEZÉSRE ÁLLÁSÁÉRT, ÉS A GYÁRTÓ SEMMILYEN MÉRTÉKBEN SEM TEHETŐ FELELŐSSÉ A HARMADIK FÉL SZERZŐDÉSES VAGY JOGI KÖTELEZETTSÉGEINEK MEGSZEGÉSÉÉRT, SEM A SZOFTVER HASZNÁLATA SORÁN

BEKÖVETKEZŐ KÁROKÉRT, VESZTESÉGÉRT, PÉNZÜGYI VAGY NEM PÉNZÜGYI KÁROKÉRT VAGY BÁRMILYEN MÁS VESZTESÉGÉRT. A GYÁRTÓ NEM FELELŐS A PASSWORD MANAGER HASZNÁLATÁVAL BEOLVASOTT, FELHASZNÁLT, TITKOSÍTOTT, TÁROLT, SZINKRONIZÁLT VAGY ELKÜLDÖTT, ILLETVE A TÁRHELYEN LÉVŐ ADATOK TARTALMÁÉRT. ÖN TUDOMÁSUL VESZI, HOGY A GYÁRTÓNAK NINCS HOZZÁFÉRÉSE A TÁROLT ADATOK TARTALMÁHOZ, ÉS NEM TUDJA AZT FIGYELNI, ILLETVE A JOGI SZEMPONTBÓL KÁRTÉKONY TARTALMAT ELTÁVOLÍTANI.

A Gyártó fenntartja magának az összes jogot a Password MANAGER szoftverrel kapcsolatos fejlesztések, frissítések és javítások („Fejlesztések") elvégzésére még abban az esetben is, ha az ilyen fejlesztések bármilyen formában az Ön visszajelzései, ötletei vagy javaslatai alapján valósultak meg. Ön semmilyen térítésre, ideértve a jogdíjakat is, sem jogosult az ilyen Fejlesztésekkel kapcsolatban.

A GYÁRTÓ ENTITÁSAI ÉS LICENCADÓI NEM VÁLLALNAK FELELŐSSÉGET SEMMILYEN IGÉNY VAGY KÖTELEZETTSÉG IRÁNT, AMELY A PASSWORD MANAGER SZOFTVER ÖN VAGY HARMADIK FELEK ÁLTALI HASZNÁLATÁBÓL ERED, ILLETVE ABBÓL, HOGY IGÉNYBE VESZI-E BÁRMILYEN KÖZVETÍTŐI CÉG VAGY KERESKEDŐ SZOLGÁLTATÁSÁT, TOVÁBBÁ VALAMILYEN BIZTONSÁGI SZOLGÁLTATÁS ÉRTÉKESÍTÉSÉVEL VAGY MEGVÁSÁRLÁSÁVAL KAPCSOLATOS, MÉG HA AZ ILYEN IGÉNYEK VAGY KÖTELEZETTSÉGEK VALAMILYEN JOGI VAGY MÉLTÁNYOSSÁGI ELVEN ALAPULNAK IS.

A GYÁRTÓ ENTITÁSAI ÉS LICENCADÓI SEMMILYEN ESETBEN SEM FELELŐSEK SEMMIFÉLE KÖZVETLEN, JÁRULÉKOS, SPECIÁLIS, KÖZVETETT VAGY KÖVETKEZMÉNYI KÁRÉRT, AMELY BÁRMELY HARMADIK FÉL SZOFTVERE, A PASSWORD MANAGER SZOFTVEREN KERESZTÜL ELÉRT ADATOK, A PASSWORD MANAGER SZOFTVER ÖN ÁLTALI HASZNÁLATÁNAK VAGY A SZOFTVER HASZNÁLHATATLANSÁGÁNAK VAGY ELÉRHETETLENSÉGÉNEK, ILLETVE A PASSWORD MANAGER SZOFTVEREN KERESZTÜL NYÚJTOTT ADATOK OKÁN KELETKEZTEK, MÉG HA AZ ILYEN KÁRIGÉNYEK VALAMILYEN JOGI VAGY MÉLTÁNYOSSÁGI ELV ALAPJÁN MERÜLNEK IS FEL. A JELEN ZÁRADÉK ÁLTAL KIZÁRT KÁROK KÖZÉ TARTOZIK KORLÁTOZÁS NÉLKÜL IDEÉRTVE AZ ÜZLETI HASZON ELMARADÁSÁBÓL, SZEMÉLY VAGY TULAJDON SÉRÜLÉSÉBŐL, AZ ÜZLET MEGHIÚSULÁSÁBÓL, ÜZLETI VAGY SZEMÉLYES ADATOK ELVESZTÉSÉBŐL SZÁRMAZÓ KÁROKAT. EGYES JOGSZABÁLYOK NEM TESZIK LEHETŐVÉ A JÁRULÉKOS VAGY KÖVETKEZMÉNYI KÁROK KORLÁTOZÁSÁT, EZÉRT ELŐFORDULHAT, HOGY EZ A KORLÁTOZÁS NEM VONATKOZIK ÖNRE. ILYEN ESETBEN A GYÁRTÓ FELELŐSSÉGÉNEK MÉRTÉKE A VONATKOZÓ JOG ALAPJÁN ENGEDÉLYEZETT MINIMÁLIS LESZ.

A PASSWORD MANAGER SZOFTVEREN KERESZTÜL BIZTOSÍTOTT INFORMÁCIÓK, TÖBBEK KÖZÖTT A RÉSZVÉNYÁRFOLYAMOK, ELEMZÉSEK, PIACI INFORMÁCIÓK, HÍREK ÉS PÉNZÜGYI ADATOK KÉSLELTETETTEK, PONTATLANOK VAGY HIÁNYOSAK LEHETNEK, ILLETVE HIBÁKAT TARTALMAZHATNAK, ÉS A GYÁRTÓ ENTITÁSAI VAGY LICENCADÓI NEM VÁLLALNAK FELELŐSSÉGET EZEKRE VONATKOZÓAN. A GYÁRTÓ FENNTARTJA A JOGOT, HOGY ELŐZETES ÉRTESÍTÉS NÉLKÜL BÁRMIKOR MÓDOSÍTSA VAGY MEGSZÜNTESSE A PASSWORD MANAGER SZOFTVER BÁRMELY ELEMÉT VAGY FUNKCIÓJÁT, ILLETVE A PASSWORD MANAGER SZOFTVERBEN FOGLALT ÖSSZES VAGY BÁRMELY FUNKCIÓ VAGY TECHNOLÓGIA HASZNÁLATÁT.

HA A JELEN CIKKBEN SZEREPLŐ RENDELKEZÉSEK BÁRMILYEN OKBÓL KIFOLYÓLAG ÉRVÉNYTELENEK, VAGY A VONATKOZÓ JOGSZABÁLYOK SZERINT A GYÁRTÓ FELELŐS A VESZTESÉGÉRT, KÁRÉRT STB., A FELEK EGYETÉRTŐLEG ELFOGADJÁK, HOGY A GYÁRTÓ FELELŐSSÉGE AZ ÖN ÁLTAL KIFIZETETT LICENCDÍJ TELJES ÖSSZEGÉRE KORLÁTOZÓDIK.

ÖN VÁLLALJA, HOGY KÁRTALANÍTJA, MEGVÉDI ÉS MENTESÍTI A GYÁRTÓT ÉS ALKALMAZOTTAIT, LEÁNYVÁLLALATAIT, TÁRSVÁLLALATAIT ÉS EGYÉB PARTNEREIT MINDEN HARMADIK FÉL (BELEÉRTVE A KÉSZÜLÉK TULAJDONOSAIT VAGY AZOKAT A FELEKET, AKIKNEK A JOGAIT ÉRINTETTÉK A PASSWORD MANAGER SZOFTVERBEN HASZNÁLT VAGY A TÁRHELYEN LÉVŐ ADATOK) ÁLTAL TÁMASZTOTT IGÉNY, KÖTELEZETTSÉG, KÁR, VESZTESÉG, KÖLTSÉG, KIADÁS, DÍJ ESETÉN, AMELY A PASSWORD MANAGER SZOFTVER HASZNÁLATA KÖVETKEZTÉBEN MERÜL FEL.

3. Adatok a Password Manager szoftverben. Ha Ön kifejezetten másként meg nem határozza, az Ön által megadott, a Password Manager szoftver adatbázisában mentett adatok tárolása a számítógépen vagy az Ön által definiált egyéb tárolóeszközön titkosított formátumban történik. Ön tudomásul veszi, hogy a Password Manager

szoftver bármely adatbázisának vagy egyéb fájlnak a törlése vagy sérülése esetén az abban tárolt adatok véglegesen elvesznek, és Ön tudomásul veszi és elfogadja az ilyen veszteség kockázatát. Az a tény, hogy személyes adatait titkosított formátumban tárolja a számítógépen, nem jelenti azt, hogy az információkat nem tudja ellopni vagy jogosulatlanul felhasználni valaki, aki megszerzi a mesterjelszavát, vagy hozzáférést szerez az ügyfél által az adatbázis megnyitásához megadott aktiválási eszközhöz. Az Ön felelőssége az összes hozzáférési módszer védelmének a biztosítása.

4. Személyes adatok átadása a Gyártónak vagy átvitele tárhelyre. Ha ezt választja, és kizárólag az automatikus adatszinkronizálás és biztonsági mentés biztosítása céljából, a Password Manager szoftver átviszi vagy elküldi a személyes adatokat – nevezetesen a jelszavakat, bejelentkezési adatokat, fiókokat vagy identitásokat – a Password Manager szoftver adatbázisából az interneten keresztül a tárhelyre. Az adatok átvitele kizárólag titkosított formában történik. Az online űrlapokon a jelszavak, bejelentkezési és egyéb adatok Password Manager segítségével történő kitöltéséhez az információkat az interneten keresztül el kell küldeni az Ön által meghatározott webhelyre. Ezt az adatátvitelt nem a Password Manager szoftver kezdeményezi, ezért a Gyártó nem tehető felelőssé a különböző gyártók által támogatott egyetlen webhellyel folytatott ilyen műveletek biztonságáért sem. Az interneten keresztüli minden műveletet – akár a Password Manager szoftver közreműködésével folyik, akár nem – a saját belátása szerint és kockázatára végzi, és Ön vállal kizárólagos felelősséget a számítógépes rendszert érintő bármilyen kárért, illetve az ilyen anyag vagy szolgáltatás letöltéséből és/vagy használatából eredő adatvesztésért. A Gyártó javasolja, hogy rendszeresen készítsen biztonsági másolatot külső meghajtókra az adatbázisról és egyéb fontos fájlokról annak érdekében, hogy minimalizálja az értékes adatok elvesztésének kockázatát. A Gyártó nem tud Önnek segítséget nyújtani az elveszett vagy megsérült adatok helyreállításához. Ha a Gyártó biztonsági mentési szolgáltatásokat nyújt a felhasználói adatbázisfájlokhoz a felhasználók számítógépein lévő fájlok károsodása vagy sérülése esetén, az ilyen biztonsági szolgáltatáshoz nem jár garancia, és nem foglalja magában a Gyártó felelősségét.

A Password Manager szoftver használatával Ön elfogadja, hogy a szoftver időről időre a Gyártó szervereihez kapcsolódhat a licencadatok, elérhető javítások, szervizcsomagok és egyéb frissítések keresése céljából, amelyekkel javítható, karbantartható, módosítható vagy továbbfejleszthető a Password Manager szoftver működése. Előfordulhat, hogy a szoftver a Password Manager szoftver működésével kapcsolatos általános rendszerinformációkat küld az Adatvédelmi szabályzatnak megfelelően.

5. Eltávolítási információk és utasítások. Az adatbázisból megtartani kívánt információkat a Password Manager szoftver eltávolítása előtt exportálni kell.

A Password Manager szoftverre vonatkozó kiegészítő rendelkezések kizárólag az ESET Smart Security Premium végfelhasználóira alkalmazhatók.

ESET LiveGuard. Kiegészítő rendelkezések vonatkoznak az ESET LiveGuard szoftverre a következők szerint:

A Szoftver tartalmaz egy további funkciót, amely Végfelhasználó által benyújtott fájlok további elemzését végzi. A Gyártó a Végfelhasználó által beküldött fájlokat és az elemzés eredményét kizárólag az Adatvédelmi szabályzatnak és a vonatkozó jogszabályi előírásoknak megfelelően használhatja fel.

A ESET LiveGuard szoftverre vonatkozó kiegészítő rendelkezések kizárólag az ESET Smart Security Premium végfelhasználóira alkalmazhatók.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Adatvédelmi szabályzat

A személyes adatok védelme különösen fontos az ESET, spol. s r. o. számára (székhelye: Einsteinova 24, 851 01 Bratislava, Slovak Republic; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B;

cégjegyzékszám: 31333532) adatkezelőként („ESET” vagy „Mi”). Szeretnénk megfelelni az EU általános adatvédelmi rendelete (GDPR) alapján jogilag szabványosított átláthatósági követelménynek. Ezért közzétesszük a jelen Adatvédelmi szabályzatot azzal a céllal, hogy tájékoztassuk ügyfelünket („Végfelhasználó” vagy „Ön”) mint adatalanyt a személyes adatvédelem következő témáiról:

- A személyes adatok feldolgozásának jogi alapja,
- Adatmegosztás és titoktartás,
- Adatbiztonság,
- Az Önt adatalanyként megillető jogok,
- Az Ön személyes adatainak feldolgozása,
- Partnerinformációk.

A személyes adatok feldolgozásának jogi alapja

Csupán néhány jogi rendelkezést alkalmazunk az adatfeldolgozáshoz a személyes adatok védelmére vonatkozó adatvédelmi rendelet szerint. A személyes adatok ESET-nél történő feldolgozása elsősorban a Végfelhasználói licencszerződést Végfelhasználónak való teljesítése céljából szükséges (GDPR 6. cikk, (1) bekezdés, b) pont), amely az ESET-termékek vagy -szolgáltatások nyújtására alkalmazandó, kivéve, ha kifejezetten másként nem jelezzük, pl.

- A jogos érdek jogalapja (GDPR 6. cikk, (1) bekezdés f) pont), amely lehetővé teszi számunkra, hogy feldolgozzunk adatokat arról, hogy ügyfeleink hogyan használják Szolgáltatásainkat és mennyire elégedettek, mert így a lehető legjobb szintű védelmet, támogatást és felhasználói élményt tudjuk nyújtani a felhasználóinknak. A vonatkozó törvények szerint a marketing is egy jogos érdek, ezért általában ezt az elvet követjük az ügyfeleinkkel folytatott marketingkommunikáció tekintetében.
- Hozzájárulás (GDPR 6. cikk, (1) bekezdés a) pont), amelyet olyan helyzetekben kérhetünk Öntől, amikor ezt a jogalapot tartjuk a legmegfelelőbbnek, vagy ha a törvény ezt írja elő.
- Jogi kötelezettségeknek való megfelelés (GDPR 6. cikk, (1) bekezdés c) pont), például az elektronikus kommunikáció, valamint a számlázási dokumentumok megőrzési idejének tekintetében.

Adatmegosztás és titoktartás

Adatait nem osztjuk meg harmadik felekkel. Az ESET azonban világszerte jelen van a kapcsolt vállalkozások, illetve partnerek révén, amelyek forgalmazói, szolgáltatói és terméktámogatási hálózatunk részét képezik. A kapcsolt vállalkozások és partnerek megkaphatják, illetve visszaküldhetik az ESET által feldolgozott licencelési, számlázási és műszaki terméktámogatási információkat a Végfelhasználói licencszerződés teljesítése céljából, így például a szolgáltatások és a terméktámogatás biztosítása érdekében.

Az ESET az Európai Unióban (EU) történő adatfeldolgozást preferálja. Azonban az Ön tartózkodási helyétől (termékeink és/vagy szolgáltatásaink EU-n kívüli használata) és/vagy az Ön által választott szolgáltatástól függően előfordulhat, hogy az adatait az EU-n kívüli országba kell továbbítani. Például harmadik féltől származó szolgáltatásokat használunk a felhőalapú szolgáltatásokkal kapcsolatban. Ezekben az esetekben gondosan választjuk ki szolgáltatóinkat, és biztosítjuk a megfelelő szintű adatvédelmet szerződéses, műszaki és szervezeti intézkedésekkel. Rendszerint megállapodunk az EU-s szabványos szerződési feltételekben, ha szükséges, kiegészítő szerződéses rendelkezésekkel.

Egyes EU-n kívüli országok, például az Egyesült Királyság és Svájc esetében az EU már meghatározta az adatvédelem összevethető szintjét. Az adatvédelem összevethető szintje miatt az adatok ezen országokba történő továbbítása nem igényel külön engedélyt vagy megállapodást.

Adatbiztonság

Az ESET megfelelő technikai és szervezeti intézkedésekkel biztosít a potenciális kockázatoknak megfelelő védelmi szintet. Mindent megteszünk annak érdekében, hogy a feldolgozó rendszerek és a szolgáltatások folyamatosan biztosítsák az adatok bizalmas kezelését, sértetlenségét, a hozzáférhetőséget és a terhelhetőséget. Ha azonban sor kerül az adatok megsértésére, ami veszélyezteti az Ön jogait és szabadságát, készen állunk értesíteni az adott felügyeleti hatóságot és az érintett Végfelhasználókat és adatalanyokat.

Az adatalany jogai

Minden Végfelhasználó jogai számítanak, és szeretnénk tájékoztatni Önt arról, hogy minden Végfelhasználó (minden EU-s és nem EU-s országból származó) rendelkezik az alábbi jogokkal az ESET-nél. Az Önt mint adatalanyt megillető jogok gyakorlása érdekében forduljon hozzánk a támogatási űrlapon keresztül vagy e-mail útján a következő címen: dpo@eset.sk. Személyazonosítás céljából a következő információkat kérjük Öntől: Név, e-mail-cím és – ha rendelkezésre áll – licenckulcs vagy ügyfélszám, valamint vállalati hovatartozás. Kérjük, tartózkodjon attól, hogy bármilyen egyéb személyes adatot, például születési dátumot küldjön nekünk. Szeretnénk felhívni a figyelmét arra, hogy a kérésének feldolgozásához, valamint személyazonosítási célokból fel fogjuk dolgozni a személyes adatait.

Jogosult visszavonni a hozzájárulását. A hozzájárulás visszavonásának joga a csak a beleegyezésen alapuló adatkezelés esetén alkalmazható. Ha személyes adatait az Ön hozzájárulása alapján dolgozzuk fel, Önnek jogában áll a hozzájárulását indokolás nélkül bármikor visszavonni. Hozzájárulásának visszavonása csak a jövőben lép érvénybe, vagyis nem érinti a visszavonás előtt feldolgozott adatok jogszerűségét.

Jogosult tiltakozni. A feldolgozás ellen való tiltakozáshoz való jog az ESET vagy egy harmadik fél jogos érdekén alapuló adatkezelés esetén alkalmazandó. Amennyiben személyes adatait jogos érdek védelme érdekében dolgozzuk fel, akkor Önnek mint adatalanynak jogában áll bármikor kifogást emelni az általunk megnevezett jogos érdek és személyes adatainak feldolgozása ellen. A kifogásolás csak a jövőben lép érvénybe, vagyis nem érinti a kifogásolás előtt feldolgozott adatok törvényszerűségét. Amennyiben személyes adatait direktmarketing céljából dolgozzuk fel, nem szükséges indokolni a kifogásolást. Ez vonatkozik a profilalkotásra is, amennyiben az ilyen jellegű direktmarketinghez kapcsolódik. Minden más esetben arra kérjük Önt, hogy röviden tájékoztasson bennünket az ESET személyes adatainak feldolgozásához fűződő jogos érdekével kapcsolatos panaszairól.

Kérjük, vegye figyelembe, hogy egyes esetekben a hozzájárulás visszavonása ellenére jogunk van arra, hogy a személyes adatait egy másik jogalap alapján továbbra is feldolgozzuk, például egy szerződés teljesítése céljából.

Joga van a hozzáféréshez. Ön mint adatalany bármikor díjmentesen lekérheti az ESET által tárolt adatairól szóló információkat.

Jog van a helyesbítéshez. Ha véletlenül helytelen személyes adatokat dolgozunk fel Önről, jogában áll ezt helyesbíteni.

Joga van a törléshez és az adatkezelés korlátozásához. Ön mint adatalany jogosult kérelmezni személyes adatainak törlését, illetve azt, hogy személyes adatainak feldolgozása korlátozott mértékben történjen meg. Ha például személyes adatait a hozzájárulásával dolgozzuk fel, de visszavonja a hozzájárulását, és nincs más jogalap – például szerződés –, akkor azonnal töröljük személyes adatait. A személyes adatait akkor is töröljük, amint a megőrzési időszak végén már nincs rájuk szükség az esetükben megadott célokból.

Ha személyes adatait kizárólag direktmarketing céljából használjuk fel, és Ön visszavonta a hozzájárulását, vagy kifogást emelt az ESET jogos érdekével szemben, akkor a személyes adatainak feldolgozását olyan mértékben korlátozzuk, hogy kapcsolattartási adatait belefoglaljuk a belső tiltólistánkba annak érdekében, hogy elkerüljük a kéretlen kapcsolatfelvételt. Ellenkező esetben az Ön személyes adatai törlődnek.

Kérjük, vegye figyelembe, hogy az adatait a törvényhozó vagy felügyeleti hatóságok által megadott adatmegőrzési kötelezettségek és határidők lejártáig tárolnunk kell. Az adatmegőrzési kötelezettségek és időszakok a szlovákiai jogszabályokból is származhatnak. Ezt követően a megfelelő adatok rutinszerűen törlődnek.

Joga van az adathordozhatósághoz. Örömmel biztosítjuk Önnek mint adatalanynak az ESET által feldolgozott személyes adatokat xls formátumban.

Jogosult panaszt emelni. Ön mint adatalany bármikor jogosult panaszt benyújtani egy felügyeleti hatósághoz. Az ESET vállalatra a szlovák törvények az irányadók, és az Európai Unió tagjaként kötelességünk betartani az adatvédelmi rendelkezéseket. Az érintett adatfelügyeleti hatóság a Szlovák Köztársaság Személyes Adatvédelmi Hivatala, amely a következő helyen található: Hraničná 12, 82007 Bratislava 27, Slovak Republic.

A személyes adatok feldolgozása

Az ESET által nyújtott és a termékeinkbe integrált szolgáltatások működését a VÉGFELHASZNÁLÓI LICENCSZERZŐDÉSszabályozza, viszont néhány szolgáltatás különös figyelmet igényel. Szeretnénk további információkat biztosítani Önnek az adatgyűjtésről a szolgáltatásaink nyújtásával kapcsolatban. A Végfelhasználói licencszerződésben és a termékdokumentációműködésére és funkcióira vonatkozó információkat is. A szolgáltatások működtetése érdekében a következő információkat kell gyűjtenünk:

Licencelési és számlázási adatok. Az ESET összegyűjti és feldolgozza a nevet, az e-mail-címet, a licenckulcsot és (ha van ilyen) címet, a vállalati hovatartozást és a fizetési adatokat annak érdekében, hogy megkönnyítse a licenc aktiválását, a licenckulcs kézbesítését, a lejáratra vonatkozó emlékeztetőket, a támogatási kérelmeket, a licenc eredetiségének ellenőrzését, a szolgáltatásunk nyújtását és egyéb értesítéseket – beleértve a marketingüzeneteket is – a vonatkozó jogszabályokkal vagy az Ön hozzájárulásával összhangban. Az ESET jogilag köteles 10 évig megőrizni a számlázási információkat, viszont a licencelési információk a licenc lejártát követő 12 hónapon belül anonimmá válnak.

Frissítés és egyéb statisztikák. A feldolgozott információk közé olyan információk tartoznak, mint a telepítési folyamat és az Ön számítógépe, ideértve azt a platformot, amelyre a termékünket telepíti, valamint a termékeink működésével és funkcióival kapcsolatos információk, például az operációs rendszer, hardverekkel kapcsolatos információk, telepítési azonosítók, licencazonosítók, IP-cím, MAC-cím, a termék konfigurációs beállításai. Mindezeket a frissítések biztosítása és a frissítési szolgáltatások, valamint a karbantartás, a biztonság és a backend infrastruktúra fejlesztése céljából dolgozzuk fel.

Ezeket az információkat a licencelési és számlázási célokból szükséges személyazonosító információktól elkülönítve tároljuk, mivel nem igényli a Végfelhasználó beazonosítását. A megőrzési idő legfeljebb 4 év.

Az **ESET LiveGrid® megbízhatósági rendszer.** A kártevőkkel kapcsolatos egyirányú kivonatokat az ESET LiveGrid® megbízhatósági rendszer céljából dolgozzuk fel. A rendszer összeveti az ellenőrzött fájlokat a felhőben tárolt engedélyező- és tiltólistaelemek adatbázisával, ezáltal fokozva a kártevőirtó szoftvereink hatékonyságát. A Végfelhasználót a folyamat során nem azonosítjuk be.

Az **ESET LiveGrid® visszajelzési rendszer.** Az ESET LiveGrid® visszajelzési rendszer által biztosított gyanús minták és metaadatok. Ez a rendszer lehetővé teszi, hogy az ESET azonnal választ adjon a végfelhasználók igényeire, és hogy biztosítsuk a hatékonyságunkat a legújabb kártevőkkel szemben. A következők elküldését kérjük Öntől:

- Kártevők, például minták vírusokról és egyéb kártékony szoftverekről, valamint gyanús, problémás, kéretlen vagy veszélyes objektumokról, például végrehajtható fájlokról, illetve az Ön vagy a termékünk által levélszemétként megjelölt e-mailek;

- Internethasználattal kapcsolatos információk, például IP-cím és földrajzi adatok, IP-csomagok, URL-címek és Ethernet-keretek;

- Összeomlási memóriaképek és a bennük található információk.

Más célból nem kívánunk adatokat gyűjteni, viszont néha lehetetlen ezt elkerülni. Előfordulhat, hogy maguk a kártevők tartalmaznak véletlenül begyűjtött adatokat (amelyek begyűjtéséről Önnek tudomása van, vagy azt jóváhagyta), illetve hogy fájlnevek vagy URL-címek részét képezik. Nem célunk, hogy az ilyen információk rendszereink vagy folyamataink részét képezzék, illetve nem dolgozzuk fel őket a jelen Adatvédelmi szabályzatban leírtak szerint.

Az ESET LiveGrid® visszajelzési rendszeren keresztül szerzett és feldolgozott összes információt a Végfelhasználó azonosítása nélkül használjuk fel.

Hálózaton keresztül csatlakozó eszközök biztonsági szempontból való felmérése. A biztonsági felmérési funkció biztosításához feldolgozzuk a helyi hálózat nevét és a helyi hálózaton található eszközökkel kapcsolatos adatokat, így például az állapotukat, típusukat, nevüket, IP-címüket és MAC-címüket a licencelési adatokkal összefüggésben. A routerek vezeték nélküli biztonsági típusára és vezeték nélküli titkosítási típusára is szükség van. A Végfelhasználót azonosító licencadatokat legkésőbb a licenc lejártát követő 12 hónapon belül anonimizáljuk.

Terméktámogatás. Szervizelés, illetve segítségnyújtás biztosításához szükség lehet az Ön által leadott terméktámogatási kérelmekben foglalt elérhetőségekre és licencelési adatokra. Attól függően, hogy Ön milyen csatornát választ a velünk történő kapcsolatfelvételre, összegyűjthetjük az Ön e-mail-címét, telefonszámát, a licencelési információkat, a termékadatokat és a támogatási eset leírását. Egyéb információk megadására is megkérhetjük a terméktámogatás megkönnyítése céljából. A műszaki terméktámogatás céljából feldolgozott adatokat 4 évig tároljuk.

Az adatokkal való visszaélés elleni védelem. Ha létrejön az ESET HOME-fiók a https://home.eset.com weboldalon, és a funkciót a Végfelhasználó aktiválja a számítógép ellopásával kapcsolatban, a következő információkat gyűjtjük be és dolgozzuk fel: helyadatok, képernyőképek, a számítógép konfigurációjával kapcsolatos adatok és a számítógép kamerája által rögzített adatok. A begyűjtött adatokat a szervereink, illetve a szolgáltatóink szerverei tárolják 3 hónapos megőrzési idővel.

Password Manager. Ha úgy dönt, hogy aktiválja a Password Manager funkcióját, a bejelentkezési adataival kapcsolatos adatok titkosított formában kerülnek tárolásra csak az Ön számítógépén vagy más kijelölt eszközön. Ha aktiválja a szinkronizálási szolgáltatást, a titkosított adatokat a szervereink, illetve a szolgáltatóink szerverei tárolják a szolgáltatás biztosítása érdekében. Sem az ESET, sem a szolgáltató nem tud hozzáférni az ilyen adatokhoz. Kizárólag Ön rendelkezik az adatok visszafejtésére lehetőséget adó kulccsal. Az adatok a funkció deaktiválásakor törlődnek.

ESET LiveGuard. Ha úgy dönt, hogy aktiválja a ESET LiveGuard funkciót, akkor mintákat kell beküldenie, például a Végfelhasználó által előre meghatározott és kiválasztott fájlokat. A távoli elemzéshez kiválasztott minták feltöltődnek az ESET szolgáltatásba, és az elemzés eredményét visszaküldjük a számítógépére. A gyanús mintákat az ESET LiveGrid® visszajelzési rendszer által összegyűjtött információk szerint dolgozzuk fel.

Felhasználói élmény javítását célzó program. Ha aktiválja Felhasználói élmény javítását célzó program , akkor a termékeink használatával kapcsolatos anonim telemetriai adatokat az Ön hozzájárulása alapján fogjuk begyűjteni és felhasználni.

Kérjük, vegye figyelembe, hogy ha a termékeinket és szolgáltatásainkat használó személy nem az a Végfelhasználó, aki megvásárolta a terméket vagy a szolgáltatást és megkötötte velünk a Végfelhasználói licencszerződést (pl. a Végfelhasználó alkalmazottja, családtagja vagy olyan személy, aki a Végfelhasználó által a Végfelhasználói licencszerződés előírásainak megfelelően a termék vagy szolgáltatás használatára felhatalmazott családtag vagy személy, akkor az adatok feldolgozása az ESET jogos érdeke alapján a GDPR 6. cikk (1) bekezdésének f) pontja értelmében annak érdekében történik, hogy a Végfelhasználó által felhatalmazott felhasználó felhasználhassa az általunk a Végfelhasználói licencszerződés értelmében nyújtott termékeket és szolgáltatásokat.

Partnerinformációk

Amennyiben gyakorolni szeretné az adatalanyként Önt megillető jogait, vagy ha bármilyen kérdése vagy kételye van, írjon nekünk a következő címre:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk