ESET Endpoint Security

Felhasználói útmutató

Ide kattintva megjelenítheti a dokumentum verzióját

Digital Security
Progress. Protected.

Copyright ©2023 – ESET, spol. s r.o.

Az ESET Endpoint 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 Endpoint Security 9 1
1.1 A jelen verzió újdonságai? 2
1.2 Rendszerkövetelmények 3
1.2 Támogatott nyelvek 4
1.3 Megelőzés 5
1.4 Súgótémakörök 6
2 Távolról felügyelt végpontok dokumentációja 7
2.1 Az ESET PROTECT ismertetése 8
2.2 Az ESET PROTECT Cloud ismertetése 10
2.3 Jelszóval védett beállítások 10
2.4 Mik a házirendek? 11
2.4 Házirendek egyesítése 11
2.5 Hogyan működnek a jelzők? 12
3 Az ESET Endpoint Security használata önállóan 13
3.1 Telepítési módszerek 13
3.1 Telepítés az ESET AV Remover eszközzel 14
3.1 ESET AV Remover 15
3.1 Az ESET AV Remover használatával történő eltávolítás hibával fejeződött be 17
3.1 Telepítés (.exe) 17
3.1 Telepítési mappa módosítása (.exe) 19
3.1 Telepítés (.msi) 19
3.1 Speciális telepítés (.msi) 21
3.1 Minimális modultelepítés 23
3.1 Parancssori telepítés 23
3.1 Központi telepítés GPO vagy SCCM segítségével 28
3.1 Frissítés egy újabb verzióra 30
3.1 Biztonsági és stabilitási frissítések 31
3.1 A telepítéssel kapcsolatos általános problémák 31
3.1 Nem sikerült az aktiválás 31
3.2 Licenc aktiválása 32
3.3 Számítógép ellenőrzése 32
3.4 Útmutató kezdő felhasználók számára 32
3.4 A felhasználói felület 32
3.4 Frissítési beállítások 36
3.4 Zónák beállítása 37
3.4 Webfelügyeleti eszközök 38
4 Az ESET Endpoint Security használata 38
4.1 Számítógép 40
4.1 Keresőmotor 42
4.1 A keresőmotor további beállításai 46
4.1 A program fertőzést észlelt 47
4.1 Valós idejű fájlrendszervédelem 49
4.1 A valós idejű védelem ellenőrzése 51
4.1 Mikor érdemes módosítani a valós idejű védelem beállításain? 51
4.1 Teendők, ha a valós idejű védelem nem működik 51
4.1 Számítógép ellenőrzése 52
4.1 Egyéni ellenőrzés indítása 54
4.1 Az ellenőrzés folyamata 56
4.1 Számítógép-ellenőrzés naplója 57
4.1 Kártevő-ellenőrzések 57

4.1 Üresjárat idején történő ellenőrzés 58
4.1 Ellenőrzési profilok 58
4.1 Ellenőrizendő célterületek 59
4.1 További ellenőrzési beállítások 59
4.1 Eszközfelügyelet 60
4.1 Eszközfelügyeleti szabályok szerkesztője 61
4.1 Észlelt eszközök 62
4.1 Eszközcsoportok 62
4.1 Eszközfelügyeleti szabályok hozzáadása 63
4.1 Behatolásmegelőző rendszer 66
4.1 A Behatolásmegelőző rendszer interaktív ablaka 68
4.1 Lehetséges zsarolóprogram-viselkedés észlelve 69
4.1 Behatolásmegelőző rendszer szabályainak kezelése 69
4.1 Behatolásmegelőző rendszer szabálybeállításai 71
4.1 A Behatolásmegelőző rendszer haladó beállításai 73
4.1 Az illesztőprogramok mindig betölthetők 73
4.1 Bemutató üzemmód 74
4.1 Rendszerindításkor futtatott ellenőrzés 74
4.1 Rendszerindításkor automatikusan futtatott fájlok ellenőrzése 75
4.1 Dokumentumvédelem 76
4.1 Kivételek 76
4.1 Teljesítménybeli kivételek 76
4.1 Teljesítménybeli kivételek felvétele vagy szerkesztése 78
4.1 Útvonalkivétel formátuma 79
4.1 Észlelési kivételek 80
4.1 Észlelési kivétel felvétele vagy szerkesztése 82
4.1 Varázsló létrehozása észlelési kivételekhez 84
4.1 Kivételek (7.1 és korábbi) 84
4.1 Folyamatkivételek 84
4.1 Folyamatkivételek felvétele vagy szerkesztése 85
4.1 HIPS-kivételek 86
4.1 ThreatSense paraméterek 86
4.1 Megtisztítási szintek 89
4.1 Ellenőrzésből kizárt fájlkiterjesztések 89
4.1 További ThreatSense-paraméterek 90
4.2 Hálózat 90
4.2 Tűzfal 92
4.2 Tanuló mód 94
4.2 Hálózati támadások elleni védelem 95
4.2 Brute-force támadás elleni védelem 95
4.2 Szabályok 95
4.2 Kivételek 98
4.2 Speciális szűrési beállítások 98
4.2 IDS-szabályok 101
4.2 Lehetséges kártevő letiltva 102
4.2 Hálózati védelem hibájának elhárítása 103
4.2 Csatlakoztatott hálózatok 103
4.2 Ismert hálózatok 104
4.2 Ismert hálózatok szerkesztése 104
4.2 Hálózati hitelesítés – Szerverkonfiguráció 107
4.2 Tűzfalprofilok 108

4.2 Hálózati adapterekhez rendelt profilok ... 108
4.2 Alkalmazások módosításának felismerése ... 109
4.2 Módosítások felismeréséből kizárt alkalmazások ... 109
4.2 Szabályok beállítása és használata ... 110
4.2 Tűzfalszabályok listája ... 110
4.2 Tűzfalszabályok hozzáadása vagy szerkesztése ... 111
4.2 Tűzfalszabály – Helyi ... 113
4.2 Tűzfalszabályok – Távoli ... 114
4.2 IP-címek ideiglenes tiltólistája ... 115
4.2 Megbízható zóna ... 115
4.2 Zónák konfigurálása ... 116
4.2 Tűzfalzónák ... 116
4.2 A tűzfal naplója ... 117
4.2 Kapcsolat létesítése – észlelés ... 117
4.2 Az ESET Tűzfallal kapcsolatos problémák megoldása ... 118
4.2 Hibaelhárítási varázsló ... 119
4.2 Naplózás és szabályok vagy kivételek létrehozása naplóból ... 119
4.2 Új szabály létrehozása naplóból ... 119
4.2 Kivételek létrehozása a személyi tűzfal értesítéseiből ... 120
4.2 A hálózati védelem speciális naplózása ... 120
4.2 Protokollszűrési problémák megoldása ... 120
4.3 Web és e-mail ... 121
4.3 Protokollszűrés ... 123
4.3 Kizárt alkalmazások ... 123
4.3 Kizárt IP-címek ... 124
4.3 SSL/TLS ... 125
4.3 Tanúsítványok ... 127
4.3 Titkosított hálózati forgalom ... 127
4.3 Ismert tanúsítványok listája ... 128
4.3 SSL/TLS szűrésű alkalmazások listája ... 128
4.3 E-mail védelem ... 129
4.3 Levelezési protokollok ... 131
4.3 E-mail-címkék ... 132
4.3 Integrálás a levelezőprogramokkal ... 133
4.3 Microsoft Outlook-eszköztár ... 133
4.3 Outlook Express- és Windows Mail-eszköztár ... 134
4.3 Megerősítés ... 134
4.3 Üzenetek újraellenőrzése ... 135
4.3 Levélszemétszűrő ... 135
4.3 Levélszemétszűrő névjegyalbumok ... 137
4.3 Tiltólista/Engedélyezőlista/Kizárási lista ... 137
4.3 Tiltólista/engedélyezőlista/kivételcímek hozzáadása/szerkesztése ... 138
4.3 Webhozzáférés-védelem ... 139
4.3 A webhozzáférés-védelem haladó beállításai ... 141
4.3 Webprotokollok ... 141
4.3 URL-címek kezelése ... 142
4.3 URL-címlista ... 143
4.3 Új lista létrehozása ... 144
4.3 URL-maszk hozzáadása ... 145
4.3 Adathalászat elleni védelem ... 146
4.3 Védett böngésző – további beállítások ... 147

4.3 Védett webhelyek 148
4.3 Böngészőn belüli értesítés 148
4.4 Webfelügyelet 149
4.4 Webfelügyeleti szabályok 150
4.4 Webfelügyeleti szabályok hozzáadása 151
4.4 Kategóriacsoportok 153
4.4 URL-csoportok 154
4.4 A Letiltott weboldal üzenet testreszabása 155
4.5 A program frissítése 157
4.5 Frissítési beállítások 161
4.5 Frissítési fájlok visszaállítása 164
4.5 Termékfrissítések 166
4.5 Kapcsolati beállítások 166
4.5 Frissítési tükör 168
4.5 HTTP-szerver és SSL a tükörhöz 169
4.5 Frissítés tükörből 170
4.5 A tükrözésből történő frissítéssel kapcsolatos hibaelhárítás 171
4.5 Frissítési feladatok létrehozása 172
4.6 Eszközök 172
4.6 Naplófájlok 173
4.6 Napló szűrése 176
4.6 Naplózási konfiguráció 177
4.6 Auditálási naplók 178
4.6 Feladatütemező 179
4.6 ESET SysInspector 182
4.6 Felhőalapú védelem 182
4.6 Kivételszűrő felhőalapú védelemhez 185
4.6 Futó folyamatok 186
4.6 Biztonsági jelentés 187
4.6 Hálózati kapcsolatok 188
4.6 ESET SysRescue Live 190
4.6 Minták elküldése elemzésre 190
4.6 Minta kiválasztása elemzésre – Gyanús fájl 191
4.6 Minta kiválasztása elemzésre – Gyanús webhely 191
4.6 Minta kiválasztása elemzésre – Tévesen jelentett fájl 192
4.6 Minta kiválasztása elemzésre – Tévesen jelentett webhely 192
4.6 Minta kiválasztása elemzésre – Egyéb 192
4.6 Karantén 192
4.6 Proxyszerver beállítása 194
4.6 Időközök 195
4.6 Microsoft Windows® frissítés 196
4.6 Licenc intervallum-ellenőrzése 197
4.7 Felhasználói felület 197
4.7 Felhasználói felület elemei 197
4.7 Hozzáférési beállítások 199
4.7 Jelszó a További beállításokhoz 200
4.7 A rendszer tálcaikonja 201
4.7 Helyi menü 202
4.7 Súgó és támogatás 203
4.7 Az ESET Endpoint Security névjegye 203
4.7 Rendszer-konfigurációs adatok küldése 204

4.7 Műszaki terméktámogatás ... 204
4.8 Értesítések ... 205
4.8 Alkalmazásállapotok ... 205
4.8 Asztali értesítések ... 206
4.8 Párbeszédablak – asztali értesítések ... 207
4.8 Az értesítések testreszabása ... 207
4.8 Interaktív riasztások ... 207
4.8 Interaktív riasztások listája ... 209
4.8 Megerősítési üzenetek ... 210
4.8 A további beállításokkal kapcsolatos ütközési hiba ... 211
4.8 Alapértelmezett böngészőben való folytatás engedélyezése ... 211
4.8 Cserélhető adathordozók ... 211
4.8 Újraindítás szükséges ... 212
4.8 Újraindítás javasolt ... 213
4.8 Továbbítás ... 215
4.8 Profilkezelő ... 217
4.8 Billentyűparancsok ... 218
4.8 Diagnosztika ... 219
4.8 Parancssori víruskereső ... 220
4.8 ESET CMD ... 223
4.8 Üresjárat idején történő ellenőrzés ... 225
4.8 Beállítások importálása és exportálása ... 225
4.8 Az összes beállítás visszaállítása alapértelmezettre ... 226
4.8 Az összes beállítás visszaállítása ezen a részen ... 226
4.8 Hiba a konfiguráció mentésekor ... 227
4.8 Távoli figyelés és kezelés ... 227
4.8 Az ERMM-parancssor ... 228
4.8 ERMM JSON-parancsok listája ... 229
4.8 get protection-status ... 230
4.8 get application-info ... 230
4.8 get license-info ... 233
4.8 get logs ... 233
4.8 get activation-status ... 234
4.8 get scan-info ... 235
4.8 get configuration ... 236
4.8 get update-status ... 237
4.8 start scan ... 238
4.8 start activation ... 238
4.8 start deactivation ... 239
4.8 start update ... 240
4.8 set configuration ... 240
5 Gyakori kérdések ... 241
5.1 Automatikus frissítések – Gyakori kérdések ... 242
5.2 Az ESET Endpoint Security frissítése ... 245
5.3 Az ESET Endpoint Security aktiválása ... 245
5.3 A licenckulcs megadása az aktiválás során ... 246
5.3 Bejelentkezés az ESET Business Account-fiókba ... 246
5.3 Újabb ESET-végponttermékek aktiválása régi típusú licenc hitelesítő adataival ... 246
5.4 Vírus eltávolítása a számítógépről ... 246
5.5 Kommunikáció engedélyezése adott alkalmazás számára ... 247
5.6 Új feladat létrehozása a feladatütemezőben ... 247

5.6 Heti számítógép-ellenőrzés ütemezése 248
5.7 Az ESET Endpoint Security csatlakoztatása az ESET PROTECT alkalmazáshoz 249
5.7 A Felülbírálás mód használata 249
5.7 Ajánlott házirend alkalmazása az ESET Endpoint Security szolgáltatásra 251
5.8 Tükrözés beállítása 253
5.9 Frissítés Windows 10-re az ESET Endpoint Security programmal 254
5.10 Távoli figyelés és kezelés aktiválása 254
5.11 Hogyan akadályozható meg bizonyos fájltípusok letöltése az internetről? 257
5.12 Az ESET Endpoint Security minimalista felhasználói felületének beállítása 258
5.13 A következő hiba elhárítása: „A Védett böngésző átirányítása nem sikerült a kért weboldalra” 258
6 Végfelhasználói licencszerződés 260
7 Adatvédelmi szabályzat 267

ESET Endpoint Security 9

Az ESET Endpoint Security 9 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 Endpoint Security 9 teljes körű biztonsági megoldás, mely a hosszú távú fejlesztések eredményeként minimális rendszerterhelés mellett kínál maximális védelmet. A korszerű technológia a mesterséges intelligencián alapuló elemző algoritmusok segítségével képes proaktív módon kivédeni a vírusok, kémprogramok, trójaiak, férgek, kéretlen reklámprogramok, rootkitek és más internetes károkozók támadását anélkül, hogy a rendszer teljesítményét visszafogná.

Az ESET Endpoint Security 9 elsősorban kisvállalati környezetben működő munkaállomásokhoz készült.

Az ESET Endpoint Security használata önállóan című szakaszban található súgótémakörök a könnyebb eligazodás érdekében több fejezetből és alfejezetből állnak, például a Letöltés, a Telepítés és az Aktiválás című fejezetből.

Az ESET Endpoint Security az ESET PROTECT szoftverrel együtt lehetővé teszi vállalati környezetben bármennyi munkaállomás egyszerű kezelését, házirendek és szabályok alkalmazását, kártevők figyelését és ügyfelek távoli konfigurálását bármely hálózati számítógépről.

A Gyakori kérdések című fejezet a leggyakoribb kérdések és problémák közül tekint át néhányat.

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 Endpoint 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 Endpoint Security alkalmazásból ellenőrizheti.

Távoli felügyelet	Az ESET PROTECT lehetővé teszi, hogy hálózati környezetben, egyetlen központi helyről felügyeljen ESET-termékeket számítógépeken, szervereken és mobilkészülékeken. Az ESET PROTECT Webkonzol (ESET PROTECT Webkonzol) segítségével ESET-megoldásokat telepíthet, feladatokat kezelhet, biztonsági irányelveket érvényesíthet, felügyelheti a rendszerállapotot, és gyorsan reagálhat a távoli számítógépeken fellépő problémákra és fertőzésekre.
Hálózati támadások elleni védelem	Elemzi a hálózati forgalom tartalmát, és védelmet biztosít a hálózati támadásokkal szemben. Minden károsnak számító adatforgalmat letilt.
Webfelügyelet (csak az ESET Endpoint Security esetén)	A Webfelügyelet lehetővé teszi az esetlegesen nem kívánt tartalmú weboldalak letiltását. Ezenkívül a munkáltatók vagy a rendszergazdák több, mint 27 előre definiált webhely-kategória és több, mint 140 alkategória elérését is megtilthatják.

A jelen verzió újdonságai?

Az ESET Endpoint Security 9 megjelent, és letölthető.

Automatikus frissítések

- biztosítják, hogy mindig a legújabb termékverziót használja
- intelligens megoldás a ESET Endpoint Securitykarbantartás minimálisra való csökkentésére

- alapértelmezés szerint engedélyezve és a mikro-programösszetevők frissítését használja
- nem telepíti újra a terméket az összes hátrányos következmény mellett, amilyen például a rendszerben való regisztráció törlése a folyamat során, a konfiguráció átvitelével együtt
- kevesebb adat letöltése (eltérő frissítés)
- egy barátságos vagy teljesen elnyomható emlékeztetőt kap a felhasználó, és kompatibilis a felügyelt hálózatokkal

A kapcsolódó végfelhasználói licencszerződés kiegészítései

- a telepítési folyamattól függetlenül egy új végfelhasználói licencszerződés jelenik meg a konzolon vagy a ESET Endpoint Security felhasználói felületén található informatív elem felhasználásával
- leegyszerűsíti a termék automatikus frissítésének folyamatát, és jobbá teszi a felhasználói élményt, mivel többé nem kell elfogadnia a végfelhasználói licencszerződést minden alkalommal, amikor az ESET-terméket egy újabb verzióra frissíti

Brute-force támadás elleni védelem

- az újratervezett Hálózati támadások elleni védelem részét képező Brute-Force támadásvédelem ellenőrzi a hálózati forgalom tartalmát és blokkolja a jelszó-találgatási támadások keretében végzett próbálkozásokat
- a rendszer nyomon követi a forrás IP-címmel végzett ismételt próbálkozásokat, és naplóbejegyzés jön létre az Ideiglenes IP-cím tiltólistán, ami elősegíti a helyzet figyelemmel kísérését
- egy bizonyos idő elteltével a helytelenül viselkedő forrás IP-cím végül levehető a tiltólistáról, ha a kapcsolat megfelelő
- nagy hálózatokon konfigurálható

Natív ARM64 build

- a 9-es verzió ARM64 buildet kínál

Ez a kiadás különböző hibajavításokat és teljesítménybeli fejlesztéseket tartalmaz.

További információkért és az ESET Endpoint Security új funkcióiról készült képernyőfotókért tekintse meg a következő ESET-tudásbáziscikket:

- Újdonságok az ESET Endpoint Security 9-es verziójában

Rendszerkövetelmények

Az ESET Endpoint Security zavartalan működéséhez a rendszernek meg kell felelnie az alábbi hardver- és szoftverkövetelményeknek (alapértelmezett szoftverbeállítások):

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

Operációs rendszerek

Microsoft® Windows® 11

Microsoft® Windows® 10

A Microsoft® Windows® 10 és Microsoft® Windows® 11 támogatott verzióinak részletes listáját a Windows operációs rendszer támogatási házirendje című rész tartalmazza.

A 2023 júliusa után kiadott ESET-termékek telepítéséhez vagy frissítéséhez minden Windows operációs rendszerre telepíteni kell az Azure Code Signing támogatást. További információ.

Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 és a legújabb Windows-frissítések (legalább a KB4474419 és a KB4490628)

Az ESET Endpoint Security 9.1-es verziója az utolsó, amely támogatja a Windows 7 és a Windows 8.1 rendszert. További információ.

A Windows XP és a Windows Vista már nem támogatottak.

Törekedjen arra, hogy az operációs rendszer mindig naprakész legyen.

Az ESET PROTECT 8.1-es és újabb verzióiban létrehozott ESET Endpoint Security telepítő támogatja a Windows 10 Enterprise for Virtual Desktops és a Windows 10 többmenetes módot.

Egyéb

- Az operációs rendszer és a számítógépen telepített egyéb szoftverek rendszerkövetelményeinek meg kell felelni

- 0,3 GB szabad rendszermemória (lásd 1. megjegyzés)
- 1 GB szabad lemezterület (lásd 2. megjegyzés)
- A minimális megjelenítési felbontás: 1024 x 768
- Internetkapcsolat vagy helyi hálózati kapcsolat a szoftverfrissítések forrásához (lásd a 3. megjegyzést)
- Ha két víruskereső program fut egyszerre egy adott eszközön, akkor ez elkerülhetetlenül ütközéseket okoz a rendszererőforrások között, például lelassítja a rendszert, és működésképtelenné válhat

Bár elképzelhető, hogy olyan rendszereken is futtatható a szoftver, amelyek nem teljesítik ezeket a követelményeket, azt ajánljuk, hogy a teljesítményt érintő követelmények alapján végezzen előzetes használhatósági tesztet.

(1): Előfordulhat, hogy a szoftver több memóriát használ, ha a memória egyébként nincs használatban egy súlyosan fertőzött számítógépen, illetve amikor terjedelmes adatlistákat importál a szoftverbe (pl. URL-címek engedélyezőlistáját).
(2): A telepítő letöltéséhez, a szoftver telepítéséhez és a telepítőcsomag egy másolatának a programadatok közötti megőrzéséhez, valamint a visszaállítási funkció támogatása céljából a termékfrissítések biztonsági másolatához szükséges lemezterület. Előfordulhat, hogy a szoftver több lemezterületet használ különféle beállítások mellett (pl. több termékfrissítési biztonságimásolat-változat tárolásakor, memóriaképek vagy nagy mennyiségű naplórekord megőrzésekor), illetve egy fertőzött számítógépen (pl. a karantén funkció következtében). Javasoljuk, hogy az operációs rendszer és az ESET szoftver frissítéseinek támogatása céljából gondoskodjon elegendő lemezterületről.
(3): Bár nem javasolt, de a szoftver cserélhető adathordozóról manuálisan is frissíthető.

Támogatott nyelvek

Az ESET Endpoint Security a következő nyelveken áll rendelkezésre telepítésre és letöltésre.

Nyelv	Nyelvkód	LCID
Angol (Amerikai Egyesült Államok)	en-US	1033
Arab (Egyiptom)	ar-EG	3073
Bolgár	bg-BG	1026
Kínai (egyszerűsített)	zh-CN	2052
Kínai (hagyományos)	zh-TW	1028
Horvát	hr-HR	1050
Cseh	cs-CZ	1029
Észt	et-EE	1061
Finn	fi-FI	1035
Francia (Franciaország)	fr-FR	1036
Francia (Kanada)	fr-CA	3084
Német (Németország)	de-DE	1031
Görög	el-GR	1032
*Héber	he-IL	1037
Magyar	hu-HU	1038
*Indonéz	id-ID	1057
Olasz	it-IT	1040
Japán	ja-JP	1041

Nyelv	Nyelvkód	LCID
Kazak	kk-KZ	1087
Koreai	ko-KR	1042
Lett	lv-LV	1062
Litván	lt-LT	1063
Nederlands	nl-NL	1043
Norvég	nb-NO	1044
Lengyel	pl-PL	1045
Portugál (brazíliai)	pt-BR	1046
Román	ro-RO	1048
Orosz	ru-RU	1049
Spanyol (Chile)	es-CL	13322
Spanyol (Spanyolország)	es-ES	3082
Svéd (Svédország)	sv-SE	1053
Szlovák	sk-SK	1051
Szlovén	sl-SI	1060
Thai	th-TH	1054
Török	tr-TR	1055
Ukrán (Ukrajna)	uk-UA	1058
*Vietnami	vi-VN	1066

*Az ESET Endpoint Security rendelkezésre áll ezen a nyelven, de online felhasználói útmutató nem érhető el (átirányít az angol verzióra).

Az online felhasználói útmutató nyelvének módosításához használja a nyelvválasztó mezőt (a jobb felső sarokban).

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

Az 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. Fontos, hogy ezeket a biztonsági frissítéseket megjelenésükkor töltse le. 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 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 Endpoint Security súgója! A súgóbeli információk segítenek a termék megismerésében és a számítógép biztonságosabbá tételében.

Első lépések

Mielőtt megkezdené az ESET Endpoint Security használatát, vegye figyelembe, hogy termékünk az ESET PROTECT segítségével csatlakozott felhasználók által vagy önállóan is használható. Ajánlatos megismerkedni a különféle kártevőtípusokkal és távoli támadásokkal, amelyekkel a számítógép használata közben találkozhat.

Az új funkciók leírásából megismerheti az ESET Endpoint Security jelen verziójában bevezetett funkciókat. Az ESET Endpoint Security alapvető beállításainak megadásához és testreszabásához rendelkezésre áll egy útmutató is.

Az ESET Endpoint Security súgótémaköreinek használata

A súgótémakörök a könnyebb eligazodás érdekében több fejezetből és alfejezetből állnak. A kapcsolódó információk megkereséséhez tallózhat a tartalomjegyzékben (a témakörök struktúrájában).

A program egyes ablakairól az **F1** billentyűt lenyomva tudhat meg többet. Ekkor megjelenik az éppen megtekintett ablakhoz kapcsolódó súgótémakör.

A súgóoldalakon kulcsszó alapján, illetve szavak vagy kifejezések beírásával kereshet. A két módszer között az a különbség, hogy a kulcsszavak logikailag olyan súgótémakörökhöz is kapcsolódhatnak, amelyek szövegében nem szerepel az adott kulcsszó. A szabadszavas keresés esetén azok a témakörök jelennek meg, amelyek tartalmazzák a keresett szót vagy kifejezést.

A konzisztencia érdekében és a félreértések elkerülése végett a jelen útmutatóban használt terminológia az ESET Endpoint 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.

Távolról felügyelt végpontok dokumentációja

Az ESET vállalati termékei és az ESET Endpoint Security távolról felügyelhetők kliensszámítógépeken, szervereken és mobilkészülékeken egy központi helyről a hálózati környezetben. A több mint 10 kliensszámítógépet felügyelő rendszergazdáknak érdemes telepíteniük az ESET távoli felügyeleti eszközök egyikét, mert így egyszerűbben telepíthetnek ESET-megoldásokat, kezelhetik a feladatokat, érvényesíthetik a biztonsági irányelveket,

felügyelhetik a rendszerállapotot, valamint egy központi helyről gyorsan tudnak reagálni a távoli számítógépeken fellépő problémákra és veszélyekre.

ESET távoli felügyeleti eszközök

Az ESET Endpoint Security, az ESET PROTECT illetve az ESET Cloud Administrator segítségével felügyelhető távolról.

- Az ESET PROTECT ismertetése
- Az ESET PROTECT Cloud ismertetése

Külső gyártású távoli felügyeleti eszközök

- Távoli figyelés és kezelés (RMM)

Bevált eljárások

- Csatlakoztassa az összes végpontot az ESET Endpoint Security segítségével az ESET PROTECThez
- Nyújtson védelmet a speciális beállításoknak a csatlakoztatott kliensszámítógépeken a jogosulatlan módosítások elkerülése érdekében
- A javasolt házirendek egyikének alkalmazásával szerezzen érvényt a rendelkezésre álló biztonsági funkcióknak
- Minimalista felhasználói felület beállításával csökkentse vagy korlátozza az ESET Endpoint Security szolgáltatással elvégezhető felhasználói műveleteket

Útmutatók

- A Felülbírálás mód használata
- Telepítés ESET Endpoint Security GPO vagy SCCM segítségével

Az ESET PROTECT ismertetése

Az ESET PROTECT lehetővé teszi, hogy hálózati környezetben, egyetlen központi helyről felügyeljen ESET-termékeket számítógépeken, szervereken és mobilkészülékeken.

Az ESET PROTECT Webkonzol használatakor ESET-megoldásokat telepíthet, feladatokat kezelhet, biztonsági házirendeket vezethet be, felügyelheti a rendszerállapotot, és gyorsan reagálhat a távoli számítógépeken fellépő problémákra és a rajtuk észlelt kártevőkre. Tekintse meg a következőket is: Az ESET PROTECT architekturális és infrastrukturális elemeinek áttekintése, Az ESET PROTECT Webkonzol használatbavétele és A támogatott asztali üzembe helyezési környezetek.

Az ESET PROTECT a következő összetevőkből áll:

- ESET PROTECT Szerver – Az ESET PROTECT Szerver Windows- és Linux-szerverekre is telepíthető, és virtuális eszközként is rendelkezésre áll. Kezeli az ügynökökkel folytatott kommunikációt, és összegyűjti és tárolja az alkalmazásadatokat az adatbázisban.
- ESET PROTECT Webkonzol – Az ESET PROTECT Webkonzol az elsődleges interfész, amely lehetővé teszi a kliensszámítógépek felügyeletét az adott környezetben. Megjeleníti a hálózaton lévő kliensek állapotát, és a segítségével ESET-megoldások telepíthetők távolról nem felügyelt számítógépekre. Az ESET PROTECT Szerver telepítése után a webböngészőben érhető el a Webkonzol. Ha elérhetővé teszi a webszervert az

interneten keresztül, akkor az ESET PROTECT bárhonnan, illetve bármilyen készülékről használhatóvá válik, ha rendelkezésre áll internetkapcsolat.

- ESET Management Ügynök – Az ESET Management Ügynök megkönnyíti a kommunikációt az ESET PROTECT Szerver és kliensszámítógépek között. Az Ügynököt telepíteni kell a kliensszámítógépre annak érdekében, hogy létrejöjjön a kommunikáció a számítógép és az ESET PROTECT Szerver között. Mivel a kliensszámítógépen található, és több biztonsági forgatókönyvet tud tárolni, az ESET Management Ügynök használatakor sokkal gyorsabban lehet reagálni az új kártevőkre. Az ESET PROTECT Webkonzol segítségével telepíthető az ESET Management Ügynök az Active Directory vagy az ESET RD-érzékelő által beazonosított felügyelet nélküli számítógépekre. Manuálisan is telepíthető az ESET Management Ügynök kliensszámítógépekre szükség esetén.
- ESET Rogue Detection Sensor – A ESET Rogue Detection Sensor észleli a hálózaton lévő felügyelet nélküli számítógépeket, és elküldi az adataikat az ESET PROTECT Szervernek. Ezáltal egyszerűen hozzáadhat új kliensszámítógépeket a biztonságos hálózatához. Az RD-érzékelő megjegyzi a beazonosított számítógépeket, így még egyszer nem küldi el ugyanazokat az információkat.
- Apache HTTP-proxy – Ez a szolgáltatás az ESET PROTECT rendszerrel együtt használható a következőkhöz:
    - Frissítések küldése a kliensszámítógépekre és telepítőcsomagok továbbítása az ESET Management Ügynöknek.
    - Kommunikáció továbbítása az ESET Management Ügynököktől az ESET PROTECT Szerverhez.
- Mobile Device Connector – Ez az összetevő lehetővé teszi az ESET PROTECT rendszerrel együtt végzett mobileszköz-felügyeletet, így mobileszközöket (Android és iOS) felügyelhet, és kezelheti az ESET Endpoint Security for Android szolgáltatást.
- ESET PROTECT Virtuális eszköz – Az ESET PROTECT VE olyan felhasználóknak készült, akik az ESET PROTECT rendszert virtualizált környezetben szeretnék futtatni.
- ESET PROTECT Virtual Agent Host – Az ESET PROTECT egyik összetevője, amely az ügynökök virtualizálásával lehetővé teszi az ügynök nélküli virtuális gépek felügyeletét. A megoldás révén lehetővé válik az automatizálás, a dinamikus csoportfelhasználás és az olyan szintű feladatkezelés, mint amit az ESET Management Ügynök nyújt a fizikai számítógépeken. A Virtuális ügynök összegyűjti az információk a virtuális gépekről, és elküldi őket az ESET PROTECT Szervernek.
- Tükrözési eszköz – A tükrözési eszközre az offline modulfrissítésekhez van szükség. Ha a kliensszámítógépek nem rendelkeznek internetkapcsolattal, a tükrözési eszköz segítségével tölthet le frissítési fájlokat az ESET frissítési szervereiről, és helyben tárolhatja őket.
- ESET Remote Deployment Tool – Ez az eszköz lehetővé teszi az <%PRODUCT%> Webkonzolban létrehozott univerzális csomagok telepítését. Segítségével kényelmesen továbbítható az ESET Management Ügynök egy ESET-termékkel a hálózaton lévő számítógépekre.
- ESET Business Account – Az ESET üzleti termékek új licencelési portálja lehetővé teszi a licencek kezelését. A jelen dokumentum ESET Business Account című szakaszában találja meg a termék aktiválására vonatkozó útmutatót, vagy nézze meg az ESET Business Account Felhasználói útmutatójában az ESET Business Account használatára vonatkozó bővebb tudnivalókat. Ha már rendelkezik ESET által kiadott felhasználónévvel és jelszóval, amelyeket licenckulcsra szeretne konvertálni, olvassa el a Régi licencadatok konvertálása című szakaszt.
- ESET Inspect – Ez egy átfogó észlelési és válaszadási rendszer, amely például a következő funkciókat tartalmazza: események észlelése, események felügyelete és reagálás, adatgyűjtés, fertőzésészlelési mutatók, anomáliák észlelése, viselkedésészlelés és házirendek megszegése.

Az ESET PROTECT Webkonzol segítségével telepíthet ESET-megoldásokat, feladatokat kezelhet, biztonsági irányelveket érvényesíthet, felügyelheti a rendszerállapotot, és gyorsan reagálhat a távoli számítógépeken fellépő problémákra és fertőzésekre.

> További információkért tekintse meg az ESET PROTECT online felhasználói útmutatóját.

Az ESET PROTECT Cloud ismertetése

az ESET PROTECT Cloud lehetővé teszi, hogy egyetlen központi helyről felügyeljen ESET-termékeket munkaállomásokon és szervereken hálózati környezetben anélkül, hogy szükség lenne fizikai vagy virtuális szerverre, mint az ESET PROTECT esetén. Az ESET PROTECT Cloud Webkonzol segítségével ESET-megoldásokat telepíthet, feladatokat kezelhet, biztonsági házirendeket érvényesíthet, felügyelheti a rendszerállapotot, és gyorsan reagálhat a távoli számítógépeken fellépő problémákra és fertőzésekre.

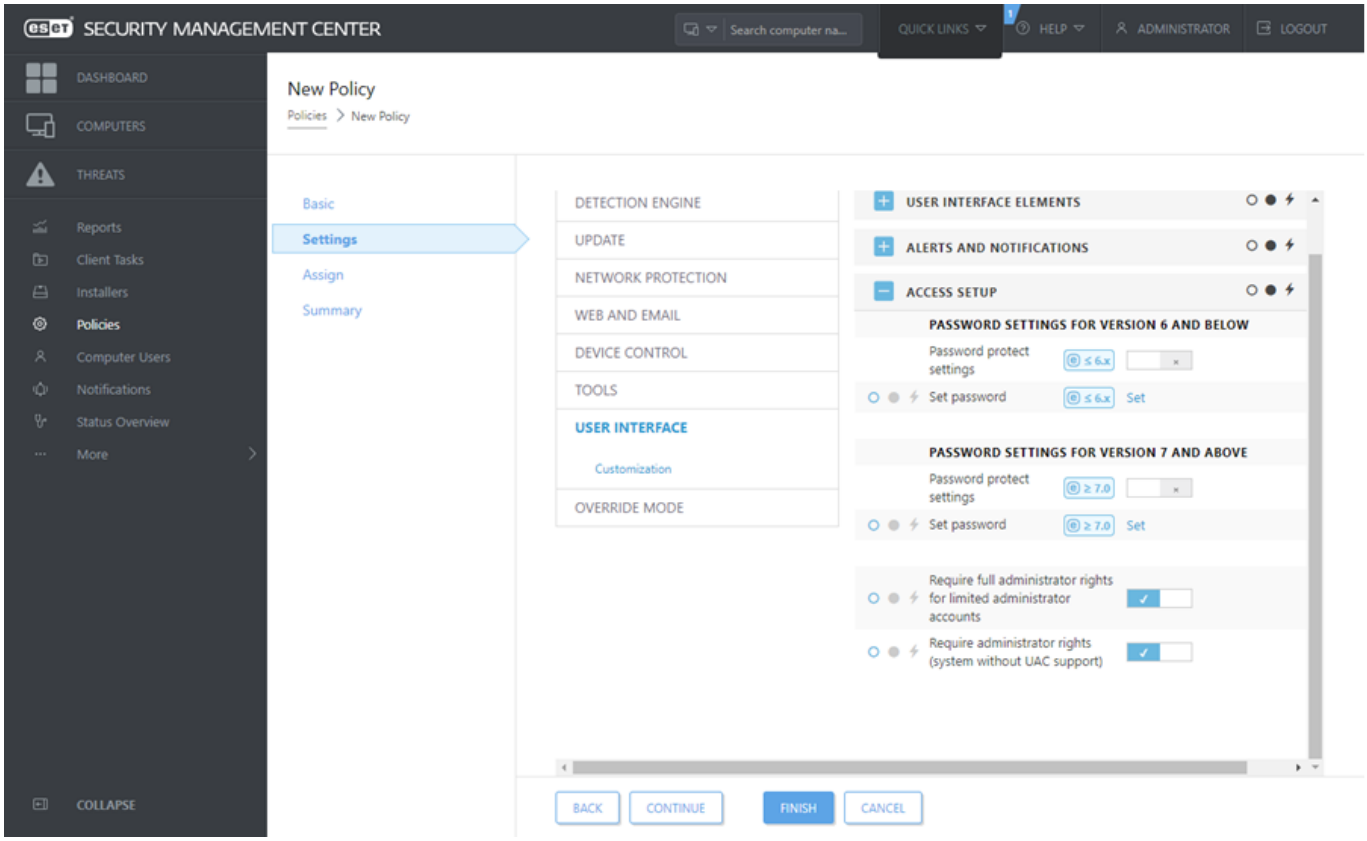
- Az ESET PROTECT Cloud online felhasználói útmutatójában bővebben olvashat erről

Jelszóval védett beállítások

A rendszer maximális biztonsága érdekében fontos, hogy az ESET Endpoint Security megfelelően legyen konfigurálva. A nem hozzáértő módosítások vagy beállítások következtében csökkenhet a kliensek védettsége és védelmi szintje. Ha nem szeretné, hogy a felhasználók hozzáférjenek a haladó beállításokhoz, egy rendszergazda jelszóval levédheti a beállításokat.

A rendszergazda egy házirend létrehozásával jelszóval megvédheti az ESET Endpoint Security speciális beállításait a csatlakoztatott kliensszámítógépeken. Új házirend létrehozása:

1. Az ESET PROTECT Webkonzolban kattintson a **Házirendek** menüpontra a bal oldali főmenüben.
2. Kattintson az **Új házirend** gombra.
3. Nevezze el az új házirendet, és – ha szeretné – adjon meg egy rövid leírást. Kattintson a **Folytatás** gombra.
4. A termékek listájában válassza ki az **ESET Endpoint for Windows** elemet.
5. Kattintson a **Felhasználói felület** elemre a **Beállítások** listában, majd bontsa ki a **Hozzáférési beállítások** szakaszt.
6. Az ESET Endpoint Security verziójának megfelelően a csúszkára kattintva engedélyezze a **Jelszó a beállítások védelméhez** funkciót. Vegye figyelembe, hogy az ESET Endpoint 7-es és újabb verziói fejlett védelmet nyújtanak. Ha az Endpoint-termékek 7-es és újabb, illetve 6-os verziója is megtalálható a hálózaton, azt javasoljuk, hogy az egyes verziókhoz hozzon létre külön házirendet különböző jelszavakkal.
7. Az előugró ablakban hozzon létre egy új jelszót, erősítse meg, majd kattintson az **OK** gombra. Kattintson a **Tovább** gombra.
8. Rendelje hozzá a házirendet a kliensekhez. Kattintson a **Hozzárendelés** elemre, és válassza ki a jelszóval védeni kívánt számítógépeket vagy számítógépcsoportokat. Az **OK** gombra kattintva erősítse meg a beállítást.
9. Ellenőrizze, hogy az összes védeni kívánt számítógép megtalálható-e a céllistában, majd kattintson a **Folytatás** gombra.
10. Tekintse át a házirend-beállításokat az összegzésben, majd a **Befejezés** kattintva mentse az új házirendet.



Mik a házirendek?

A rendszergazda bizonyos konfigurációkat tud továbbítani a kliensszámítógépeken futó ESET-termékekre az ESET PROTECT Webkonzol házirendjei segítségével. A házirendek közvetlenül egy-egy számítógépre, illetve akár számítógépcsoportokra is alkalmazható. Több házirend is alkalmazható egy számítógépre vagy egy csoportra.

A felhasználónak a következő engedélyekkel kell rendelkeznie egy új házirend létrehozásához: **Olvasás** engedély a házirendlisták olvasásához, **Használat** engedély a házirendek célszámítógépekhez való hozzárendeléséhez, valamint **Írás** engedély házirendek létrehozásához, módosításához és szerkesztéséhez.

A házirendek alkalmazására a Statikus csoportok elrendezése szerinti sorrendben kerül sor. Ez nem vonatkozik a Dinamikus csoportokra, ahol a házirendek alkalmazása először a gyermek Dinamikus csoportok esetén megy végbe. Ezáltal a házirendek nagyobb hatással alkalmazhatók a csoportfa tetejére, és részletesebb házirendek alkalmazhatók az alcsoportokra. Jelzők segítségével a fában magasabban elhelyezkedő csoportokhoz hozzáférő ESET Endpoint Security-felhasználó felül tudja írni az alsóbb csoportok házirendjeit. Az algoritmus magyarázata az ESET PROTECT online súgójában található.

> **i** Azt javasoljuk, hogy általánosabb házirendeket rendeljen hozzá (például a frissítési szerver házirendje) olyan csoportokhoz, amelyek magasabban vannak a csoportfában. Részletesebb házirendeket (például az eszközfelügyeleti beállítások) érdemes hozzárendelni a csoportfa alsóbb szintjeihez. Az alsóbb házirend általában felülírja a felsőbb házirendek beállításait egyesítés esetén (kivéve, ha más beállítást ad meg házirendjelzők segítségével).

Házirendek egyesítése

Egy kliensre alkalmazott házirend általában több házirend egyesítéséből jön létre. A házirendek egyenként egyesíthetők. A házirendek egyesítésekor az általános szabály, hogy a későbbi házirend mindig leváltja az előző

által meghatározott beállításokat. Ennek módosításához házirendjelzőket használhat (mindegyik beállításhoz rendelkezésre állnak).

Házirendek létrehozásakor néhány beállításnál van egy további szabály (csere/hozzáfűzés/eléhelyezés), amely konfigurálható.

- **Csere** – a teljes lista cseréje; új értékek hozzáadása és az összes előző érték eltávolítása.
- **Hozzáfűzés** – elemek hozzáadása az aktuálisan alkalmazott lista aljához (kell egy másik házirend, a helyi lista mindig felülíródik).
- **Eléhelyezés** – elemek hozzáadása a lista tetejéhez (a helyi lista felülíródik).

Az ESET Endpoint Security újfajta módon teszi lehetővé a helyi beállítások távoli házirendekkel való egyesítését. Ha a beállítás egy lista (például letiltott webhelyek listája), és a helyi házirend ütközik egy meglévő helyi beállítással, akkor a távoli házirend felülírja. Megadhatja a helyi és a távoli listák összevonásának módját a különböző egyesítési szabályok kiválasztásával:

- Egyesítési szabályok távoli házirendek esetén.
- Távoli és helyi házirendek egyesítése – helyi beállítások a létrejövő távoli házirenddel.

Ha bővebben szeretne tájékozódni a házirendek egyesítéséről, tekintse meg az ESET PROTECT online felhasználói útmutatóját és ezt a példát.

Hogyan működnek a jelzők?

Egy kliensszámítógépre alkalmazott házirend általában több házirend egyesítéséből jön létre. Házirendek egyesítésekor házirendjelzők segítségével megadhatja a végső házirendtől elvárt működésmódot, az alkalmazott házirendek sorrendjétől függően. A jelzők határozzák meg, hogy a házirend hogyan fog kezelni egy bizonyos beállítást.

Mindegyik beállításhoz a következő jelzők közül választhat egyet:

Nincs alkalmazás	Az ilyen jelzővel ellátott beállítást nem alkalmazza a házirend. Mivel a házirend nem alkalmazza a beállítást, más, később alkalmazott házirendek módosítani tudják.
Alkalmaz	Az **Alkalmazás** jelzővel ellátott beállításokat alkalmazza a rendszer a kliensszámítógépre. Házirendek egyesítésekor azonban más, később alkalmazott házirendek át tudják írni. Ha egy olyan házirendet küld egy kliensszámítógépre, amely ezzel a jelzővel van ellátva, akkor az adott beállítások módosítják a kliensszámítógép helyi konfigurációját. Mivel nem kerül sor a beállítás kényszerítésére, más, később alkalmazott házirendek alkalmazni tudják.
Kényszerítés	A **Kényszerítés** jelzővel ellátott beállítások elsőbbséget élveznek, így nem tudják átírni később alkalmazott házirendek (akkor sem, ha szintén a **Kényszerítés** jelzővel rendelkeznek). Ez biztosítja, hogy a később alkalmazott házirendek ne tudják módosítani ezt a beállítást az egyesítés során. Ha egy olyan házirendet küld egy kliensszámítógépre, amely ezzel a jelzővel van ellátva, akkor az adott beállítások módosítják a kliensszámítógép helyi konfigurációját.

Forgatókönyv: A *rendszergazda* szeretné engedélyezni *János* felhasználónak, hogy létrehozhasson és szerkeszthessen házirendeket az otthoni csoportjában, és hogy megtekinthesse a *rendszergazda* által létrehozott összes házirendet, így a Kényszerítés jelzővel ellátott házirendeket is. A *rendszergazda* azt szeretné, hogy *János* megnézhesse az összes házirendet, viszont azt nem, hogy szerkeszthesse is a *rendszergazda* által létrehozott házirendeket. *János* csak a San Diego nevű otthoni csoportjában hozhat létre és szerkeszthet házirendeket.
Megoldás: *A rendszergazdának* a következő lépéseket kell követnie:
Egyéni statikus csoportok és engedélycsoportok létrehozása
1. Hozzon létre egy *San Diego* elnevezésű új statikus csoportot.
2. Hozzon létre egy új *Házirend – Összes John* elnevezésű engedélycsoportot, amely hozzáférhet az *Összes* nevű statikus csoporthoz, és amelynek **Olvasás** engedélye van a **Házirendekhez**.
3. Hozzon létre egy új *Házirend, János* nevű engedélycsoportot, amely hozzáférhet a *San Diego* statikus csoporthoz, és **Írás** engedélye van a **Csoport és számítógépek** és a **Házirendek** elemhez. Ez az engedélycsoport lehetővé teszi *Jánosnak*, hogy létrehozzon és szerkesszen házirendeket a *San Diego* nevű otthoni csoportjában.
4. Hozza létre a *János* nevű új felhasználót, és az **Engedélycsoportok** szakaszban válassza ki a *Házirend – Összes János* és a *Házirend, János* lehetőséget.
Házirendek létrehozása
5. Hozza létre az *Összes – Tűzfal engedélyezése* nevű házirendet, bontsa ki a **Beállítások** szakaszt, válassza ki az **ESET Endpoint for Windows** elemet, navigáljon a **Személyes Tűzfal** > **Általános** lapra, majd alkalmazza az összes beállítást a **Kényszerítés** jelzővel. Bontsa ki a **Hozzárendelés** szakaszt, és válassza ki az *Összes* nevű statikus csoportot.
6. Hozza létre az *János csoportja – Tűzfal engedélyezése* nevű házirendet, bontsa ki a **Beállítás** szakaszt, válassza ki az **ESET Endpoint for Windows** elemet, navigáljon a **Személyes Tűzfal** > **Általános** lapra, majd alkalmazza az összes beállítást az **Alkalmazás** jelzővel. Bontsa ki a **Hozzárendelés** szakaszt, és válassza ki a *San Diego* nevű statikus csoportot.
Eredmény
A *rendszergazda* által létrehozott házirendek alkalmazása fog megtörténni először, mivel a **Kényszerítés** jelzőket alkalmazta a házirend-beállításokra. A Kényszerítés jelzővel ellátott beállítások elsőbbséget élveznek, és nem tudják átírni más, később alkalmazott házirendek. A *János* felhasználó által létrehozott házirendek alkalmazására a rendszergazda által létrehozott házirendek után kerül sor.
A házirendek végső sorrendjének megtekintéséhez lépjen a **Továbbiak** > **Csoportok** > **San Diego** lapra. Válassza ki a számítógépet, majd a **Részletek megjelenítése** lehetőséget. A **Konfiguráció** szakaszban kattintson az **Alkalmazott házirendek** elemre.

Az ESET Endpoint Security használata önállóan

A felhasználói útmutató jelen szakasza és Az ESET Endpoint Security használata című szakasza az ESET Endpoint Security alkalmazást az ESET PROTECT vagy ESET PROTECT Cloud nélkül használó felhasználóknak készült. A felhasználói fiók jogosultságaitól függően teljes mértékben elérhető az ESET Endpoint Security összes szolgáltatása és funkciója.

Telepítési módszerek

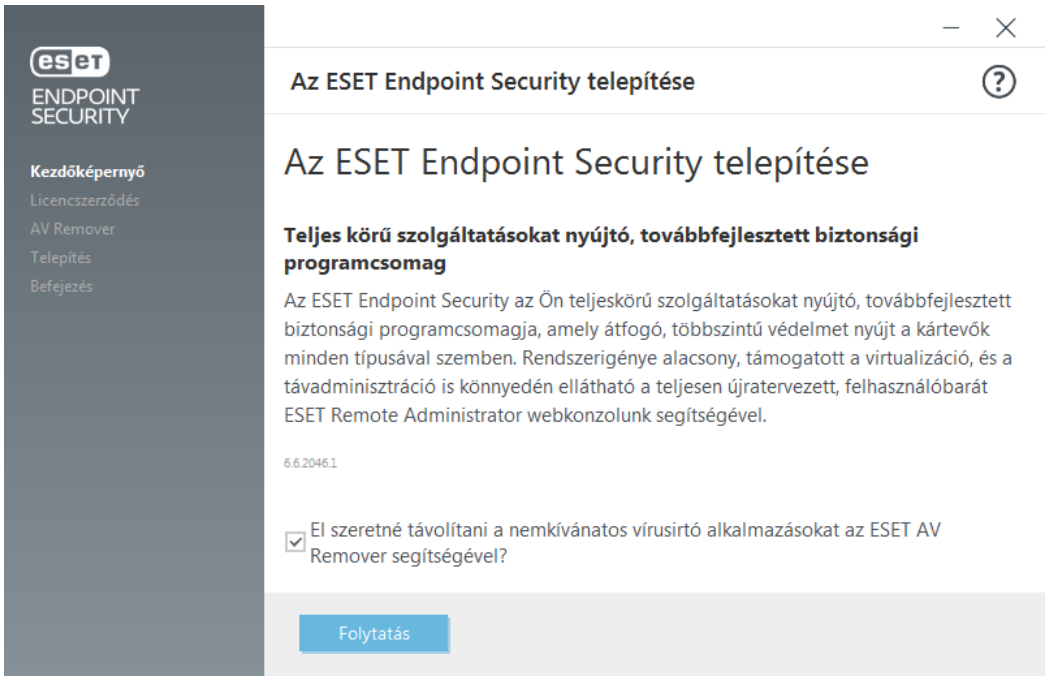
Többféle módon telepíthetők az ESET Endpoint Security 9.x verziói a kliensszámítógépekre, ha nem az ESET Endpoint Security segítségével távolról telepíti a kliensszámítógépekre az ESET PROTECT vagy az ESET PROTECT Cloud segítségével.

Módszerek	Cél	Letöltési link
Telepítés az ESET AV Remover eszközzel	Az ESET AV Remover eszköz segítségével a rendszeren korábban telepített szinte bármely víruskereső szoftver eltávolítható a telepítés előtt.	64 bites letöltése 32 bites letöltése
***Telepítés (.exe)	Telepítési folyamat az ESET AV Remover nélkül.	N/A
Telepítés (.msi)	Üzleti környezetben érdemes az .msi telepítőcsomagot választani. Ennek oka leginkább az offline és a távoli központi telepítés, amelyek különböző eszközökkel, például az ESET PROTECT segítségével hajthatók végre.	64 bites letöltése 32 bites letöltése
Parancssori telepítés	ESET Endpoint SecurityAz helyileg a parancssor segítségével telepíthető, illetve távolról az ESET PROTECT programban egy kliensfeladat végrehajtásával.	N/A
Központi telepítés GPO vagy SCCM segítségével	Használjon felügyeleti eszközöket – például GPO vagy SCCM – az ESET Management Agent és az ESET Endpoint Security kliensszámítógépekre való telepítéséhez.	N/A
Telepítés RMM-eszközökkel	Az RMM eszközhöz (Remote Management and Monitoring) használható ESET DEM beépülő modulok segítségével központilag telepíthető az ESET Endpoint Security a kliensszámítógépekre	N/A

Az ESET Endpoint Security több mint 30 nyelven áll rendelkezésre.

Telepítés az ESET AV Remover eszközzel

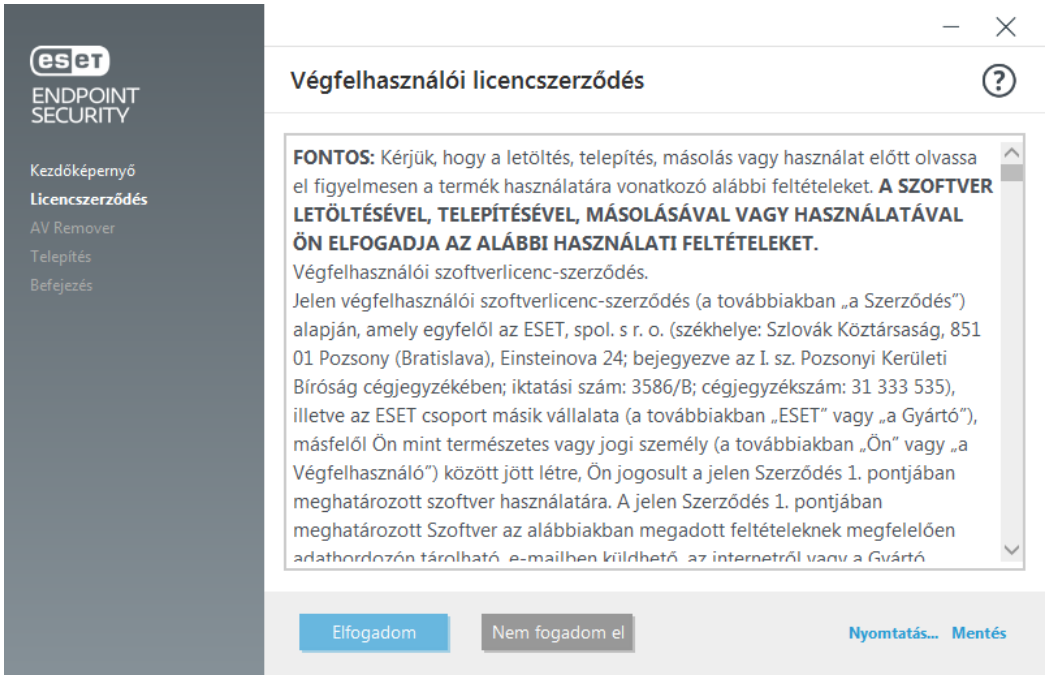
A telepítési folyamat folytatása előtt fontos eltávolítani minden meglévő biztonsági alkalmazást a számítógépről. Jelölje be az **El szeretném távolítani a nemkívánatos vírusirtó alkalmazásokat az ESET AV Remover** használatával jelölőnégyzetet ahhoz, hogy az ESET AV Remover ellenőrizze a rendszerét, és eltávolítsa a támogatott biztonsági alkalmazásokat. Hagyja üresen a jelölőnégyzetet, és kattintson a **Folytatás** gombra, ha az ESET Endpoint Security alkalmazást az ESET AV Remover használata nélkül szeretné telepíteni.



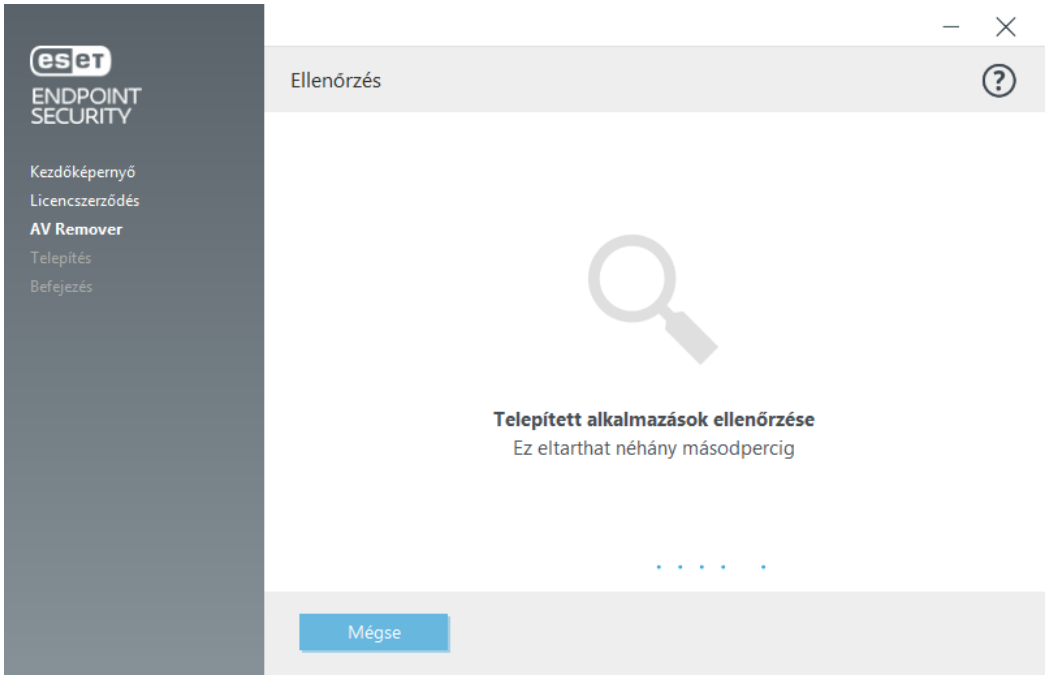
ESET AV Remover

Az ESET AV Remover eszköz segítségével a rendszeren korábban telepített szinte bármely víruskereső szoftver eltávolítható. Ha az ESET AV Remover használatával szeretne meglévő víruskereső programokat eltávolítani, kövesse az alábbi utasításokat:

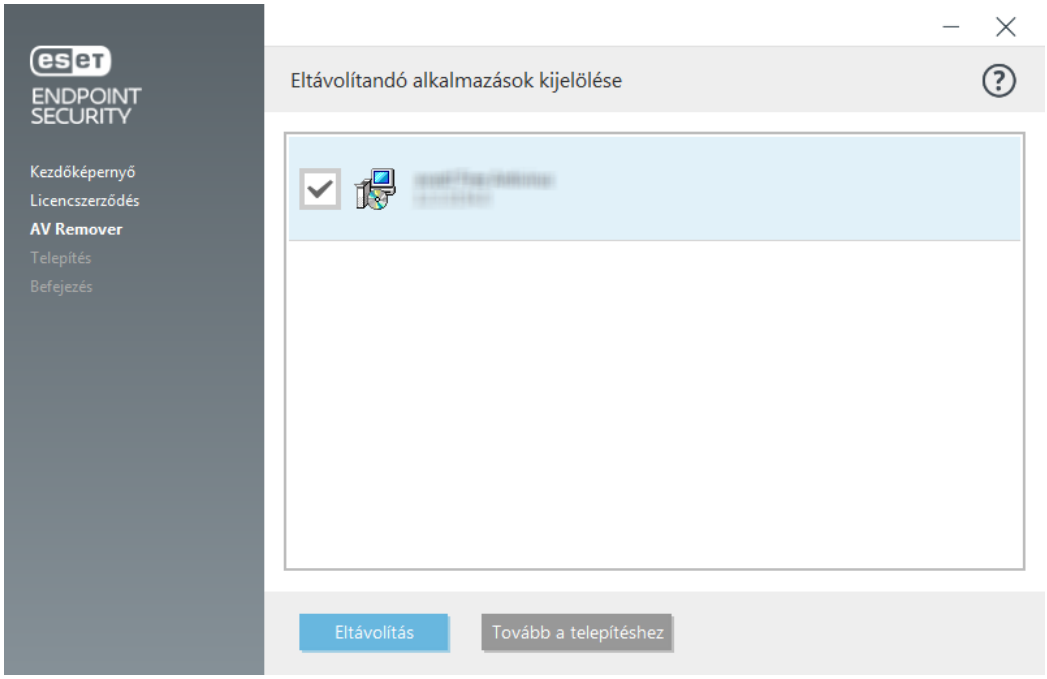
1. Az ESET AV Remover eszközzel eltávolítható víruskereső szoftverek listája az ESET tudásbázisának cikkében található.
2. A végfelhasználói licencszerződés átolvasását követően az **Elfogadom** választógombot bejelölve jelezheti, hogy elfogadja a szerződésben foglaltakat. Ha a **Nem fogadom el** választógombot jelöli be, a számítógépen lévő biztonsági alkalmazás eltávolítása nélkül folytatódik az ESET Endpoint Security telepítése.



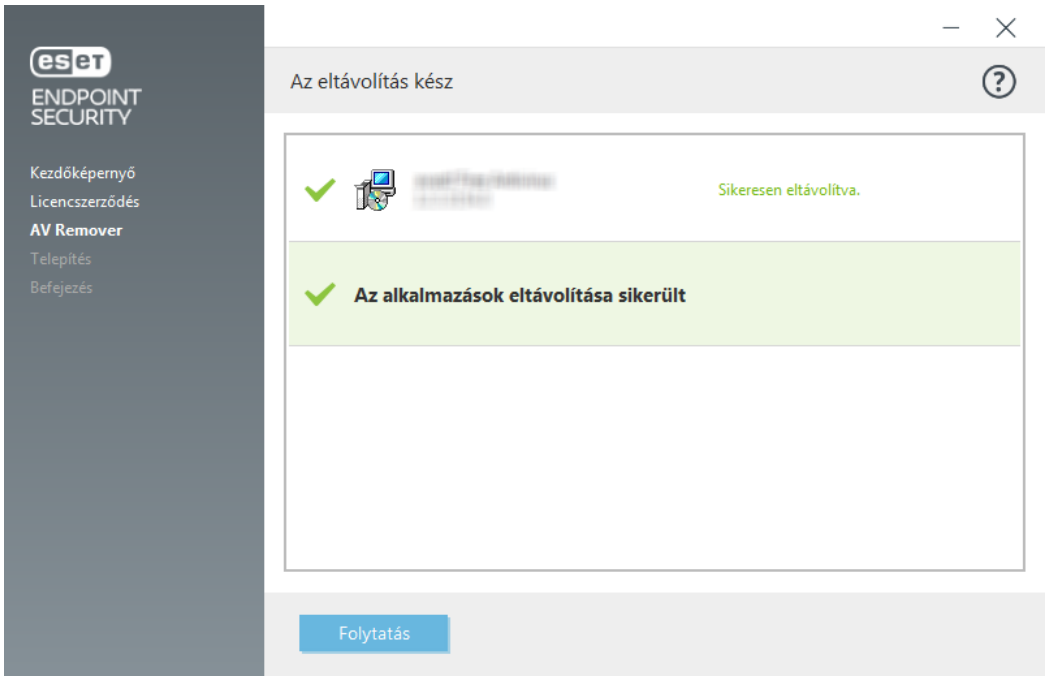
2. Az ESET AV Remover elkezdi a víruskereső szoftverek keresését a rendszerben.



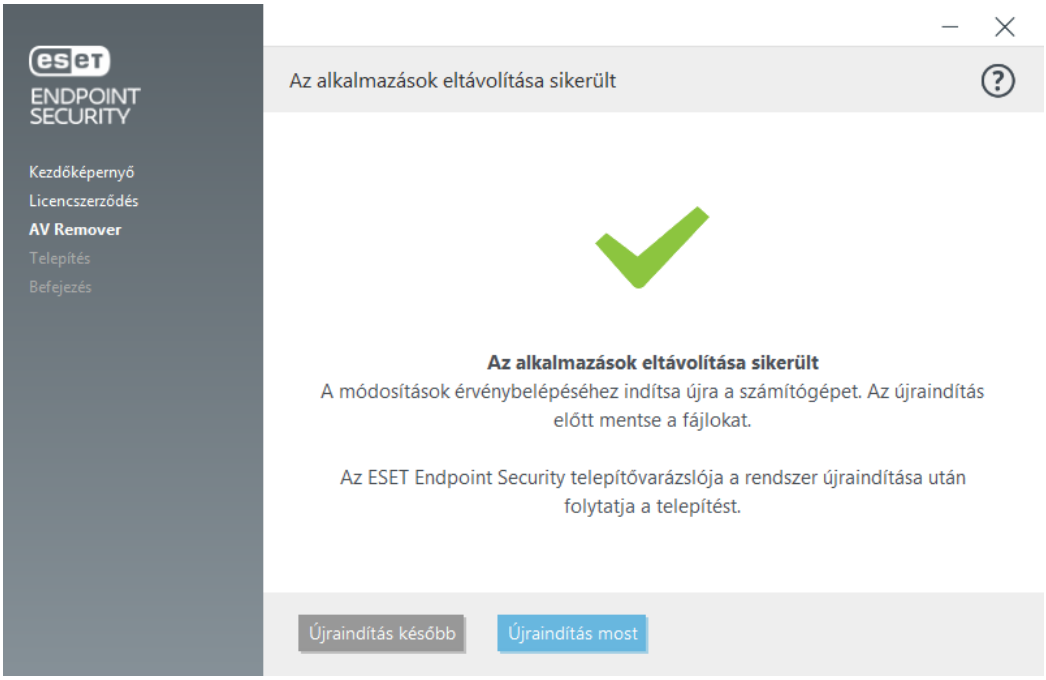
2. Jelölje ki bármelyik víruskereső alkalmazást a listában, és kattintson az **Eltávolítás** elemre. Az eltávolítás eltarthat kis ideig.



2. Amikor az eltávolítás sikerült, kattintson a **Folytatás** gombra.



6. Indítsa újra a számítógépet a módosítások alkalmazásához és az ESET Endpoint Security telepítésének folytatásához. Ha az eltávolítás sikertelen, olvassa el a jelen útmutatónak Az ESET AV Remover használatával történő eltávolítás hibával fejeződött be című szakaszát.



Az ESET AV Remover használatával történő eltávolítás hibával fejeződött be

Ha az ESET AV Remover eszközzel nem tud eltávolítani egy víruskereső programot, értesítést kap arról, hogy az ESET AV Remover nem feltétlenül támogatja az eltávolítani kívánt alkalmazást. Az Eset tudásbázisában keresse meg a támogatott termékek listáját vagy a Windows általános víruskeresője eltávolítóit, és állapítsa meg, hogy ez az adott program eltávolítható-e.

Ha nem sikerült a biztonsági szoftver eltávolítása, illetve egyes összetevőinek eltávolítása csak részlegesen történt meg, a rendszer kéri, hogy végezzen **újraindítást és újraellenőrzést**. A rendszerindítás után hagyja jóvá az UAC-t, és folytassa az ellenőrzési és eltávolítási folyamatot.

Szükség esetén az ESET műszaki támogatási szolgálatot felkeresve nyújtson be egy támogatási kérelmet, és az **AppRemover.log** fájlt bocsássa az ESET technikusai rendelkezésére. Az **AppRemover.log** fájl az **eset** mappában található. A mappa eléréséhez keresse meg a *%TEMP%* elérési utat a Windows Intézőben. Az ESET műszaki támogatási szolgálata lehetőség szerint gyorsan válaszol, és segít a probléma megoldásában.

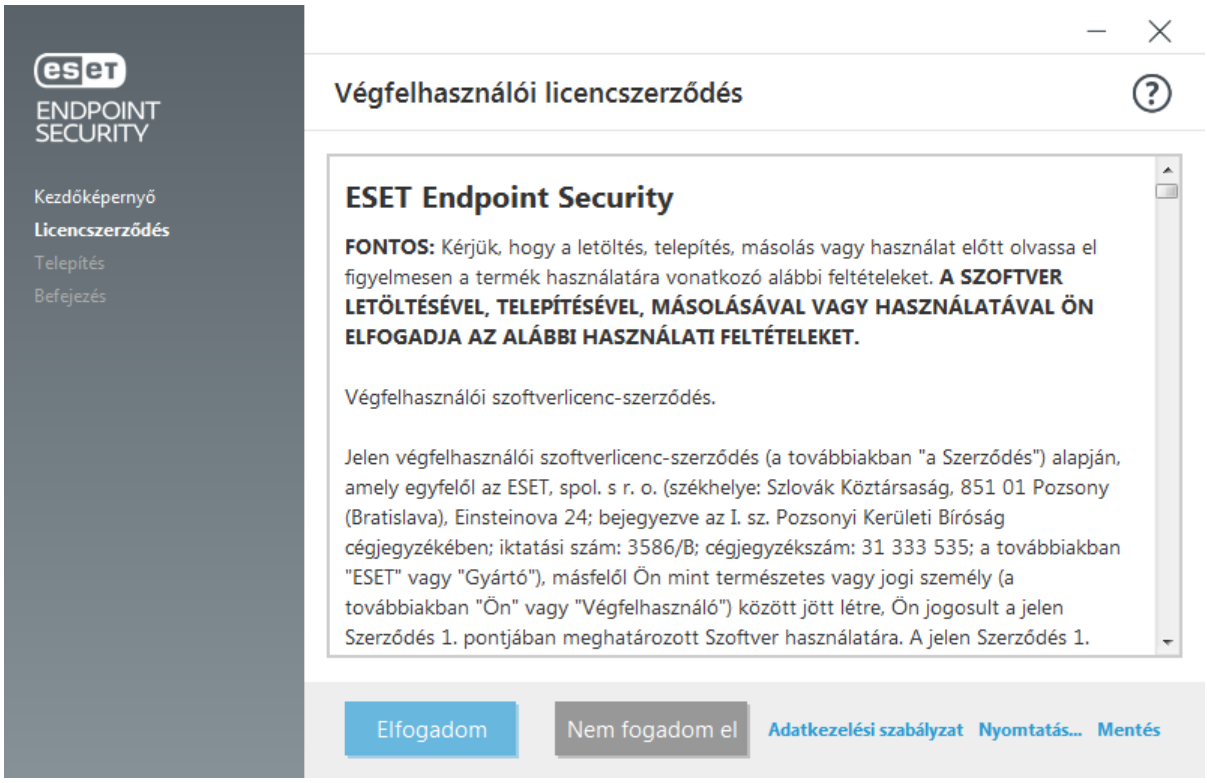
Telepítés (.exe)

Az .exe telepítő elindítása után a telepítővarázsló végigvezeti Önt a telepítési folyamaton.

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 víruskereső szoftverek eltávolítására szolgáló eszközök listáját tudásbáziscikkünk tartalmazza (angolul és néhány más nyelven).



1. Olvassa el a Végfelhasználói licencszerződést. Kattintson **Az összes engedélyezése és folytatás** gombra, ha be szeretné állítani a kéretlen alkalmazások észlelését és engedélyezni szeretné az ESET LiveGrid® visszajelzési rendszert. Az ESET LiveGrid® segítségével az ESET azonnal és folyamatosan értesül az új fertőzésekről, így biztosíthatja ügyfelei fokozottabb védelmét. A rendszer lehetővé teszi, hogy a felhasználó elküldje az új kártevőket az ESET víruslaborjába, ahol elemzik és feldolgozzák az adatokat, és felveszik azokat a keresőmotorba. Kattintson a **Folytatás** gombra a Végfelhasználói licencszerződés elfogadásának jelzéséhez. A **Telepítési mappa módosítása** gombra kattintva a kívánt mappába telepítheti az ESET Endpoint Security alkalmazást.



2. A telepítés befejeződése után felszólítást kap az ESET Endpoint Security aktiválására.

Telepítési mappa módosítása (.exe)

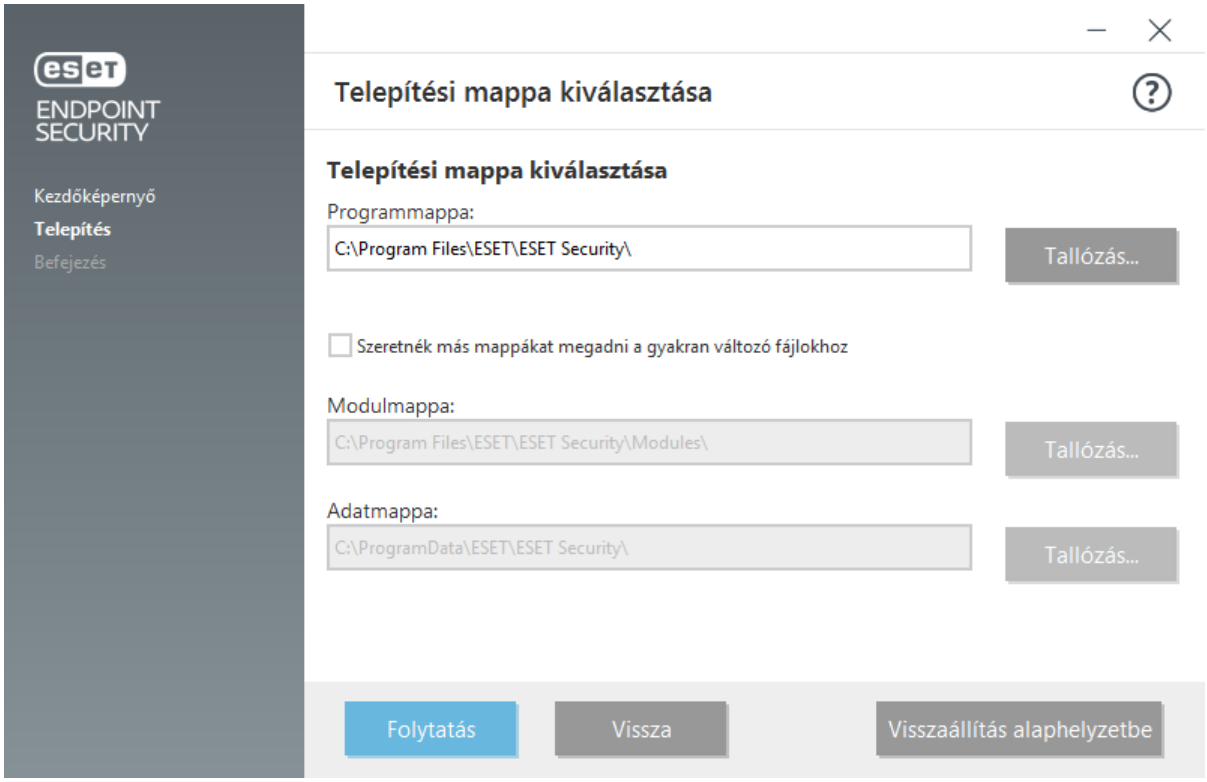
A potenciálisan kéretlen alkalmazások keresésére vonatkozó beállítások megadása és a **Telepítési mappa módosítása** gombra kattintást követően a rendszer kéri, hogy válassza ki az ESET Endpoint Security telepítési mappájának helyét. Alapértelmezés szerint a program telepítése az alábbi könyvtárba történik:

C:\Program Files\ESET\ESET Security

A program moduljainak és adatainak helyét saját maga is meghatározhatja. Ezek alapértelmezés szerint az alábbi könyvtárakba kerülnek:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

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



Kattintson a **Vissza** gombra, majd folytassa a telepítési folyamatot.

Telepítés (.msi)

Az .msi telepítő elindítása után a telepítővarázsló végigvezeti Önt a telepítési folyamaton.

Üzleti környezetben érdemes az .msi telepítőcsomagot választani. Ennek oka leginkább az offline és a távoli központi telepítés, amelyek különböző eszközökkel, például az ESET PROTECT segítségével hajthatók végre.

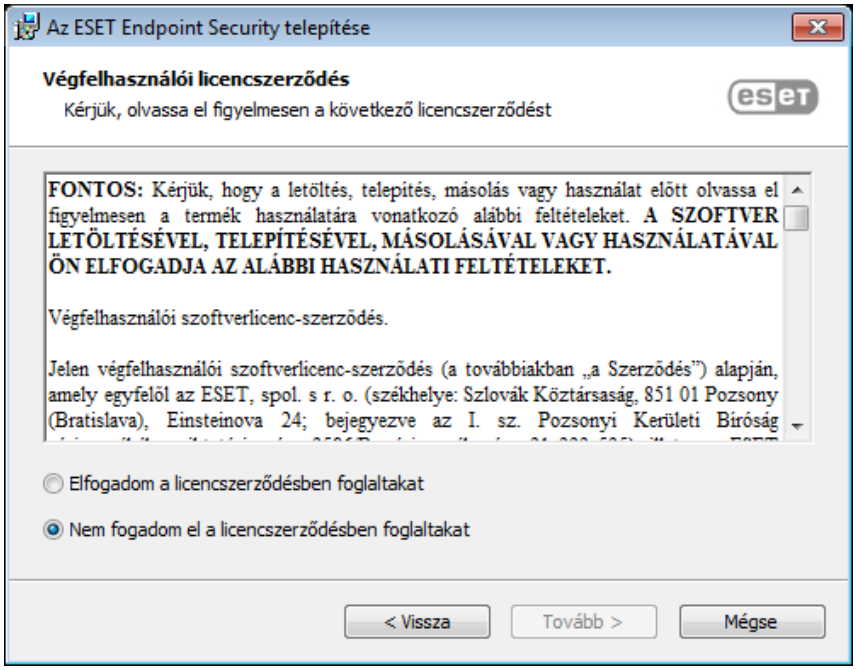
Győződjön meg arról, hogy a számítógépen nincs másik víruskereső program telepítve. Ha több vírusvédelmi megoldás üzemel egy számítógépen, megzavarhatják egymás tevékenységét. Ajánlatos az esetleges további víruskereső programokat eltávolítani a rendszerből. Az általános víruskereső szoftverek eltávolítására szolgáló eszközök listáját tudásbáziscikkünk tartalmazza (angolul és néhány más nyelven).

Az ESET PROTECT 8.1-es és újabb verzióiban létrehozott ESET Endpoint Security telepítő támogatja a Windows 10 Enterprise for Virtual Desktops és a Windows 10 többmenetes módot.

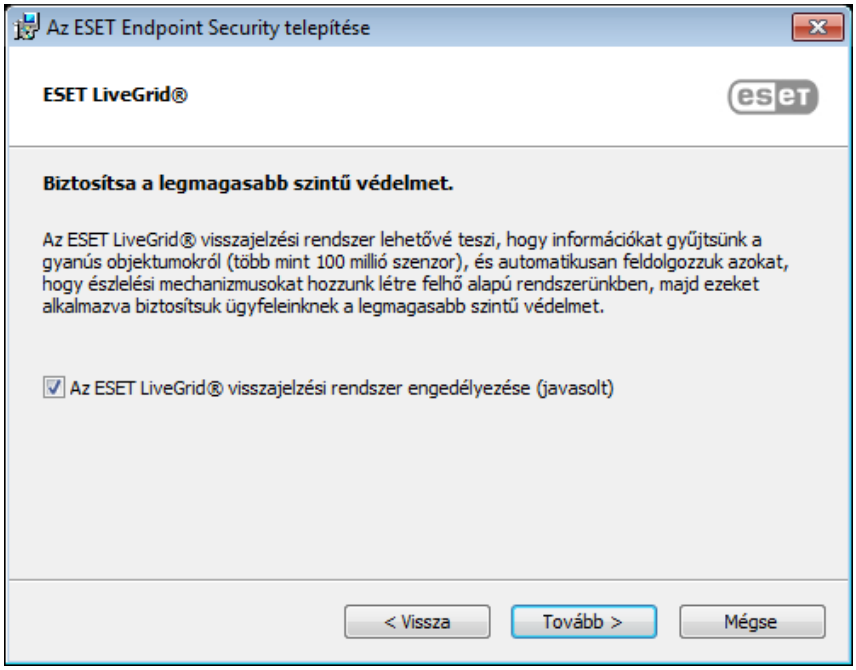
1. Válassza ki a kívánt nyelvet, majd kattintson a **Tovább** gombra.



2. Olvassa el a végfelhasználói licencszerződést, majd az **Elfogadom a licencszerződés feltételeit** választógombra kattintva jelezze, hogy elfogadja a benne foglaltakat. A feltételek elfogadását követően kattintson a **Tovább** gombra a telepítés folytatásához.



3. Adja meg, hogy engedélyezi-e az ESET LiveGrid® visszajelzési rendszert. Az ESET LiveGrid® segítségével az ESET azonnal és folyamatosan értesül az új fertőzésekről, így biztosíthatja ügyfelei fokozottabb védelmét. A rendszer lehetővé teszi, hogy a felhasználó elküldje az új kártevőket az ESET víruslaborjába, ahol elemzik és feldolgozzák az adatokat, és felveszik azokat a keresőmotorba. Kattintson a **További beállítások** elemre, ha speciális telepítést (.msi) szeretne végrehajtani.



5. Utolsó lépésként a **Telepítés** gombra kattintva hagyja jóvá a telepítést. A telepítés befejeződése után felszólítást kap az ESET Endpoint Security aktiválására.

Speciális telepítés (.msi)

A speciális telepítés során számos olyan telepítési paramétert testre szabhat, amely a tipikus telepítés során nem érhető el.

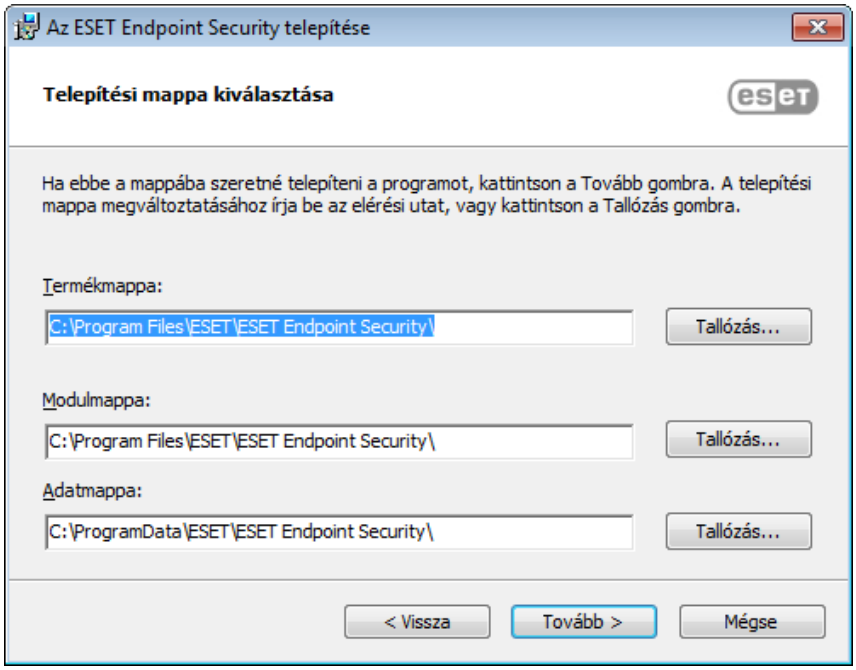
5. A kéretlen alkalmazások keresésére vonatkozó beállítások megadása és a **További beállítások** gombra kattintást követően a rendszer kéri, hogy válassza ki az ESET Endpoint Security telepítési mappájának helyét. Alapértelmezés szerint a program telepítése az alábbi könyvtárba történik:

C:\Program Files\ESET\ESET Security

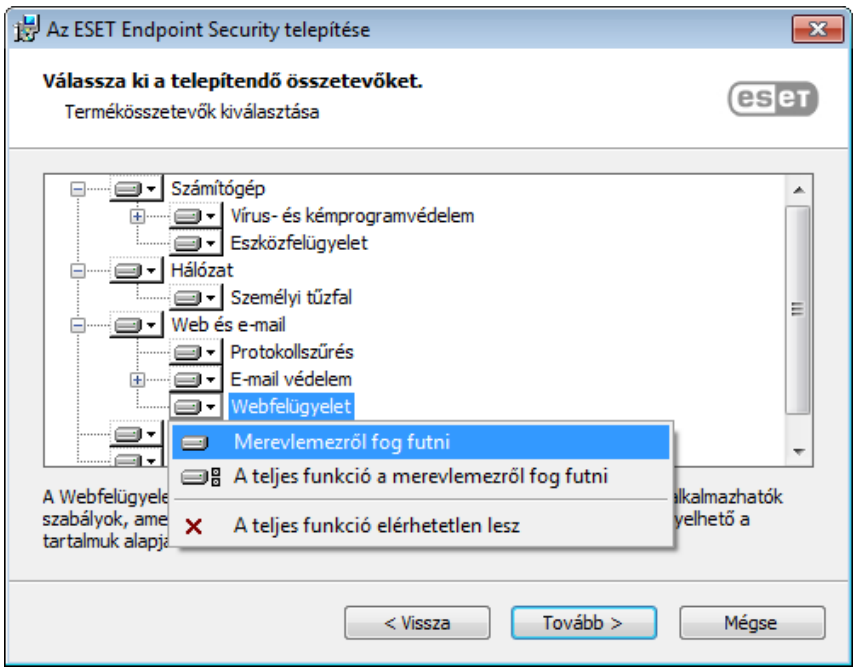
A program moduljainak és adatainak helyét saját maga is meghatározhatja. Ezek alapértelmezés szerint az alábbi könyvtárakba kerülnek:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

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



6. Válassza ki a telepítendő összetevőket. A Számítógép csoportban található programösszetevők közé tartozik a Valós idejű fájlrendszervédelem, a Számítógép ellenőrzése, a Dokumentumvédelem és az Eszközfelügyelet. Ne feledje, hogy az első két összetevő elengedhetetlen a program használatához. A Hálózat összetevő tartalmazza az ESET-tűzfal telepítésének lehetőségét. Ez a modul figyeli a teljes bejövő és kimenő hálózati forgalmat, és szabályokat alkalmaz az egyedi hálózati kapcsolatokra. A tűzfal védelmet nyújt a távoli számítógépek felől érkező támadásokkal szemben is. Hálózati támadások elleni védelem (IDS) – Elemzi a hálózati forgalom tartalmát, és védelmet biztosít a hálózati támadásokkal szemben. Minden károsnak számító adatforgalmat letilt. A Web és e-mail csoportban található összetevők feladata a védelem biztosítása az internetes böngészés és az e-mailes levelezés során. A Frissítési tükör összetevő használható a hálózaton lévő többi számítógép frissítésére. A Távoli figyelés és kezelés (RMM) a szoftveres rendszerek felügyeletét és vezérlését végző folyamat, amely egy felügyeleti szolgáltatótól beszerzett helyileg telepített ügynök segítségével hajtható végre.



7. Utolsó lépésként a **Telepítés** gombra kattintva hagyja jóvá a telepítést.

Minimális modultelepítés

A telepítő mérete miatt fellépő hálózati forgalom csökkentése és az erőforrások kímélése érdekében az ESET biztosítani tud egy minimális modultelepítőt. A telepítő csak alapvető modulokat tartalmaz, az összes többi modul pedig a kezdeti modulfrissítés során töltődik le a termék aktiválása után. Ennek fő előnye az, hogy sokkal kisebb a telepítő, és az ESET Endpoint Security csak a legújabb alkalmazásmodulokat tölti le, amikor aktiválja a terméket.

A minimális modultelepítő is tartalmazza a következő modulokat:

- Betöltők
- Anti-Stealth támogatási modul
- Direct Cloud kommunikációs modul
- Fordítástámogatási modul
- Konfigurációs modul
- SSL modul

A termékaktiválás után megjelenik a **Védelem inicializálása** állapot, amely tájékoztatja a funkciók inicializálásáról.

Modulletöltéssel kapcsolatos probléma esetén (pl. proxybeállítások, nincs hálózat stb.) a **Beavatkozás szükséges** figyelmeztető alkalmazásállapot jelenik meg. A program főablakában kattintson a **Frissítés** > **Frissítések keresése** gombra a frissítési folyamat újraindításához.

Több sikertelen kísérlet után megjelenik **A védelem beállítása nem sikerült** vörös alkalmazásállapot.

Ha a kliensszámítógépek nem rendelkeznek internetkapcsolattal, vagy offline módban működnek és a frissítésük szükséges, a következő módszerekkel tölthet le frissítési fájlokat az ESET frissítési szervereiről:
- Frissítés tükörből
- A tükrözési eszköz használata

Ha az inicializálási folyamat nem sikerült, és továbbra sem tudja letölteni a modulokat, akkor töltse le a teljes MSI-telepítőket itt.

Parancssori telepítés

Az ESET Endpoint Security helyileg a parancssor segítségével, távolról pedig az ESET PROTECTben egy kliensfeladat végrehajtásával telepíthető.

Támogatott paraméterek

APPDIR =<path>

- Path – Könyvtár érvényes elérési útja
- Alkalmazás telepítési könyvtára.

APPDATADIR =<path>

- Path – Könyvtár érvényes elérési útja
- Alkalmazásadatok telepítési könyvtára.

MODULEDIR =<path>

- Path – Könyvtár érvényes elérési útja
- Modul telepítési könyvtára.

ADDLOCAL=<list>

- Összetevő telepítése – helyileg telepítendő nem kötelező funkciók listája.
- Használat ESET .msi csomagokkal: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- További információ az **ADDLOCAL** tulajdonságról: http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<list>

- Az ADDEXCLUDE lista a telepítésből kizárni kívánt funkciók nevének vesszővel elválasztott listája, amely az elavult REMOVE helyébe lépett.
- Ha kizár egy funkciót a telepítésből, akkor a teljes elérési utat (vagyis az összes alfunkciót) és a kapcsolódó látható funkciókat is explicit módon szerepeltetni kell a listában.
- Használat ESET .msi csomagokkal: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> Az **ADDEXCLUDE** paraméter nem használható az **ADDLOCAL** paraméterrel együtt.

Lásd a megfelelő parancssori kapcsolókhoz használt **msiexec**-verzió dokumentációját.

Szabályok

- Az **ADDLOCAL** lista a telepítendő összes funkció nevének vesszővel elválasztott listája.
- Amikor kijelöl egy telepítendő funkciót, a teljes elérési útnak (az összes szülőfunkciónak) kifejezetten szerepelnie kell a listában.
- A megfelelő használat további szabályai.

Összetevők és funkciók

> Az ADDLOCAL/ADDEXCLUDE paraméterrel történő összetevő-telepítés nem fog működni az ESET Endpoint Antivirus szolgáltatással.

A funkciók 4 kategóriába sorolhatók:

- **Kötelező** – a funkció telepítése mindig végbemegy.
- **Választható** – törölhető a funkció kijelölése, így nem megy végbe a telepítése.
- **Láthatatlan** – egyéb funkciók megfelelő működéséhez kötelező logikai funkció.
- **Helyőrző** – ez a funkció nincs hatással a programra, de fel kell sorolni az alfunkciókkal

Az ESET Endpoint Security funkciókészlete a következő:

Leírás	Funkció neve	Funkciószülő	Állapot
Alapvető programösszetevők	`Computer`		Helyőrző
Keresőmotor	`Antivirus`	`Computer`	Kötelező
Keresőmotor/Kártevő-ellenőrzések	`Scan`	`Computer`	Kötelező

Leírás	Funkció neve	Funkciószülő	Állapot
Keresőmotor/Valós idejű fájlrendszervédelem	RealtimeProtection	Computer	Kötelező
Keresőmotor/ Kártevő-ellenőrzések/Dokumentumvédelem	DocumentProtection	Antivirus	Választható
Eszközfelügyelet	DeviceControl	Computer	Választható
Hálózati védelem	Network		Helyőrző
Hálózati védelem/Tűzfal	Firewall	Network	Választható
Hálózati védelem/Hálózati támadások elleni védelem/...	IdsAndBotnetProtection	Network	Választható
Védett böngésző	OnlinePaymentProtection	WebAndEmail	Választható
Web és e-mail	WebAndEmail		Helyőrző
Web és e-mail/Protokollszűrés	ProtocolFiltering	WebAndEmail	Láthatatlan
Web és e-mail / Webhozzáférés-védelem	WebAccessProtection	WebAndEmail	Választható
Web és e-mail / E-mail védelem	EmailClientProtection	WebAndEmail	Választható
Web és e-mail/E-mail-védelem/Levelezőprogramok	MailPlugins	EmailClientProtection	Láthatatlan
Web és e-mail / E-mail védelem / Levélszemétszûrõ	Antispam	EmailClientProtection	Választható
Web és e-mail/Webfelügyelet	WebControl	WebAndEmail	Választható
Eszközök/ESET RMM	Rmm		Választható
Frissítés/Profilok/Frissítési tükör	UpdateMirror		Választható
ESET Inspect bővítmény	EnterpriseInspector		Láthatatlan

Csoportos funkciókészlet:

Leírás	Funkció neve	Funkció megléte
Az összes kötelező funkció	_Base	Láthatatlan
Az összes rendelkezésre álló funkció	ALL	Láthatatlan

További szabályok

- Ha a **WebAndEmail** funkciók bármelyike ki van jelölve telepítésre, a láthatatlan **ProtocolFiltering** funkciónak szerepelnie kell a listában.
- Az összes funkciónév esetén különbséget jelentenek a kis- és nagybetűk; például az UpdateMirror és az UPDATEMIRROR nem ugyanaz.

A konfigurációs paraméterek listája

Paraméter	Érték	Funkció
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – Letiltva 1 – Engedélyezve	Kéretlen alkalmazások észlelése
CFG_LIVEGRID_ENABLED=	Lásd lent	Lásd lent a LiveGrid paramétert
FIRSTSCAN_ENABLE=	0 – Letiltva 1 – Engedélyezve	Számítógép-ellenőrzés ütemezése és futtatása a telepítés után

Paraméter	Érték	Funkció
CFG_PROXY_ENABLED=	0 – Letiltva 1 – Engedélyezve	Proxyszerver beállításai
CFG_PROXY_ADDRESS=	<ip>	Proxyszerver IP-címe
CFG_PROXY_PORT=	<port>	Proxyszerver portszáma
CFG_PROXY_USERNAME=	<username>	Felhasználónév hitelesítéshez
CFG_PROXY_PASSWORD=	<password>	Jelszó hitelesítéshez
ACTIVATION_DATA=	Lásd lent	Termékaktiválás, licenckulcs vagy offline licencfájl
ACTIVATION_DLG_SUPPRESS=	0 – Letiltva 1 – Engedélyezve	Ha a beállítás „1”, akkor a licencaktiválási párbeszédpanel nem fog megjelenni az első alkalommal történő indítás után
ADMINCFG=	<path>	Az exportált XML-konfiguráció elérési útja (alapértelmezett érték: *cfg.xml*)

Csak az ESET Endpoint Security szolgáltatásban elérhető konfigurációs paraméterek

CFG_EPFW_MODE=	0 – Automatikus (alapértelmezett) 1 – Interaktív 2 – Házirendalapú 3 – Tanuló mód	Tűzfal szűrési üzemmódja
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	A Tanuló mód záró dátuma Unix-időbélyegként

LiveGrid® tulajdonság

Az ESET Endpoint Security CFG_LIVEGRID_ENABLED paraméterrel való telepítése esetén a termék a következőképpen fog működni a telepítés után:

Funkció	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid® megbízhatósági rendszer	Be	Be
ESET LiveGrid® visszajelzési rendszer	Ki	Be
Anonim statisztikai adatok küldése	Ki	Be

Az ACTIVATION_DATA paraméter

Formátum	Módszerek
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Aktiválás ESET-licenckulccsal (aktív internetkapcsolat szükséges)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Aktiválás offline licencfájllal

Nyelvi paraméterek

Az ESET Endpoint Security nyelve (mindkét paramétert meg kell adnia).

Paraméter	Érték
PRODUCT_LANG=	LCID-decimális (Locale ID); például 1033 az angolé (Egyesült Államok); a nyelvkódok listája.
PRODUCT_LANG_CODE=	LCID-sztring (Language Culture Name) kisbetűvel; például en-us az angolé (Egyesült Államok); a nyelvkódok listája.

Újraindítási tulajdonságok

Adja meg a következő paramétereket a számítógép telepítés utáni újraindításához:

Paraméter	Érték	Funkció
REBOOT_WHEN_NEEDED=	0 – Letiltva 1 – Engedélyezve	Ha engedélyezve van, a telepítés után a számítógép újraindul.
REBOOT_CANCELABLE=	0 – Letiltva 1 – Engedélyezve	Ha engedélyezve van, a felhasználó megszakíthatja a számítógép újraindítását.
REBOOT_POSTPONE=	érték másodpercben	Az a maximális időtartam másodpercben, ameddig a felhasználó elhalasztja a számítógép újraindítását.

Az REBOOT_CANCELABLE és az REBOOT_POSTPONE csak akkor érhető el, ha az REBOOT_WHEN_NEEDED engedélyezve van.

Példák parancssori telepítésre

A telepítés futtatása előtt mindenképpen olvassa el a végfelhasználói licencszerződést, és győződjön meg arról, hogy rendszergazdai jogosultságokkal rendelkezik.

A **NetworkProtection** szakasz kizárása a telepítésből (meg kell adnia az összes gyermekvédelmi funkciót is):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Ha azt szeretné, hogy az ESET Endpoint Security konfigurálása automatikusan megtörténjen a telepítést követően, a telepítési parancsban megadhat alapvető konfigurációs paramétereket.
Az ESET Endpoint Security telepítése úgy, hogy az ESET LiveGrid® engedélyezve legyen:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Telepítés nem az alapértelmezett könyvtárba, hanem egy másik alkalmazástelepítési könyvtárba:
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Az ESET Endpoint Security telepítése és aktiválása az ESET-licenckulccsal:
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Beavatkozás nélküli telepítés részletes naplózással (hasznos a hibaelhárításhoz) és RMM csak a kötelező összetevőkkel:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Kényszerített, beavatkozás nélküli, teljes telepítés megadott nyelvvel.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Telepítés utáni parancssori lehetőségek

- ESET CMD – .xml konfigurációs fájl importálása vagy egy biztonsági funkció be-/kikapcsolása
- Parancssori vírusirtó – számítógép-ellenőrzés futtatása a parancssorból

Központi telepítés GPO vagy SCCM segítségével

Az ESET Endpoint Security nem csupán közvetlenül kliensszámítógépekre, hanem felügyeleti eszközökkel is telepíthető, például Group Policy Object (GPO), a Software Center Configuration Manager (SCCM), Symantec Altiris vagy a Puppet segítségével.

Felügyelt (ajánlott)

Felügyelt számítógépek esetén először telepítse az ESET Management Agentet, majd végezze el az ESET Endpoint Security telepítését az ESET PROTECT segítségével. Az ESET PROTECT-nek telepítve kell lennie a hálózaton.

1. Töltse le az ESET Management Agent önálló telepítőjét.
2. Készítse elő a GPO/SCCM távoli telepítési szkriptet.
3. Telepítse az ESET Management Agentet a GPO vagy az SCCM segítségével.
4. Győződjön meg arról, hogy a kliensszámítógépek hozzá vannak adva az ESET PROTECT-hez.
5. Telepítse és aktiválja az ESET Endpoint Security szolgáltatást a kliensszámítógépeken.

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
- Az ESET Management Agent telepítése SCCM vagy GPO segítségével
- Az ESET Management Agent telepítése GPO (Group Policy Object) segítségével

---

Nem felügyelt

Nem felügyelt számítógépek esetén az ESET Endpoint Security közvetlenül telepíthető a kliensszámítógépekre. Ez a megoldás nem ajánlott, mert nem tudná felügyelni és érvényesíteni a házirendeket az összes ESET végponttermék esetén a számítógépeken.

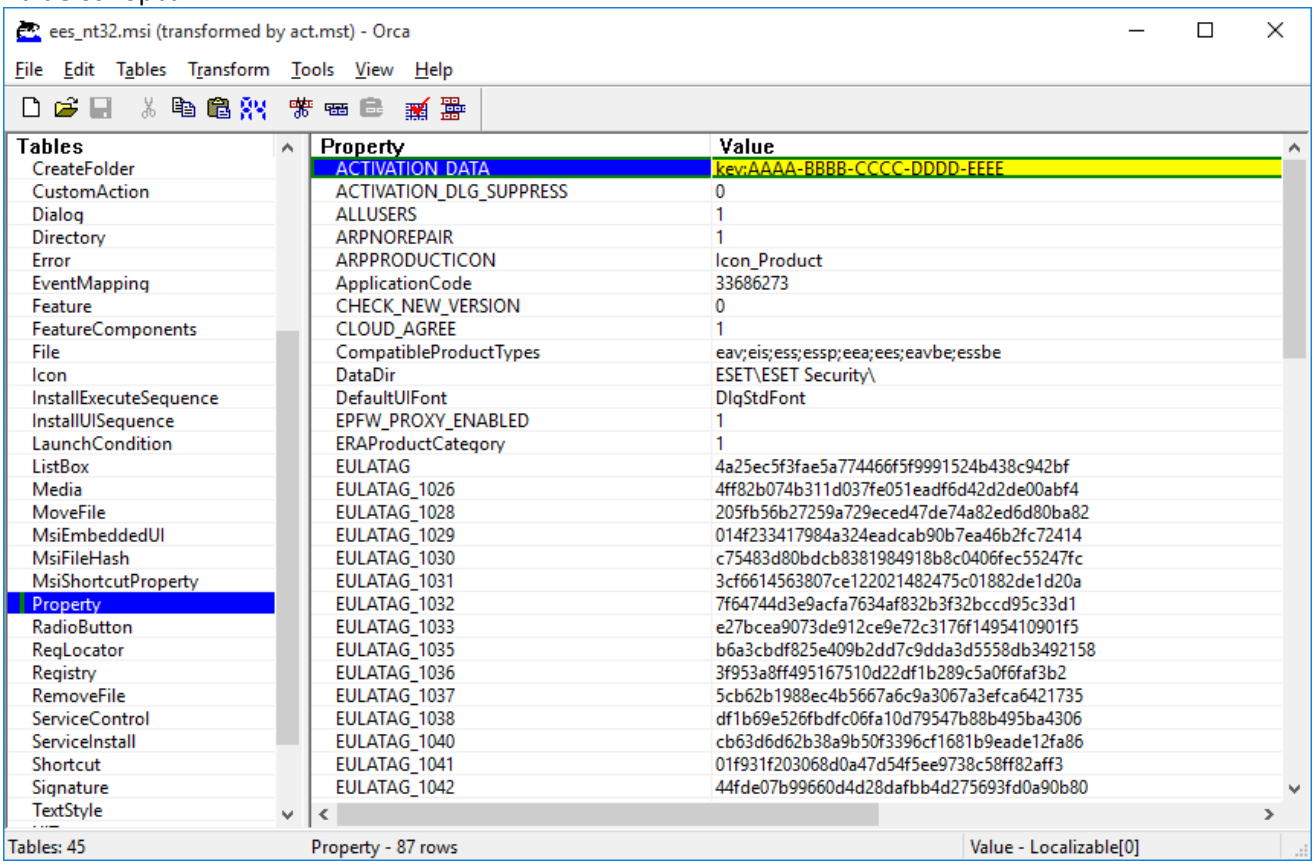
Alapértelmezés szerint az ESET Endpoint Security nincs aktiválva a telepítést követően, ezért nem is működik.

1. lehetőség (szoftvertelepítés)

1. Töltse le az ESET Endpoint Security .msi telepítőjét.
2. Hozzon létre .mst átalakítócsomagot az .msi fájlból (például az Orca .msi szerkesztővel) a termékaktiválási tulajdonság megadásával (lásd az `ACTIVATION_DATA` szakaszt a Parancssori telepítés oldalon).

Az .mst létrehozása az Orcában

1. Nyissa meg az Orca szolgáltatást.
2. Töltse be az .msi telepítőt a **File** > **Open** menüpontra kattintva.
3. Kattintson a **Transform** > **New Transform** elemre.
4. Kattintson a **Property** elemre a **Tables** szakaszban, majd a **Tables** > **Add row** menüben.
5. Az **Add Row** ablakban írja be azt, hogy ACTIVATION_DATA a **Property** oszlopban, a licencadatokat pedig a **Value** oszlopban.



6. A **Transform** > **Generate Transform** elemre kattintva mentse az .mst fájlt.

1. Opcionális: Az ESET Endpoint Security .xml konfigurációs fájl importálásához (például az RMM engedélyezéséhez vagy a proxyszerver-beállítások konfigurálásához) helyezze a cfg.xml fájlt ugyanoda, ahol az .msi telepítő található.
2. Telepítse távolról az .msi telepítőt az .mst fájl segítségével az egyik módszerrel – GPO (szoftvertelepítéssel) vagy SCCM.

2. lehetőség (ütemezett feladattal)

1. Töltse le az ESET Endpoint Security .msi telepítőjét.
2. Készítsen egy parancssori telepítési szkriptet a termékaktiválási paraméter megadásával (lásd: `ACTIVATION_DATA`).
3. Tegye elérhetővé a hálózaton az .msi telepítőt és a .cmd szkriptet az összes számítógép számára.
4. Opcionális: Az ESET Endpoint Security .xml konfigurációs fájl importálásához (például az RMM engedélyezéséhez vagy a proxyszerver-beállítások konfigurálásához) helyezze a cfg.xml fájlt ugyanoda, ahol az .msi telepítő található.
5. Alkalmazzon egy parancssori telepítési szkriptet a GPO vagy az SCCM segítségével.

    - GPO esetén használja a következőket: Group Policy Preferences > Group Policy Schedule Tasks > Immediate task

Ha nem az ESET PROTECT segítségével szeretné távolról felügyelni az ESET-végponttermékeket, az ESET Endpoint Security tartalmazza az ESET beépülő modult az RMM-hez, amellyel felügyelheti és vezérelheti a szoftverrendszereket egy felügyeleti szolgáltató révén elérhető helyileg telepített ügynök segítségével.
• További információk

Frissítés egy újabb verzióra

Az ESET Endpoint Security új verziói továbbfejlesztett funkciókat tartalmaznak, és a programmodulok automatikus frissítésével nem megszüntethető problémákat orvosolnak.

Többféleképpen lehet frissíteni egy újabb verzióra:

1. Automatikusan az ESET PROTECT vagy az ESET PROTECT Cloud segítségével. Az ESET Endpoint Security 9-as verziója nem felügyelhető az ESET Remote Administrator segítségével.
2. Automatikusan GPO vagy SCCM segítségével.
3. 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.
   Győződjön meg arról, hogy engedélyezte a **Frissítési módot** a **További beállítások** (F5) > **Frissítés** > **Profilok** > **Termékfrissítések** lapon.
4. Manuálisan, egy újabb verzió letöltésével és telepítésével (az előző verzióra).

Javasolt frissítési eljárások

Távolról felügyelem vagy szeretném felügyelni az ESET-termékeket

Ha több, mint 10 ESET Endpoint terméket felügyel, akkor érdemes az ESET PROTECT, az ESET PROTECT Cloud segítségével kezelni a frissítéseket.

Tekintse meg a következő dokumentációt:

- ESET PROTECT | Az ESET szoftver frissítése kliensfeladat révén
- ESET PROTECT | Útmutató kis és közepes méretű vállalatok számára, amelyek legfeljebb 250 darab Windows ESET-végponttermékét kezelnek
- Az ESET PROTECT Cloud ismertetése

Manuális frissítés kliensszámítógépen

Ne telepítse a 9-as verziót 4.x verzióra, illetve ha régebbi/nem működő ESET Endpoint Security 5.x vagy 6.x verzióval rendelkezik.

Ha manuálisan szeretné kezelni a frissítéseket az egyes kliensszámítógépeken:

1. Ellenőrizze, hogy az operációs rendszere támogatott-e Windows Vista és Windows XP nem támogatott a verzió esetén.

2. Töltsön le egy újabb verziót, és telepítse az előzőre.

Ha maximalizálni szeretné a legújabb, 9.x verzióra való sikeres frissítés esélyét, frissítsen az ESET Endpoint Security következő verzióinak egyikéről:
• 5.0.2272.x
• 6.5.2132.x
• 7.3.2044.x
Ellenkező esetben először távolítsa el az ESET Endpoint Security terméket. Az ESET Endpoint Security kliensszámítógépeken történő frissítéséről ebben az ESET tudásbáziscikkében talál további információt.

Biztonsági és stabilitási frissítések

Az ESET Endpoint Security frissítése alapvető fontosságú a rosszindulatú kódok elleni teljeskörű védelem fenntartásában. Az ESET Endpoint Security rendszeres frissítését javasoljuk a biztonsági rések és a kártevők elkerülése érdekében. Az ESET Endpoint Security rendszeres frissítését javasoljuk a biztonsági rések és a kártevők elkerülése érdekében. Az ESET Endpoint Security a többi ESET-termékhez hasonlóan a termékéletciklus egy bizonyos pontjába illeszkedik.

Itt bővebben olvashat erről:
Élettartam végéről szóló irányelv (üzleti termékek)
Termékfrissítések
Biztonsági és stabilitási gyorsjavítások
Az ESET Endpoint Security újdonságairól bővebben ebben az ESET-tudásbáziscikkünkben olvashat.

Az automatikus frissítések maximális biztonságot és stabilitást biztosítanak a terméknek. Nem tilthatók le a biztonsági és stabilitási frissítések.

A telepítéssel kapcsolatos általános problémák

Ha telepítéskor problémákba ütközik, a telepítéssel kapcsolatos problémák és megoldásaik segíthetnek elhárítani a hibát.

Nem sikerült az aktiválás

Ha az ESET Endpoint Security aktiválása nem sikerült, a leggyakoribb okok 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

Győződjön meg arról, hogy helyes licenckulcsot adott meg, illetve hogy csatolt egy offline licencet, majd próbálkozzon újra az aktiválással.

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

- Az ESET termékaktiválási hibaelhárítás indítása

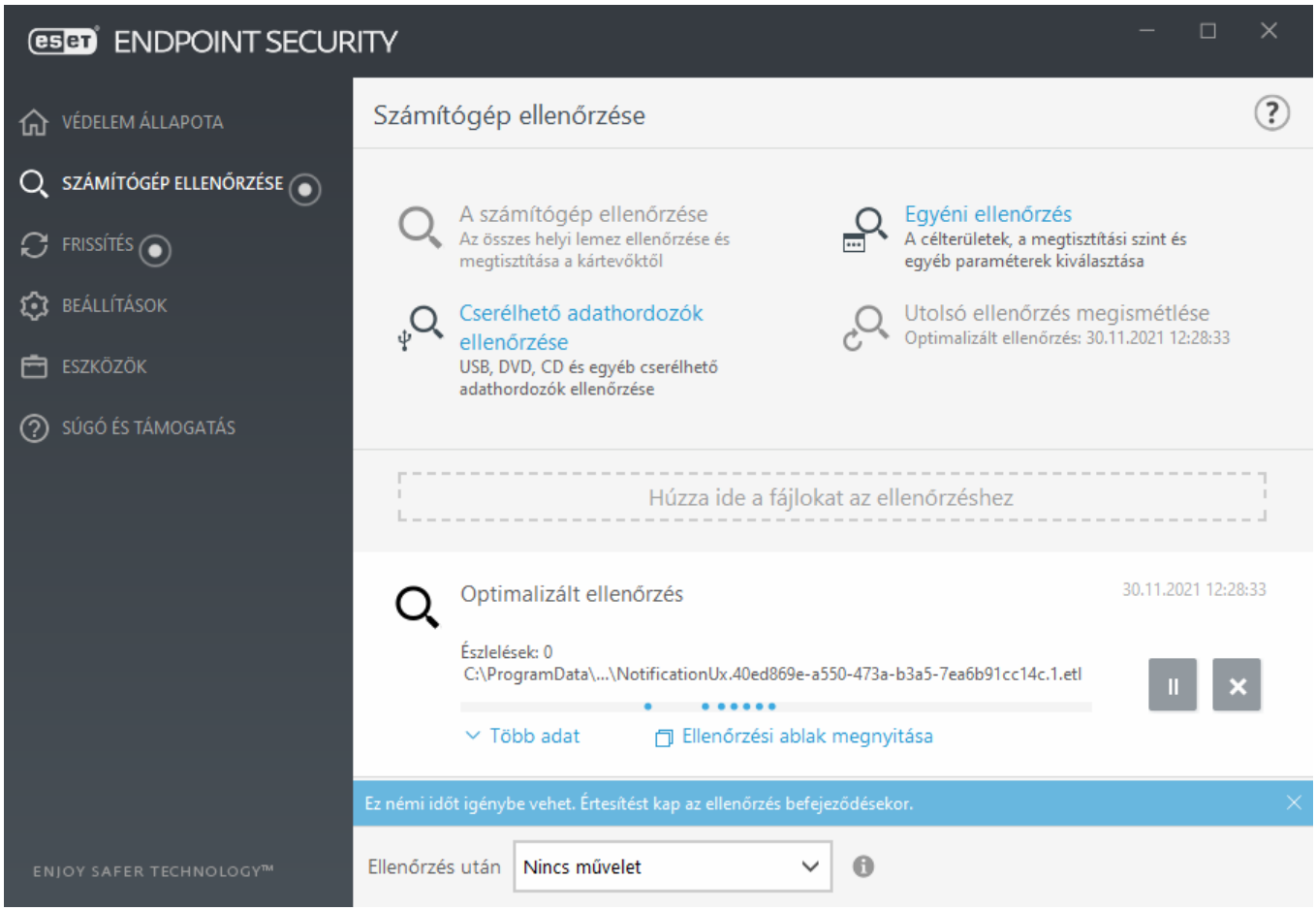
Licenc aktiválása

A telepítés végeztével a rendszer kéri a szoftver licencének aktiválását.

Az ESET Endpoint Security licencének aktiválásához válasszon a rendelkezésre álló módok közül. További információt Az ESET Endpoint Security aktiválása című témakörben talál.

Számítógép ellenőrzése

Javasoljuk, hogy rendszeresen ellenőrizze, hogy a számítógépen nem található-e kártevő, illetve ütemezzen egy rendszeres ellenőrzést. A program főablakában kattintson a **Számítógép ellenőrzése**, majd az **A számítógép ellenőrzése** lehetőségre. A számítógép ellenőrzéséről a Számítógép ellenőrzése című témakörben olvashat részletesebben.



Útmutató kezdő felhasználók számára

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

A felhasználói felület

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

Az alábbi szakaszok a főmenüben található lehetőségeket ismertetik.

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

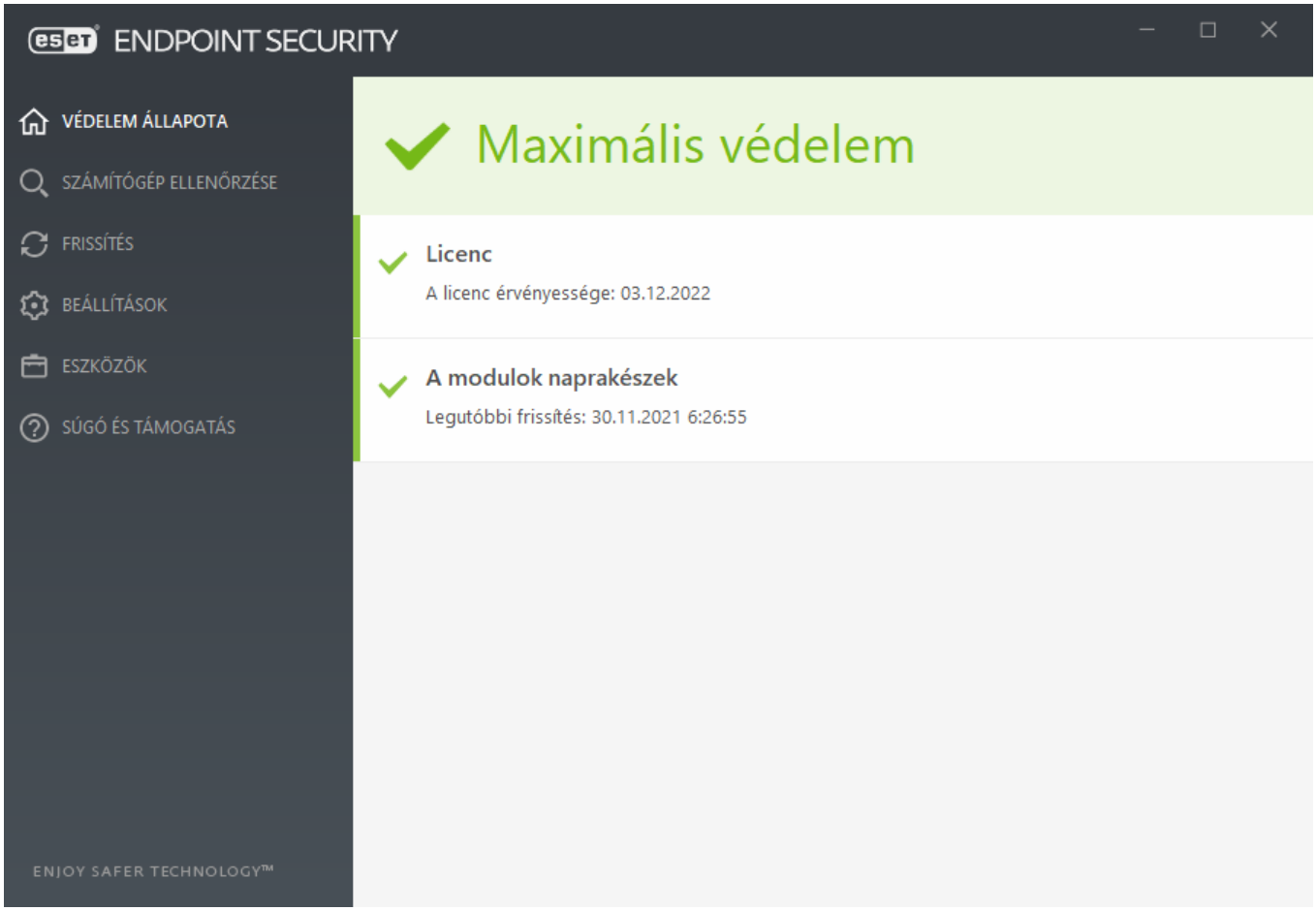
Számítógép ellenőrzése – Itt választhatja ki, hogy számítógépes ellenőrzést, egyéni ellenőrzést, illetve cserélhető adathordozón történő ellenőrzést szeretne-e beállítani vagy indítani. A legutóbb futtatott ellenőrzés megismétlésére is van lehetőség.

Frissítés – Megjeleníthetők információk a keresőmotorról, és frissítéseket lehet keresni manuálisan.

Beállítások – Ezt a lehetőséget választva módosíthatja a Számítógép, a Hálózat és a Web és e-mail biztonsági beállítást.

Eszközök – A lapon elérheti a naplófájlokat, a védelmi statisztikákat, az aktivitást, a futó folyamatokat, a feladatütemezőt, a karantént, a hálózati kapcsolatokat, valamint az ESET SysInspector és a helyreállító CD létrehozására szolgáló ESET SysRescue modult. Mintát is elküldhet elemzés céljára.

Súgó és támogatás – Elérheti a súgófájlokat, az ESET tudásbázisát és az ESET vállalat webhelyét. A műszaki támogatási kérések, támogatási eszközök és a termékaktiválással kapcsolatos információk megnyitására szolgáló hivatkozásokat is találhat.

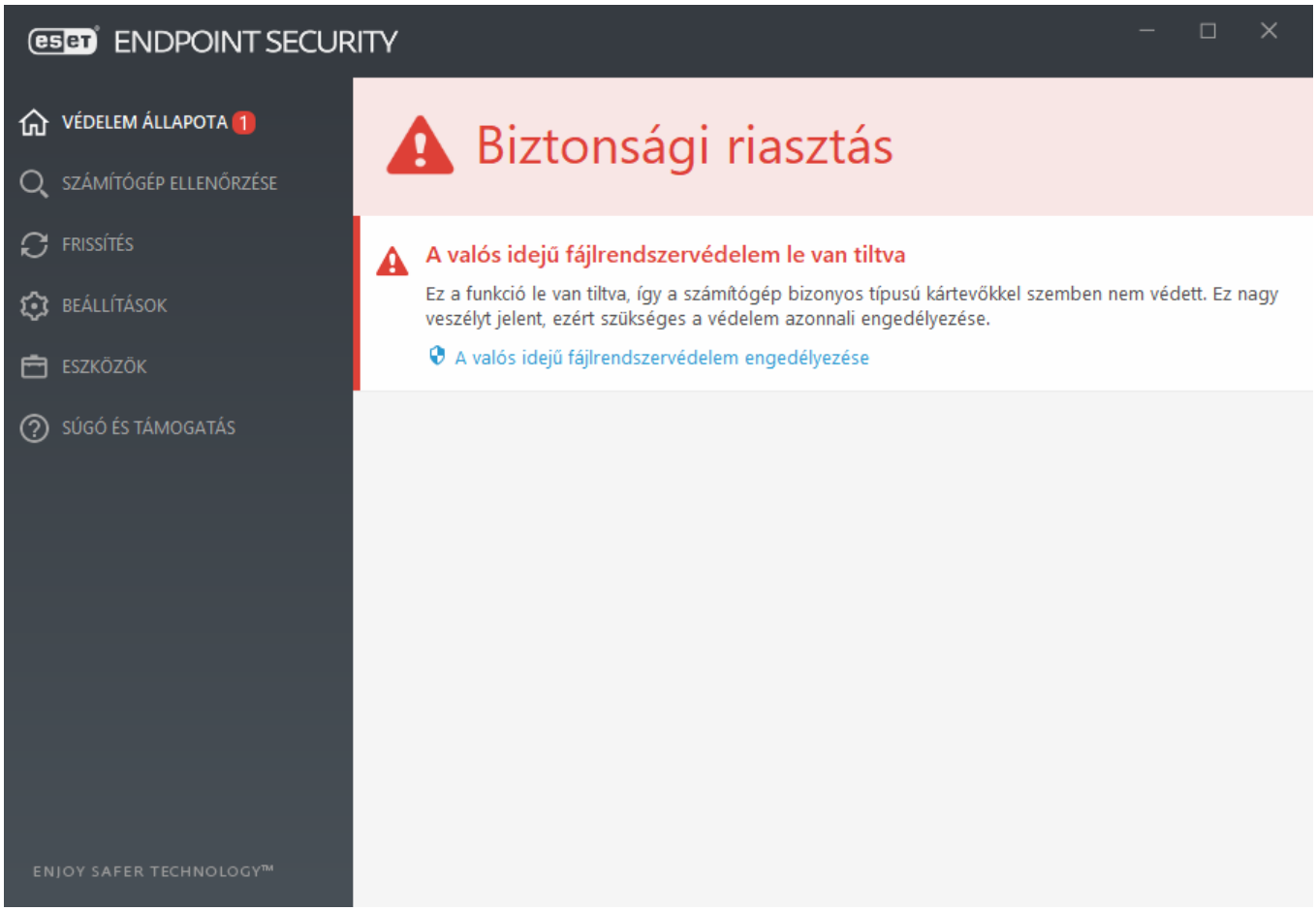


A **Védelem állapota** lap a számítógép biztonságáról és aktuális védelmi szintjéről nyújt tájékoztatást. A védelem állapotát jelző zöld ikon azt jelöli, hogy biztosított a **maximális védelem**.

Az állapotablakban megtalálhatók továbbá az ESET Endpoint Security programban gyakran használt funkciókra mutató gyorshivatkozások és a legutóbbi frissítéssel kapcsolatos információk.

Teendők, ha a program nem működik megfelelően?

A teljesen működőképes programmodulok mellett egy zöld pipa jelenik meg. Vörös felkiáltójel vagy narancssárga értesítő ikon jelzi, ha a modul beavatkozást igényel. Az ablak felső részében további információ található a modulról, beleértve a teljes működés visszaállítására vonatkozó javaslatunkat is. Az egyes modulok állapotának megváltoztatásához a főmenüben kattintson a **Beállítások** lehetőségre, majd a kívánt modul nevére.



A vörös felkiáltójel (!) kritikus problémákat jelez – ekkor nem biztosított a számítógép maximális védelme. Ilyen típusú értesítés a következő esetekben jelenik meg:

- **A vírus- és kémprogramvédelem fel van függesztve** – A vírus- és kémprogramvédelem újbóli engedélyezéséhez a **Védelem állapota** panelen kattintson **Az összes vírus- és kémprogramvédelmi modul indítása** lehetőségre vagy a program főablakának **Beállítások** paneljén **A vírus- és kémprogramvédelem engedélyezése** elemre.
- A vírusvédelem nem működik – Nem sikerült a víruskereső indítása. Az ESET Endpoint Security legtöbb modulja nem működik megfelelően.
- **Az adathalászat elleni védelem nem működik** – Ez a funkció nem működik, mert más szükséges programmodulok nem aktívak.
- **Az ESET tűzfal letiltva** – A problémát egy vörös ikon és biztonsági értesítés jelzi a **Hálózat** elem mellett. A hálózati védelem újbóli engedélyezéséhez kattintson a **Szűrési üzemmód engedélyezése** hivatkozásra.
- **A tűzfal inicializálása nem sikerült** – Rendszerintegrálási hibák miatt a tűzfal ki van kapcsolva. Amint lehetséges, indítsa újra a számítógépet.
- **A keresőmotor elavult** – Ez a hibaüzenet a keresőmotor (korábban vírusdefiníciós adatbázis) 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 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 behatolásmegelőző rendszer le van tiltva** – Ez a probléma akkor fordul elő, amikor a További beállítások között le van tiltva a behatolásmegelőző rendszer. A számítógép bizonyos típusú kártevőkkel szemben nem védett, és a **Behatolásmegelőző rendszer engedélyezése** elemre kattintva haladéktalanul engedélyezni kell.
- Az **ESET LiveGrid® le van tiltva** – Ez a probléma akkor fordul elő, amikor a További beállítások között le van tiltva az ESET LiveGrid®.
- **Az automatikus frissítési feladatok ki vannak kapcsolva** – Az ESET Endpoint Security csak a frissítési feladatok ütemezése esetén keres és fogad fontos frissítéseket.
- **Az Anti-Stealth le van tiltva** – A funkció engedélyezéséhez kattintson az **Anti-Stealth engedélyezése** lehetőségre.
- **Hálózathoz való hozzáférés letiltva** – Akkor jelenik meg, ha aktiválódik a munkaállomás **Számítógép elkülönítése a hálózattól** kliensfeladata az ESET PROTECT felől. Lépjen kapcsolatba a rendszergazdával további információkért.
- **A valós idejű fájlrendszervédelem fel van függesztve** – A felhasználó letiltotta a valós idejű fájlrendszervédelmet. A számítógép nem védett a kártevőkkel szemben. A funkció újbóli engedélyezéséhez kattintson A valós idejű védelem engedélyezése hivatkozásra.

 Az „i” jelű narancssárga ikon azt jelzi, hogy az ESET-szoftver nem kritikus hiba miatti beavatkozást igényel. A lehetséges okok:

- **A webhozzáférés-védelem le van tiltva** – Újból engedélyezheti a webhozzáférés-védelmet, ha a biztonsági értesítésre, majd a **Webhozzáférés-védelem engedélyezése** elemre kattint.
- **Az Ön licence hamarosan lejár** – Ezt a védelmi állapot ikonján megjelenő felkiáltójel jelzi. A licenc lejárta után a program nem frissül, és a védelmi állapot ikonja vörös lesz.
- **A botnet elleni védelem fel van függesztve** – A funkció újbóli engedélyezéséhez kattintson a **Botnet elleni védelem engedélyezése** elemre.
- **A hálózati támadások elleni védelem (IDS) fel van függesztve** – A funkció újbóli engedélyezéséhez kattintson a **Hálózati támadások elleni védelem engedélyezése (IDS)** elemre.
- **A levélszemétszűrés fel van függesztve** – A funkció újbóli engedélyezéséhez kattintson a **Levélszemétszűrés engedélyezése** elemre.
- **A webfelügyelet fel van függesztve** – A funkció újbóli engedélyezéséhez kattintson a **Webfelügyelet engedélyezése elemre**.
- **Házirend felülbírálása aktív** – A házirend által megadott konfiguráció ideiglenesen felül van bírálva, feltételezhetően amíg a hibaelhárítás be nem fejeződik. A házirend-beállításokat csak jogosult felhasználó bírálhatja felül. További információt A Felülbírálás mód használata című témakör tartalmaz.
- **Az eszközfelügyelet fel van függesztve** – A funkció újbóli engedélyezéséhez kattintson az **Eszközfelügyelet engedélyezése** elemre.

Ha módosítani szeretné a terméken belüli láthatósági állapotokat az ESET Endpoint Security első ablaktábláján, tekintse meg az Alkalmazásállapotok című részt.

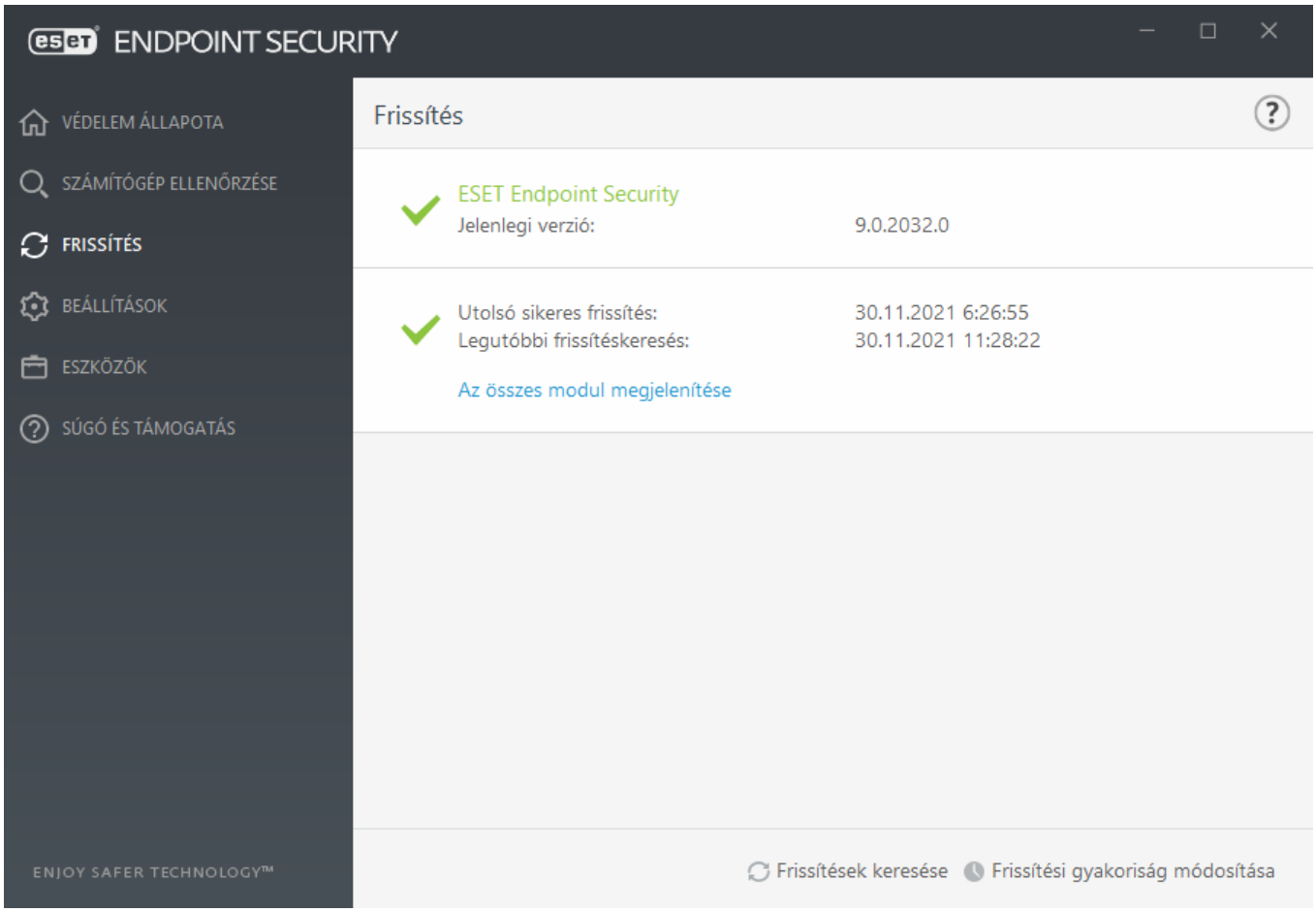
Ha a javasolt megoldásokkal nem szüntethető meg a probléma, a **Súgó és támogatás** hivatkozásra kattintva megnyithatja a súgófájlokat, illetve az ESET tudásbázisában is kereshet megoldást. Ha további segítségre van szüksége, elküldhet egy támogatási kérelmet az ESET részére. Az ESET műszaki támogatási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

Ha egy állapot az ESET PROTECT házirendje által letiltott funkcióhoz tartozik, a hivatkozásra nem lehet kattintani.

Frissítési beállítások

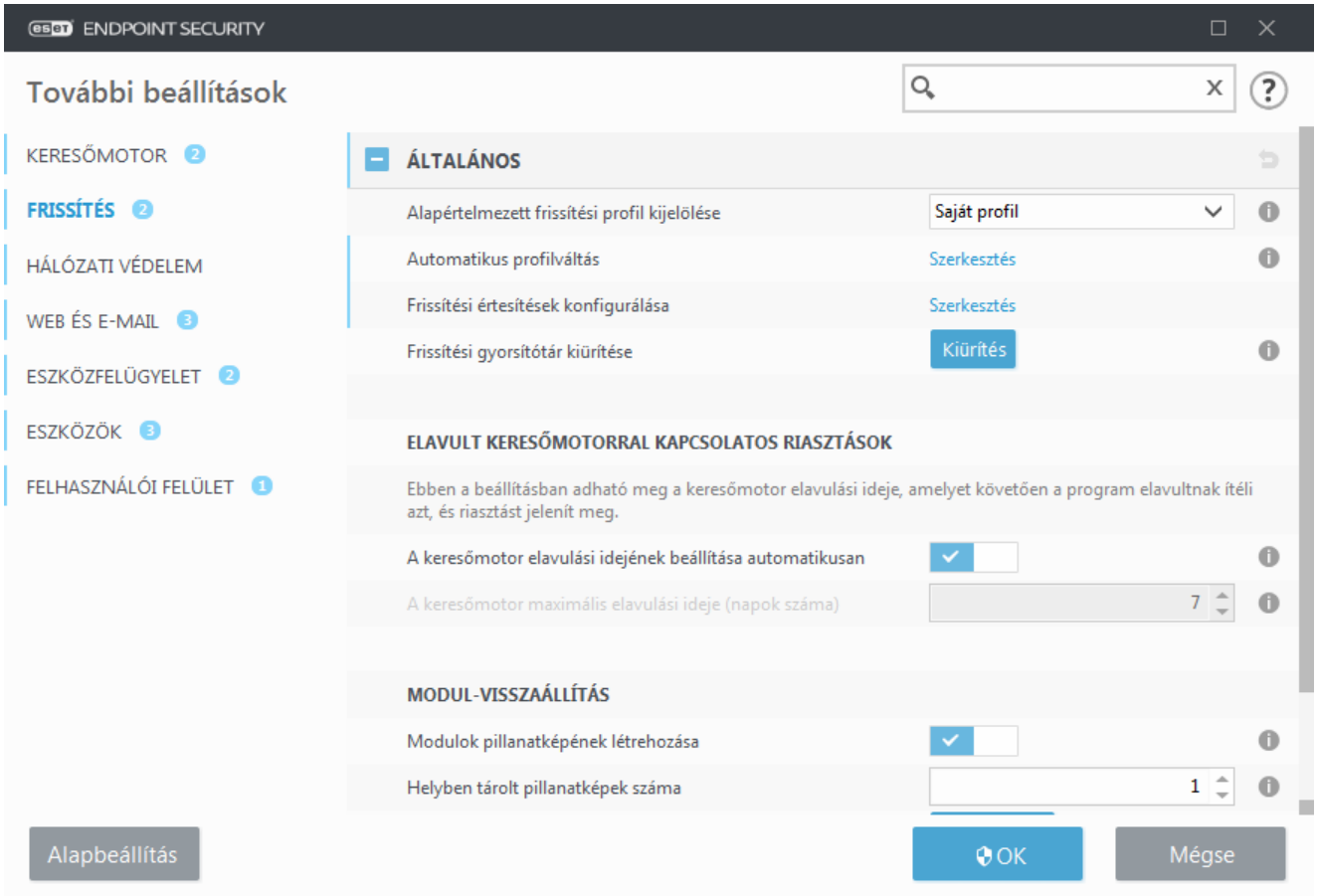
A kártevők elleni maradéktalan védelem fontos összetevője a modulok frissítése. Ezért a beállításukra és a működésükre különösen oda kell figyelni. A főmenüből válassza ki a **Frissítés** > **Frissítések keresése** lehetőséget újabb modulfrissítések kereséséhez.

Ha még nem adta meg a **licenckulcsát**, nem tud új frissítéseket beszerezni, és a rendszer a licenc aktiválására kéri.



A További beállítások ablakban (a főmenüben kattintson a **Beállítások** > **További beállítások elemre, vagy nyomja meg** az **F5** billentyűt) további frissítési lehetőségek állnak rendelkezésre. A további frissítési beállítások – például a frissítési mód, a proxyszerver elérhetőségi adatai, a helyi hálózati kapcsolatok és a keresőmotor másolatainak készítése – megadásához a További beállítások fában kattintson a **Frissítés** elemre.

- Ha a frissítésekkel kapcsolatban problémát tapasztal, a **Kiürítés** gombra kattintva ürítse ki az ideiglenes frissítési gyorsítótárat.



- Az **Automatikus kiválasztás** beállítás alapértelmezés szerint engedélyezve van a **Profilok** > **Frissítések** > **Modulfrissítés** lapon. Azt javasoljuk, ne módosítsa a beállítást, amikor frissítéseket fogad az ESET frissítési szervereitől.
- Ha nem szeretné, hogy a képernyő jobb alsó sarkában, a rendszertálcán értesítések jelenjenek meg a sikeres frissítésekről, bontsa ki a **Profilok** > **Frissítések** csomópontot, kattintson a **Szerkesztés** elemre **A kapott frissítési értesítések kiválasztása** szöveg mellett, majd állítsa be a kívánt módon **A keresőmotor frissítése sikerült** értesítéshez kapcsolódó jelölőnégyzeteket.

Az optimális működéshez fontos a program rendszeres, automatikus frissítése. Ez csak akkor lehetséges, ha helyes **licenckulcsot** adott meg a **Súgó és támogatás** > **Licenc aktiválása** ablakban.

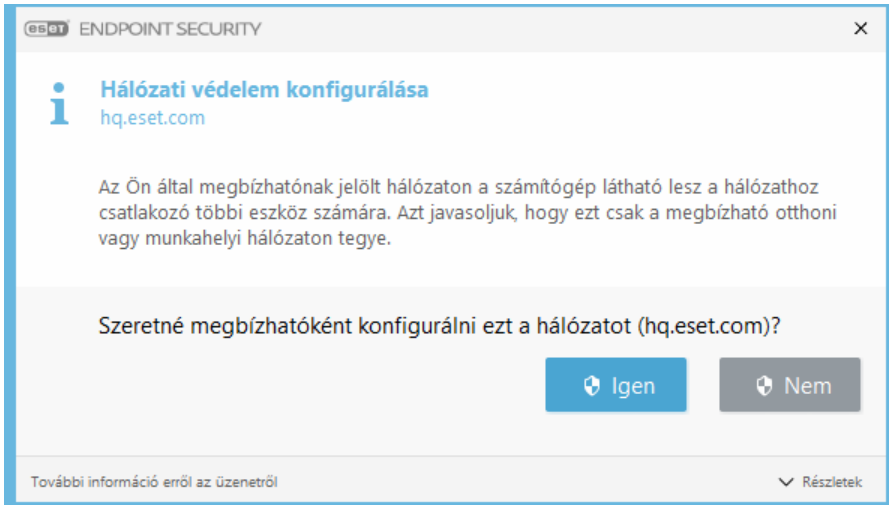
Ha a program telepítését követően nem adta meg a **licenckulcsát**, később bármikor megteheti azt. Az aktiválásról olvassa el Az ESET Endpoint Security aktiválása című témakörben található részletes információkat, és a **Licenc részletei** ablakban adja meg az ESET biztonsági termékkel együtt kapott hitelesítő adatokat.

Zónák beállítása

Megbízható zónák beállításával biztosíthatja, hogy számítógépe hálózati környezetben is védett legyen. Ha egy megbízható zónát a megosztás engedélyezésére állít be, lehetővé teheti másoknak a számítógépéhez való hozzáférést. A megbízható zónák beállításainak megnyitásához kattintson a **További beállítások** (F5) > **Hálózati védelem** > **Tűzfal** > **Speciális** > **Zónák** lehetőségre.

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

az adott zóna védelmi szintjének a megadását.



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

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

A funkcióról az ESET alábbi tudásbáziscikkében talál további részleteket:

- A program új hálózati kapcsolatot észlelt ESET Endpoint Security

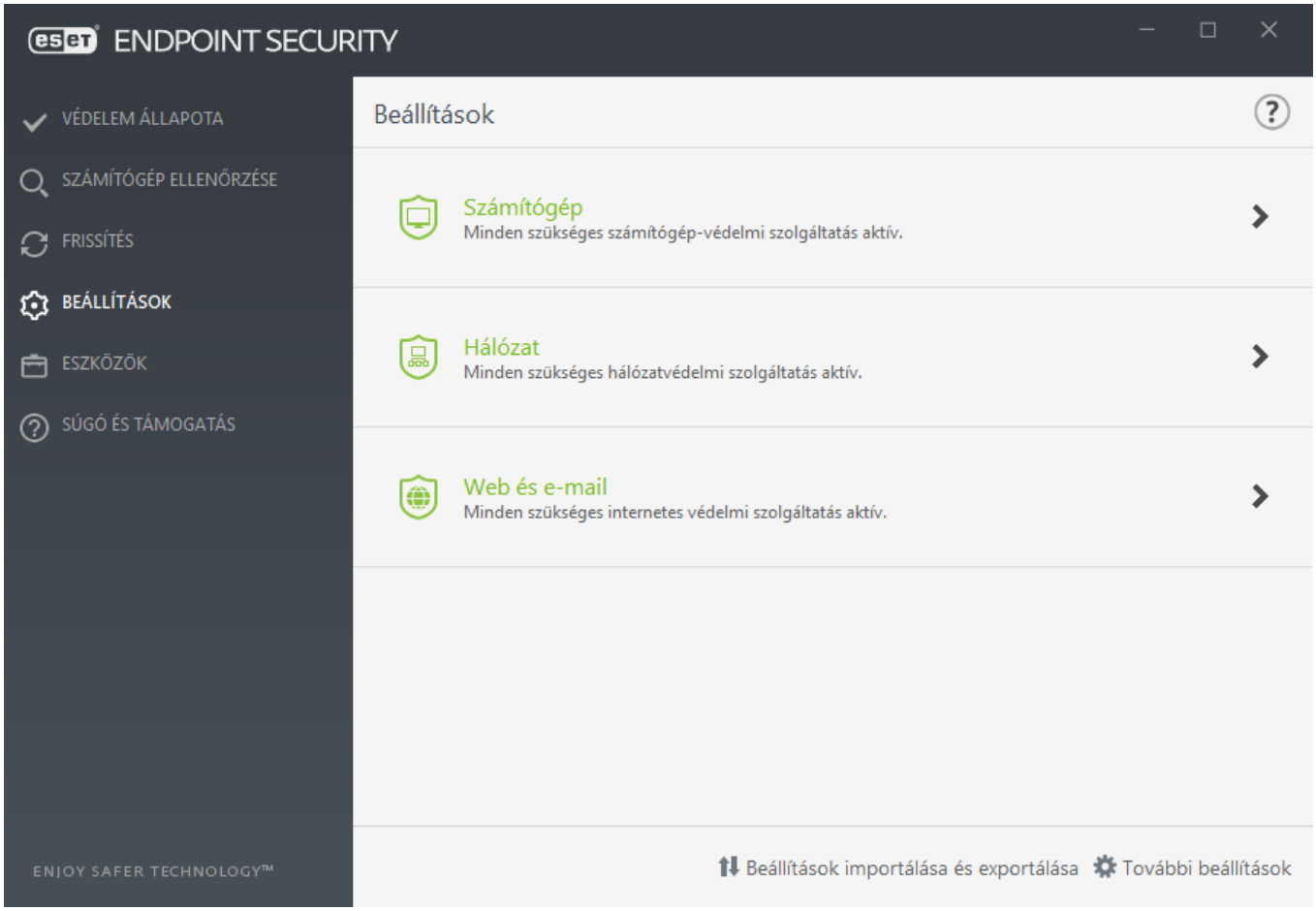
Webfelügyeleti eszközök

Ha már engedélyezte a Webfelügyeletet az ESET Endpoint Security programban, a funkció megfelelő működéséhez konfigurálnia is kell azt a kívánt felhasználói fiókokhoz. A Webfelügyelet című fejezetből megtudhatja, hogy miként hozhat létre korlátozásokat a munkaállomások számára az esetlegesen nem kívánt tartalmú weboldalakkal szembeni védelmük biztosítása céljából.

Az ESET Endpoint Security használata

Az ESET Endpoint Security beállításai lehetővé teszik a számítógépek, a webes tevékenységek, a levelezés és a hálózat védelmi szintjének megadását.

Amikor házirendet hoz létre az ESET PROTECT webkonzolon, minden beállításhoz kijelölheti a jelölőt. A Kényszerítés jelölővel megadott beállítások elsőbbséget élveznek, és későbbi házirenddel nem lehet őket felülbírálni (még ha a későbbi házirend rendelkezik is Kényszerítés jelölővel). Ez biztosítja, hogy a beállítást ne lehessen módosítani (pl. felhasználó vagy későbbi házirendek által az egyesítés során). További információkat a Jelölők az ESET PROTECT-ben című online súgótémakörben talál.



A **Beállítások** rész az alábbi csoportokat tartalmazza:

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

A Számítógép szakaszban az alábbi összetevőket engedélyezheti vagy tilthatja le:

- **Valós idejű fájlrendszervédelem** – A program a fájlok megnyitásakor, létrehozásakor vagy futtatásakor ellenőrzi, hogy nem tartalmaznak-e kártevő kódot.
- **Eszközfelügyelet** – lehetővé teszi eszközök (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.
- **Behatolásmegelőző rendszer (HIPS)** – A behatolásmegelőző rendszer felügyeli az operációs rendszeren belüli eseményeket, és a testre szabott szabályegyüttesek alapján reagál rájuk.
- A **Speciális memória-ellenőrzés** 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** – 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.
- **Zsarolóprogram elleni védelem** – Ez 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.

- **Bemutató 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 processzor terhelését. A Bemutató üzemmód engedélyezése biztonsági kockázatot hordoz, ezért a védelmi állapot ikonja a tálcán narancssárgára változik.

A **Hálózat** csoportban konfigurálhatja a tűzfalat, a hálózati támadások elleni védelmet (IDS) és a botnet elleni védelmet.

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

- **Védett böngésző** – Megvédi a bizalmas adatokat az interneten való böngészés közben (például pénzügyi adatok az online tranzakciók során).
- **Webfelügyelet** – Letiltja az esetlegesen nem kívánt tartalmú weboldalakat. Ezenkívül a rendszergazdák 27 előre definiált webhely-kategóriához adhatnak meg hozzáférési beállításokat.
- **Webhozzáférés-védelem** – Ha engedélyezi ezt a beállítást, a program a HTTP vagy a HTTPS protokoll teljes forgalmát ellenőrzi kártevő szoftvereket keresve.
- **E-mail védelem** – A POP3 és az IMAP protokollon keresztül érkező kommunikációt figyeli.
- **Levélszemétszűrő** – Kiszűri a kéretlen e-maileket vagy a levélszemetet.
- **Adathalászat elleni védelem** – Védelmet nyújt a magukat szabályszerű webhelyeknek láttató, de nem szabályszerű webhelyek által a jelszavak, banki adatok és más bizalmas információk megszerzésére irányuló kísérletekkel szemben.

Az egyes modulok átmeneti letiltásához kattintson a zöld kapcsolóra  a kívánt modul mellett. Ne feledje, hogy ez gyengítheti a számítógép védelmét.

A letiltott biztonsági összetevők ismételt engedélyezéséhez kattintson a piros kapcsolóra .

Az ESET PROTECT házirend alkalmazásakor az adott összetevő mellett egy zár ikon  látható. Az ESET PROTECT által alkalmazott házirend helyileg felülbírálható a bejelentkezett felhasználó (pl. rendszergazda) hitelesítése után. További információt az ESET PROTECT online súgójában talál.

Minden ily módon letiltott védelmi eljárás ismét engedélyezve lesz a számítógép újraindítása után.

A biztonsági összetevők részletes beállításainak megtekintéséhez kattintson bármely összetevők mellett a fogaskerék ikonra .

A beállítási ablak alsó részén további lehetőségek találhatók. Egy *.xml* konfigurációs fájl segítségével betöltheti a beállítási paramétereket, illetve a **Beállítások importálása és exportálása** lehetőségre kattintva egy konfigurációs fájlba mentheti az aktuális beállítási paramétereket. Részletesebb információkért olvassa el a Beállítások importálása és exportálása című témakört.

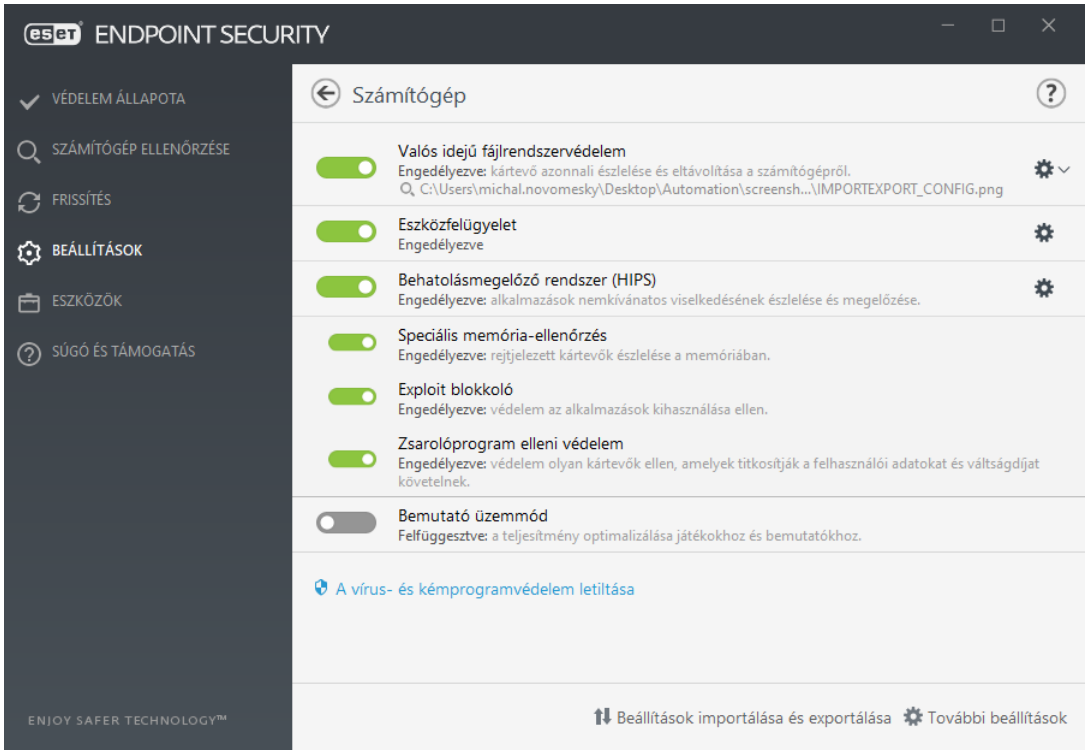
Részletesebb beállítások megnyitásához kattintson a **További beállítások** gombra vagy nyomja le az **F5** billentyűt.

Számítógép

A **Számítógép** modul a **Beállítások** > **Számítógép** elemre kattintva érhető el. A modul az előző fejezetben ismertetett védelmi modulok áttekintését jeleníti meg. Ebben a csoportban a következő beállítások érhetők el:

Kattintson a fogaskerék ikonra  a **Valós idejű fájlrendszervédelem** felirat mellett, majd a **Kivételek szerkesztése** elemre kattintva nyissa meg a Kivételek párbeszédpanelt, ahol kizárhat fájlokat és mappákat az ellenőrzésből. A

Valós idejű fájlrendszervédelem további beállításainak megnyitásához kattintson a **Konfigurálás** gombra.



A **Számítógép** szakaszban az alábbi összetevőket engedélyezheti vagy tilthatja le:

- **Valós idejű fájlrendszervédelem** – A program a fájlok megnyitásakor, létrehozásakor vagy a számítógépen történő futtatásakor ellenőrzi, hogy nem tartalmaznak-e kártevő kódot.
- **Eszközfelügyelet** – lehetővé teszi eszközök (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.
- **Behatolásmegelőző rendszer (HIPS)** – A behatolásmegelőző rendszer felügyeli az operációs rendszeren belüli eseményeket, és a testre szabott szabályegyüttesek alapján reagál rájuk.
- A **Speciális memória-ellenőrzés** 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** – 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.
- **Zsarolóprogram elleni védelem** – Ez 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.
- **Bemutató 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 processzor terhelését. A Bemutató üzemmód engedélyezése biztonsági kockázatot hordoz, ezért a védelmi állapot ikonja a tálcán narancssárgára változik.

A vírus- és kémprogramvédelem letiltása – Minden alkalommal, amikor átmenetileg letiltja a vírus- és kémprogramvédelmet, a legördülő menüben megadhatja azt az időtartamot, amelyre a kijelölt összetevőt le szeretné tiltani, majd az **Alkalmaz** gombra kattintva letilthatja a biztonsági összetevőt. A védelem ismételt engedélyezéséhez kattintson **A vírus- és kémprogramvédelem engedélyezése** elemre.

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.

Ebben a szakaszban:

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

> A 7.2-es verziótól kezdve a Keresőmotor szakaszban nem találhatók meg a BE/KI kapcsolók, ahogy a 7.1-es és korábbi verziókban. A BE/KI gombok helyett a következő négy küszöb található meg: Mélyreható, Kiegyensúlyozott, Mérsékelt és Ki.

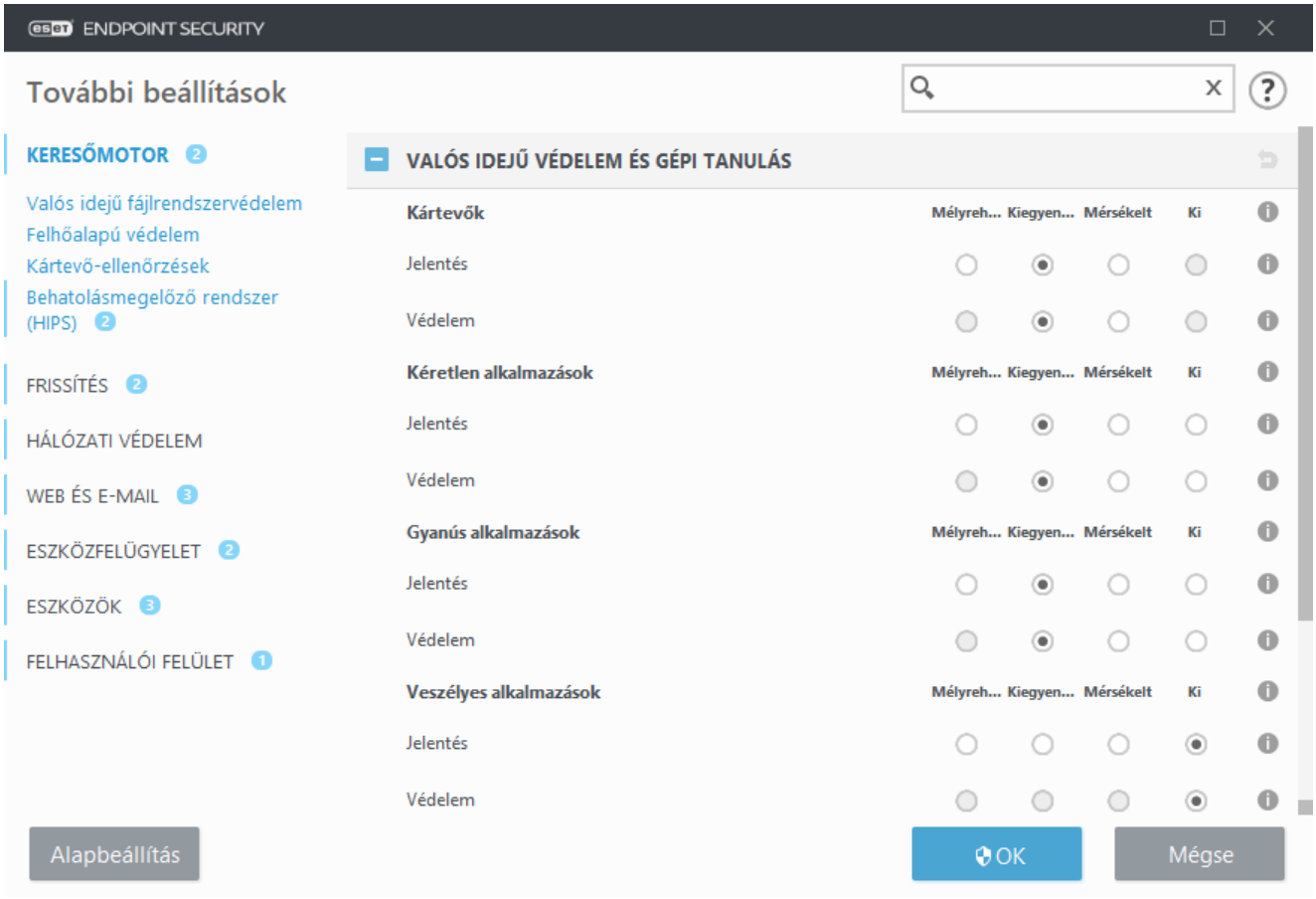
Valós idejű védelmi és gépi tanulási kategóriák

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.
- **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.

- 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.



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.

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 Endpoint 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 Endpoint 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 Endpoint Security 7.2-es és újabb verzióiban áll rendelkezésre.
** Nem javasolt

Termékverziók, programmodul-verziók és builddátumok meghatározása

1. Kattintson a **Súgó és támogatás** > **Az ESET Endpoint Security** névjegye elemre.
2. A **Névjegy** képernyőn a szöveg első sorában az ESET-termék verziószáma látható.
3. A **Modulok megjelenítése** 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 Endpoint Security korábbi (7.1-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 Endpoint 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.

Az ESET PROTECT házirend-átalakítási táblázata az ESET Endpoint Security 7.1-es és korábbi verziói esetén

Az ESET PROTECT ellenőrzési beállításokhoz készült házirendszerkesztője már nem tartalmazza a BE/KI kapcsolókat az egyes KATEGÓRIÁKNÁL. A következő táblázat bemutatja a védelmi küszöb és a kapcsoló végleges állapotát az ESET Endpoint Security 7.1-es és korábbi verziójában.

KATEGÓRIA küszöbállapota	Mélyreható	Kiegyensúlyozott	Mérsékelt	Ki
Alkalmazott KATEGÓRIA-kapcsoló	✓	✓	✓	✗

A 7.1-es vagy korábbi verzióról a 7.2-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

---

Bevált eljárások

NEM FELÜGYELT KÖRNYEZET (önálló kliensszámítógépek)

Ne módosítsa az ajánlott alapértelmezett értékeket.

FELÜGYELT KÖRNYEZET

Általában a következő beállításokat alkalmazzák a munkaállomásokra házirend segítségével.

1. Kezdeti szakasz

Ez a szakasz legfeljebb egy hetet vesz igénybe.

- Állítsa az összes **Jelentés** küszöböt **Kiegyensúlyozott** értékre.
  MEGJEGYZÉS: Szükség esetén állítsa be a **Mélyreható** értéket.
- A kártevőkre vonatkozó **Védelem** beállításnál adja meg vagy hagyja meg a **Kiegyensúlyozott** értéket.
- A többi KATEGÓRIÁRA vonatkozó **Védelem** beállításnál adja meg a **Mérsékelt** értéket.
  MEGJEGYZÉS: A **Védelem** küszöböt ebben a szakaszban nem ajánlott **Mélyreható** értékre állítani, mert akkor a program az összes megtalált elemet kezelné, ideértve a tévesen beazonosított elemeket is.
- Először azonosítsa be a tévesen beazonosított objektumokat az Észlelési naplóban, és adja hozzá őket az Észlelés kivételek listához.

2. Átmeneti szakasz

- Tesztelési célból vezesse be az „Éles szakaszt” néhány munkaállomáson (ne a hálózaton lévő összes munkaállomáson).

3. Éles szakasz

- Állítsa be az összes **Védelem** küszöböt **Kiegyensúlyozott** értékre.
- Távoli felügyelet esetén használjon egy előre meghatározott megfelelő vírusirtó-házirendet az ESET Endpoint Security programhoz.
- A **Mélyreható** védelmi küszöb akkor állítható be, ha a legmagasabb észlelési arányra van szükség, és elfogadhatók tévesen beazonosított objektumok.
- Ellenőrizze az Észlelési naplóban vagy az ESET PROTECT-jelentésekben, hogy nem hiányoznak-e észlelések.

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, 11 esetén).

A program fertőzést észlelt

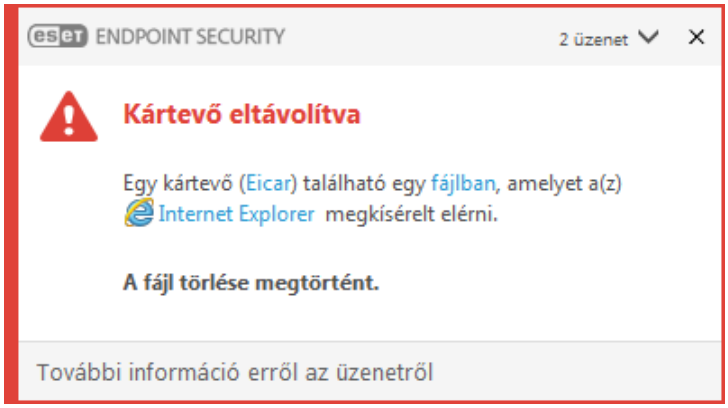
A fertőzések számos különböző ponton keresztül juthatnak be a rendszerbe, például weboldalakról, megosztott mappákból, e-mailen keresztül vagy cserélhető eszközökről (USB-eszközökről, külső lemezekről, CD, DVD vagy hajlékonylemezekről stb.).

Szokásos viselkedés

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

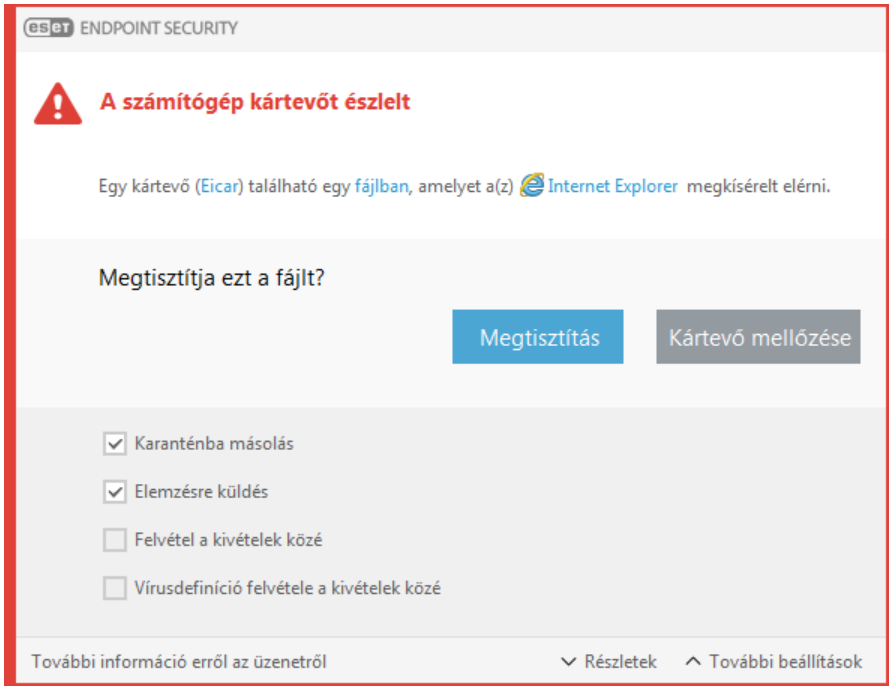
- Valós idejű fájlrendszervédelem
- Webhozzáférés-védelem
- E-mail védelem
- Kézi indítású számítógép-ellenőrzés

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 Megtisztítás című fejezetben olvashat bővebben.



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 Endpoint Securityfő programablakából érhető el az **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.

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.

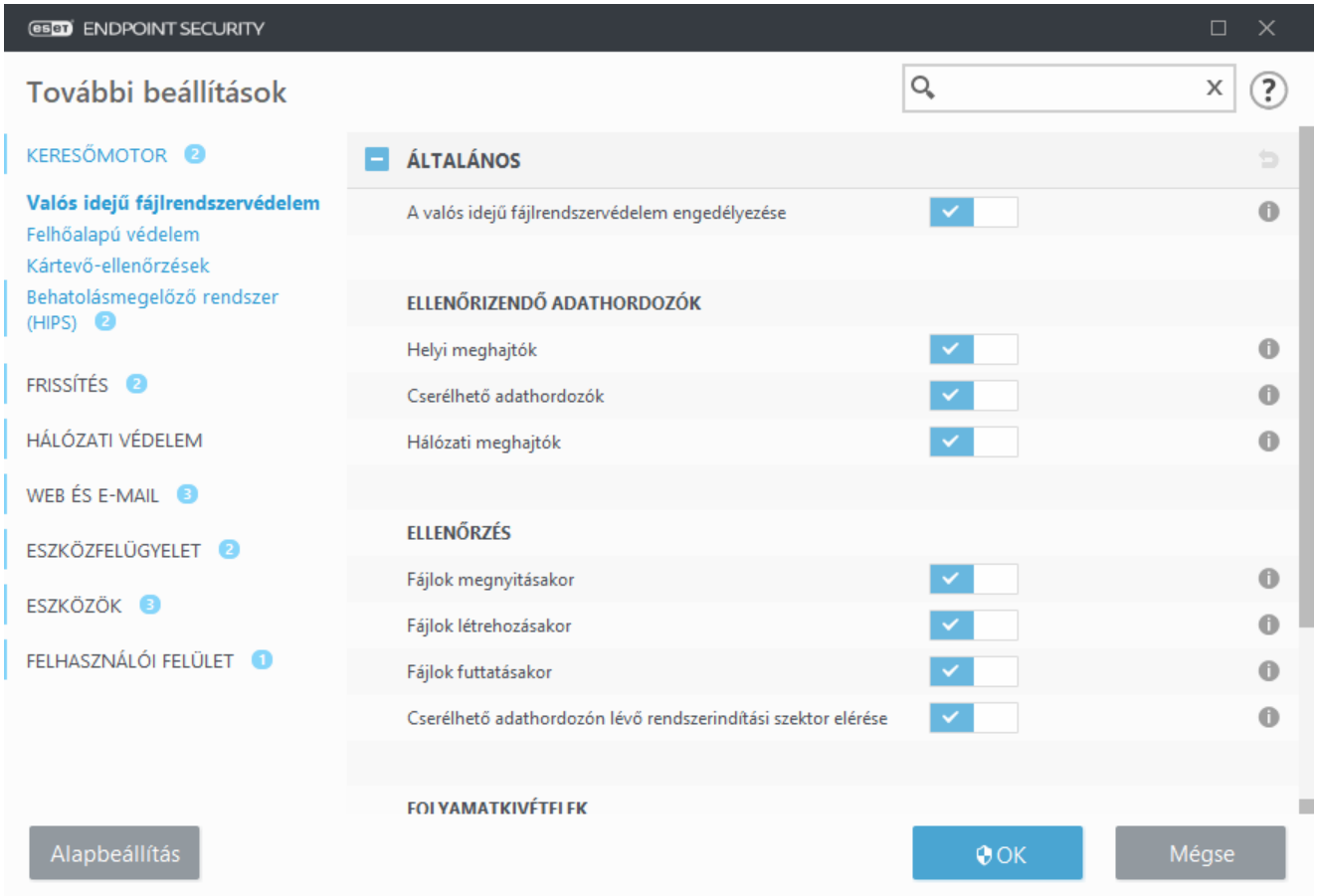
Ha a számítógép fertőzés jeleit mutatja, azaz működése lelassul, gyakran lefagy stb., ajánlatos elvégeznie az alábbiakat:

- Nyissa meg az ESET Endpoint Security programot, és kattintson a Számítógép ellenőrzése ikonra.
- Kattintson az **Optimalizált ellenőrzés** hivatkozásra (további információért lásd:Számítógép ellenőrzése).
- 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.

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.

Ellenőrzésből kizárandó folyamatok – Erről a típusú kivételről a Folyamatkivételek című fejezetben olvashat bővebben.

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** funkciót.

A valós idejű védelem ellenőrzése

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

Mikor érdemes módosítani a valós idejű védelem beállításain?

A valós idejű fájlrendszervédelem a biztonságos rendszerek fenntartásának legfontosabb összetevője. Ezért a paramétereket csak körültekintően módosítsa. Azt javasoljuk, hogy ezt csak különleges esetekben tegye.

Telepítése után az ESET Endpoint 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**).

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.

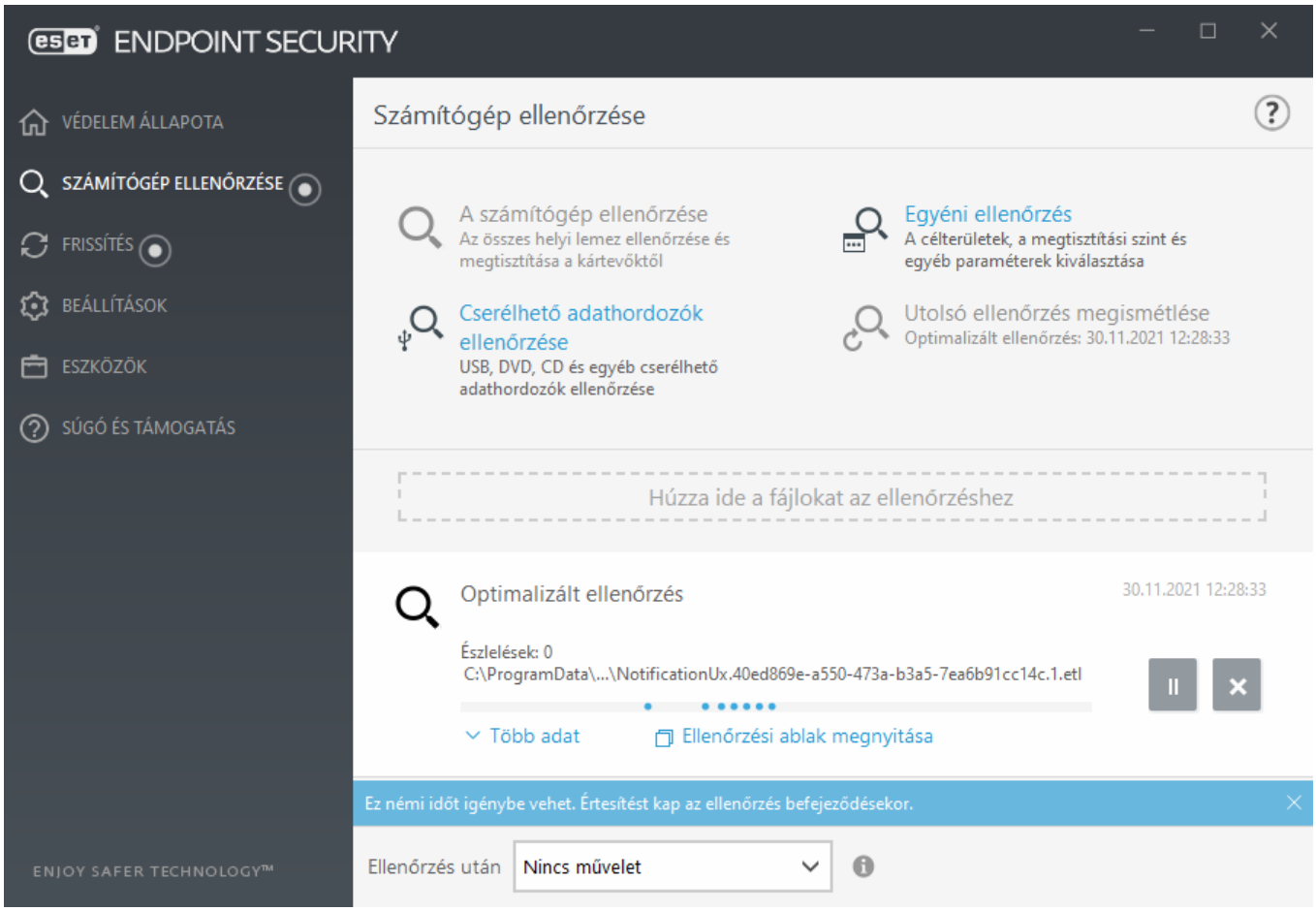
A valós idejű védelem nem indul el

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 forduljon az ESET műszaki terméktámogatáshoz. ESET SysInspector-napló létrehozásával az ESET műszaki terméktámogatának való elküldésével elősegítheti a probléma elhárítását. További információkért

olvassa el ezt az ESET-tudásbáziscikket.

Számítógép ellenőrzése

A kézi indítású víruskereső az ESET Endpoint Security 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 (például havi) ellenőrzése a Valós idejű fájlrendszervédelem által nem észlelt vírusok észleléséhez. Ilyen akkor történhet, ha a Valós idejű fájlrendszervédelem ki volt kapcsolva az adott időben, a keresőmotor elavult volt, illetve a lemezre íráskor a program nem ismerte fel vírusként a fájlt.



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

Az ellenőrzési folyamatról Az ellenőrzés folyamata című fejezetben olvashat bővebben.

A számítógép ellenőrzése

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

Egyéni ellenőrzés

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

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

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

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.

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.

Kiválaszthatja a **Nincs művelet**, **Kikapcsolás**, **Újraindítás**, **Újraindítás szükség esetén** vagy a **Szükség esetén az újraindítás kényszerítése** vagy az **Újraindítás kényszerítése** lehetőséget **Az ellenőrzést követő művelet** legördülő menüben. Az **Alvás** vagy a **Hibernálás** műveletek elérhetősége a számítógép operációs rendszerének Bekapcsolás és alvó állapot beállításaitól, illetve a számítógép/laptop funkcióitól függ. A kiválasztott művelet a futó ellenőrzések befejeződése után fog megkezdődni. A **Kikapcsolás** kiválasztása esetén a kikapcsolás megerősítésére szolgáló párbeszédpanel megjeleníti a 30 másodperces visszaszámlálást (a **Mégse** gombra kattintva deaktiválja a kikapcsolást). A További ellenőrzési beállítások című rész bővebb információk tartalmaz erről.

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

Egyéni ellenőrzés indítása

Ha csak egy adott célterületet szeretne ellenőrizni, használhatja az Egyéni ellenőrzés eszközt. Az ellenőrizendő célterületek kiválasztásához kattintson a **Számítógép ellenőrzése** > **Egyéni ellenőrzés** hivatkozásra, és válasszon egy területet az ⚙ > **Ellenőrizendő célterületek** legördülő listában, vagy a mappa fastruktúrájában jelöljön ki adott célterületeket.

Az ellenőrizendő célterületek ablaka lehetővé teszi annak meghatározását, hogy mely objektumokban (memória, meghajtók, szektorok, fájlok és mappák) legyenek ellenőrizve a fertőzések.

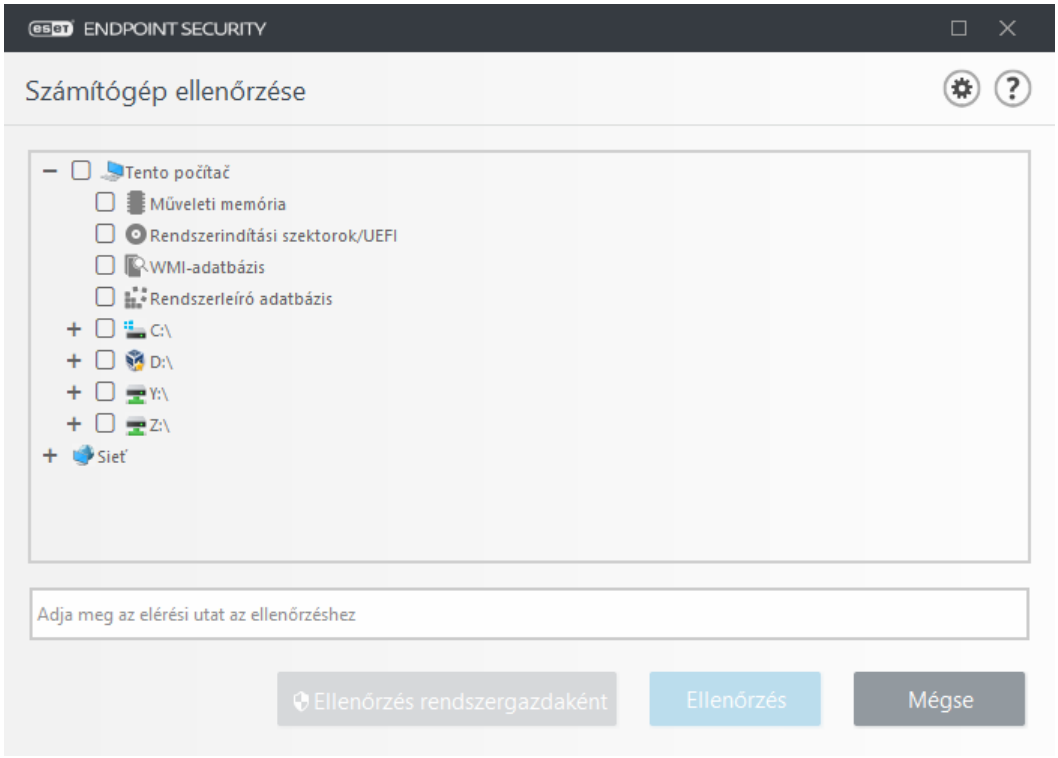
Az **Ellenőrizendő célterületek** legördülő listában előre definiált ellenőrizendő célterületeket választhat ki.

- **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.



A program nem tisztítja meg automatikusan a fertőzött elemeket. A megtisztítás nélküli ellenőrzés arra használható, hogy képet kapjon az aktuális fertőzöttségi állapotról. Ezenkívül három megtisztítási szint közül is választhat a **További beállítások** > **Keresőmotor** > **Kézi indítású ellenőrzés** > **ThreatSense-paraméterek** > **Megtisztítás** csoportban. Ha csak információszerzés céljából, megtisztítás nélkül szeretné ellenőrizni a rendszert, jelölje be a **Csak ellenőrzés megtisztítás nélkül** jelölőnégyzetet. 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.

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

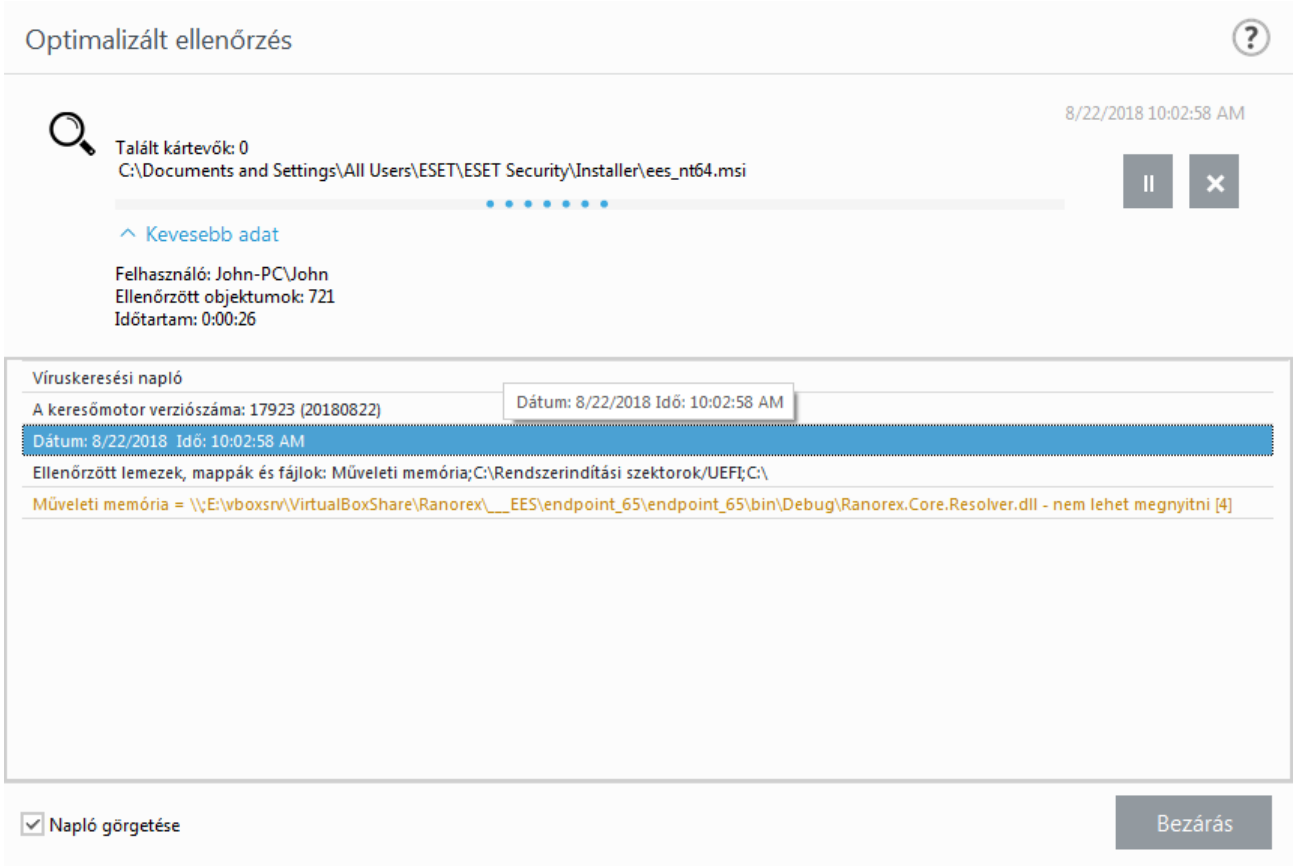
Kattintson az **Ellenőrzés** gombra az ellenőrzés végrehajtásához a beállított egyéni paraméterek alapján.

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 hozzáféréséhez. Ne feledje, hogy 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.

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.

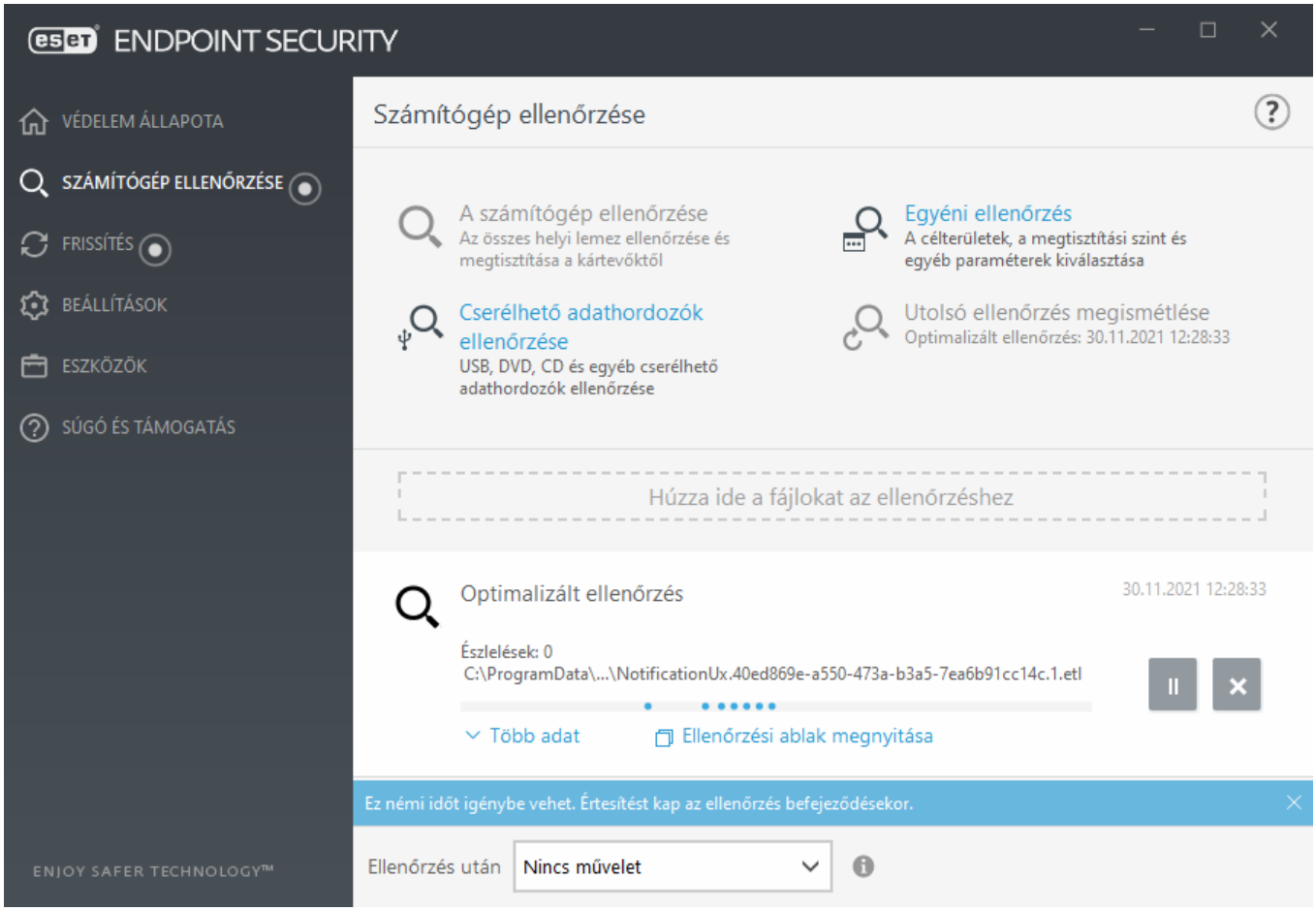
A víruskereső kártevőket talált – Itt látható a program által az ellenőrzés során észlelt kártevők száma.

Felfüggesztés – Felfüggeszti az ellenőrzést.

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

Leállítás – Megszakítja az ellenőrzést.

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



Számítógép-ellenőrzés naplója

A számítógép-ellenőrzés naplója általános információkat nyújt az ellenőrzésről, például:

- Ellenőrzés dátuma és időpontja
- Ellenőrzött lemezek, mappák és fájlok:
- Ellenőrzött objektumok száma
- Talált kártevők száma
- Befejezés ideje
- Ellenőrzés teljes ideje

Kártevő-ellenőrzések

A **Kártevőellenőrzések** szakasz a További beállítások menüben található. Nyomja meg az **F5** billentyűt, kattintson a **Keresőmotor** > **Kártevőellenőrzések** elemre, majd válassza ki az ellenőrzési paramétereket. Ez a szakasz a következő beállításokat tartalmazza:

- **Kiválasztott profil** – A kézi indítású víruskereső által használt paraméterek adott csoportja.
  Új profil létrehozásához kattintson a Szerkesztés gombra a Profilok listája felirat mellett. További információkért tekintse meg az Ellenőrzési profilok című részt.
- **Kézi indítású ellenőrzés és gépi tanulás védelem** – Lásd a Keresőmotor (7.2 és újabb) című részt.
- **Ellenőrizendő célterületek** – Ha csak egy meghatározott célterületet szeretne ellenőrizni, kattintson az **Ellenőrizendő célterületek** felirat mellett a **Szerkesztés** gombra, és 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 állítsa az **Üresjárat idején történő ellenőrzés engedélyezése** kapcsolót **Be** állásba. 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 aktiválja a **Futtatás akkor is, ha a számítógép akkumulátorról működik** kapcsolót.

Kapcsolja be állásba a **Naplózás engedélyezése** kapcsolót, ha meg szeretné jeleníteni a számítógép-ellenőrzés kimenetét a Naplófájlok szakaszban (a program főablakában kattintson az **Eszközök** > **Naplófájlok** elemre, és a **Naplófájlok** legördülő listában válassza a **Számítógép ellenőrzése** elemet).

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 Endpoint 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 **automatikus megtisztítást** 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 ablaka lehetővé teszi annak meghatározását, hogy mely objektumokban (memória, meghajtók, szektorok, fájlok és mappák) legyenek ellenőrizve a fertőzések.

Az **Ellenőrizendő célterületek** legördülő listában előre definiált ellenőrizendő 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.

További ellenőrzési beállítások

Ebben az ablakban adhat meg további beállításokat az ütemezett számítógép-ellenőrzési feladatokhoz. A legördülő menüben megadhatja, hogy az ellenőrzés befejezését követően milyen műveletet végezzen el

automatikusan a program:

- **Leállítás** – A számítógép kikapcsolása egy ellenőrzés befejezését követően.
- **Újraindítás** – Az összes program bezárása és a számítógép újraindítása egy ellenőrzés befejezését követően.
- **Újraindítás szükség esetén** – Az összes program bezárása és a számítógép újraindítása, ha az ellenőrzés ezt kívánja meg.
- **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.
- **Nincs művelet** – Az ellenőrzés befejezését követően nincs végrehajtandó művelet.

> 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 felhasználó nem szakíthatja meg a műveletet opciót választva elutasíthatja, 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 című fejezetet.

Eszközfelügyelet

Az ESET Endpoint 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 (akkumulátorral működő eszközök, például médialejátszók, okostelefonok, plug-and-play eszközök stb.)
- Minden eszköztípus

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

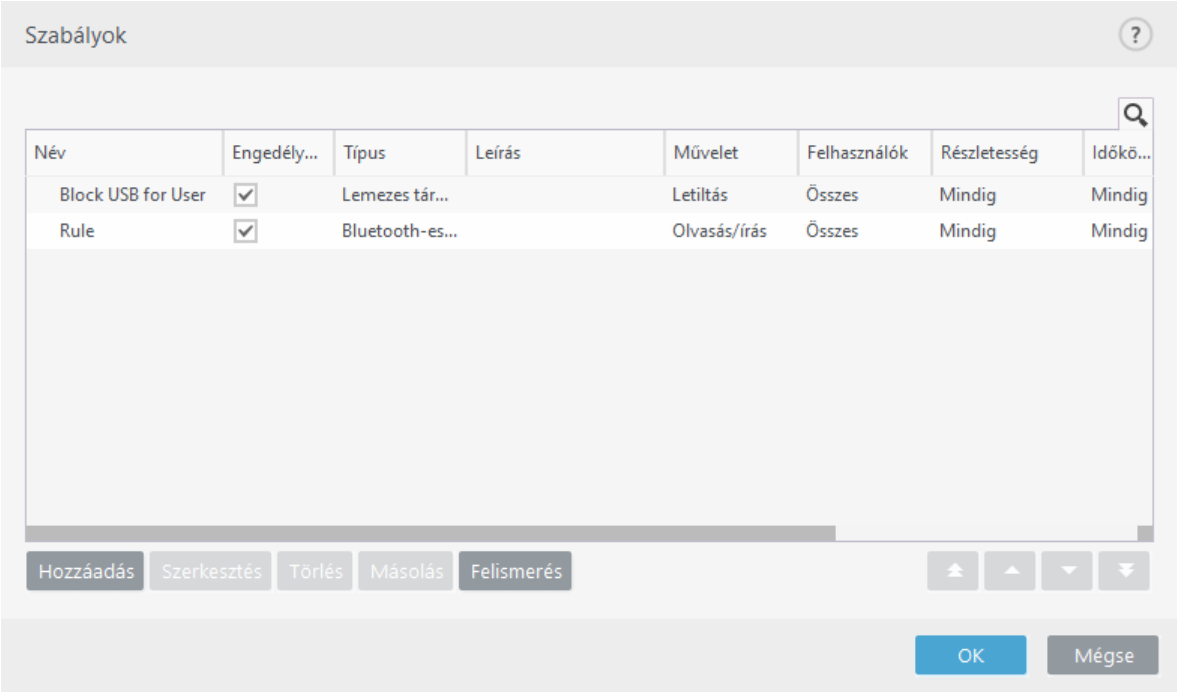
Az eszközfelügyelet engedélyezése szöveg melletti kapcsoló átállításával aktiválható az ESET Endpoint Security Eszközfelügyelet funkciója; a módosítás érvénybelépéséhez újra kell indítani a számítógépet. Az Eszközfelügyelet engedélyezését követően aktív lesz a **Szabályok** gomb, amellyel megnyithatja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

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. Tekintse meg a következőt is: Eszközfelügyeleti szabályok hozzáadása.

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
- Eszközfelügyeleti szabályok hozzáadása és módosítása ESET-végponttermékekkel



Adott eszközök engedélyezhetők vagy letilthatók a felhasználójuk vagy a felhasználócsoport szerint, illetve a szabály konfigurációjában megadható számos paraméter alapján. 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.

Szabály kezeléséhez kattintson a **Hozzáadás** vagy a **Szerkesztés** gombra. Törölje az egyes szabályok melletti **Engedélyezve** jelölőnégyzet bejelölését az adott szabály letiltásához a jövőbeli használatáig. Jelöljön ki egy vagy több szabályt, és a végleges törléséhez kattintson a **Törlés** elemre.

Másolás – Erre kattintva létrehozhat egy új szabályt egy másik kijelölt szabályhoz használt előre definiált beállításokkal.

Kattintson a **Felismerés** gombra a számítógéphez csatlakoztatott cserélhető médiaeszközök paramétereinek automatikus feltöltéséhez.

A szabályok prioritási sorrendben vannak felsorolva úgy, hogy a legnagyobb prioritású szabályok vannak a lista

tetején. A szabályok a  **Tetejére/Fel/Le/Aljára** gombra kattintva egyesével vagy csoportosan is áthelyezhetők.

Az Eszközfelügyelet naplója feljegyzi az eszközfelügyeletet kiváltó összes eseményt. A naplóbejegyzések az ESET Endpoint Security főablakában az **Eszközök** > **Naplófájlok** csoportban tekinthetők meg.

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).

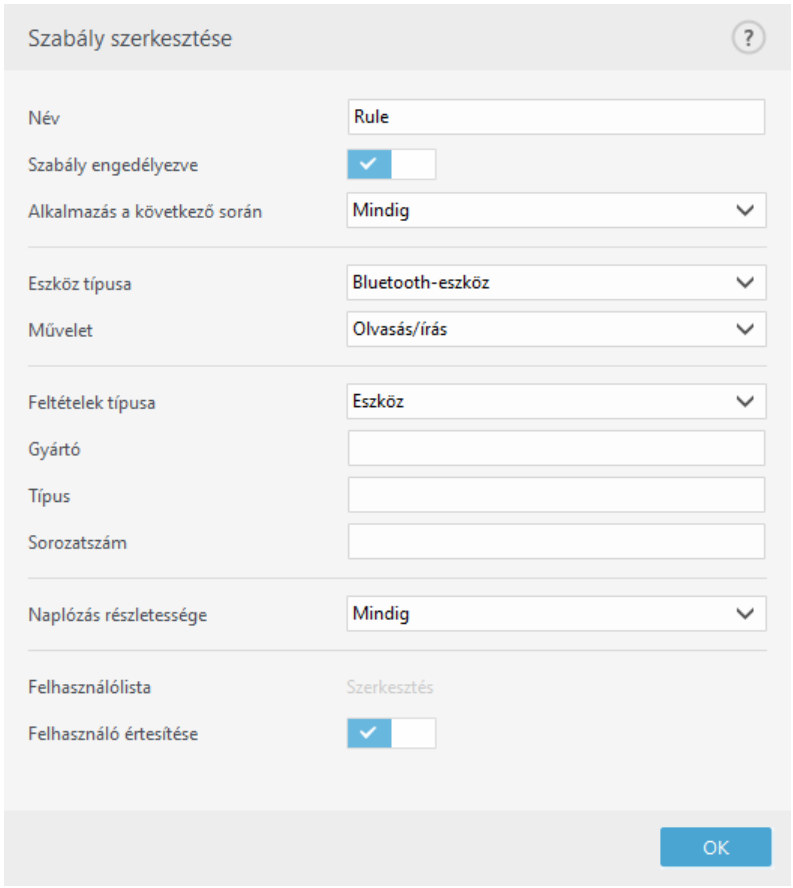
Amikor elkészült a testreszabással, kattintson az **OK** gombra. A **Mégse** gombra kattintva a módosítások mentése nélkül bezárhatja az **Eszközcsoportok** ablakot.

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 kapcsolóra. Ez akkor lehet hasznos, ha nem szeretné véglegesen törölni a szabályt.

Alkalmazás a következő során – A létrehozott szabály alkalmazása a megadott időpontban. A legördülő menüben válassza ki a létrehozott időközt. További információk az időközökről.

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.

A modemeszköz típusa nem támogatja a felhasználói lista funkciót. Az alkalmazás ezt a szabályt alkalmazza az összes felhasználóra, és törli a jelenlegi felhasználói listát.

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 minden paraméternél különbséget jelentenek:

- **Gyártó** – Szűrés a gyártó neve vagy azonosítója 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 minden szöveges mező esetén különbséget jelentenek a kis- és a nagybetűk, 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

- **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 hibák és figyelmeztető üzenetek rögzítése, és elküldésük az ERA Server felé.
- **Nincs** – Nem rögzít naplókat.

A szabályok bizonyos felhasználókra vagy felhasználócsoportokra korlátozhatók, ha felveszi őket a **felhasználólistára**:

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

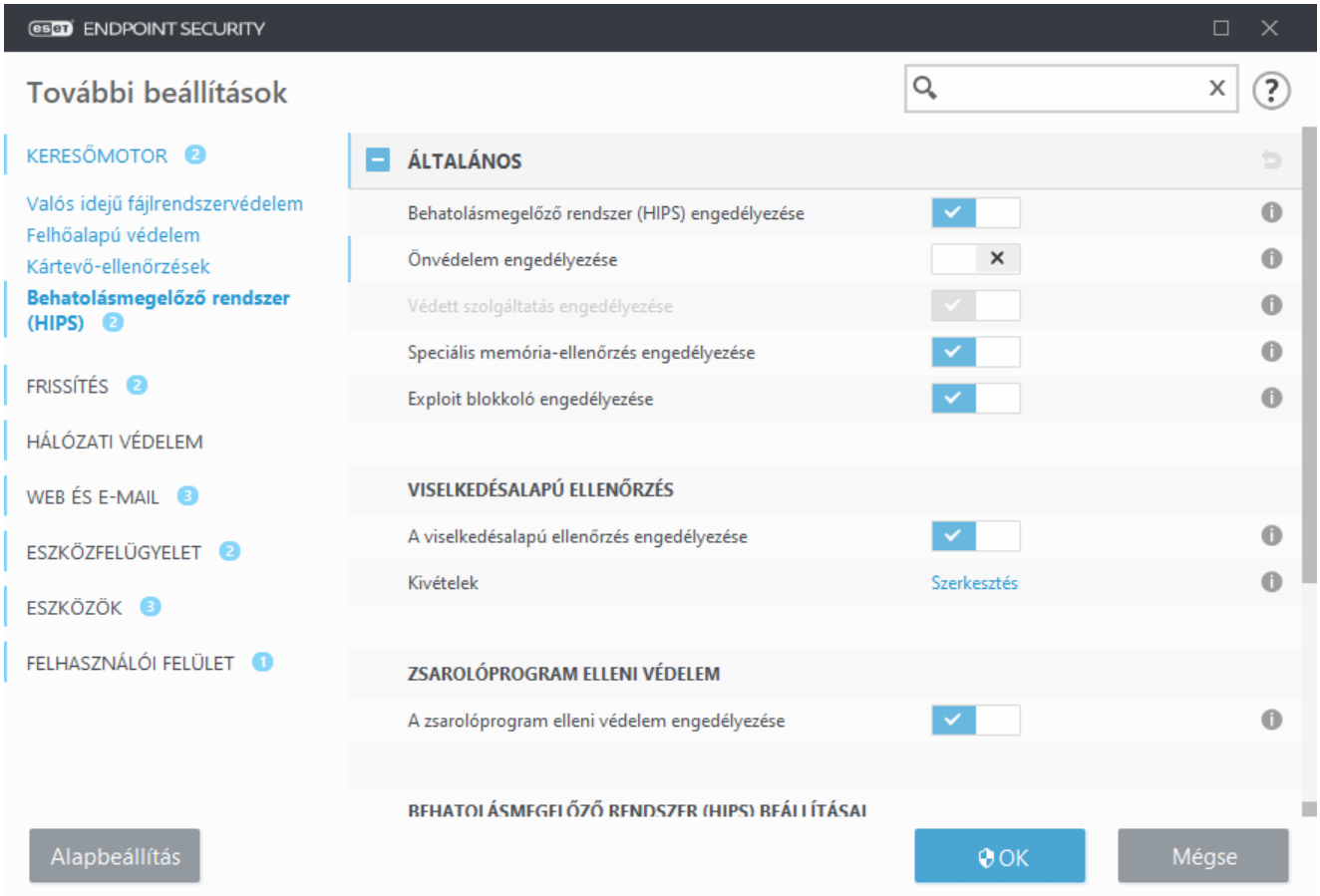
> Nem minden eszköz szűrhető a felhasználói szabályok szerint (a képeszközök például csak a műveletekről nyújtanak információkat, a felhasználókról nem).

Behatolásmegelőző rendszer

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 Endpoint Security fő programablakának **Beállítások** > **Számítógép** részén látható.



Általános

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

Önvédelem engedélyezése – Az ESET Endpoint 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. Az ESET Management Agent is védelmet kap, ha telepítve van.

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 és a Windows 10 rendszerben 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.

Naplózási mód engedélyezése – a rendszer nem tiltja le a Zsarolóprogram elleni védelem által észlelt összes elemet, hanem a Figyelmeztetés jelzéssel naplózza őket, majd elküldi őket a felügyeleti konzolhoz a „NAPLÓZÁSI MÓD” jelzéssel. A rendszergazda kizárhatja az ilyen elemeket a későbbi észlelés megakadályozása érdekében, vagy megtarthatja őket aktív állapotban, amely esetben a Naplózási mód végén a rendszer letiltja vagy eltávolítja őket. A rendszer a Naplózási mód engedélyezését/letiltását is naplózza a ESET Endpoint Security szolgáltatásban. Ez a funkció csak az ESET PROTECT házirend-konfiguráló szerkesztőjében áll rendelkezésre.

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.

Szűrési üzemmód	Leírás
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).

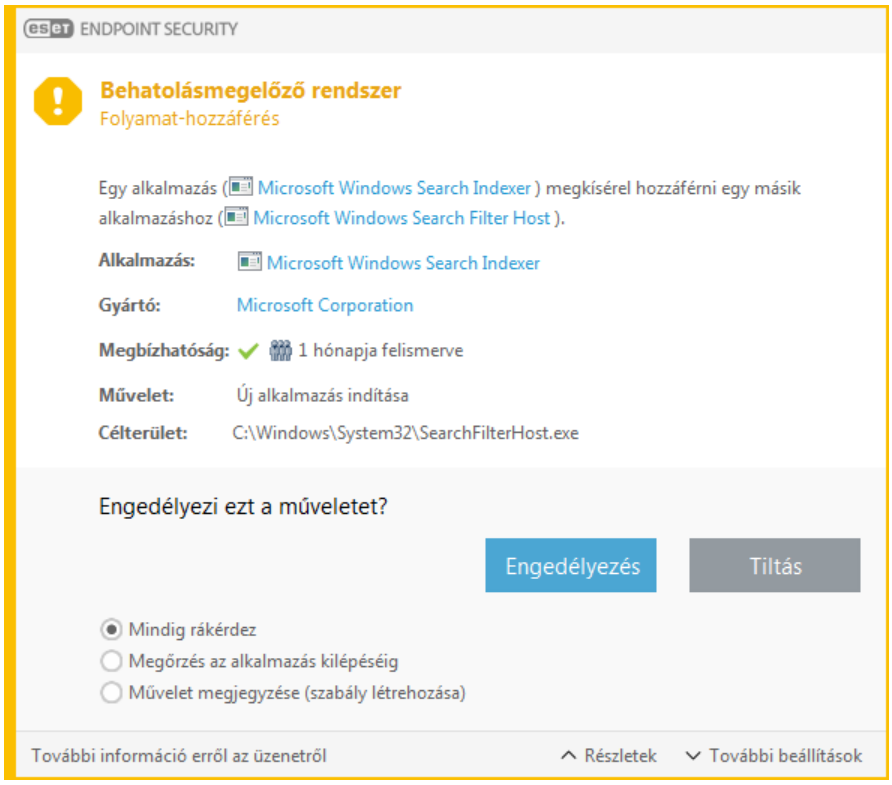
A lent található **Részletek** elemre kattintva megtekintheti, hogy mely alkalmazás váltja ki a műveletet, mennyire megbízható a fájl, illetve hogy Ön milyen műveletet engedélyez vagy tilt.

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.

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

Az alábbiakban a Behatolásmegelőző rendszer felhasználó által definiált

és automatikusan létrehozott szabályainak listája látható. A szabályok létrehozásáról és a Behatolásmegelőző rendszer műveleteiről A Behatolásmegelőző rendszer szabályainak beállítása 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 – Kapcsolja ki ezt a funkciót, 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 ablakban értesítés 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)

Behatolásmegelőző rendszer szabálybeállításai

Lásd: Behatolásmegelőző rendszer szabályainak kezelése

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 ezt a kapcsolót, 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** műveletre új fájlok vagy mappák hozzáadásához, illetve ha az összeset hozzá szeretné adni, a legördülő listában választhatja **Az összes bejegyzés** elemet is.

i A Behatolásmegelőző rendszer által előre létrehozott speciális szabályok egyes műveletei alapértelmezés szerint engedélyezettek, és nem tilthatók le. Ráadásul nem minden rendszerműveletet figyel a Behatolásmegelőző rendszer (HIPS). A Behatolásmegelőző rendszer (HIPS) felügyeli azokat a műveleteket, amelyek nem tekinthetők biztonságosnak.

i Útvonal megadásakor a C:\example formátum a mappával kapcsolatos műveletekre van hatással, a C:\example*.* formátum pedig a mappában lévő fájlokat célozza.

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.

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 például 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.

Helyettesítő karakterek használata
A szabályokban a csillag csak egy adott kulcs helyettesítésére használható, pl A szabályokban a csillag csak egy adott kulcs helyettesítésére használható, pl „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start”. Más módon nem használhatók helyettesítő karakterek.

A HKEY_CURRENT_USER kulcsot célzó szabályok létrehozása
Ez a kulcs csak egy kapocs a HKEY_USERS megfelelő alkulcsához, amely a SID (biztonságos azonosító) által beazonosított felhasználóhoz kapcsolódik. Ha csak az aktuális felhasználónak szeretne szabályt létrehozni – a HKEY_CURRENT_USER kulcshoz vezető útvonal használata helyett – használjon egy olyan útvonalat, amely a HKEY_USERS\%SID% kulcshoz vezet. SID-ként használhat csillagot, így a szabály mindegyik felhasználóra vonatkozni fog.

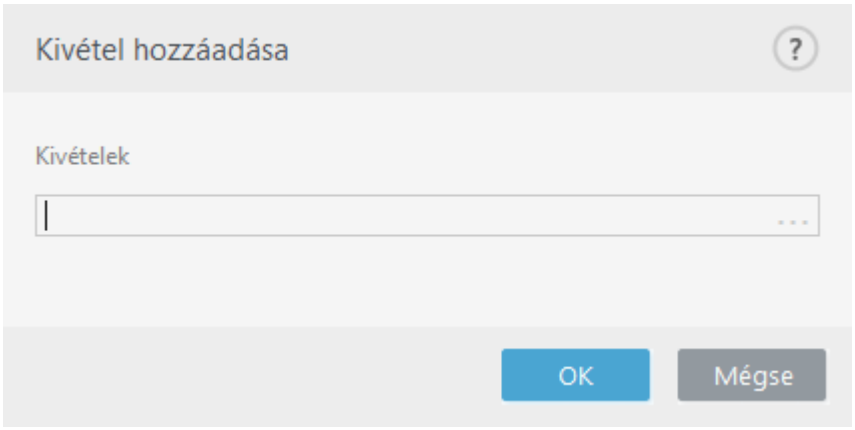
Ha nagyon általános szabályt hoz létre, a program figyelmeztetést jelenít meg erről a szabálytípusról.

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. Kapcsolja be a **Felhasználó értesítése** opciót, 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.



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.

Bemutató üzemmód

A bemutató 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 processzor terhelését. A bemutató üzemmód olyan bemutatók során használható, amelyeket nem szakíthat meg semmiféle vírusvédelmi művelet. Engedélyezése esetén minden felugró ablak le van tiltva és az ütemezett feladatok nem futnak. A rendszervédelem változatlanul működik a háttérben, felhasználói beavatkozást azonban nem igényel.

Kattintson a **Beállítások** > **Számítógép** elemre, és a bemutató üzemmód kézi engedélyezéséhez jelölje be a **Bemutató üzemmód mellett lévő jelölőnégyzetet. Az** F5 billentyű lenyomásával megnyitható **További beállítások** párbeszédpanelen kattintson az **Eszközök** > **Bemutató üzemmód** elemre, és jelölje be a **Bemutató üzemmód engedélyezése automatikusan az alkalmazások teljes képernyős módban való futtatásakor jelölőnégyzetet, ha azt szeretné, hogy a teljes képernyős alkalmazások futtatásakor az ESET Endpoint Security automatikusan bemutató üzemmódban működjön**. A bemutató üzemmód engedélyezése lehetséges 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 bemutató üzemmód mellett **A bemutató üzemmód engedélyezve van** narancssárga felirat látható.

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

A **Bemutató üzemmód letiltása automatikusan ezt követően** jelölőnégyzetet bejelölve megadhatja, hogy a program hány perc múlva tiltsa le automatikusan a bemutató üzemmódot.

Ha a tűzfal interaktív módban van, és a bemutató üzemmód engedélyezett, internetelérési problémák jelentkezhetnek. Ez akkor okozhat problémát, ha egy internetkapcsolatot igénylő játékot indít el. A program ilyenkor általában megerősítést kér a művelet elvégzésére (ha nincsenek külön kommunikációs szabályok vagy kivételek megadva), bemutató üzemmódban azonban a felhasználói beavatkozás nem engedélyezett. A probléma megoldásához hozzon létre egy kommunikációs szabályt minden olyan alkalmazáshoz, amelyik ütközhet ezzel a funkcióval, vagy állítson be más szűrési módot a tűzfalban. Ne feledje továbbá, hogy bemutató üzemmódban a felkeresett webhelyek és a futtatott alkalmazások biztonsági kockázatot hordozhatnak, illetve előfordulhat, hogy a rendszer letiltja a webhelyeket vagy az 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 modulfrissítésekkor alapértelmezés szerint elvégzi a rendszerindításkor automatikusan futtatott fájlok ellenőrzését. Az ellenőrzés a Feladatütemezőben meghatározott beállításoktól és feladatoktól függ.

A rendszerindításkor futtatott ellenőrzés beállítása a feladatütemező **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** feladatának a része. A rendszerindításkor futtatott ellenőrzés beállításainak módosításához nyissa meg az **Eszközök** > **Feladatütemező** ablakot, jelölje be a **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése** jelölőnégyzetet, majd kattintson a **Szerkesztés** gombra. 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 listái az említett egyes csoportokhoz vannak meghatározva.

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** ablakot (nyomja le az **F5** billentyűt), válassza ki a **Keresőmotor** > **Kártevőellenőrzések** > **Dokumentumvédelem** elemet, majd kattintson **A dokumentumvédelem engedélyezése** kapcsolóra.

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 objektumokat zárhat ki a tisztításból 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.

A 7.1-es és a korábbi verziókban a Teljesítménybeli kivételek és az Észlelési kivételek egyesültek.

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

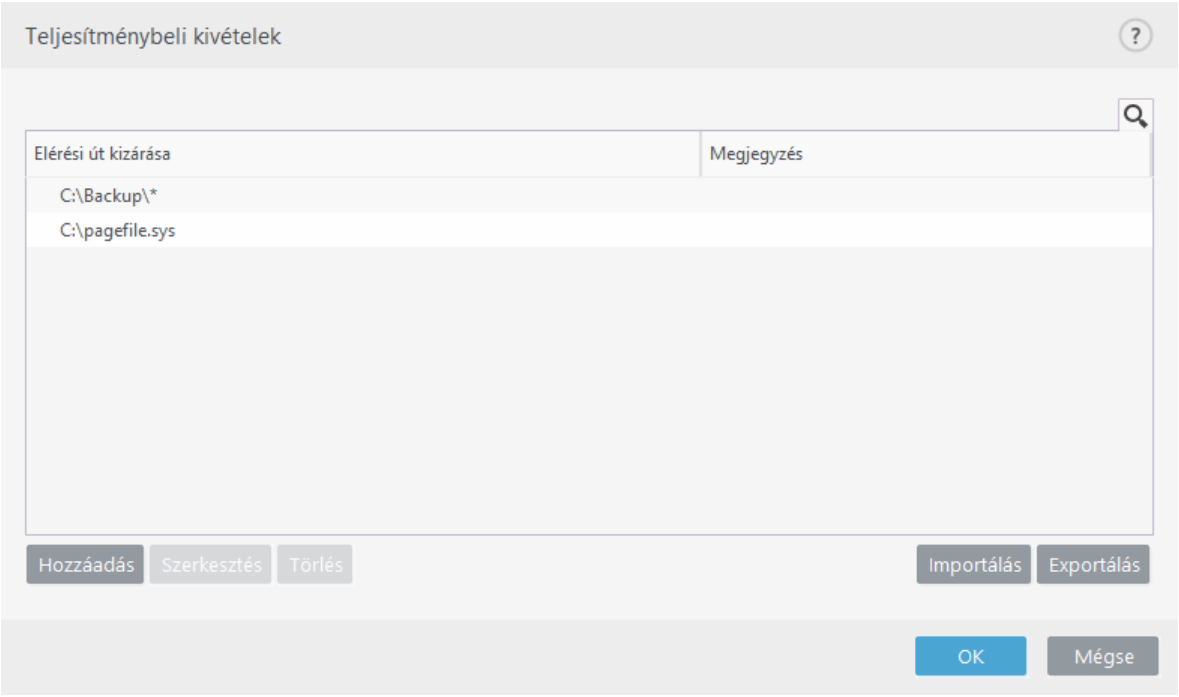
Teljesítménybeli kivételek

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.

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** – Hozzáadhat egy új bejegyzést, ha ki szeretne zárni objektumokat a megtisztításból.
- **Szerkesztés** – A kijelölt bejegyzések szerkesztését teszi lehetővé.
- **Törlés** – A kijelölt bejegyzések eltávolítása (több bejegyzés kijelöléséhez tartsa lenyomva a CTRL billentyűt, és kattintson a bejegyzésekre.
- **Importálás/Exportálás** – Mindkét művelet hasznos abban az esetben, ha a teljesítménybeli kivételekről későbbi felhasználás céljából biztonsági másolatot szeretne készíteni. Az exportálási funkció emellett arra is alkalmas nem felügyelt környezetben, hogy a .txt fájl importálásával a felhasználók egyszerűen átvihessék és más számítógépeken is beállíthassák a megfelelő konfigurációt.
  Példa megjelenítése importálási/exportálási fájlformátumra

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManageme
nt.PerformanceExclusions","columns":["Path","Description"]}

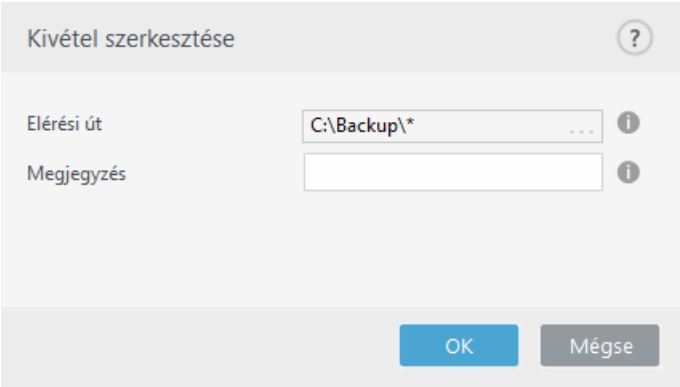
C:\Backup\*,custom comment

C:\pagefile.sys
```

Teljesítménybeli kivételek felvétele vagy szerkesztése

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

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.

• 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.

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.

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.

• 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.

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

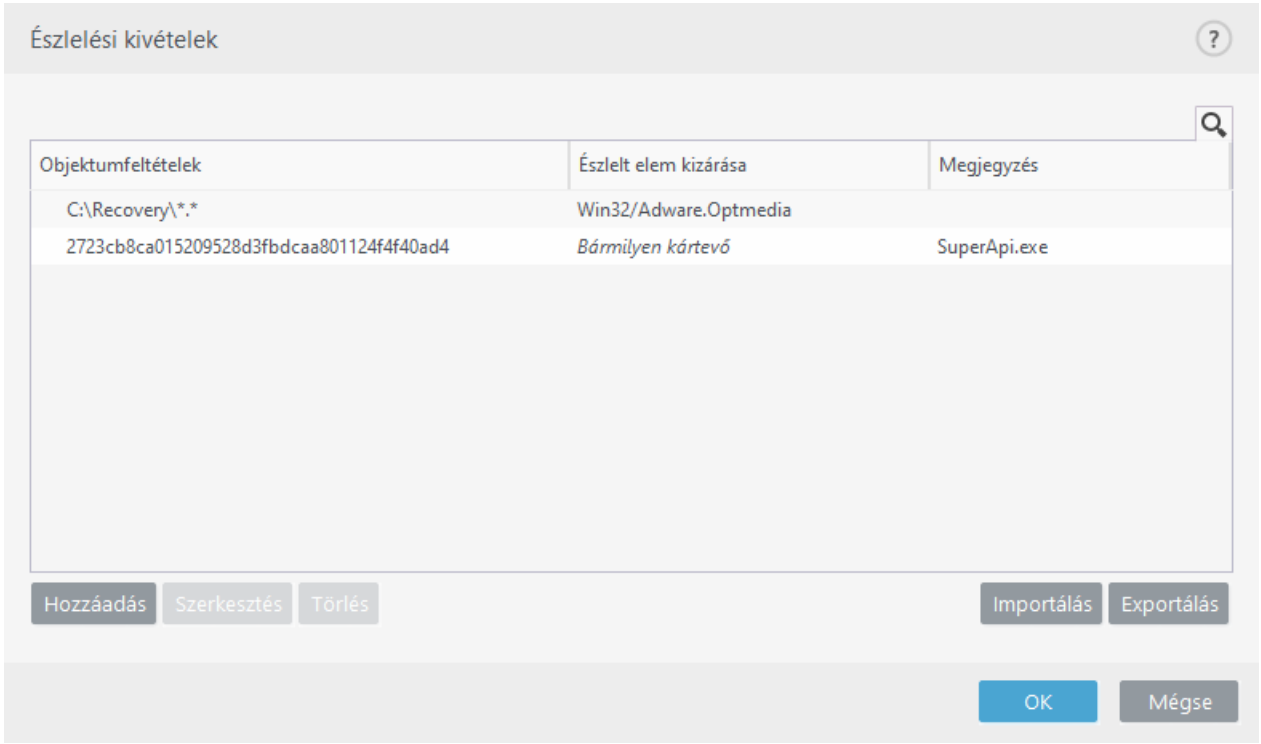
A következő változók használhatók az útvonalkivétel formátumában:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

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

Észlelési kivételek

Az Észlelési kivételek csoportban objektumokat zárhat ki a tisztításból 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.
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.

Ha ki szeretne zárni egy objektumot (neve vagy kivonata alapján) a megtisztításból, 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** > **Karantén** elemet kiválasztva, 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.

Vezérlőelemek

- **Hozzáadás** – Hozzáadhat egy új bejegyzést, ha ki szeretne zárni objektumokat a megtisztításból.
- **Szerkesztés** – A kijelölt bejegyzések szerkesztését teszi lehetővé.
- **Törlés** – A kijelölt bejegyzések eltávolítása (több bejegyzés kijelöléséhez tartsa lenyomva a CTRL billentyűt, és kattintson a bejegyzésekre.
- **Importálás/Exportálás** – Mindkét művelet hasznos abban az esetben, ha az aktuális kivételekről későbbi felhasználás céljából biztonsági másolatot szeretne készíteni. Az exportálási funkció emellett arra is alkalmas nem felügyelt környezetben, hogy a .txt fájl importálásával a felhasználók egyszerűen átvihessék és más számítógépeken is beállíthassák a megfelelő konfigurációt.
  Példa megjelenítése importálási/exportálási fájlformátumra

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManageme
nt.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileH
ash"]}

4c59cd02-357c-4b20-a0ac-
ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

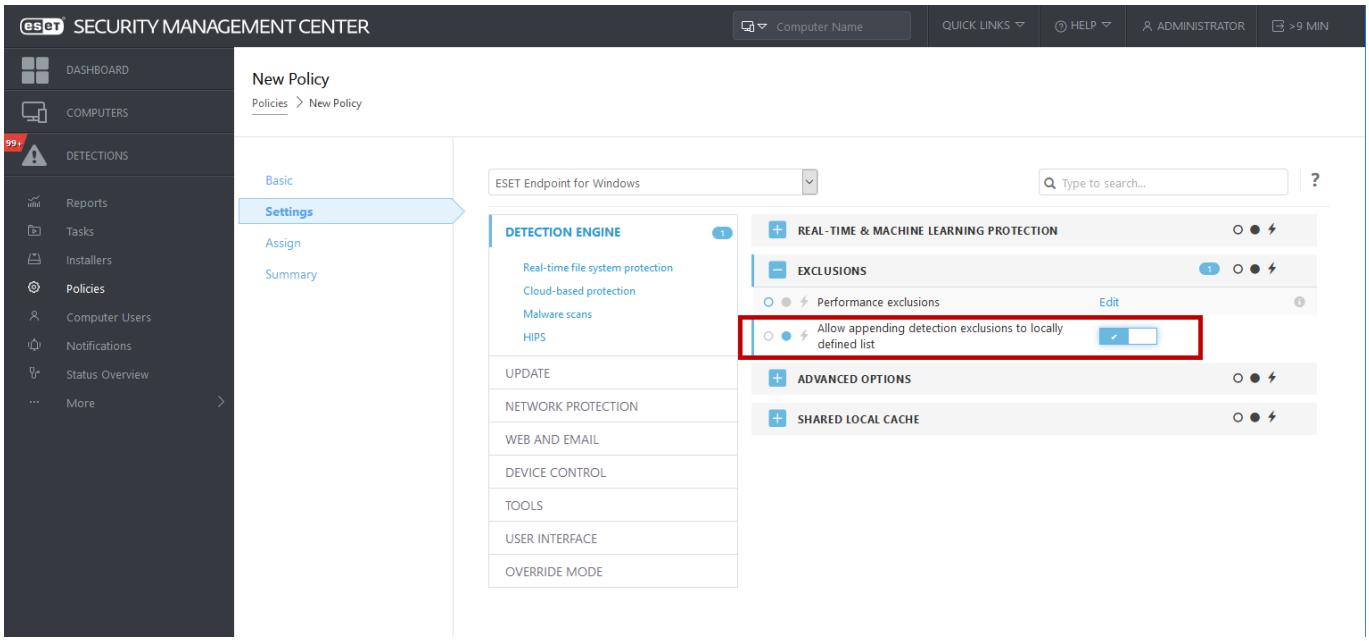
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Az ESET PROTECT segítségével beállított észlelési kivételek

Az ESET PROTECT 8.0 egy új varázslót tartalmaz az észlelési kivételek kezeléséhez – létrehozhat egy észlelési kivételt, majd alkalmazhatja több számítógépre/csoportra.

A potenciális észlelési kivételek felülírása az ESET PROTECT felől

Ha van egy észlelési kivételeket tartalmazó helyi lista, a rendszergazdának alkalmaznia kell egy házirendet a következővel: **Az észlelési kivételek hozzáfűzhetők helyileg definiált listához**. Ezután a megszokott módon hozzáfűzhetők észlelési kivételek az ESET PROTECT-ből.

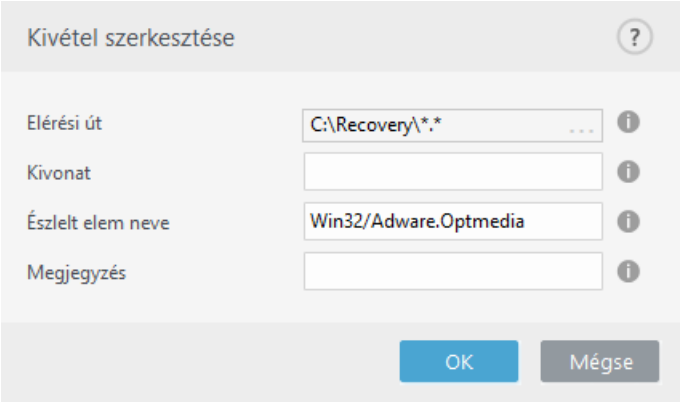


Észlelési kivétel felvétele vagy szerkesztése

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 Endpoint 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.

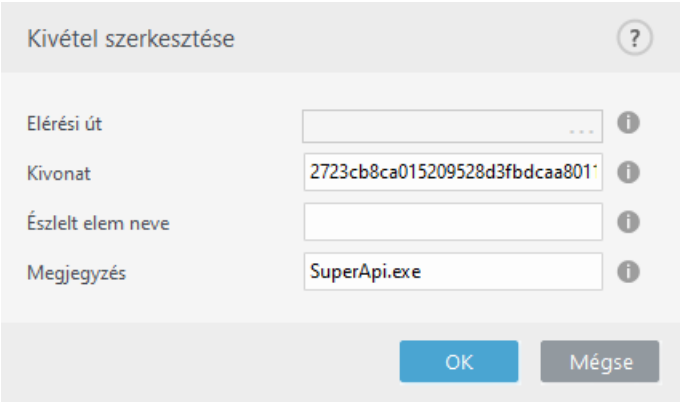
Tekintse meg az Útvonalkivétel formátuma című részt is.



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.



Ha ki szeretne zárni egy kártevőt, adjon meg érvényes kártevőnevet:
Win32/Adware.Optmedia
A következő formátumot is használhatja, amikor kizár egy fertőzést az ESET Endpoint 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 fő programablakban kattintson az **Eszközök** > **Naplófájlok** elemre.
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:

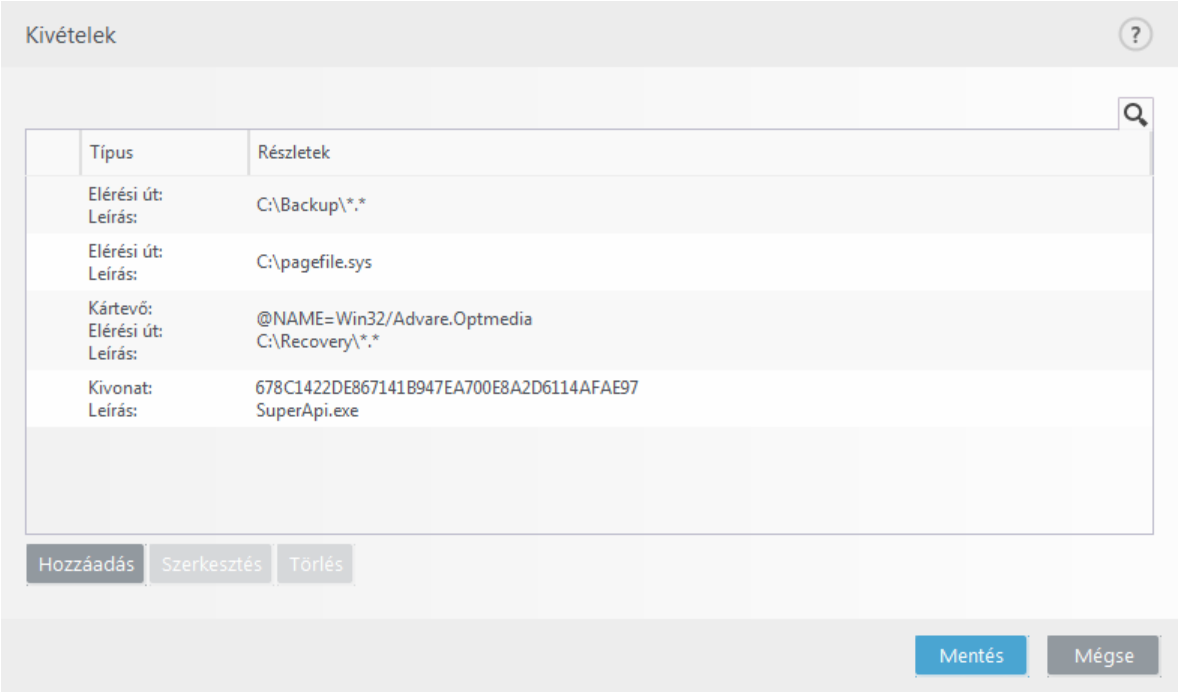
- **Pontosan a fájlok** – Mindegyik fájl kizárása SHA-1 hash alapján.
- **Észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve alapján.
- **Elérési út + Észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve és elérési útja alapján (pl. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

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

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

Kivételek (7.1 és korábbi)

A 7.1-es és a korábbi verziókban a Teljesítménybeli kivételek és az Észlelési kivételek egyesültek.



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. Hasonló problémák léphetnek fel

virtuális gépek élő áttelepítésekor. 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.

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 Endpoint 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 Endpoint 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.

HIPS-kivételek

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

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.

Tekintse meg a Kivételek című fejezetet.

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 Endpoint Security mit tegyen az objektumok megtisztítása során.

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.

Megtisztítási szintek

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

A Valós idejű védelem és az egyéb védelmi modulok a következő kezelési (vagyis megtisztítási) szintekkel rendelkeznek.

Kezelés az ESET Endpoint Security 9 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. A **Mindig kezelje a fertőzést** az alapbeállítás felügyelt környezetben.
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.



Ellenőrzésből kizárt fájlkiterjesztések

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 összekeverendők más típusú Kivételekkel:

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

További ThreatSense-paraméterek az új és módosított fájlokhoz – A fertőzés valószínűsége az újonnan létrehozott vagy módosított fájloknál nagyobb, mint a meglévő fájlok esetében, ezért a program további ellenőrzési paraméterekkel ellenőrzi a fájlt. A szokásos vírusdefiníció-alapú ellenőrzési módszerek mellett a szoftver kiterjesztett heurisztikát is alkalmaz, ami még a keresőmotor frissítésének a megjelenése előtt észleli az új kártevőket. Az újonnan létrehozott fájlok mellett az ellenőrzés kiterjed az önkicsomagoló (.sfx) fájlokra és a futtatás közbeni tömörítőkre (belsőleg tömörített végrehajtható fájlokra) is. A tömörített fájlokat a program alapértelmezés szerint a 10. mélységi szintig ellenőrzi, az ellenőrzés a fájlok méretétől függetlenül megtörténik. 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.

A Futtatás közbeni tömörítők, az Önkicsomagoló tömörített fájlok és a Kiterjesztett heurisztika részletes leírását A ThreatSense keresőmotor beállításai című témakör tartalmazza.

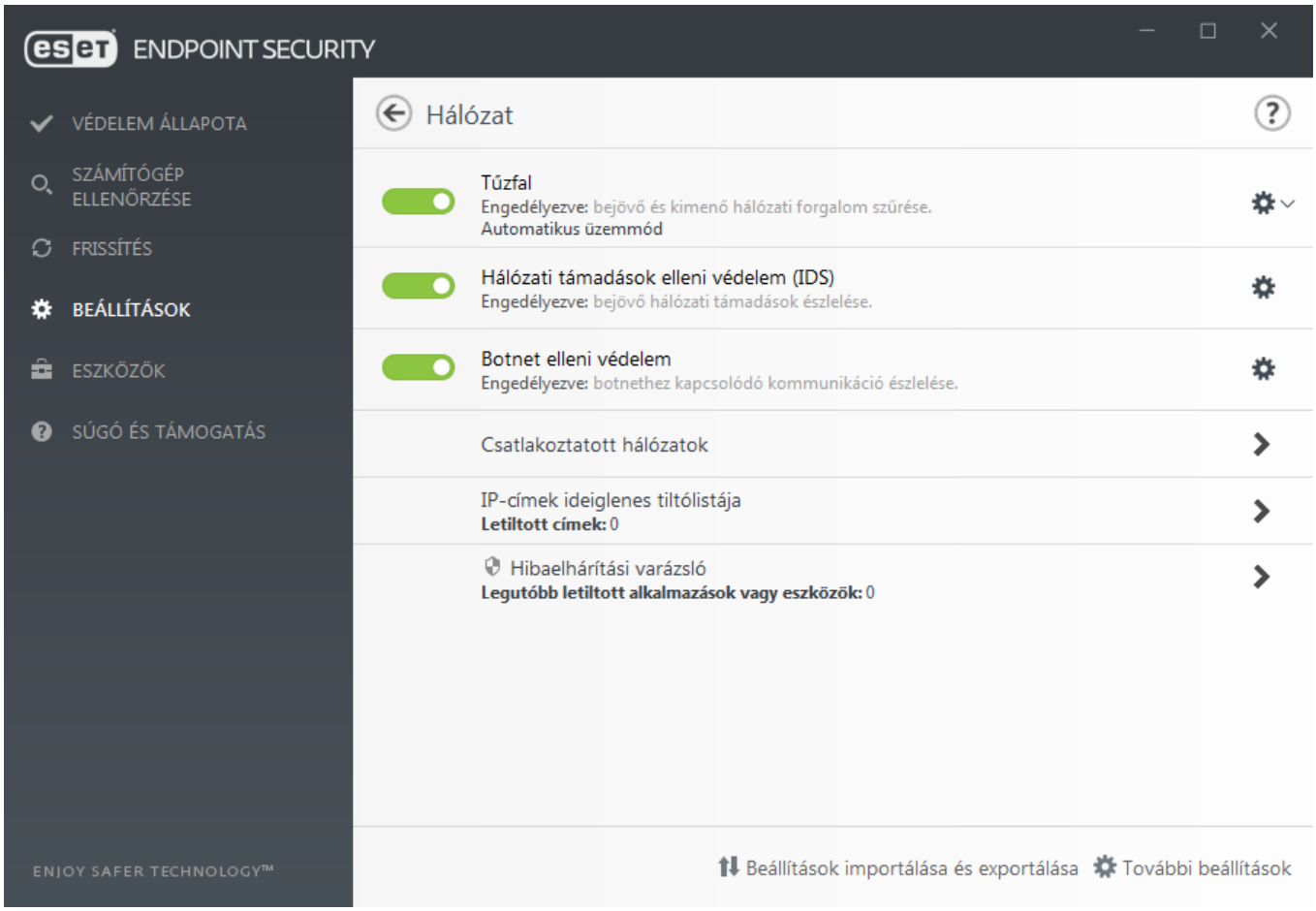
További ThreatSense-paraméterek a futtatott fájlokhoz – Alapértelmezés szerint a program kiterjesztett heurisztikát használ a fájlok futtatásakor. Ha be van jelölve, azt javasoljuk, hogy a rendszer teljesítményére gyakorolt hatás csökkentése végett tartsa meg az optimalizálás és az ESET LiveGrid® engedélyezését.

Hálózat

A **Hálózat** szakaszból gyorsan elérheti a következő összetevőket és beállítások a **További beállítások** lapon:

- **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.
- **Hálózati támadások elleni védelem (IDS)** – Elemzi a hálózati forgalom tartalmát, és védelmet biztosít a hálózati támadásokkal szemben. Minden károsnak számító adatforgalmat letilt. Az ESET Endpoint Security tájékoztatja Önt, ha egy védtelen vezeték nélküli hálózathoz vagy egy gyenge védelemmel rendelkező hálózathoz csatlakozik.
- **Botnet elleni védelem** – Gyorsan és pontosan azonosítja a kártékony programokat a rendszerben. Adott időtartamra letilthatja a botnet elleni védelmet, ha a következő kapcsolóra kattint:  (nem javasolt).
- **Csatlakoztatott hálózatok** – Megjeleníti azokat a hálózatokat, amelyekhez hálózati adapterek vannak csatlakoztatva. Kattintson a fogaskereket ábrázoló ikonra ⚙ annak a hálózatnak a védelmi típusának kiválasztásához, amelyhez csatlakozik. Az egyes hálózati adapterek, valamint a hozzájuk rendelt tűzfalprofil és megbízhatósági zóna megtekintéséhez kattintson a **Csatlakoztatott hálózatok** > **Hálózati adapterek** elemre. Részletesebb információkért olvassa el a Hálózati adapterek című témakört.

- **IP-címek ideiglenes tiltólistája** – A hivatkozásra kattintva megtekintheti azokat az IP-címeket, amelyeket támadások forrásaként észlelt a program, és felvett a tiltólistára, hogy bizonyos időre letiltsa a kapcsolatokat. 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.



Kattintson a **Tűzfal** melletti fogaskerék ikonra az alábbi beállítások megnyitásához:

- **Konfigurálás** – Megnyitja a Tűzfal ablakot a További beállítások párbeszédpanelen, ahol megadhatja, hogy a tűzfal hogyan kezelje a hálózati kommunikációt.
- **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.
- **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. Amikor a hálózati forgalom szűrése ebben a módban van, kattintson **A tűzfal engedélyezése** elemre a tűzfal újbóli engedélyezéséhez.
- **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).

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.

A Windows tűzfal Csoportházirenddel (GPO) konfigurált szabályait a rendszer nem értékeli ki.

Szűrési üzemmód

A szűrési üzemmódtól függően változik a tűzfal működése. A szűrési üzemmódok a szükséges felhasználói beavatkozás szintjét is meghatározzák.

Az ESET Endpoint 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 Endpoint 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.

A Profilok csoportban testre szabhatja az ESET Endpoint Security Tűzfal viselkedését, ha különböző szabálykészleteket definiál a különféle helyzetekhez.

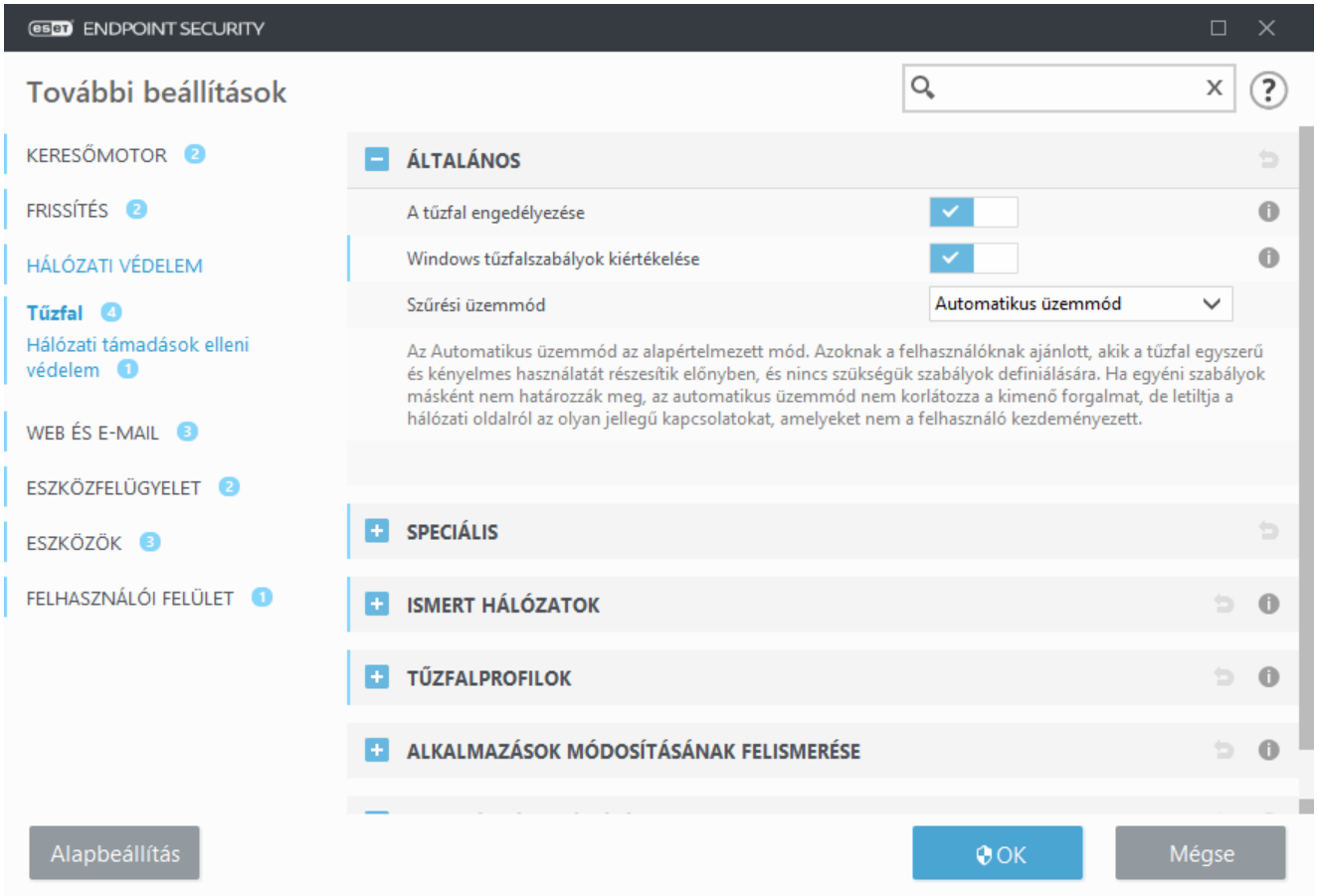
Speciális

Szabályok

A szabályok beállítási párbeszédpanelén megtekintheti az egyes alkalmazások által a megbízható zónákban és az interneten generált forgalomra vonatkozó összes szabályt.

Zónák

Egy-egy zóna olyan hálózati címek gyűjteménye, amelyek egy logikus csoportot alkotnak.



Ha Botnet-támadás érte a számítógépét, létrehozhat egy IDS-szabályt. A kivételek a **További beállítások** (F5) > **Hálózatvédelem** > **Hálózati támadások elleni védelem** > **IDS-szabályok** elemet kiválasztva, majd a **Szerkesztés** elemre kattintva módosíthatók.

Tanuló mód

A tanuló mód a rendszerben létesített minden kommunikációhoz automatikusan létrehoz és ment egy szabályt. Ebben a folyamatban nincs szükség felhasználói beavatkozásra, mert az ESET Endpoint 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 Endpoint 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. (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

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.

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 Endpoint Security ellenőrzi a hálózati forgalom tartalmát és blokkolja a jelszó-találgatási támadások keretében végzett próbálkozásokat.

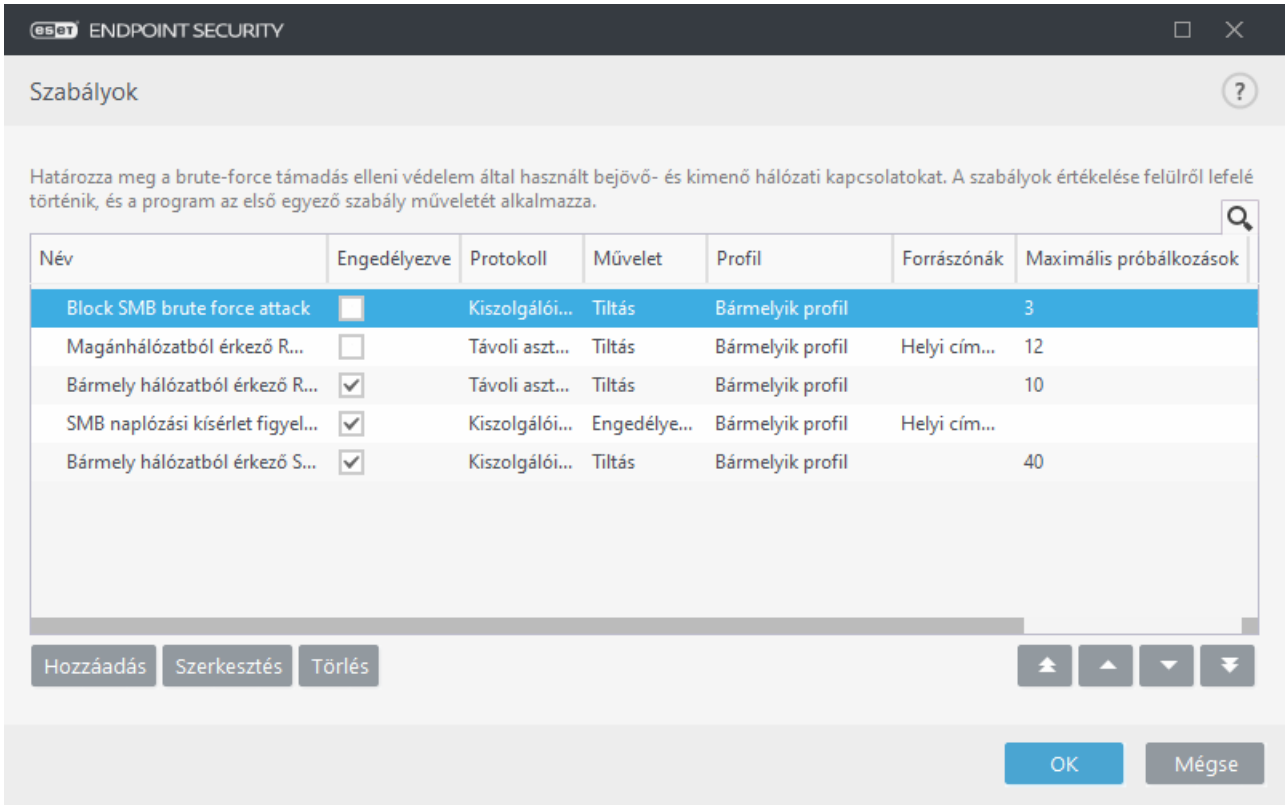
Szabályok – Lehetővé teszik a bejövő és kimenő hálózati kapcsolatok szabályainak létrehozását, szerkesztését és megtekintését. További információkért tekintse meg a Szabályok fejezetet.

Kivételek – Az IP-cím vagy az alkalmazás elérési útja által meghatározott kizárt észlelések listája. A kizárásokat az ESET PROTECT konzolon hozhatja létre és szerkesztheti. További információkért tekintse meg a Kivételek című 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.

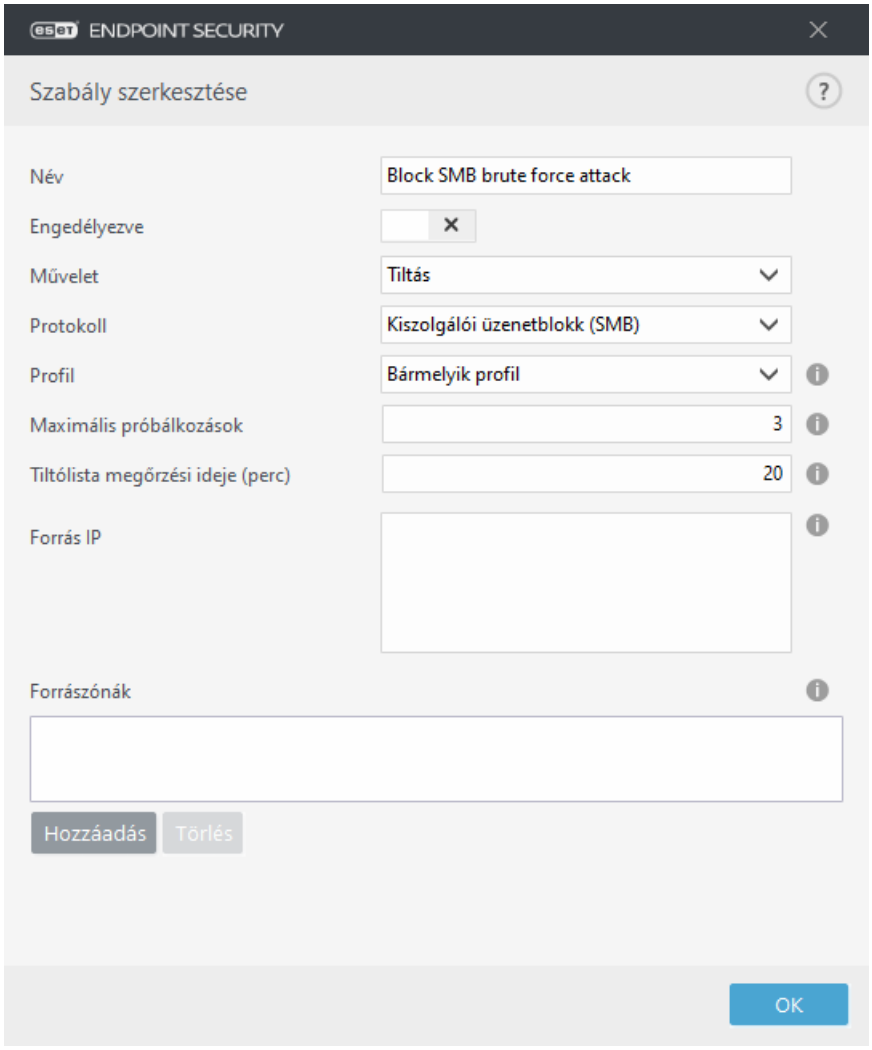
A brute-force támadás elleni védelem kezelése



- **Hozzáadás** – Erre kattintva létrehozhat egy új brute-force támadásvédelmi szabályt.
- **Szerkesztés** – Erre kattintva szerkeszthet egy meglévő brute-force támadásvédelmi szabályt.
- **Eltávolítás** – Válassza ki, majd kattintson, ha egy meglévő kivételt szeretne eltávolítani az IDS-kivételek listájáról.
- **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.

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.

Kivételek

A Brute-force kizárások felhasználhatók a Brute-force észlelésének elfojtására bizonyos kritériumok esetén. Ezek a kizárások az ESET PROTECT segítségével hozhatók létre a Brute-force észlelés alapján.

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. Több címet vesszővel kell elválasztani.

A kizárások kezelése

A kizárások akkor jelennek meg, ha egy rendszergazda Brute-force kivételeket hoz létre az ESET PROTECT Webkonzolban. A kivételek tartalmazhatnak csak engedélyezési szabályokat, és kiértékelésük az IDS-szabályok előtt történik meg.

Speciális szűrési beállítások

A Tűzfal és a Hálózati támadások elleni védelem szakaszban speciális szűrőbeállítások konfigurálhatók a számítógépre leselkedő támadások és biztonsági rések észleléséhez.

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.

A tűzfalmodul típusától vagy verziójától, valamint az operációs rendszer verziójától függ, hogy a **További beállítások** (F5) > **Hálózati védelem** > **Tűzfal** és a **További beállítások** (F5) > **Hálózati védelem** > **Hálózati támadások elleni védelem** lapon milyen beállítások állnak rendelkezésre.

Engedélyezett szolgáltatások

E csoport beállításaival egyszerűbben konfigurálható a számítógép szolgáltatásaihoz a megbízható zónából való hozzáférés. Számos közülük előre definiált tűzfalszabályokat engedélyez vagy tilt le.

- **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 távoli eljáráshívás (RPC) engedélyezése a megbízható zónában** – A jelölőnégyzet bejelölésével engedélyezhetők a Microsoft RPC protokollhoz kapcsolódó porthozzárendelő és DCOM szolgáltatáson keresztül létesített kapcsolatok a megbízható zónán belül.
- **Távoli asztal engedélyezése a megbízható zónában** – Ezt a jelölőnégyzetet 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. Tekintse meg azt is, hogyan engedélyezhetők RDP-kapcsolatok a megbízható zónán kívül.

- **Naplózás engedélyezése csoportcímes küldési csoportokba az IGMP protokollon keresztül** – Ezzel a jelölőnégyzettel 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** – A jelölőnégyzet 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-csomagokon 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 igénybe vétele nélkül. Ezzel a beállítással engedélyezhetők a bejövő, csoportos címzésű DNS-kérések a tűzfalon keresztül a megbízható zónából.
- **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

- **SMB protokoll** – Számos biztonsági problémát észlel és blokkol az SMB protokollban, nevezetesen az alábbiakat:

- **Engedélyezetlen szerverekről érkező hitelesítéses támadás észlelése** – Védelmet nyújt a felhasználói hitelesítő adatok megszerzése érdekében a hitelesítés során alkalmazott szerverkérdéses támadásokkal szemben.

- **IDS elkerülésének észlelése a folyamatok közötti kommunikáció megnyitásakor** – Az MSRPC nevesített csövek megnyitásához használt ismert elkerülési technikák felismerése az SMB protokollban.

- **Gyakori biztonsági rések és kitettségek felismerése** – Az SMB protokollon keresztüli különféle támadások, férgek, biztonsági rések és kitettségek használt felismerési módszerei. A gyakori biztonsági rések és kitettségek (CVE-k) azonosítóiról a cve.mitre.org szervezet webhelyén talál részletesebb információkat.

- **RPC protokoll** – Észleli és letiltja a különféle gyakori biztonsági réseket és kitettségeket az elosztott számítógépes környezethez (DCE) kifejlesztett távoli eljáráshívási rendszerben.
- **RDP protokoll** – 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 kliens kérelmeket 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

- **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. 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. Az MSRPC az elosztott számítógépes környezet (DCE) távoli eljáráshívási (RPC) mechanizmus megvalósítása a Microsoft által. Az MSRPC használhat továbbá az átvitelhez az SMB (hálózati fájlmegosztási) protokollba továbbított nevesített csöveket (ncacn_np transport). Az MSRPC szolgáltatások a Windows rendszerek távoli hozzáféréséhez és kezeléséhez szükséges felületeket biztosítanak. Mostanáig számos biztonsági rést fedeztek fel és használtak ki a Windows MSRPC rendszerében (Conficker féreg, Sasser féreg stb.). Tiltsa le a kommunikációt azokkal az MSRPC szolgáltatásokkal, amelyekre nincs szüksége, így csökkentheti a biztonsági kockázatokat (ilyen például a kódok távoli futtatása vagy a szolgáltatáshibát okozó támadások).

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.

> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> - IDS-szabályok létrehozása kliensszámítógépeken az ESET Endpoint Security szolgáltatásban
> - IDS-szabályok létrehozása kliensszámítógépekhez az ESET PROTECT szolgáltatásban

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. Több címet vesszővel kell elválasztani.
- **Tiltás** – Minden rendszerfolyamathoz saját alapértelmezett viselkedés és hozzárendelt művelet (tiltás vagy engedélyezés) tartozik. Ha felül szeretné bírálni az ESET Endpoint Security alapértelmezett viselkedését, a legördülő menü segítségével letilthatja vagy engedélyezheti azt.
- **Értesítés** – Válassza ki az Igen beállítást, ha szeretne kapni asztali értesítéseket a számítógépén. A Nem beállítást válassza, ha nem szeretne asztali értesítéseket kapni. A rendelkezésre álló lehetőségek az Alapértelmezett/Igen/Nem.
- **Napló** – Válassza ki az **Igen** beállítást, ha naplózni szeretné az eseményeketESET Endpoint Security naplófájlokba. A **Nem** beállítást válassza, ha nem szeretne eseményeket naplózni. A rendelkezésre álló lehetőségek az **Alapértelmezett**/**Igen**/**Nem**.

A lapkivételek akkor jelennek meg, ha egy rendszergazda IDS-kivételeket hoz létre az ESET PROTECT Webkonzolban. Az IDS-kivételek tartalmazhatnak csak engedélyezési szabályokat, és kiértékelésük az IDS-szabályok előtt történik meg.

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, ha egy meglévő kivételt szeretne eltávolítani az IDS-kivételek listájáról.
-  **Tetejére/Fel/Le/Aljára** – A szabályok prioritási szintjének módosítása (a kivételek értékelése fentről 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 riasztást az **Észlelés** legördülő menüben.
3. Kattintson a **...** ikonra, majd válassza ki annak a fájlnak az elérési útvonalát, amelyre alkalmazni szeretné az értesítést.
4. Hagyja meg az **Alapértelmezett** beállítást a **Tiltás** legördülő menüben. Ezzel az ESET Endpoint 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 ismétlődő értesítéseket kapni egy olyan típusú kártevő esetén, amelyet nem tart veszélyesnek:
1. A **Hozzáadás** gombra kattintva adja hozzá az új IDS-kivételt.
2. Válassza ki a kívánt riasztást 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 valaki portszkennelést kísérel meg a hálózatában.

Kártevő – A kártevő neve.

Forrás – A forrás hálózati címe.

Cél – A cél hálózati címe.

Letiltás megszüntetése – IDS-szabály létrehozása a feltételezett kártevőhöz a kommunikáció engedélyezésére vonatkozó beállításokkal.

Letiltás megtartása – Az észlelt kártevő letiltása. Ha a kártevő kommunikációját letiltó beállításokkal szeretne IDS-szabályt létrehozni, válassza a **Ne értesítsen újból** opciót.

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.

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**.

Csatlakoztatott hálózatok

A **Csatlakoztatott hálózat** szakasz az ESET Endpoint Security fő programablakából érhető el a **Beállítások** > **Hálózat** > **Csatlakoztatott hálózatok** elemre kattintva.

Megjeleníti azokat a hálózatokat, amelyekhez hálózati adapterek vannak csatlakoztatva. Miután a hálózatnév alatti hivatkozásra kattintott, a rendszer arra kéri, hogy válasszon ki egy védelmi típust (szigorú vagy engedélyezett) a hálózathoz, amelyhez a hálózati adapter segítségével kapcsolódik. A fogaskerékre kattintva, a **További beállításokban** is módosíthatja ezt a választást. Ez a beállítás megadja, hogy mennyire férnek hozzá a hálózaton lévő számítógépek az Ön gépéhez.

Három hálózati helytípushoz csatlakozhat:

- **Nem megbízható hálózat** – Ez a fajta hálózat nyilvános helyeken használatos, és nem megbízható. Az eszköze nem lesz látható a hálózaton, és Ön sem láthat semmilyen más eszközt a hálózaton. A hálózatfelderítés alapértelmezés szerint le van tiltva nyilvános hálózatok esetében.
- **Megbízható hálózat** – A nyilvános hálózattól eltérően magánhálózaton megoszthat erőforrásokat más számítógépekkel a LAN segítségével. Akkor válassza az **Otthoni vagy irodai hálózat** lehetőséget, ha ismeri és megbízhatónak találja a hálózaton lévő eszközöket.
- **Tartományi hálózat** – A hálózati rendszergazda vezérli ezt a típusú hálózatot, ezért Ön nem választhatja ki vagy módosíthatja ezt a típusú hálózatot. A tartományi hálózat akkor észlelhető, ha a helyi számítógép tagja egy Active Directory Domain Services szolgáltatásnak. A helyi számítógép az adott tartomány egyik hálózati kapcsolatán keresztül tudja hitelesíteni a tartományvezérlőjét.

A hálózati hely kiválasztásával biztosítható, hogy a számítógép mindig a megfelelő biztonsági szintre legyen

beállítva.

Ha a **Hálózati adapterek** lehetőségre kattint az ablak jobb alsó sarkában, megtekintheti az egyes hálózati adaptereket és a hozzájuk rendelt tűzfalprofilt és megbízható zónát. Részletesebb információkért olvassa el a Hálózati adapterek című témakört.

> A **Windows-beállítások használata** lehetőség választása esetén nem jelenik meg egy ablak, és a program automatikusan a Windows-beállításoknak megfelelően fogja megjelölni a hálózatot, amelyhez kapcsolódik. A beállítás hatására bizonyos funkciók (például a fájlmegosztás és a távoli asztal) elérhetővé válnak az új hálózatokról.

Ismert hálózatok

Ha olyan számítógépet használ, amely gyakran csatlakozik nyilvános vagy a szokásos munkahelyi hálózatán kívüli hálózatokhoz, azt ajánljuk, hogy ellenőrizze azoknak az új hálózatoknak a megbízhatóságát, amelyekhez csatlakozni szeretne. Ha vannak definiálva hálózatok, az ESET Endpoint Security a **Hálózati azonosítás** párbeszédpanelen konfigurált számos hálózati paraméter használatával képes felismerni a megbízható (Otthoni/munkahelyi) hálózatokat. A számítógépek gyakran a megbízható hálózathoz hasonló IP-címekkel lépnek be a hálózatokra. Ilyen esetekben előfordulhat, hogy az ESET Endpoint Security megbízhatónak (Otthoni/munkahelyi) tekint egy ismeretlen hálózatot. Ennek elkerülése érdekében tanácsos a **Hálózati azonosítás** használata.

Amikor egy hálózati adaptert csatlakoztat egy hálózathoz vagy újrakonfigurálja az adapter hálózati beállításait, az ESET Endpoint 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 **Nyilvános hálózat** védelmi típust használja. **A program új hálózati kapcsolatot észlelt** párbeszédpanelen választhat a **Nem megbízható hálózat**, az **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: Windows-beállítások használata, Felhasználó megkérdezése vagy Megjelölés nyilvánosként.

> 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.

Az ismert hálózatok manuálisan az Ismert hálózatok szerkesztése ablakban konfigurálhatók.

Ismert hálózatok szerkesztése

Az ismert hálózatokat kézzel a **További beállítások** > **Hálózatvédelem** > **Alap** > **Ismert hálózatok** , majd az **Ismert hálózatok** melletti **Szerkesztés** elemre kattintva konfigurálhatja.

Oszlopok

Név – Az ismert hálózat neve.

Védelem típusa – Megjeleníti, hogy a hálózat **Megbízható hálózat**, **Nem megbízható hálózat** vagy **Windows-beállítások használata** értékre 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.

Törlés – Ha el szeretne távolítani egy hálózatot az ismert hálózatok listájáról, jelölje ki, és kattintson a **Törlés** 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 neve** beállítás és a hálózat **Védelem típusa** beállításának értékét (Nem megbízható hálózat, Megbízható hálózat, illetve Windows-beállítások használata). A **Tűzfalprofil** legördülő listában kiválaszthatja a hálózat profilját. Ha a hálózat az **Megbízható hálózat** 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 Endpoint 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.

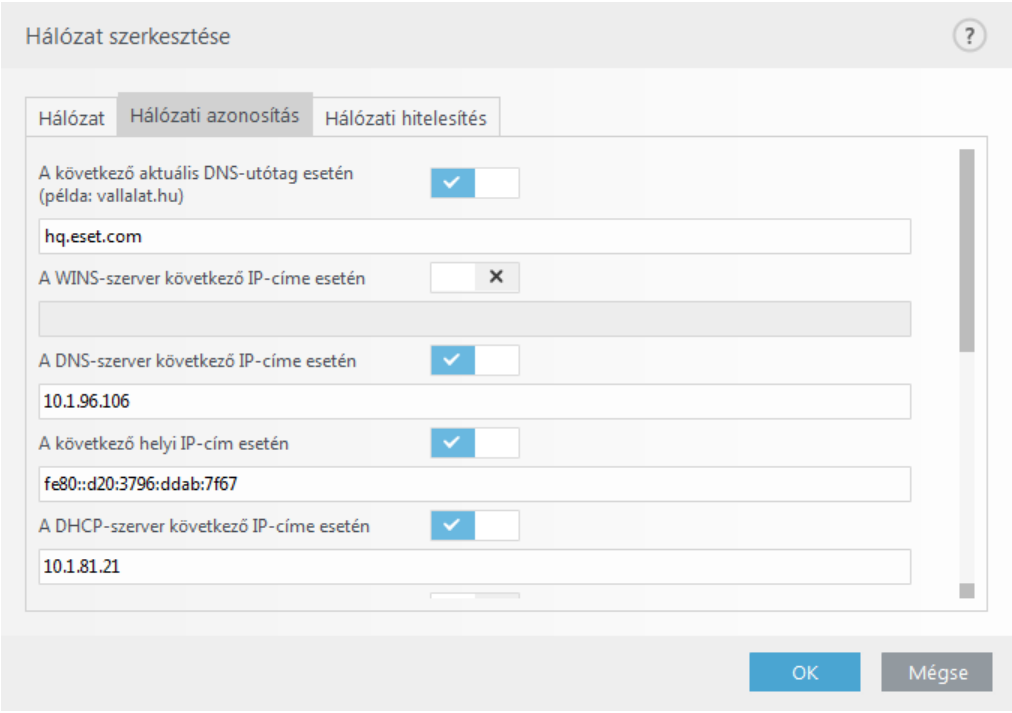
Frissítési profil – Kiválaszthatja azt a profilt, amelyet használni szeretne ehhez a hálózathoz kapcsolódva.

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.



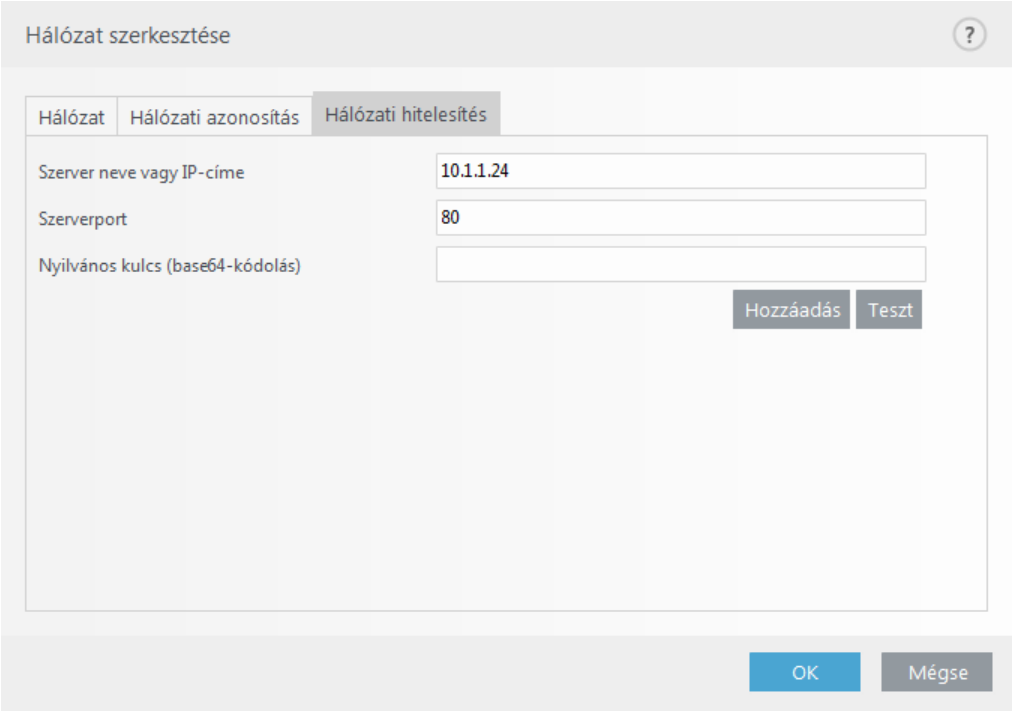
Hálózati hitelesítés

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 névben különbséget kell tenni a kis- és nagybetűk között. 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 hálózat 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 Hálózati hitelesítés csoportban, amikor a tűzfal beállításaiban beállít egy hálózatot.

Tűzfalprofilok

Globális alapértelmezett profil – Ha nincs a hálózatról vagy adapterkonfigurációból származó profil, a rendszer a globális alapértelmezett profilt használja.

Profilok listája – A profilok használhatók az ESET Endpoint 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.

Hálózati adapterekhez rendelt profilok – 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) > **Tűzfal** > **Ismert hálózatok** 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, jelölje ki a profilt az **Alapértelmezett tűzfalprofil** legördülő menüből, és kattintson az **OK** gombra.

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

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 – A hálózati adapter használhatja a csatlakoztatott ismert hálózathoz konfigurált tűzfalprofilt. Ha az adott hálózathoz nem tartozik profil, illetve a hálózati adapter úgy van beállítva, hogy ne használja a hálózat profilját, a rendszer az adapter alapértelmezett profilját használja.

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.

Alkalmazások módosításának felismerése

Az Alkalmazások módosításának felismerése funkció értesítéseket jelenít meg, ha azok a módosított alkalmazások, amelyekhez tartozik tűzfalszabály, kapcsolatot próbálnak létesíteni. Ez azért hasznos, mert így elkerülhető, hogy nem megfelelő szabályokat konfiguráljon egy másik alkalmazás bizonyos alkalmazásokhoz úgy, hogy átmenetileg vagy véglegesen lecseréli az eredeti alkalmazás végrehajtható fájlját a másik alkalmazás végrehajtható fájljára, illetve kártékony célból módosítja az eredeti alkalmazás végrehajtható fájlját.

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.

Módosítások felismeréséből kizárt alkalmazások

Az ESET Endpoint 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.

Szabályok beállítása és használata

A szabályok feltételkészletet jelentenek, amely célja a hálózati kapcsolatok és a feltételekkel társított műveletek tesztelése. A tűzfalszabályokkal megadhatja a különböző típusú hálózati kapcsolatok létrehozásakor végrehajtandó műveleteket. A szabályszűrési beállítások megjelenítéséhez lépjen a **További beállítások** (F5) > **Hálózati védelem** > **Tűzfal** > **Speciális** lapot. Egyes előre megadott szabályok az **engedélyezett szolgáltatások** (Engedélyezett szolgáltatások és további beállítások) jelölőnégyzeteihez tartoznak, és közvetlenül nem, hanem csak a megfelelő jelölőnégyzetekkel kapcsolhatók ki.

Az ESET Endpoint 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 alkalmazások letöltésére a munkaállomásokra. A tűzfallal észlelheti és bonthatja az ilyen kapcsolatokat.

Tűzfalszabályok listája

A tűzfalszabályok listáját úgy tekintheti meg, hogy a **További beállítások** (F5) > **Hálózati védelem** > **Tűzfal** > **Általános** 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.

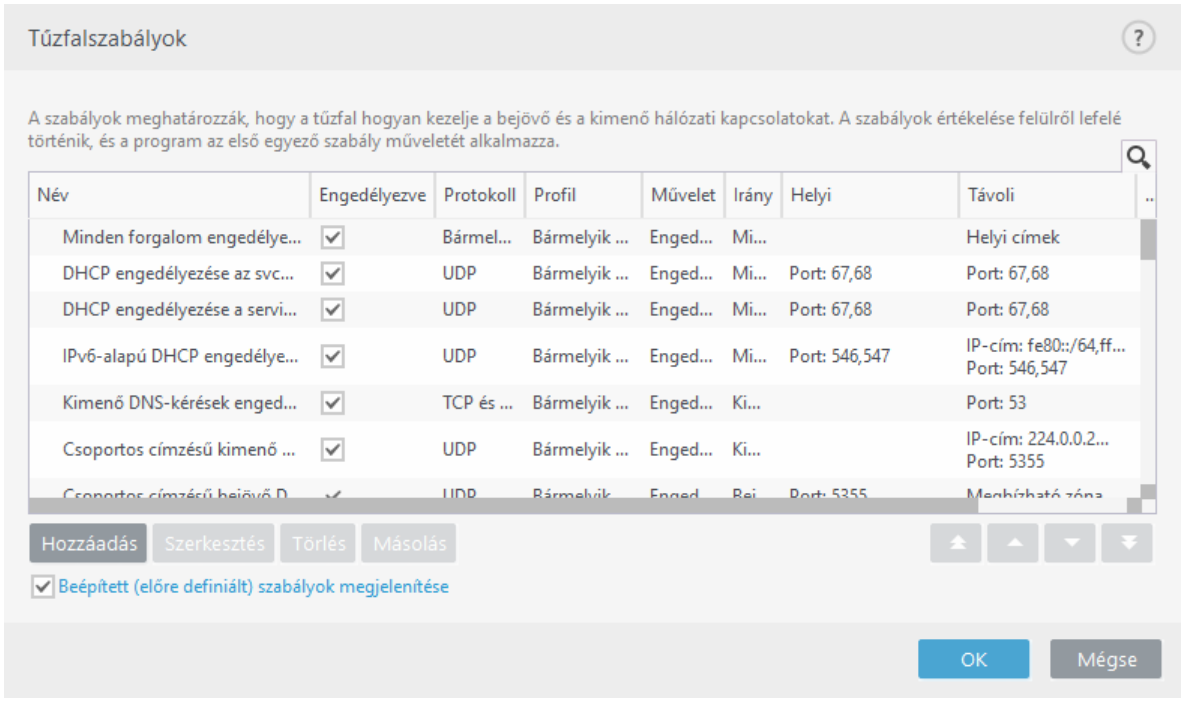
Művelet – Megjeleníti a kommunikáció állapotát (letiltás/engedélyezés/kérdés).

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.

Alkalmazások – 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 Endpoint 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

A tűzfalszabályok szerkesztésére vagy hozzáadására akkor lehet szükség, ha a hálózati beállítások megváltoznak (például a távoli oldal hálózati címe vagy portszáma megváltozott), hogy biztosítva legyen a szabály által érintett alkalmazás megfelelő működése.

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
- Tűzfalszabályok létrehozása vagy szerkesztése az ESET Endpoint Security **szolgáltatásban**
- Kliensszámítógépekre vonatkozó tűzfalszabályok létrehozása vagy szerkesztése a ESET PROTECT szolgáltatásban

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. Lehetővé teszi, hogy egy előre definiált vagy létrehozott zónát adjon hozzá IP-címtartományhoz a **Hozzáadás** gombra kattintva.
- **Távoli** – Ezen a lapon a távoli port (vagy porttartomány) adatai találhatók. Ugyanitt van lehetőség a szabályban érintett távoli IP-címek vagy zónák listájának megadására. Lehetővé teszi, hogy egy előre definiált vagy létrehozott zónát adjon hozzá IP-címtartományhoz a **Hozzáadás** gombra kattintva.

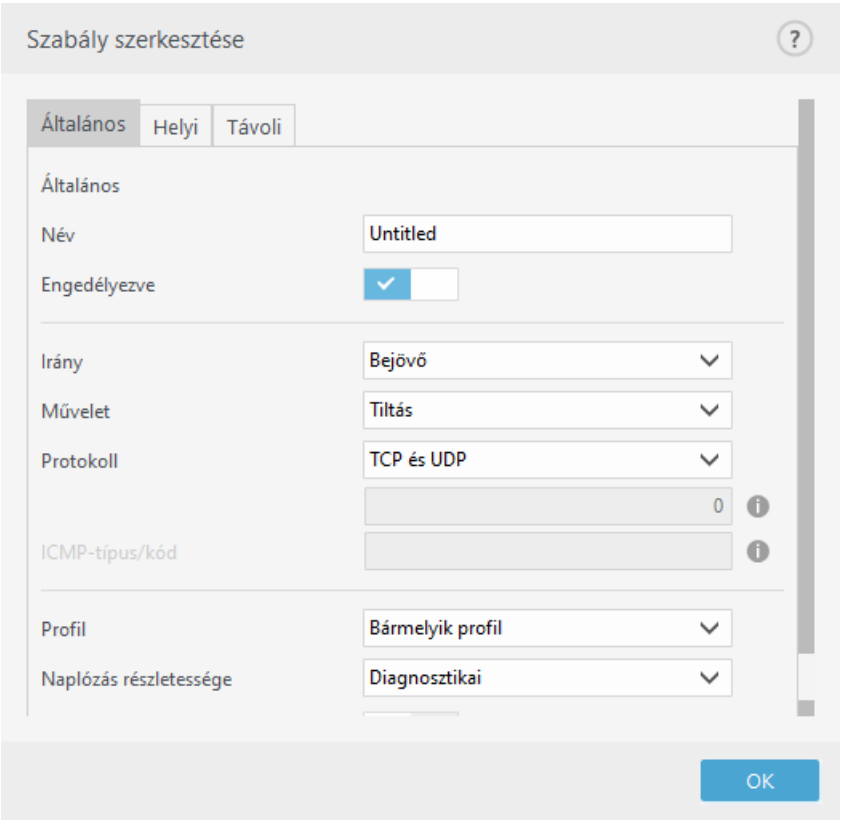
Új szabály létrehozásakor a **Név** mezőben meg kell adni a szabály nevét. Az **Irány** legördülő listában kijelölheti, hogy milyen irányú kommunikációra vonatkozik a szabály, a **Művelet** legördülő listában pedig megadhatja, hogy milyen műveletet hajtson végre a program, amikor egy kommunikáció megfelel 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 **Profilok** 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.



A **Tiltás** művelettel rendelkező és a **Figyelmeztetés** naplózási részletességű tűzfalnaplókat tudjabegyűjteni az ESET PROTECT.

Ebben a példában létrehozunk egy olyan szabályt, amely engedélyezi a Firefox böngészőalkalmazásnak az internethez/helyi hálózathoz való hozzáférést:
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.

Az előre megadott szabályok korlátozottan módosíthatók.

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.

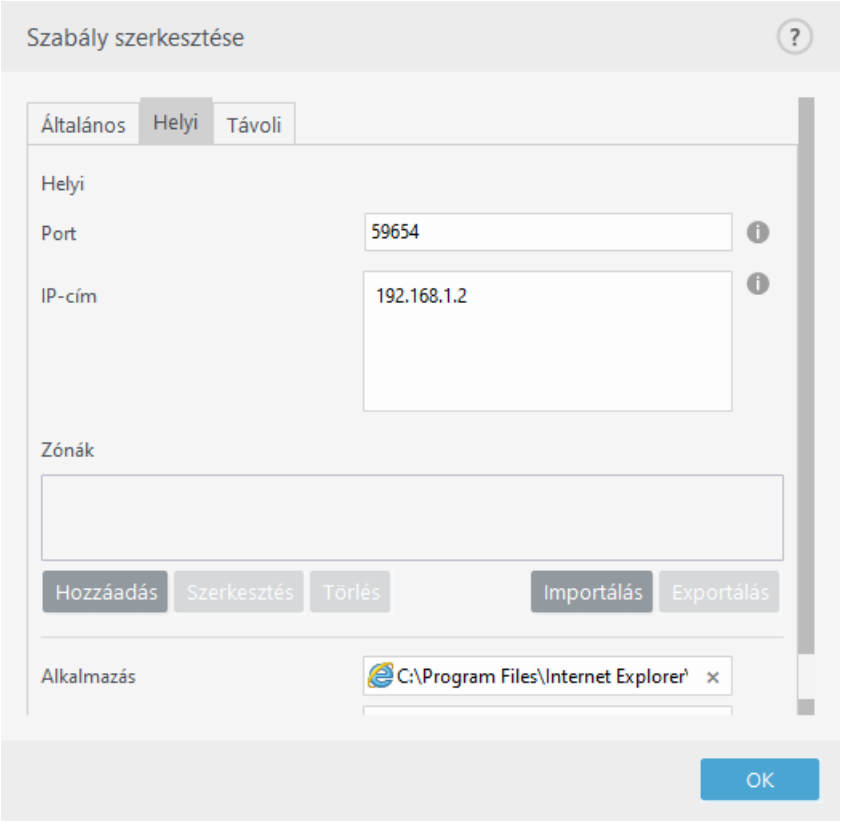
Hozzáadás – Létrehozott zóna hozzáadása a legördülő menüből. A zónák létrehozásáról a Zóna beállításai című témakörben tájékozódhat.

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

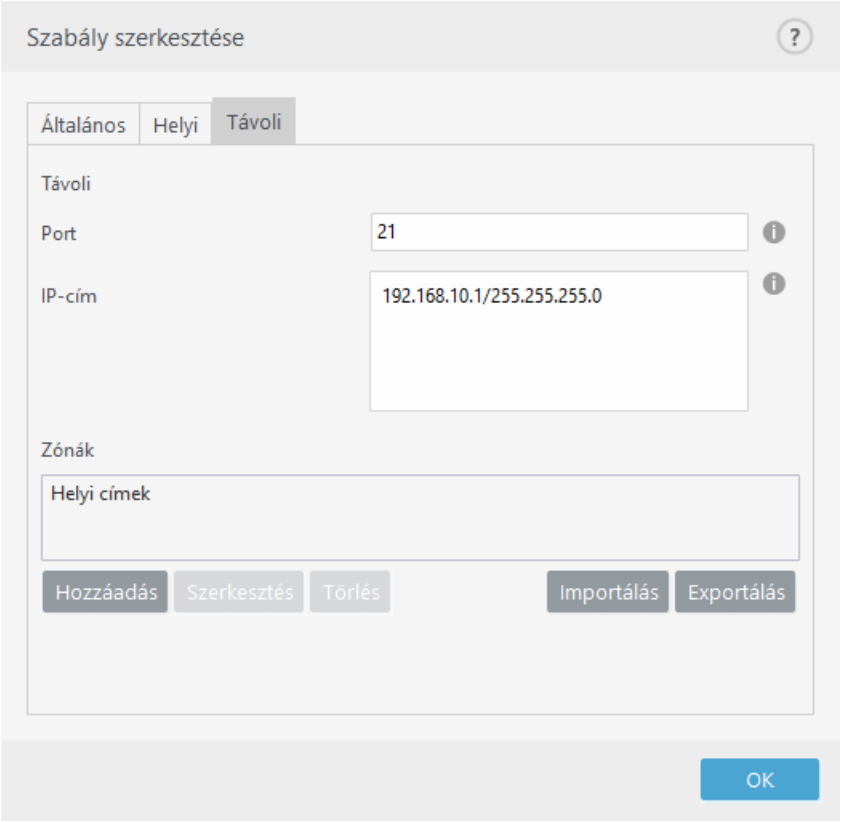
Port – Távoli portszám(ok). Ha nincs megadva szám, a szabály minden portra vonatkozni fog. Egyetlen kommunikációs portot vagy porttartományt is hozzáadhat.

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.



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 Endpoint Security programból a **Beállítások** > **Hálózat** > **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.

Megbízható zóna

A megbízható zóna olyan hálózati címek csoportja, amelyekből a tűzfal engedélyez bizonyos bejövő adatforgalmat az alapértelmezett beállítások használatával. A megbízható zónán belüli fájlmegosztás és távoli asztal beállításai az Engedélyezett szolgáltatások és további beállítások lapon határozhatók meg.

A program a tényleges megbízható zónát minden egyes hálózati adapterhez dinamikusan és külön számítja ki azon hálózat alapján, amelyhez a számítógép jelenleg kapcsolódik. A megbízható zónán belül a Zónaszerkesztőben megadott címeket mindig megbízhatónak tekinti a program. Ha egy hálózati adapter egy ismert hálózathoz kapcsolódik, akkor a **További megbízható címek** listában a hálózathoz konfigurált címek bekerülnek az adapter megbízható zónájába. Ha egy hálózat védelmi típusa Otthoni/munkahelyi, akkor minden közvetlenül csatlakoztatott alhálózat szerepel a megbízható zónában. Az egyes hálózati adapterekhez tartozó tényleges megbízható zóna a **Beállítások** ablak **Hálózat** > **Hálózati adapterek** lapján tekinthető meg.

Zónák konfigurálása

A zóna olyan hálózati címekből áll, amelyek az IP-címek egy logikai csoportját alkotják, és akkor lehet hasznos, ha több szabályban is fel kell használnia 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. A Megbízható zóna hálózati címek csoportja, amelyeket a tűzfal semmilyen módon nem blokkol. A zónák a **További beállítások** > **Hálózati védelem** > **Alap** > **Zónák** elemre, majd a **Zónák** felirat melletti **Szerkesztés** hivatkozásra kattintva konfigurálhatók. Új zóna hozzáadásához kattintson a **Hozzáadás** gombra, írja be a zóna nevét a **Név** mezőbe, adjon meg hozzá leírást a **Leírás** mezőben, és vegyen fel egy távoli IP-címet a **Távoli számítógép címe (IPv4, IPv6, tartomány, maszk)** mezőben. Tekintse meg a Tűzfalzónák című részt is.

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) – Lehetővé teszi újabb távoli címek, címtartományok és alhálózatok megadását.

Törlés – Zóna eltávolítása a listából.

Ne feledje, hogy az előre definiált zónák nem távolíthatók el.

A tűzfal naplója

Az ESET Endpoint Security Tűzfal minden fontos eseményt egy naplófájlba ment, amely közvetlenül a főmenüből tekinthető meg. Kattintson az **Eszközök** > **Naplófájlok** hivatkozásra, majd a **Napló** legördülő listában válassza **Hálózati védelem** elemet. A tűzfal naplózásának engedélyezéséhez keresse meg a **További beállítások** > **Eszközök** > **Naplófájlok** részt, és a naplók minimális részletességét állítsa **Diagnosztikai** értékre. A program ekkor minden elutasított kapcsolatot feljegyez.

A naplófájlok segítségével észlelhetők a hibák és felfedhetők a rendszerbe történő behatolások. Az ESET Tűzfal naplója az alábbi adatokat tartalmazza:

- **Idő** – Az esemény dátuma és időpontja.
- **Esemény** – Az esemény neve.
- **Forrás** – A forrás hálózati címe.
- **Cél** – A cél hálózati címe.
- **Protokoll** – A hálózati kommunikációs protokoll.
- **Szabály/féreg neve** – Az alkalmazott szabály, illetve a féreg neve (ha talált ilyet a program).
- **Alkalmazás** – Az érintett alkalmazás.
- **Felhasználó** – Annak a felhasználónak a neve, aki a fertőzés észlelésének idején be volt jelentkezve.

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.

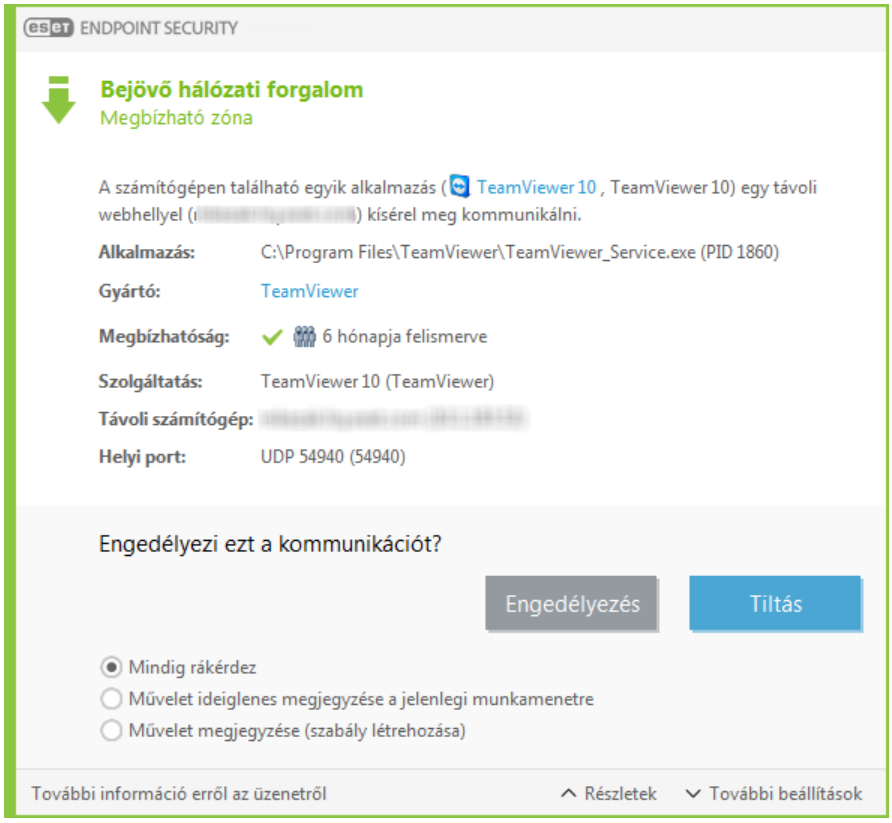
> A biztonsági rés kihasználásáról szóló üzenet naplózásra kerül akkor is, ha az adott rést már kijavították a támadási kísérlet észlelése óta, és hálózati szinten blokkolták, mielőtt tényleges támadásra kerülhetett volna sor.

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 kapcsolathoz. 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. Eldöntheti, hogy engedélyezi vagy elutasítja (letiltja) a kapcsolatot. Ha többször engedélyezi ugyanazt a kapcsolatot a párbeszédpanelen, ajánlatos új szabályt létrehozni a kapcsolathoz. Ehhez jelölje be a **Művelet megjegyzése (szabály létrehozása)** jelölőnégyzetet, és mentse a műveletet új tűzfalszabályként. Ha a tűzfal a jövőben ugyanezt a kapcsolatot észleli, felhasználói beavatkozás nélkül is a meglévő szabályt alkalmazza rá.

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



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

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

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

Az ESET Tűzfallal kapcsolatos problémák megoldása

Ha a telepített ESET Endpoint 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 személyi 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** > **Hálózat** elemre kattintva érhető el.

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
• Tűzfalkivétel hozzáadása a Hibaelhárítási varázslóval

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 tűzfal, engedélyezze a hálózati védelem speciális naplózását a **Diagnosztika** szakaszban a **További beállítások** lapon, amely az **Eszközök** > **Diagnosztika** útvonalon érhető el. Ha a naplóban az látható, hogy a tűzfal nem kívánt elemet tilt le, egy szabályt vagy IDS-szabályt létrehozva orvosolhatja a problémát. Ehhez kattintson a jobb gombbal az adott elemre, és válassza ki a **Ne tiltson le hasonló eseményeket a jövőben** lehetőséget. 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 tűzfal milyen sorrendben tiltotta le a kapcsolatokat. Ezenkívül szabályokat is létrehozhat a naplóból, így pontosan azt teheti, amit szeretne.

Új szabály létrehozása naplóból

Az ESET Endpoint Security új verziója lehetővé teszi új szabály létrehozását a naplóból. A főmenüben kattintson az **Eszközök** > **Naplófájlok** pontra. A legördülő listában válassza ki a **Hálózati védelem** 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 Endpoint Security alkalmazásban az alábbi beállításokat kell megadni:

- a naplózás minimális részletességi szintjét állítsa **Diagnosztikai** értékre a **További beállítások** (F5) > **Eszközök** > **Naplófájlok** részen;
- 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 személyi 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 kivételt 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 Endpoint 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

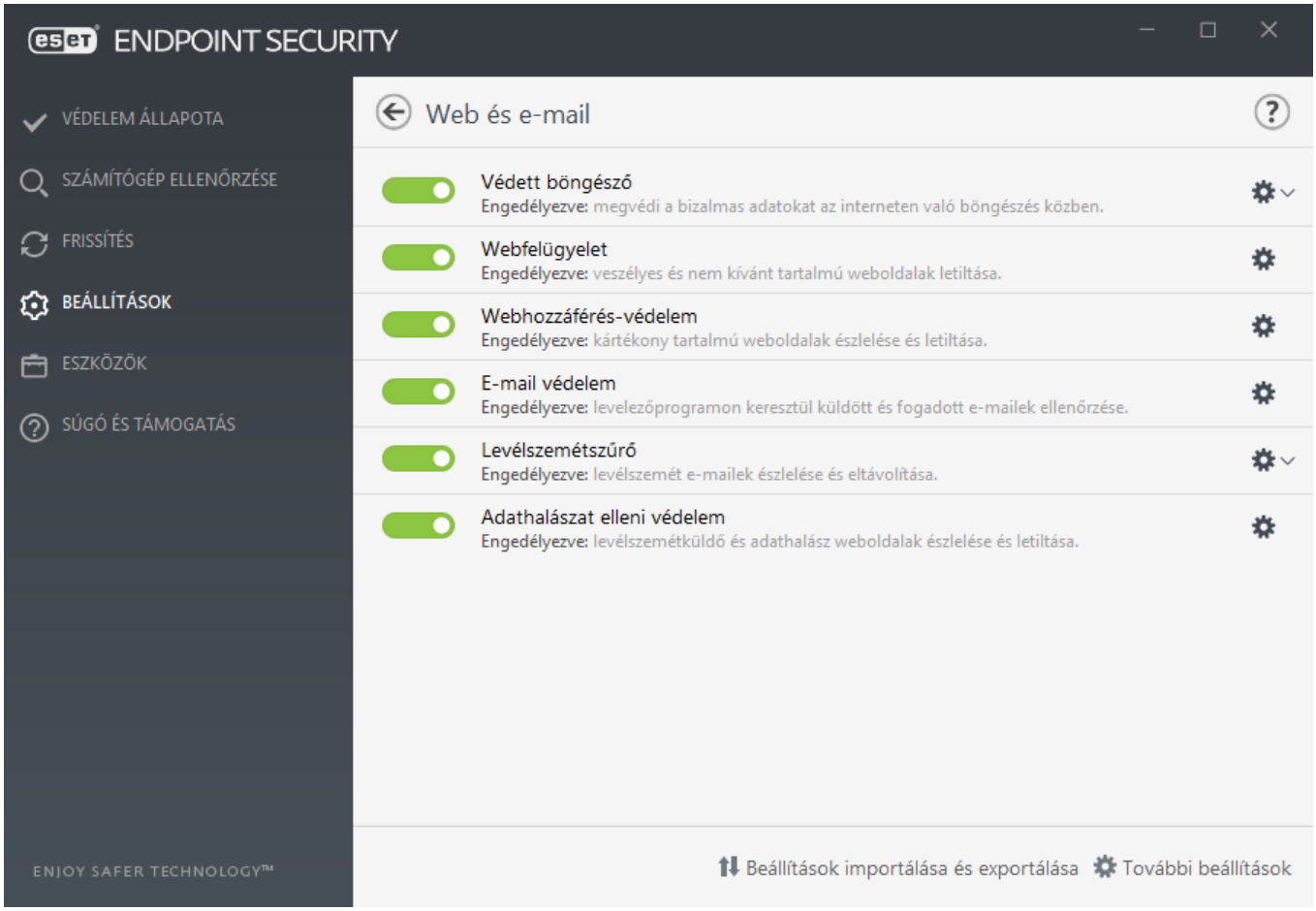
Az SSL-protokollszűrés engedélyezésekor az ESET Endpoint Security meggyőződik arról, hogy a telepített alkalmazások megbíznak abban a módban, ahogyan a program az SSL-szűrést végzi. Ehhez egy tanúsítványt importál azok tanúsítványtárába. Egyes alkalmazások esetében ez nem lehetséges, amíg fut az alkalmazás. 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.

Web és e-mail

A web- és e-mail beállításokat a **Beállítások** > **Web és e-mail** elemre kattintva érheti el. Innen a részletesebb programbeállításokat is elérheti.



Védett böngésző – Megvédi a bizalmas adatokat az interneten való böngészés közben.

A Webfelügyelet modullal konfigurálható beállítások olyan automatizált eszközöket biztosítanak a rendszergazdáknak, amelyekkel megvédhetik munkaállomásaikat, és korlátozásokat állíthatnak be az internetböngészésre vonatkozóan. A Webfelügyelet funkció célja, hogy védelmet biztosítson a nem megfelelő vagy káros tartalmú oldalakhoz való hozzáféréshez. További információt a Webfelügyelet című témakörben talál.

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 Endpoint Security a levelezőprogramtól érkező minden kommunikáció ellenőrzésére képes.

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

A Levélszemétszűrő felirat melletti fogaskerék ikonra ⚙ kattintva az alábbi beállítások jelennek meg:

Konfigurálás – Megnyitja a levélszemétszűrő speciális beállításait.

Felhasználói címlista – Megnyit egy párbeszédpanelt, ahol felveheti, szerkesztheti, illetve törölheti a biztonságosnak vagy nem biztonságosnak tartott e-mail címeket. Az itt definiált szabályok alapján az ezekről a címekről érkező üzeneteket a program nem fogja ellenőrizni, illetve levélszemétként kezelni. A Felhasználó kizárási listája elemre kattintva megnyithat egy párbeszédpanelt, ahol felveheti, szerkesztheti, illetve törölheti az esetleg hamisított és kéretlen levelek küldésére használt e-mail címeket. A kizárási listán szereplő címekről érkező e-maileket a program mindig ellenőrzi.

Az **Adathalászat elleni védelem** további védelmet biztosít azokkal a nem szabályszerű webhelyekkel szemben, amelyek jelszavakat és más bizalmas információkat kísérelnek meg megszerezni. Az adathalászati védelem beállításai a Beállítások munkaablak Web és e-mail csoportjában találhatók. További információt az Adathalászat elleni védelem című témakörben talál.

A web/e-mail/adathalászat elleni védelem/levélszemétszűrő védelmi moduljának átmeneti kikapcsolásához kattintson az  elemre.

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-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 Endpoint Security számos összetevője (Webhozzáférés-védelem, E-mail védelem, Adathalászat elleni védelem, Webfelügyelet) 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.

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*

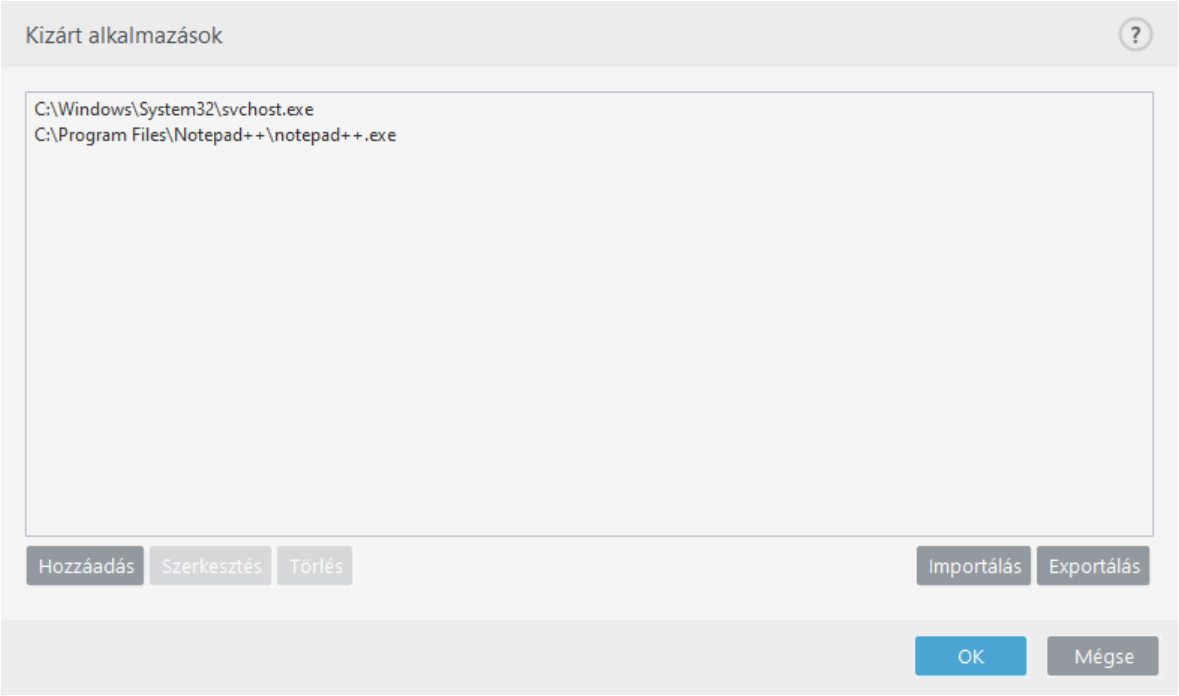
Kizárt alkalmazások

A rendszer nem végez protokollszűrést a listán szereplő hálózati alkalmazások adatforgalmán. Az adott alkalmazásokhoz irányuló és általuk kezdeményezett HTTP/POP3/IMAP-alapú adatforgalmon a program nem végez kártevő-ellenőrzést. Azt ajánljuk, hogy csak azokban az esetekben használja ezt a módszert, amikor a protokollszűrés engedélyezése esetén az alkalmazások nem működnek megfelelően.

Azok az alkalmazások és szolgáltatások, amelyekre már hatással volt a protokollszűrés, automatikusan megjelenek, miután a **Hozzáadás** gombra kattintott.

Szerkesztés – A listában kijelölt bejegyzések szerkesztése.

Törlés – A kijelölt bejegyzések eltávolítása a listáról.



Kizárt IP-címek

A listában szereplő IP-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.

Hozzáadás – Erre a gombra kattintva távoli IP-címet, IP-címtartományt vagy alhálózatot vehet fel, amelyhez szabályt alkalmazott.

Szerkesztés – A listában kijelölt bejegyzések szerkesztése.

Törlés – A kijelölt bejegyzések eltávolítása a listáról.



SSL/TLS

Az ESET Endpoint Security képes kártevőkeresést végezni az SSL protokollt használó kommunikáció tartalmán. Az SSL protokollal védett kommunikáció ellenőrzéséhez többféle 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 engedélyezve van alapértelmezés szerint. Az SSL/TLS-protokollszűrés a **További beállítások** > **Web és e-mail** > **SSL/TLS** lapon, illetve házirend segítségével tiltható le. 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.
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 Endpoint Security viselkedésének testreszabását adott alkalmazásokhoz.

Az **Ismert tanúsítványok listája** lehetővé teszi az ESET Endpoint 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.

> Nem kerül sor a címek szűrésére, ha aktív a **Megbízható tartományokkal való kommunikáció kizárása** beállítás, és a tartomány megbízható.

Legfelső szintű tanúsítvány

Legfelső szintű tanúsítvány – 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.

Tanúsítvány érvényessége

Művelet, ha a tanúsítvány megbízhatósága nem állapítható meg – Bizonyos esetekben a webhelytanúsítvány nem igazolható a megbízható legfelső szintű hitelesítésszolgáltatók (TRCA) tárolójával (például lejárt a tanúsítvány, nem megbízható a tanúsítvány, az adott tartományra nem érvényes tanúsítvány vagy olyan aláírás, amely elemezhető, de nem írja alá megfelelően a tanúsítványt). A legitim webhelyek mindig megbízható tanúsítványokat használnak. Ha nem biztosítanak tanúsítványt, az azt jelentheti, hogy egy támadó visszafejti az Ön kommunikációját, vagy a webhely technikai nehézségekkel küzd.

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 megbízható tanúsítványokat használó webhelyek titkosított kapcsolatait.

Művelet sérült tanúsítványok esetén – A sérült tanúsítvány azt jelenti, hogy a tanúsítvány olyan formátumot használ, amelyet nem ismer fel az ESET Endpoint Security, vagy megsérült (például véletlenszerű adatokkal lett felülírva). Ilyen esetben azt javasoljuk, hogy 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.

> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> • Tanúsítványokkal kapcsolatos értesítések az ESET-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 Endpoint 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 Endpoint Security alkalmazásnak **mellőznie** kell az adott adatforgalmat ahhoz, hogy működőképes maradjon.

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
- Tanúsítványokkal kapcsolatos értesítések az ESET-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 Endpoint 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 – Tanúsítvány betölthető manuálisan *.cer*, *.crt* vagy *.pem* kiterjesztésű fájlként. Kattintson a **Fájl** lehetőségre egy helyi tanúsítvány feltöltéséhez, vagy az **URL-cím** elemre kattintva adja meg egy tanúsítvány online helyét.

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 mentheti a módosításokat, a **Mégse** gombra kattintva pedig kiléphet a módosítások mentése nélkül.

SSL/TLS szűrésű alkalmazások listája

Az **SSL/TLS szűrésű alkalmazások listája** használható az ESET Endpoint 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.

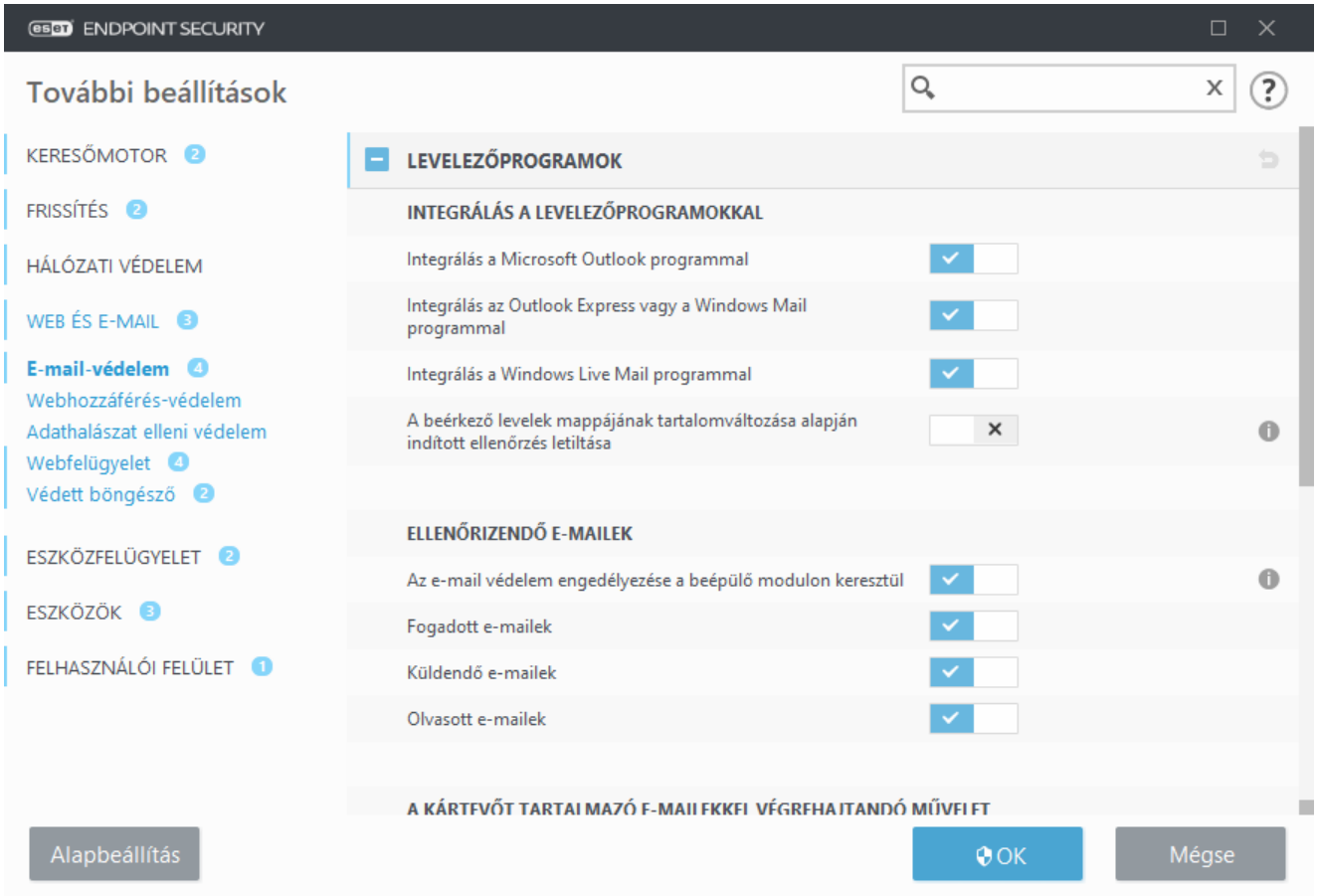
Szerkesztés – Jelölje ki a konfigurálni kívánt tanúsítványt, és kattintson a **Szerkesztés** gombra.

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.

E-mail védelem

Az ESET Endpoint Security és az e-mail-kliens integrálása növeli az e-mailekben található rosszindulatú kódok elleni aktív védelem szintjét. A támogatott levelezőprogramok integrálása az ESET Endpoint Security programban engedélyezhető. Ha integrálva van a levelezőprogramba, az ESET Endpoint 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** > **Levelezőprogramok** lehetőséget választva érheti el.



Ellenőrizendő e-mailek

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

Fogadott e-mailek – Ha engedélyezve van, végbemegy a fogadott e-mailek ellenőrzése.

Küldendő e-mailek – Ha engedélyezve van, végbemegy az elküldött e-mailek ellenőrzése.

Olvasott e-mailek – Ha engedélyezve van, végbemegy az elolvasott e-mailek ellenőrzése.

> 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.

Ellenőrzés megismétlése frissítés után – Ha engedélyezve van, végbemegy a fertőzött e-mailek ismételt ellenőrzése a keresőmotor frissítése után.

Más modulok által végrehajtott ellenőrzések eredményeinek elfogadása – Lehetővé teszi, hogy az e-mail-védelmi modul elfogadja a többi védelmi modultól kapott ellenőrzési eredményt az ismételt ellenőrzés helyett.

Levelezési protokollok

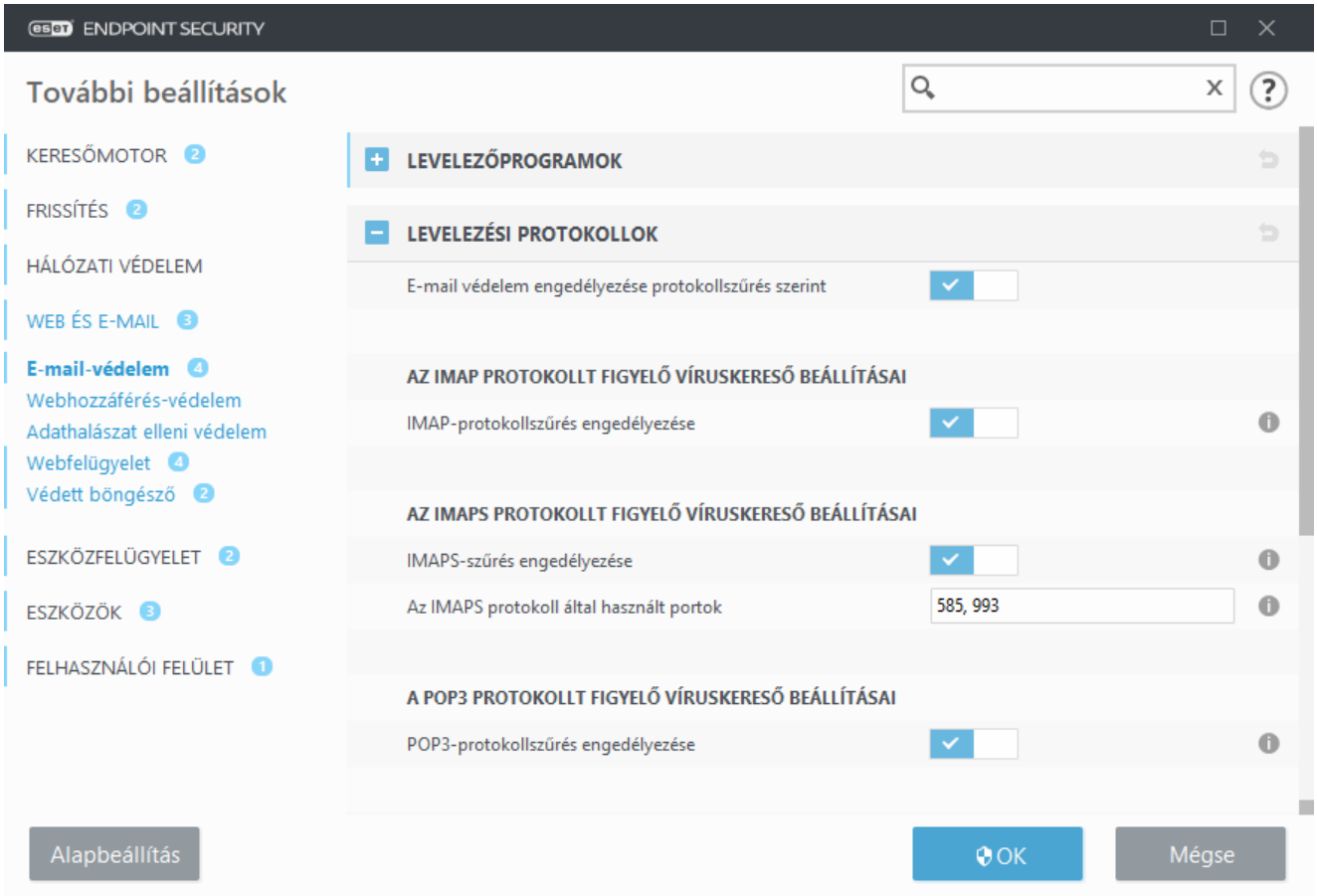
Az IMAP és POP3 a legelterjedtebb protokollok, amelyek segítségével fogadható az e-mail-kommunikáció a levelezőprogramokban. Az IMAP (Internet Message Access Protocol) egy másik internetes protokoll, amely az e-mailek beolvasására szolgál. Az IMAP-nek van néhány előnye a POP3 protokollal szemben, például 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 Endpoint 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 MAPI 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 Endpoint 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 Endpoint 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 a További beállítások szakaszban keresse meg az SSL/TLS csoportot, kattintson a **Web és e-mail** > **SSL/TLS** elemre, majd jelölje be az **SSL/TLS-protokollszűrés engedélyezése** elemet.



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.

Elküldött e-mail tárgyának frissítése – Törölje ennek a jelölőnégyzetnek a bejelölését, ha nem szeretné, hogy az e-mailek védelmét ellátó funkció vírusra utaló figyelmeztetést fűzzön a fertőzött levelek tárgyához. Ezzel a módszerrel egyszerűen, a tárgy alapján szűrheti a fertőzött leveleket (ha ezt a használt levelezőprogram támogatja). Így a címzett számára megnő az üzenetek hitelességi szintje, és fertőzés észlelése esetén értékes információk nyerhetők az adott üzenet vagy feladója veszélyességi szintjéről.

A fertőzött e-mailek tárgyához hozzáfűzendő szöveg – A 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.

Integrálás a levelezőprogramokkal

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.

Speciális beállítások

Mellékletkezelés optimalizálása – Ha az optimalizálás le van tiltva, azonnal végbemegy az összes melléklet ellenőrzése. Amikor le van tiltva, lassabb lehet az e-mail-kliens működése.

Speciális levelezőprogram-feldolgozás – Kapcsolja ki ezt a funkciót, ha a levelezőprogram használatakor a rendszer lassulását tapasztalja.

Microsoft Outlook-eszköztár

A Microsoft Outlook védelme beépülő modulként működik. Az ESET Endpoint 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 Endpoint Security – Az ikonra kattintva megnyithatja az ESET Endpoint Security főablakát.

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 Endpoint 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 Endpoint Security – Az ikonra kattintva megnyithatja az ESET Endpoint Security főablakát.

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

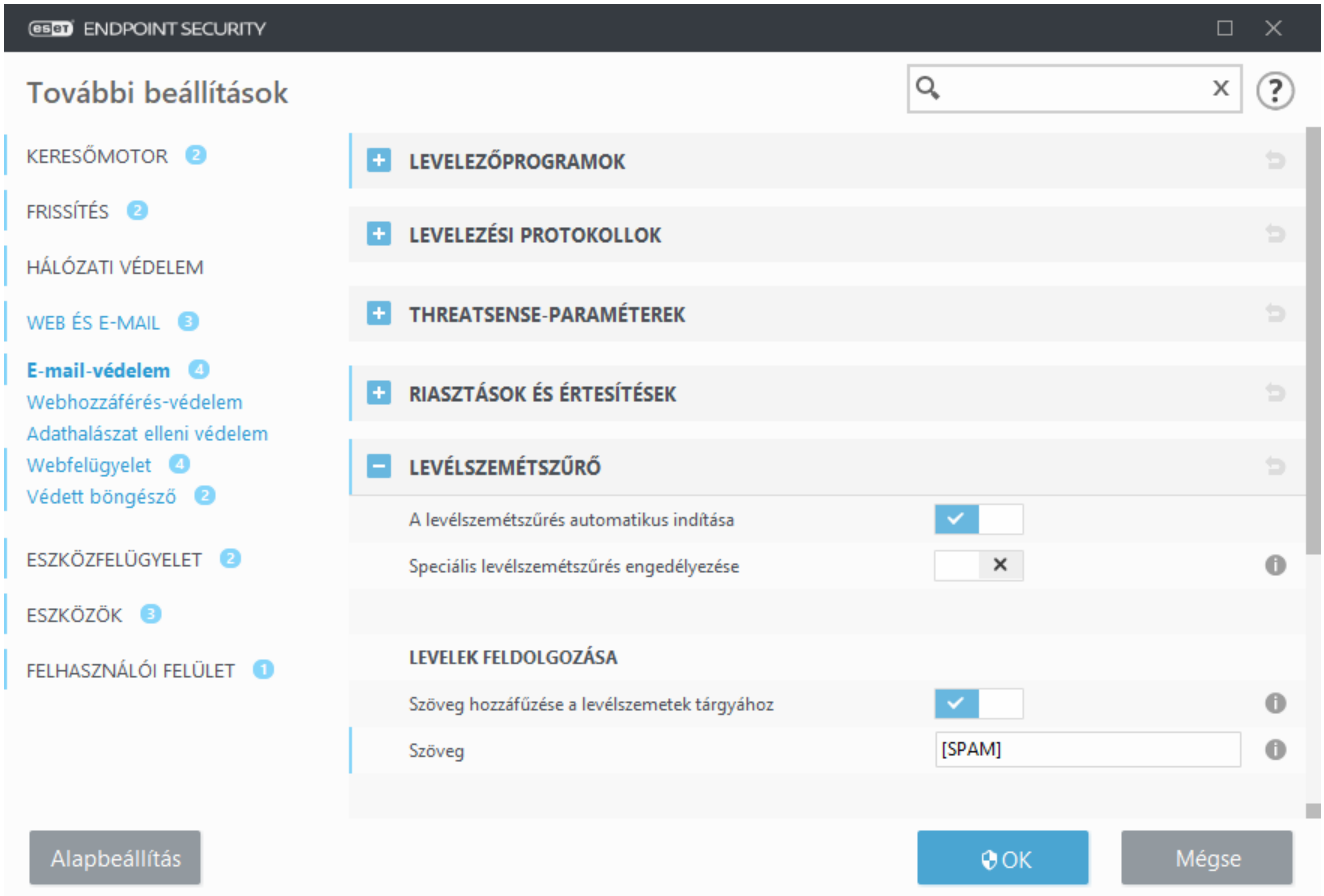
Az aktuális mappában lévő összes üzenetet – A levelezőprogramban megjelenített mappa üzeneteinek ellenőrzése.

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.

Levélszemétszűrő

Az elektronikus kommunikáció egyik legnagyobb problémáját a kéretlen levelek, más néven levélszemét áradata jelenti. A levélszemét a teljes levelezés mintegy 50 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 levélszemét észlelésének egyik fontos elve a kéretlen levél felismerése az előre definiált, megbízható címeket (engedélyezőlista), illetve a tiltott címeket (tiltólista) tartalmazó listák alapján. A névjegyzékében található címeket a program automatikusan hozzáadja az engedélyezőlistához, illetve további címeket is megjelölhet biztonságosként.

A levélszemét észlelésének elsődleges módszere az e-mail tulajdonságainak ellenőrzése. A beérkezett üzeneteket

a program különböző alapvető feltételek (üzenetdefiníciók, statisztikai heurisztika, felismerőalgoritmusok és egyéb egyedi módszerek) alapján ellenőrzi, és az eredményként kapott indexérték határozza meg, hogy az üzenet levélszemét-e.

A levélszemétszűrés automatikus indítása – 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 Endpoint Security levélszemétszűrője lehetővé teszi, hogy a levelezőlisták kezelése érdekében különböző paramétereket állítson be. A beállítások az alábbiak:

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

- **Nincs** – A levélszemétszűrőtől származó pontszám nem kerül bele a naplóba.
- **Átminősítve és levélszemétként megjelölve** – Az opciót bejelölve rögzítheti a levélszemétként 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 Endpoint Security támogatja a levélszemétszűrést a Microsoft Outlook, az Outlook Express, a Windows Mail és a Windows Live Mail esetén.

Levélszemétszűrő névjegyalbumok

Az ESET Endpoint Security levélszemétszűrő szolgáltatása lehetővé teszi a névjegyalbumok különböző paramétereinek a beállítását.

Névjegyalbumok

Felhasználói címlisták engedélyezése – A jelölőnégyzet bejelölésével aktiválhatja a felhasználók által a saját levelezőprogramjukban létrehozott névjegyalbumot.

Globális címlisták engedélyezése – A jelölőnégyzet bejelölésével aktiválhatja az összes felhasználó által megosztott globális névjegyalbumot a munkaállomáson, az e-mail rendszer könyvtárszolgáltatását. A globális címlista az összes e-mail felhasználóra, címzettcsoportra és erőforrásra vonatkozó információkat tartalmazza.

Felhasználó engedélyezőlistája – Kapcsolatok listája, amelyen felvehet, szerkeszthet vagy törölhet olyan címeket, amelyek biztonságosnak számítanak, és amelyekről a felhasználó meg szeretné kapni az üzeneteket.

Felhasználó tiltólistája – Partnerek listája, amelyen felvehet, szerkeszthet vagy törölhet olyan címeket, amelyek nem számítanak biztonságosnak, és amelyekről a felhasználó nem szeretne üzeneteket kapni.

Felhasználó kizárási listája – Ez a kapcsolatlista olyan e-mail címeket tartalmaz, amelyek hamisítottak lehetnek, és amelyeket levélszemét küldésére használhatnak. Lásd még: Kizárási lista.

Globális engedélyezőlista/tiltólista/kizárási lista – Ezekkel a listákkal levélszemét-házirendek alkalmazhatók az összes olyan felhasználóra, akik az ESET Endpoint Security terméket használják ezen a munkaállomáson. Az ESET Endpoint Security távoli felügyeletekor az ESET PROTECT-/ECA-házirend érvényesül az összes hozzárendelt munkaállomáson.

Automatikus felvétel a felhasználó engedélyezőlistájára

Címek hozzáadása a névjegyalbumból – Címek felvétele a névjegyalbumból az engedélyezőlistára.

Címzettek címeinek hozzáadása a kimenő levelekből – A címzettek címeinek felvétele a kimenő levelekből az engedélyezőlistára.

Címek hozzáadása a JÓ levéllé átminősített levelekből – A feladók e-mail címének felvétele a JÓ levéllé átminősített levelekből az engedélyezőlistára.

Automatikus felvétel a felhasználó kizárási listájára

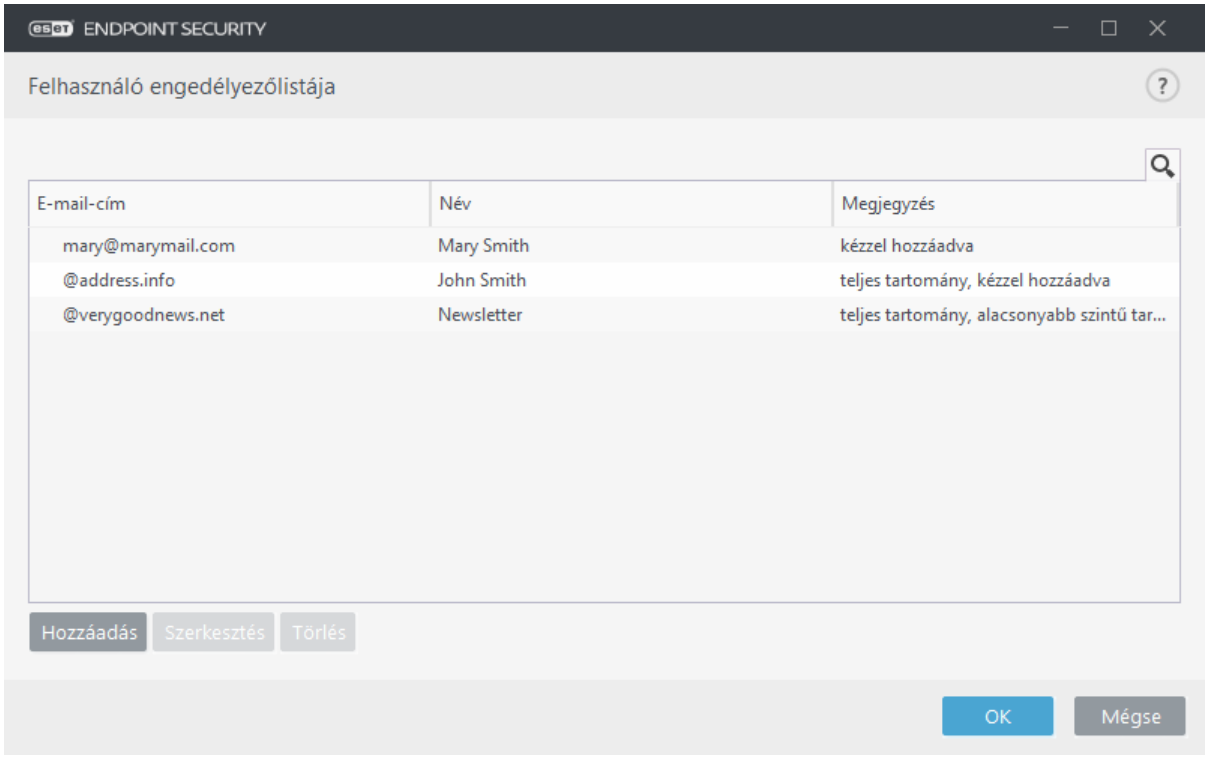
Címek hozzáadása saját fiókokból – Címei felvétele a meglévő levelezőprogram fiókjaiból a kizárási listára.

Tiltólista/Engedélyezőlista/Kizárási lista

Az ESET Endpoint Security a kéretlen e-mailek elleni védelem biztosítására speciális listák segítségével teszi lehetővé az e-mail címek minősítését. Az engedélyezőlista a biztonságosnak tartott e-mail címeket tartalmazza. Az engedélyezőlistán szereplő felhasználók üzenetei mindig elérhetők a beérkező levelek mappájában. A tiltólistán szereplő e-mail címek levélszemétküldőnek minősülnek, és a program megfelelő jelzéssel látja el az itt szereplő feladóktól érkező üzeneteket. A kizárási lista olyan e-mail címeket tartalmaz, amelyek esetén a program mindig

ellenőrzi, hogy az e-mail levélszemét-e, emellett azonban olyan kéretlen e-mail üzenetekből származó címeket is tartalmazhat, amelyeket a program kezdetben nem ismert fel levélszemétként.

Minden lista szerkeszthető az ESET Endpoint Security főablakában a **További beállítások** > **Web és e-mail** > **E-mail védelem** > **Levélszemétszűrő névjegyalbumok** elemre, majd az egyes listák párbeszédpaneljén a **Hozzáadás**, **Szerkesztés** vagy **Eltávolítás** gombra kattintva, illetve a **Beállítások** > **Web és e-mail** lehetőséget választva, miután a fogaskerék ikonra kattintott a **Levélszemétszűrő** felirat mellett.



Az ESET Endpoint Security alapértelmezés szerint a támogatott levelezőprogramok névjegyalbumában szereplő összes címet hozzáadja az engedélyezőlistához. A tiltólista alapértelmezés szerint üres. A kizárási lista alapértelmezés szerint csak a felhasználó saját e-mail címeit tartalmazza.

Tiltólista/engedélyezőlista/kivételcímek hozzáadása/szerkesztése

Ezen a párbeszédpanelen nyílik lehetőség az engedélyezőlista és a tiltólista bejegyzéseinek felvételére és módosítására. Nyissa meg az ESET Endpoint Security fő programablakát itt: **További beállítások** > **Web és e-mail** > **E-mail védelem** > **Levélszemétszűrő névjegyalbumok**.

E-mail cím – A felvenni vagy módosítani kívánt e-mail cím.

Név – A bejegyzés neve.

Teljes tartomány – A jelölőnégyzet bejelölése esetén a bejegyzés 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.

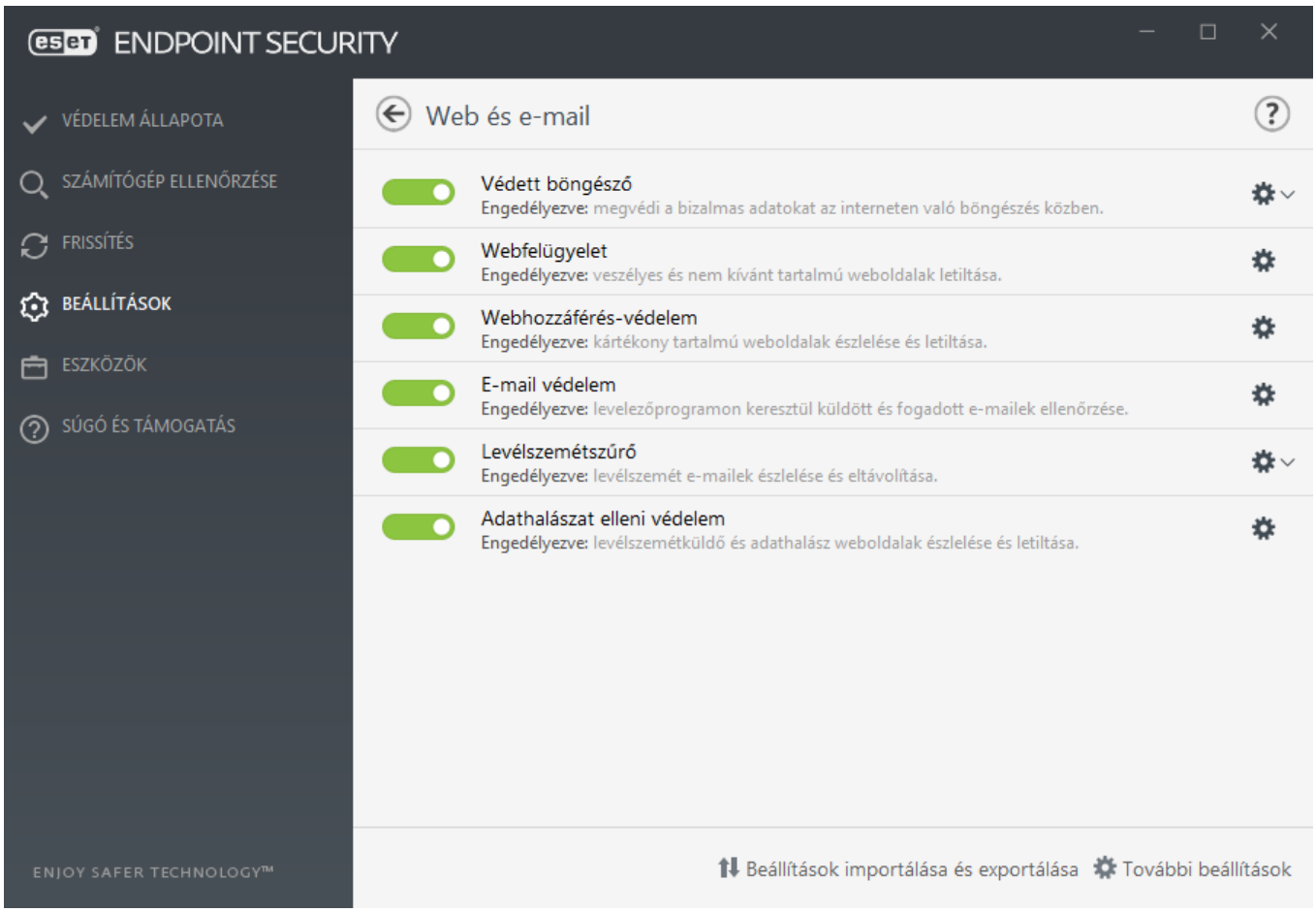
Alacsonyabb szintű tartományok – Ezt a jelölőnégyzetet bejelölve a bejegyzés az alsóbb szintű tartományokra is érvényes lesz – a fenti példánál maradva a *cim.info* tartomány mellett a *sajat.cim.info* altartományra is.

Webhozzáférés-védelem

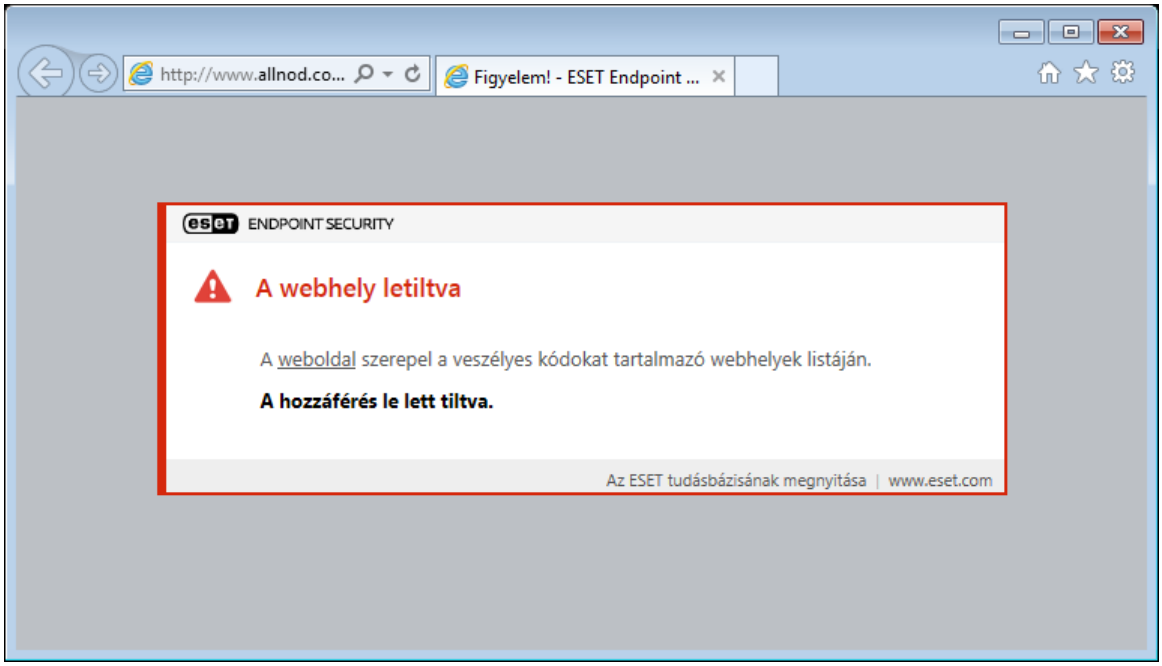
Az internetelérés a személyi számítógépek alapvető szolgáltatásaihoz tartozik. Sajnos a kártevők is ezt használják ki a terjedéshez. A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP és a HTTPS (titkosított kommunikáció) protokollon alapuló szabályokat.

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. Ez a beállítás az ESET Endpoint Security főablakából érhető el a **Beállítások** > **Internetes védelem** > **Webhozzáférés-védelem** lehetőség segítségével.



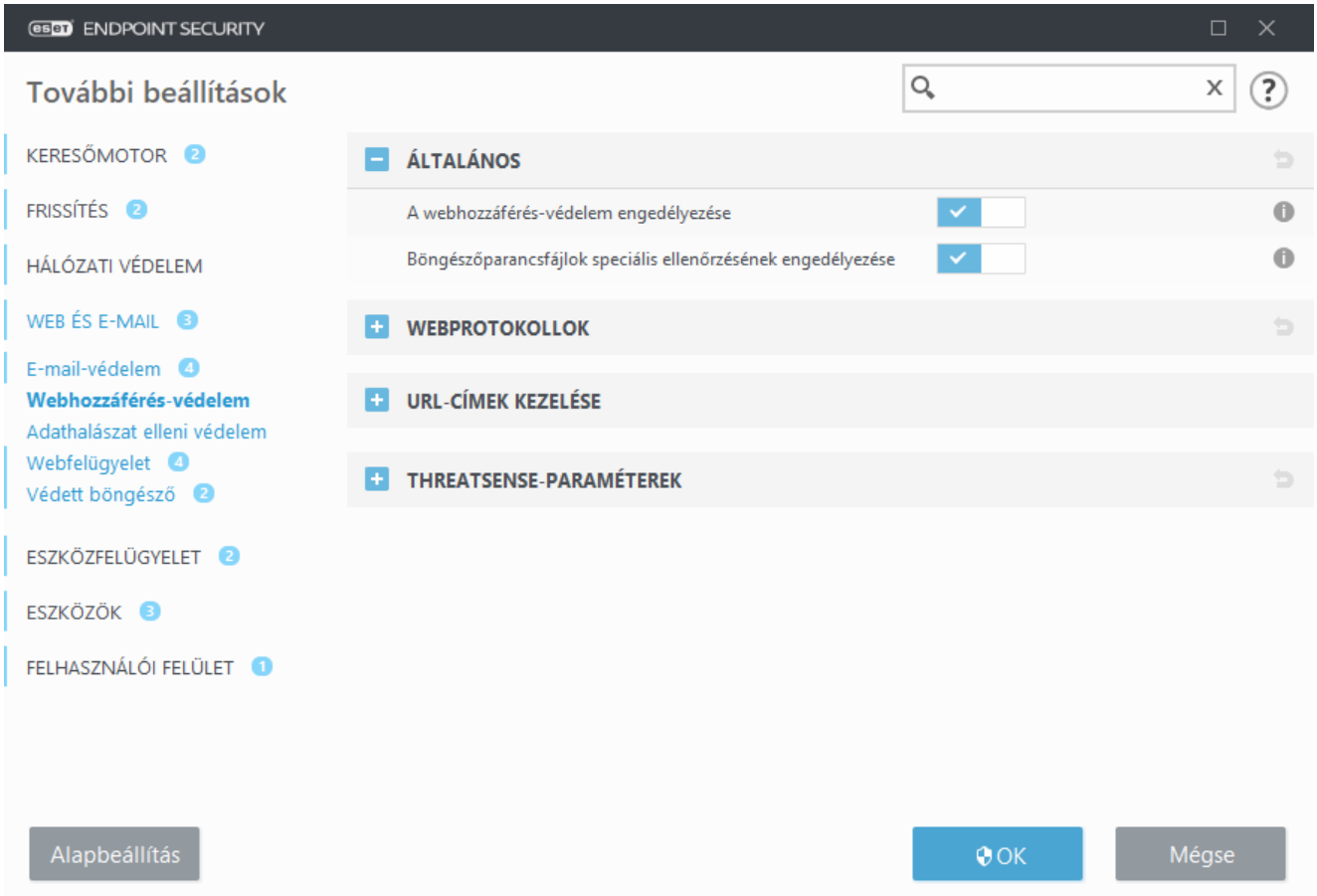
A webhozzáférés-védelem a következő üzenetet jeleníti meg a böngészőben, ha a webhely le van tiltva:



Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
- Biztonságos webhely feloldása önálló munkaállomáson az ESET Endpoint Security **programban**

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.

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 Endpoint 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 Endpoint Security támogatja a HTTPS-protokollszűrést is. A HTTPS kommunikációtípus titkosított csatornán keresztül továbbítja az adatokat a szerver és a kliens között. Az ESET Endpoint 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 a További beállítások szakaszban keresse meg az SSL/TLS csoportot, kattintson a **Web és e-mail** > **SSL/TLS** elemre, majd jelölje be az **SSL/TLS-protokollszűrés engedélyezése** elemet.

URL-címek kezelése

A témakörből megtudhatja, miként tilthat le, engedélyezhet és zárhat ki a tartalomellenőrzésből HTTP-címeket.

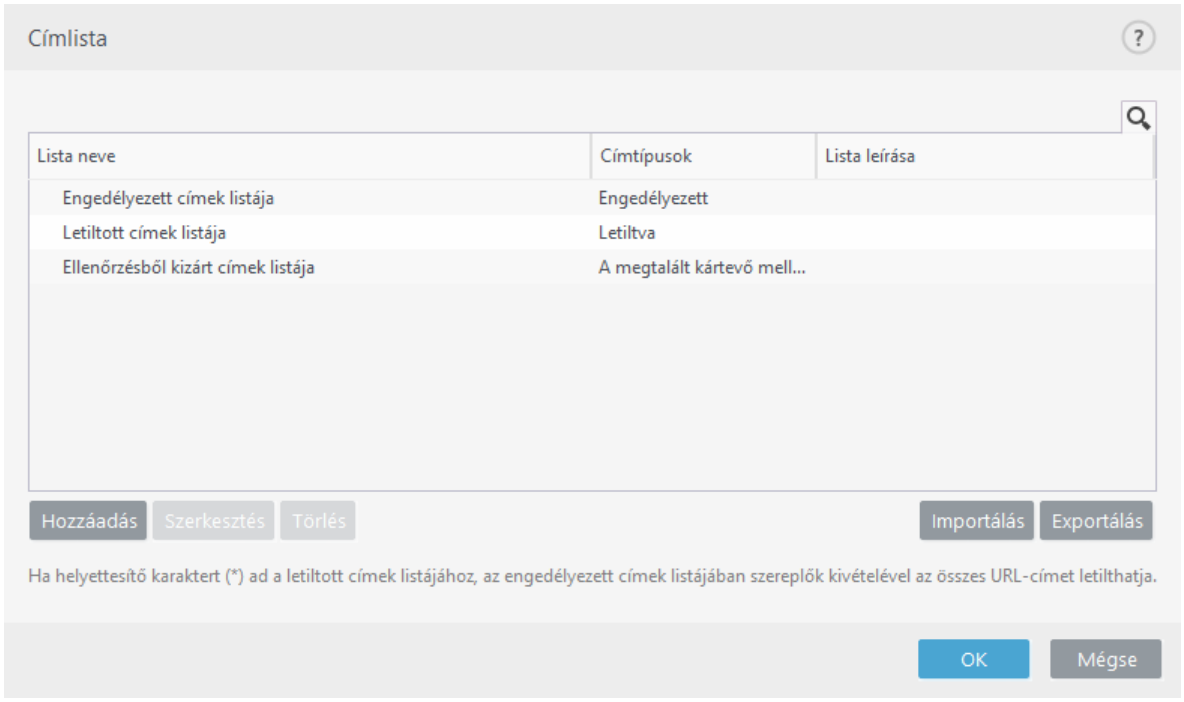
Ha a HTTP-weboldalak mellett a HTTPS-címeket is szeretné szűrni, jelölje be az **SSL/TLS-protokollszűrés engedélyezése** jelölőnégyzetet. Egyébként csak a felkeresett HTTPS-webhelyek tartományait veszi fel a program, a teljes URL-címet nem.

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.

> 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.

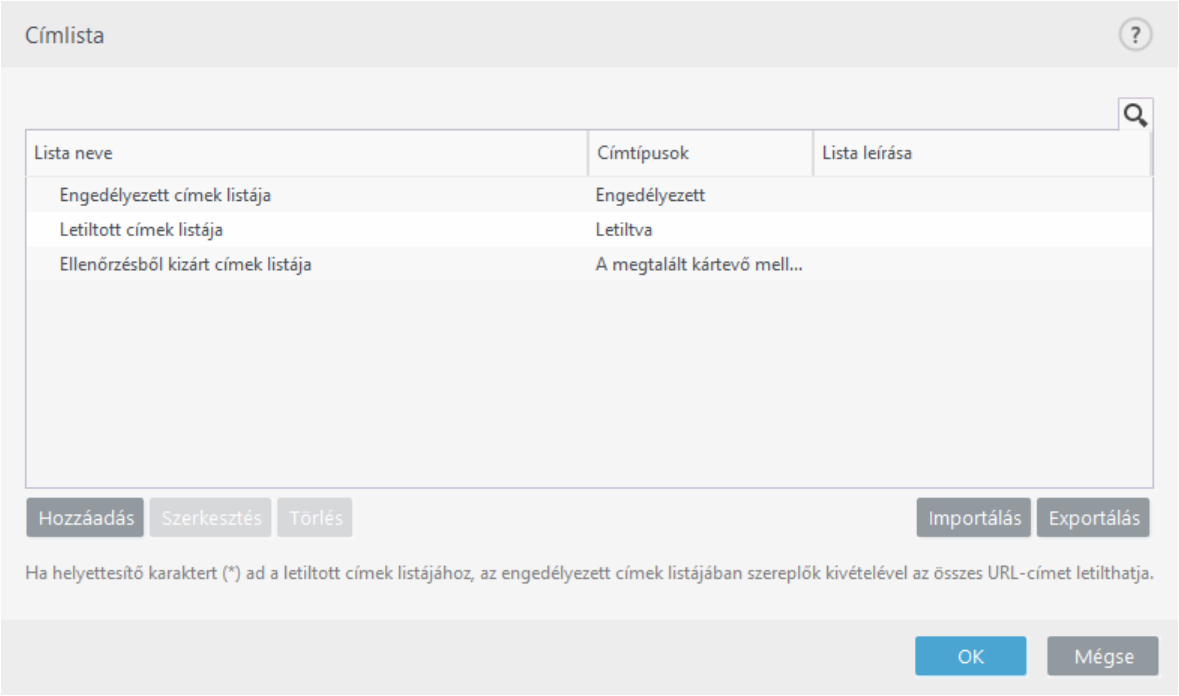
URL-címlista

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.



Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
• Biztonságos webhely feloldása önálló munkaállomáson az ESET Endpoint Security **programban**

További információt az URL-címek kezelése című témakörben talál.

Új lista létrehozása

A párbeszédablak segítségével konfigurálhat egy új listátURL-címekről/maszkokról, amelyek tiltva, engedélyezve vagy kizárva lesznek az ellenőrzésből.

Az alábbi beállításokat adhatja meg:

Címlista típusa – Három listatípus áll rendelkezésre:

- **A megtalált kártevő mellőzve** – A program a listában szereplő egyetlen cím esetén sem keres kártevő kódokat.
- **Tiltott** – A listában megadott címekhez való hozzáférés tiltva lesz.
- **Engedélyezett** — A listában megadott címekhez való hozzáférés engedélyezve lesz. A listában található címek akkor is engedélyezettek, ha szerepelnek a letiltott címek listájában.

Lista neve – Ebben a mezőben adható meg a lista neve. Ez a mező nem lesz elérhető az előre definiált listák egyikének szerkesztésekor.

Lista leírása – A mezőben rövid ismertetőt írhat a listához (nem kötelező). Az előre definiált listák egyikének szerkesztésekor nem érhető el.

Ha aktiválni szeretne egy listát, jelölje be a kívánt lista melletti **Lista aktiválása** jelölőnégyzetet. Ha értesítést szeretne kapni, amikor a rendszer egy adott listát használ a webhelyek elérésekor, válassza ki az **Értesítés alkalmazáskor** lehetőséget. Ebben az esetben értesítést fog kapni például arról, ha a rendszer letilt vagy engedélyez egy webhelyet, mert az szerepel a letiltott vagy engedélyezett címek listáján. Az értesítésben szerepelni fog a lista neve.

Naplózás részletessége – A legördülő listában válassza ki a naplózás részletességét. A Figyelmeztetés részletességű rekordokat a ESET PROTECT gyűjtheti.

Az Információk és a Figyelmeztetés naplózási részletesség csak olyan szabályok esetén érhető el, amelyek legalább két komponenst tartalmaznak helyettesítő karakterek nélkül a tartományon belül. Példa:
- *.domain.com/*
- *www.domain.com/*

Vezérlőelemek

Hozzáadás – Új URL-cím hozzáadása a listához (több érték esetén használjon elválasztójelet).

Szerkesztés – A meglévő cím módosítása a listában. Csak a **Hozzáadás** opció segítségével létrehozott címek esetén érhető el.

Eltávolítás – Meglévő címek eltávolítása a listából. Csak a **Hozzáadás** opció segítségével létrehozott címek esetén érhető el.

Importálás – Fájl importálása URL-címekkel (az értékeket sortöréssel válassza el egymástól, például: UTF-8 kódolást használó *.txt).

További információkért tekintse meg az URL-maszk hozzáadása című fejezetet.

URL-maszk hozzáadása

A kívánt cím- vagy tartománymaszk megadása előtt tanulmányozza a párbeszédpanelen megjelenő információkat.

Az ESET Endpoint 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 karakterek például az összes olyan címet lefedik, amelynek utolsó része c betűvel kezdődik, m betűvel végződik, és a kettő között egyetlen karakter szerepel (.com, .cam stb.).

A *x? maszk például olyan címet jelöl, amelynek „x” az utolsó előtti karaktere. A teljes tartomány kijelöléséhez adja meg azt **.domain.com/** formátumban. A *http://*, *https://* protokollelőtag megadása a maszkban kötelező. Ha kihagyja, a maszk az összes protokollra vonatkozik. 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 **.domain.com**.tartomany.hu maszk például nem fog megfelelni a http://barmelytartomany.hu/barmelyeleresiut#.tartomany.hu*http://anydomain.com/anypath#.domain.com* 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 **.domain.com**.tartomany.hu maszk például a http://tartomany.hu*http://domain.com* címnek is megfelel. A **domain.com**tartomany.hu használata helytelen lenne, mivel az a

http://masiktartomany.hu*http://anotherdomain.com* címnek is megfelelne.

Az Információk és a Figyelmeztetés naplózási részletesség csak olyan szabályok esetén érhető el, amelyek legalább két komponenst tartalmaznak helyettesítő karakterek nélkül a tartományon belül. Példa:
- *.domain.com/*
- *www.domain.com/*

Adathalászat elleni védelem

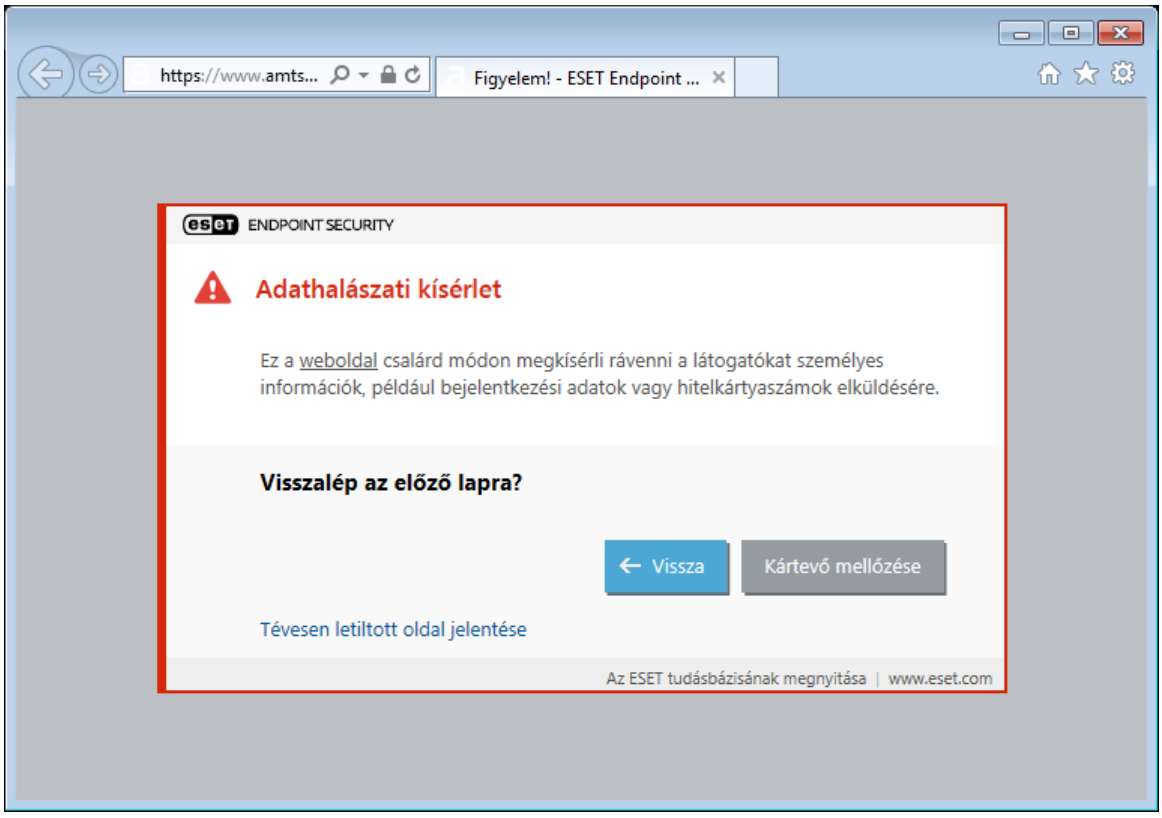
Az adathalászat olyan bűncselekmény, amely pszichológiai manipulációt alkalmaz (vagyis bizalmas információk kiszolgáltatására veszik rá a felhasználót). Az adathalászatot érzékeny adatokhoz – például bankszámlaszámokhoz, PIN-kódokhoz stb. – való hozzáférésre használják. További információkat lásd a szószedetet. Az ESET Endpoint Security az ilyen tartalommal rendelkező ismert weboldalak letiltásának lehetővé tételével támogatja az adathalászat elleni védelmet.

Az Adathalászat elleni védelem alapértelmezés szerint engedélyezve van. Ez a beállítás a fő programablakból érhető el > **További beállítások** (F5) > **Web és e-mail > Adathalászat elleni védelem**.

A tudásbáziscikkünk további információkat tartalmaz az ESET Endpoint Security adathalászat elleni védelméről.

Adathalász webhely elérése

Amikor egy ismert adathalász webhelyet nyit meg, webböngészője a következő párbeszédablakot jeleníti meg. 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. Az (F5 billentyű lenyomásával) megnyitható **További beállítások** párbeszédpanelen kattintson a **Web és e-mail** > **Webhozzáférés-védelem** > **URL-címek kezelése** > **Címlista** elemre, majd a **Szerkesztés** gombra, és vegye fel a 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. Ebben az esetben bejelenthet egy téves adathalászati riasztást.

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.).

Védett böngésző – további beállítások

Ezek a beállítások a **További beállítások** (F5) > **Web és e-mail** > **Védett böngésző** lapon találhatók.

Általános

Védett böngésző engedélyezése – Ha engedélyezve van, aktiválódik a védett webhelyek listája, és megnyithatja a Védett webhelyek ablakot.

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.

Biztonságos online banki és fizetési oldalak — Alapértelmezés szerint letiltva. A Védett webhelyek listáján kívül az ESET belső listáján szereplő webhelyek átirányításra kerülnek az ESET által védett böngészőhöz. Az ESET által beazonosított webhelyek rendszeresen frissülnek.

Védett böngésző

Fejlett memóravédelem – Ha engedélyezve van, a biztonságos böngésző memóriája védve lesz attól, hogy más folyamatok megvizsgálhassák.

Billentyűzetvédelem – 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 böngésző ablaka körüli zöld keret és a kapcsolódó böngészőn belüli értesítés rövid ideig megjelenik a böngésző indításakor, majd eltűnik. A zöld keret azt jelzi, hogy böngészője teljes mértékben védett. További információk az ESET súgójában.

A Védett böngésző interaktív riasztásainak konfigurálása – Segítségével megnyitható az Interaktív riasztások ablak.

> Bizonyos esetekben egy adott interaktív figyelmeztetés csak akkor jelenik meg, ha hiba történt a Védett böngésző megfelelő indításakor. További információkat az Interaktív riasztások című fejezetben talál.

Védett webhelyek

Az ESET Endpoint 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** > **Védett böngésző** > **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.

Normál böngésző – Ezzel a beállítással az alapértelmezett webböngészőben folytathatja a műveletet (például egy 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.

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.
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.

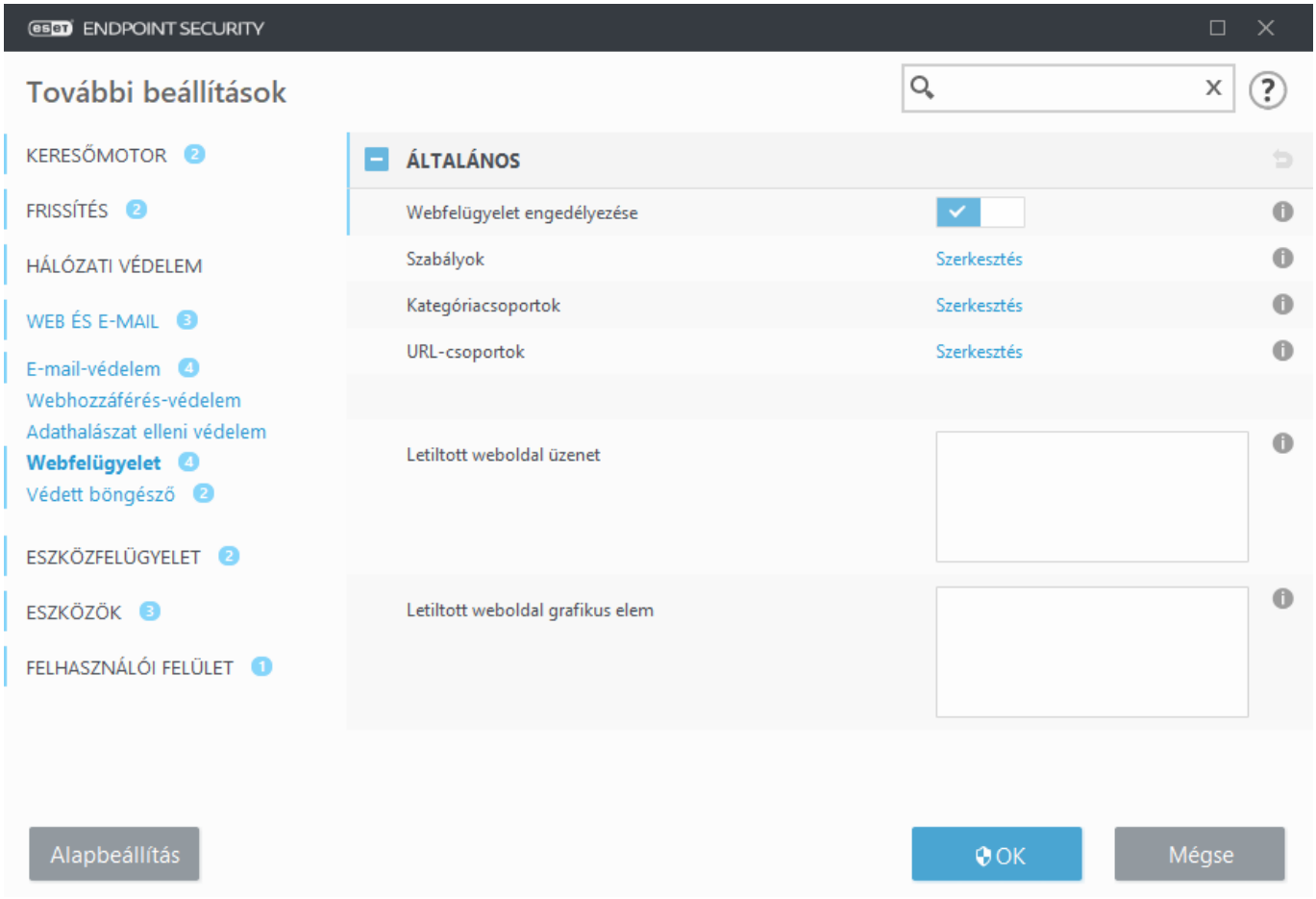
Webfelügyelet

A Webfelügyelet csoportban olyan beállításokat adhat meg, amelyekkel megvédheti vállalatát a jogi felelősséggel járó kockázatoktól. A Webfelügyelet segítségével szabályozható a hozzáférés a szellemi tulajdonjogot megsértő weboldalakhoz. További cél emellett, hogy az alkalmazottak ne férhessenek hozzá nem megfelelő vagy káros tartalmakhoz, illetve a teljesítményre negatív hatással lévő oldalakhoz.

A Webfelügyelet lehetővé teszi az esetlegesen nem kívánt tartalmú weboldalak letiltását. Ezenkívül a munkáltatók vagy a rendszergazdák több, mint 27 előre definiált webhely-kategória és több, mint 140 alkategória elérését is megtilthatják.

A webfelügyelet alapértelmezés szerint le van tiltva. A bekapcsolásához:

1. Nyomja le az **F5** billentyűt a **További beállítások** fa megnyitásához, és bontsa ki a **Web és e-mail** > **Webfelügyelet** csomópontot.
2. Válassza ki a **Webfelügyelet engedélyezése** lehetőséget a Webfelügyelet ESET Endpoint Security szolgáltatásban való engedélyezéséhez.
3. Ha konfigurálni szeretné a hozzáférést bizonyos weboldalakhoz, kattintson a **Szerkesztés** elemre a **Szabályok** felirat mellett a Webfelügyeleti szabályok szerkesztője ablak megnyitásához.

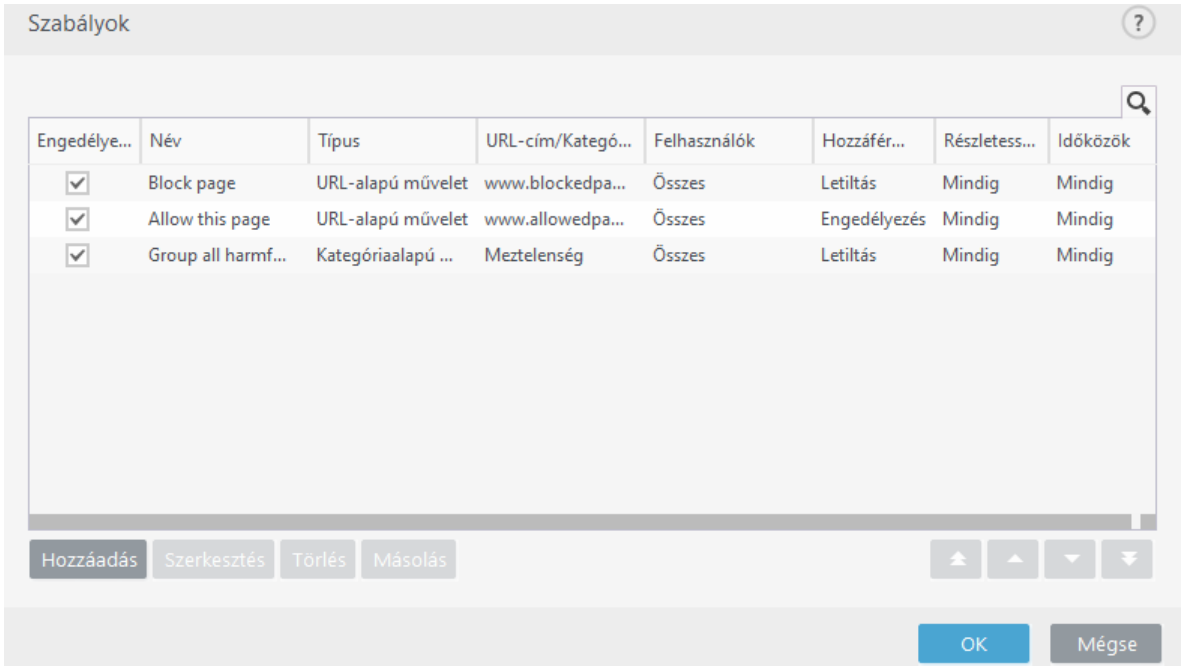


A **Letiltott weboldal üzenet** és a **Letiltott weboldal grafikus elem** mezőben egyszerűen testre szabhatja a megjelenített üzenetet a webhely letiltása esetén.

> Ha le szeretné tiltani az összes weblapot, és csak bizonyos weblapokat szeretne megtartani elérhetőnek, használja az URL-címek kezelése funkciót.

Webfelügyeleti szabályok

A **Szabályszerkesztő** ablakban láthatók az URL- és kategóriaalapú meglévő szabályok.



A szabályok listája a szabályokra vonatkozó számos leírást, többek között a nevet, a tiltás típusát és a webfelügyeleti szabály és a napló súlyosságának egyeztetését követően végrehajtandó műveletet tartalmaz.

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 **Ctrl** billentyűt lenyomva több szabályt is kijelölhet, illetve törölheti az összes kijelölt szabályt. Az **Engedélyezve** jelölőnégyzettel letilthatja vagy engedélyezheti a szabályt; ez akkor lehet hasznos, ha nem kívánja véglegesen törölni azt, mert a jövőben esetleg még szeretné használni.

A szabályok a legnagyobb prioritásúval kezdődően, a prioritásuk sorrendjében vannak rendezve. Ha módosítani szeretné az egyik szabály prioritását, válassza ki a szabályt, majd a nyílgombra kattintva növelje vagy csökkentse a prioritást. A dupla nyílra kattintva a lista teteje vagy alja felé közelítheti a szabályt.

További információk a szabályok létrehozásáról.

Webfelügyeleti szabályok hozzáadása

A Webfelügyeleti szabályok ablakban manuálisan létrehozhat szabályokat, illetve módosíthatja a meglévő webfelügyeleti szűrőszabályt.

Név

A **Név** mezőbe írt leírás segítségével a könnyebben azonosítható.

Engedélyezve

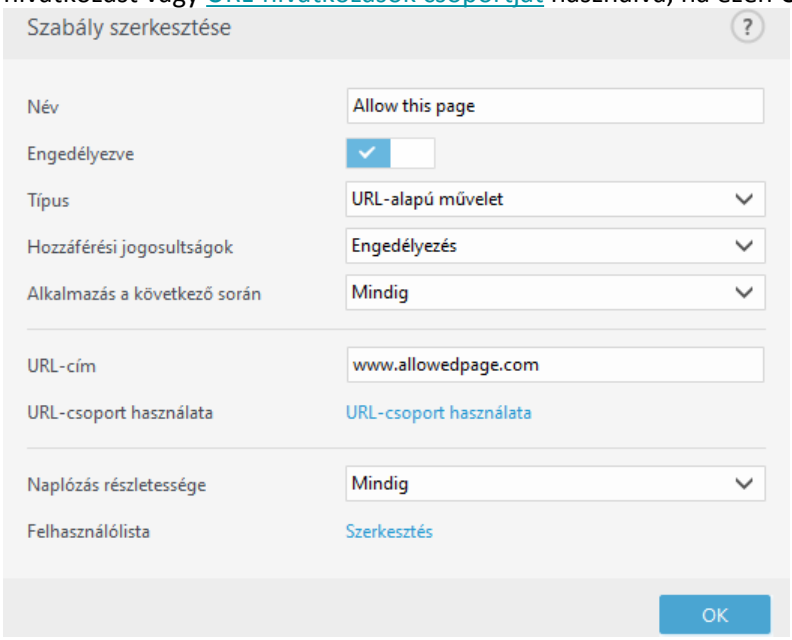
Kattintson az **Engedélyezve** kapcsolóra a szabály letiltásához vagy engedélyezéséhez. Ez akkor lehet hasznos, ha nem szeretné véglegesen törölni a szabályt.

Művelet

Válassza ki az **URL-alapú művelet** vagy a **Kategóriaalapú művelet** lehetőséget:

URL-alapú művelet

Adott webhelyek hozzáférését meghatározó szabályokhoz az **URL-cím** mezőben adja meg az URL-címet. A * (csillag) és a ? (kérdőjel) szimbólum nem használható az URL-címlistában. Több legfelső szintű tartománnyal rendelkező webhelyet tartalmazó URL-csoport létrehozásakor minden legfelső szintű tartományt külön kell felvenni. Amikor felvesz egy tartományt a csoporthoz, a tartományban és az altartományokban található összes tartalom (például az *al.mintaoldal.com*) letiltott vagy engedélyezett lesz a kiválasztott URL-alapú művelet alapján.
URL-cím vagy **URL-csoport használata** – A felhasználó engedélyezése, letiltása vagy figyelmeztetése URL-hivatkozást vagy URL-hivatkozások csoportját használva, ha ezen URL-címek valamelyikét észleli a program.



Kategóriaalapú művelet

Ha ezt a lehetőséget választja, adja meg a művelethez a webhely-kategóriát a legördülő listában.
URL-kategória vagy **Csoport használata** – A webhely-kategória vagy a Kategóriacsoportok segítségével engedélyezi, letiltja vagy figyelmezteti a felhasználót, ha ezen csoportok egyikét észleli a program.

Hozzáférési jogosultságok

- **Engedélyezés** – Az URL-címhez/kategóriához való hozzáférés megadása.
- **Figyelmeztetés** – Az URL-címre/kategóriára vonatkozó figyelmeztetés küldése a felhasználónak.
- **Figyelmeztetés mindig** – A felhasználó figyelmeztetése az URL-címről/kategóriáról. A rendszergazda letiltotta ezt a webhelyet. Továbbléphet a webhelyre, a rendszergazda azonban értesítést kap róla.
- **Tiltás** – Az URL-cím/kategória letiltása.

Alkalmazás a következő során

A létrehozott szabály alkalmazása a megadott időpontban. A legördülő menüben válassza ki a létrehozott időközt.

- További információk az időközökről

Naplózás részletessége

- **Mindig** – A teljes online kommunikáció 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 jönnek létre naplók.

A Naplózás részletessége beállítás listánként külön konfigurálható. A **Figyelmeztetés** állapotú naplókat az ESET PROTECT gyűjtheti.

Felhasználólista

- **Hozzáadás** – Megnyitja a **Felhasználók és csoportok** párbeszédpanelt, ahol kiválaszthatja a kívánt felhasználókat. Ha nincs megadva felhasználó, a program az összes felhasználóra alkalmazza a szabályt.
- **Eltávolítás** – Eltávolítja a szűrőből a kijelölt felhasználót.

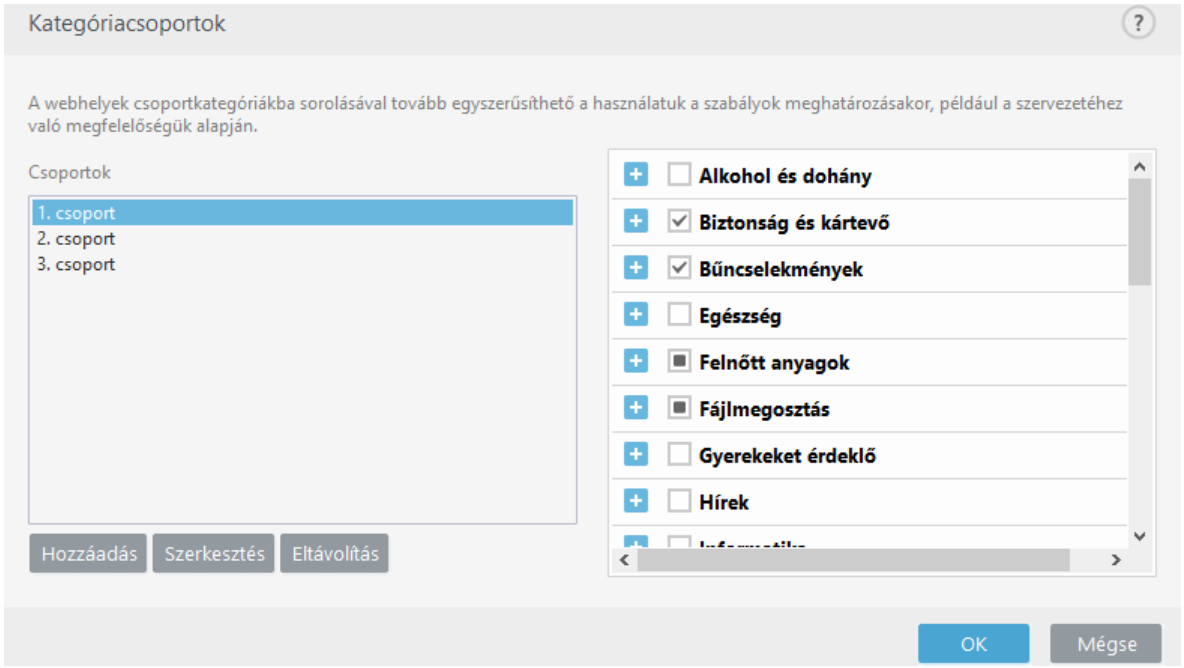
Kategóriacsoportok

A Kategóriacsoportok ablak két részből áll. Az ablak bal oldali részén kategóriacsoportok listája látható.

- **Hozzáadás** – Ide kattintva új kategóriacsoportot hozhat létre.
- **Szerkesztés** – Itt kattintva egy meglévő kategóriacsoportot szerkeszthet.
- **Eltávolítás** – Jelölje ki, és kattintson, ha el szeretne távolítani egy meglévő kategóriacsoportot a Kategóriacsoportok listájából.

Az ablak jobb oldali részén kategóriák és alkategóriák listája látható. Az alkategóriák megjelenítéséhez jelöljön ki egy kategóriát a Kategória listában. Az egyes csoportok felnőtt és/vagy többnyire nem megfelelő alkategóriákat, valamint általában elfogadhatónak tekintett kategóriákat tartalmaznak. A Kategóriacsoportok ablak megnyitásakor és az első csoportra kattintáskor hozzáadhat vagy eltávolíthat kategóriákat/alkategóriákat a megfelelő csoportok (például Erőszak vagy Fegyverek) listájából. Letilthatók a nem megfelelő tartalmú weboldalak, illetve a felhasználók értesíthetők egy előre megadott műveleteket tartalmazó szabály létrejöttekor.

A megfelelő jelölőnégyzet bejelölésével adjon hozzá alkategóriákat egy adott csoporthoz, illetve távolítsa el abból.



Az alábbiakban a felhasználók által kevésbé ismert kategóriákra talál példákat:

Egyéb – Általában magán (helyi) IP-címek, például az intranet,192.168.0.0/16 stb. Ha 403-as vagy 404-es hibakódot kap, a webhely megegyezik ezzel a kategóriával is.

Nincs feloldva – Ebbe a kategóriába tartoznak azok a weboldalak, amelyek csatlakozásakor a Webfelügyelet adatbázis motorjához hiba történt, és a webhelyek még nincsenek feloldva.

Nincs besorolva – A Webfelügyelet adatbázisában még nem szereplő ismeretlen weboldalak.

Proxyk – Weboldalak, például azonosíthatóságelfedők, átirányítók vagy nyilvános proxyszerverek használhatók az általában a webfelügyeleti szűrővel letiltott weboldalak (névtelen) eléréséhez.

Fájlmegosztás – Az ilyen weboldalak nagy mennyiségű adatot, például fényképeket, videókat vagy e-könyveket tartalmaznak. Fennáll a veszélye annak, hogy ezek a webhelyek nem kívánt vagy felnőtteknek szóló tartalommal rendelkeznek.

Az alkategóriák bármely csoporthoz tartozhatnak. Néhány alkategória nem szerepel előre definiált csoportokban (ilyen például a Játékok). Ha webfelügyeleti szűrővel szeretne egy kívánt alkategóriát egyeztetni, vegye fel azt a kívánt csoportba.

URL-csoportok

Az URL-csoportok lehetővé teszik olyan URL-hivatkozásokat tartalmazó csoportok létrehozását, amelyekhez szabályt szeretne létrehozni (adott webhely engedélyezéséhez/letiltásához).

Új URL-csoport létrehozása

Egy új URL-csoport létrehozásához kattintson a **Hozzáadás** gombra, majd adja meg az új URL-csoport nevét.

Egy új URL-csoport akkor lehet hasznos, ha a rendszergazda több weboldalhoz szeretne létrehozni egy szabályt

(tetszés szerint tiltást vagy engedélyezést).

URL-címek hozzáadása az URL-csoportlistához – manuálisan

Az új URL-cím listához való hozzáadásához válassza ki a kívánt URL-csoportot, majd kattintson a **Hozzáadás** gombra az ablak jobb alsó sarkában.

A * (csillag) és a ? (kérdőjel) szimbólum nem használható az URL-címlistában.

Nem szükséges megadni a tartomány teljes nevét a http:// vagy a https:// előtaggal.

Ha tartományt ad hozzá a csoporthoz, akkor az adott tartományon és az összes altartományon (például *sub.examplepage.com*) található összes tartalom tiltva, illetve engedélyezve lesz a kiválasztott URL-alapú művelet alapján.

Ha ellentmondás áll fenn két szabály között, például az első szabály letiltja a tartományt, a második szabály pedig engedélyezi ugyanazt a tartományt, akkor az adott tartomány és IP-cím mindenképpen tiltva lesz. A szabályalkotásról lásd az URL-alapú művelet oldalt.

URL-címek hozzáadása az URL-csoportlistához – importálás .txt fájl használatával

Az **Importálás** gombra kattintva importálja az URL-címek listáját tartalmazó fájlt (sortöréssel válassza el az értékeket, például UTF-8 kódolású .txt fájlban). A * (csillag) és a ? (kérdőjel) szimbólum nem használható az URL-címlistában.

URL-csoportok használata a Webfelügyeletben

Ha be szeretné állítani, hogy egy művelet végbemenjen egy adott URL-csoport esetén, nyissa meg a Webfelügyeleti szabályok szerkesztője ablakot, jelölje ki az URL-csoportot a legördülő listában, állítsa be a többi paramétert, és kattintson az **OK** gombra.

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

A Letiltott weboldal üzenet testreszabása

A **Letiltott weboldal üzenet** és a **Letiltott weboldal grafikus elem** mezőben egyszerűen testre szabhatja a megjelenített üzenetet a webhely letiltása esetén.

Ez az alapértelmezett üzenet és a böngészőben megjelenő értesítés kinézete, amikor a felhasználó letiltott webhelyet próbál megnyitni:

Használat

Tiltsuk le a „Fegyverek” webhely-kategóriát.

Példa letiltott weboldalról szóló üzenetre:

```
A rendszer letiltotta a(z) %URL_OR_CATEGORY% weboldalt, mert nem megfelelő, illetve
 káros tartalom található rajta.
Részletekért forduljon a rendszergazdához.
```

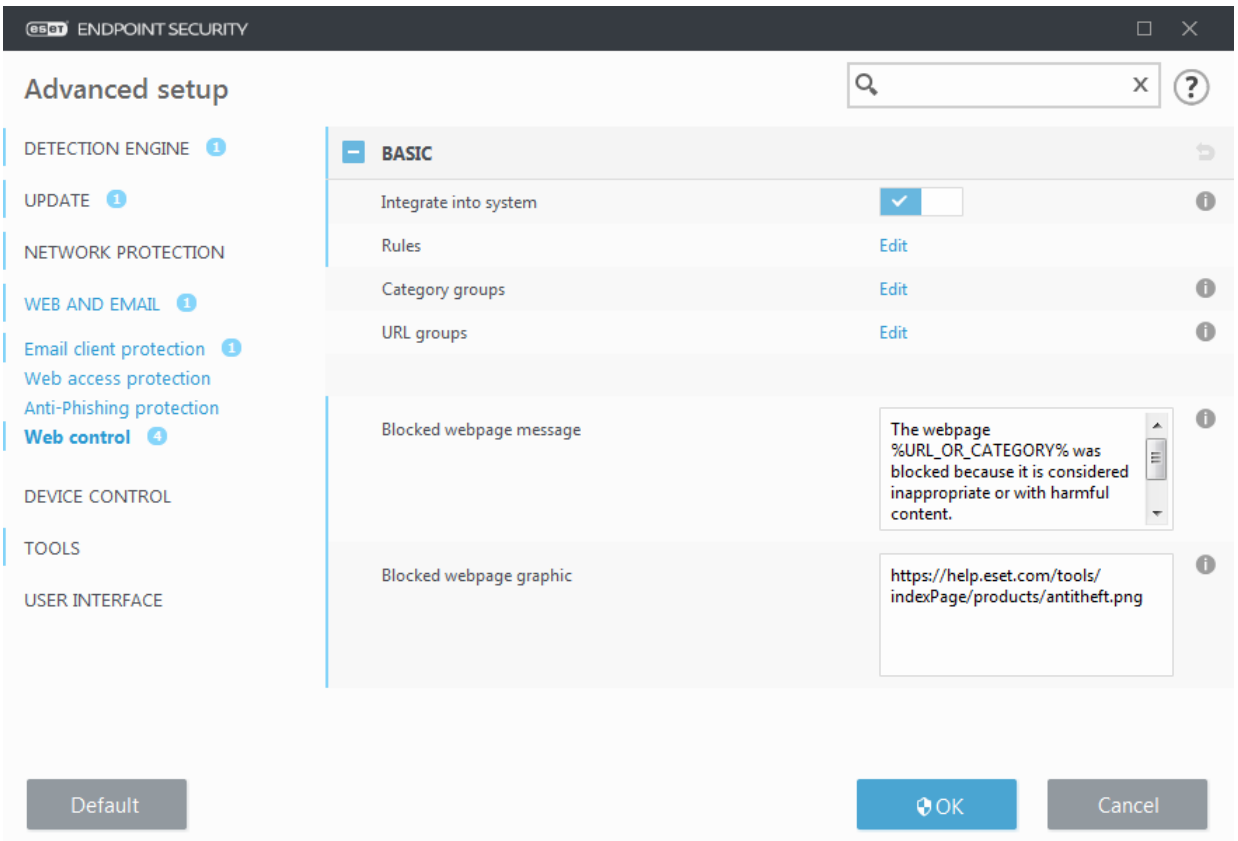
Változó	Leírás
%CATEGORY%	Letiltott webfelügyeleti kategória.
%URL_OR_CATEGORY%	Letiltott webfelügyeleti webhely vagy kategória (a webfelügyeleti tiltó szabálytól függ).
%STR_GOBACK%	A „Vissza” gomb értéke.
%product_name%	Az ESET-termék neve (ESET Endpoint Security)
%product_version%	Az ESET-termék verziója.

Példa letiltott weboldalról szóló grafikára:

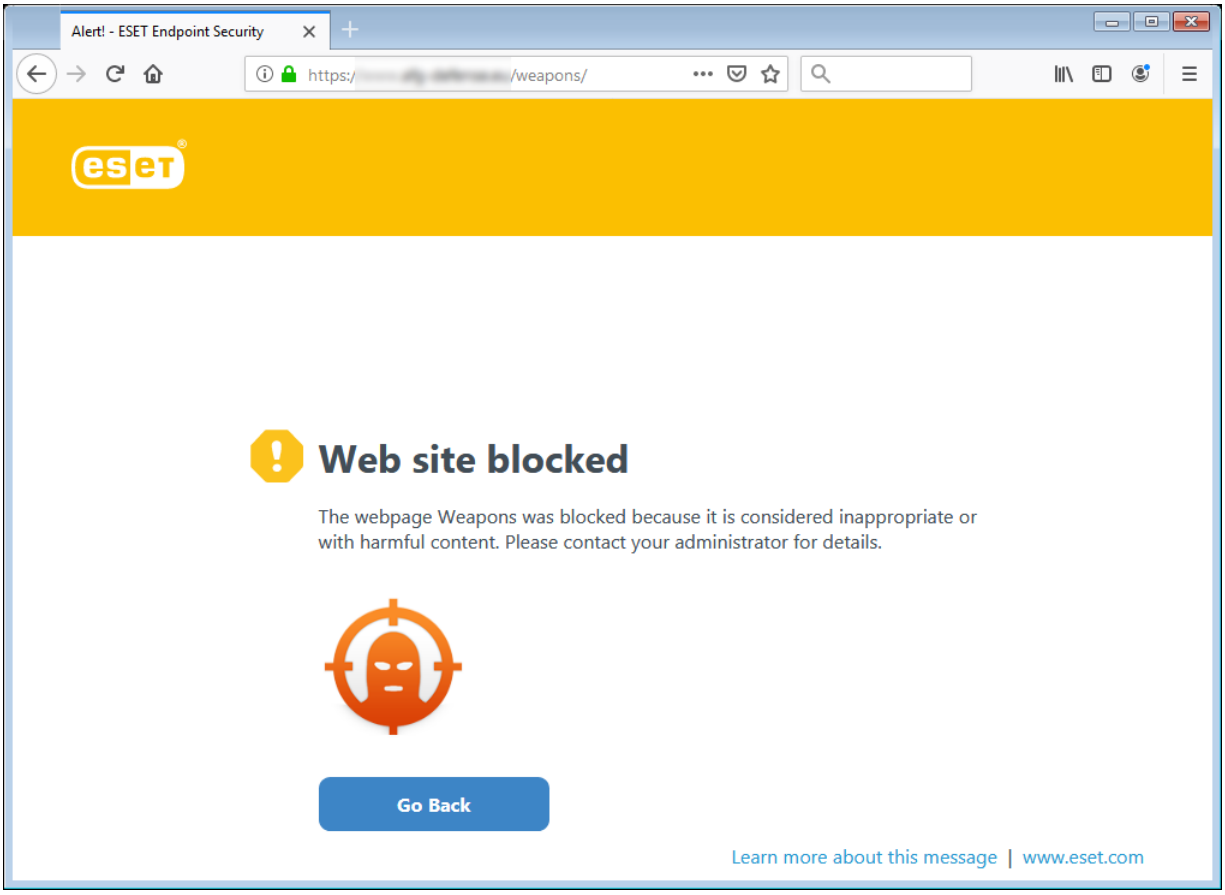
```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

A képméret (szélesség/magasság) automatikusan igazodik, ha a méret túl magas.

Az ESET Endpoint Security konfigurációja a következő lesz:



A böngészőben megjelenő egyéni értesítés így fog kinézni, amikor a felhasználó letiltott webhelyet próbál megnyitni:



A program frissítése

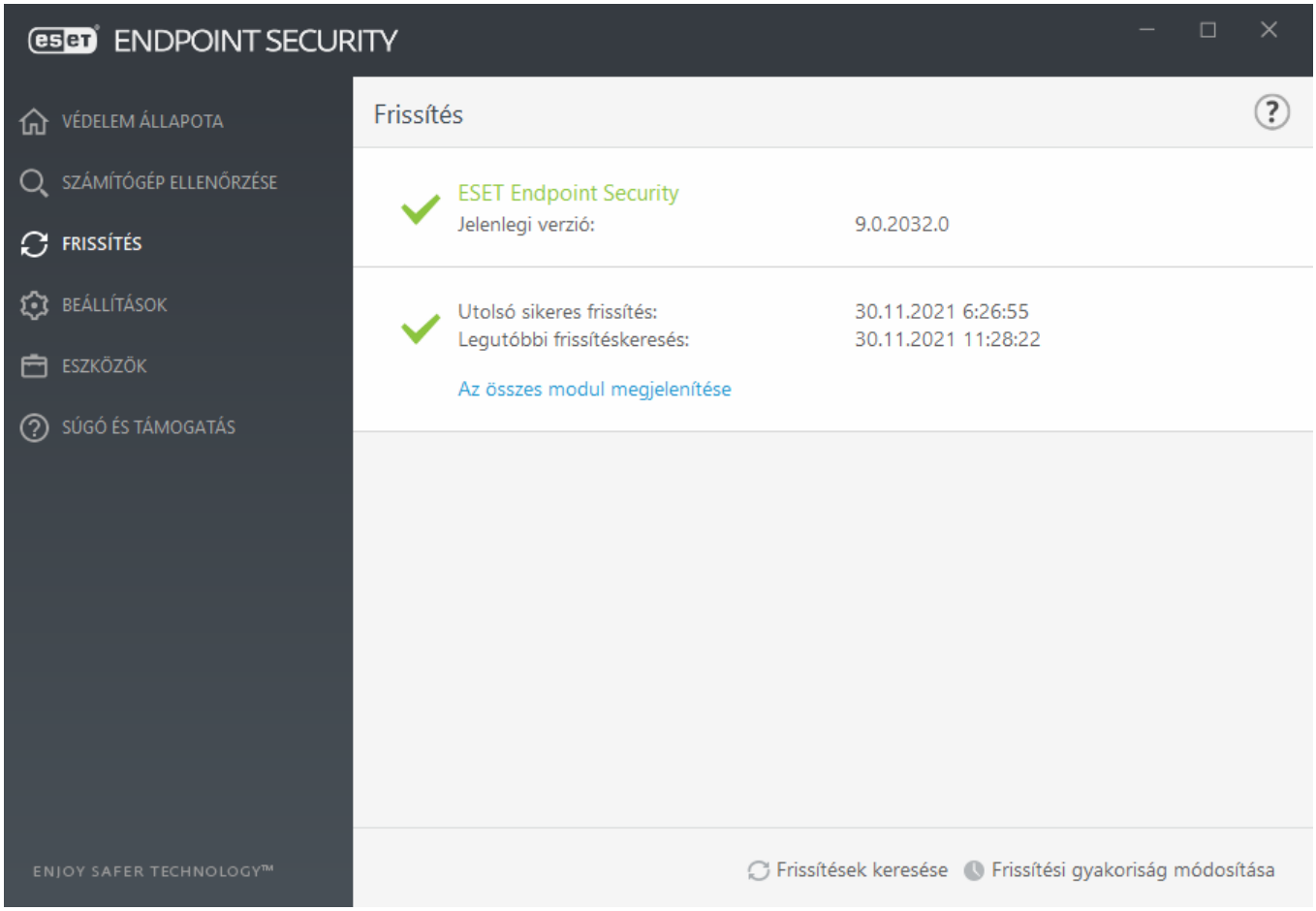
Az ESET Endpoint Security rendszeres frissítésével biztosítható a leghatékonyabban a számítógép maximális védelme. A Frissítés modul két módon biztosítja, hogy a program mindig naprakész legyen: a keresőmotor és a rendszerösszetevők frissítésével. A frissítések alapértelmezés szerint automatikusan végbemennek a program aktiválása után.

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 összes modul megjelenítése** gombra kattintva megnyithatja a telepített modulok listáját és ellenőrizheti az adott modul verzióját.

Emellett itt található **Frissítések keresése** hivatkozás, amellyel kézzel indítható a frissítési folyamat. A kártevő kódok elleni maradéktalan védelem fontos része a keresőmotor és a programösszetevők rendszeres frissítése. Kérjük, ügyeljen a beállításukra és a működésükre. Ha a telepítés során nem adta meg a licencadatokat, **A licenc aktiválása** elemre kattintva megadhatja a licenckulcsot, amikor az ESET frissítési szervereihez való hozzáférésre frissít.

Ha az ESET Endpoint Security aktiválását a kapcsolat nélküli licencfájllal végzi felhasználónév és jelszó nélkül, és frissíteni próbál, piros **Modulok frissítése sikertelen** üzenet jelzi, hogy csak a tükörről töltheti le a frissítéseket.

A licenckulcsot az ESET adja meg az ESET Endpoint Security megvásárlása után.



Jelenlegi verzió – A(z) ESET Endpoint Security verziószáma.

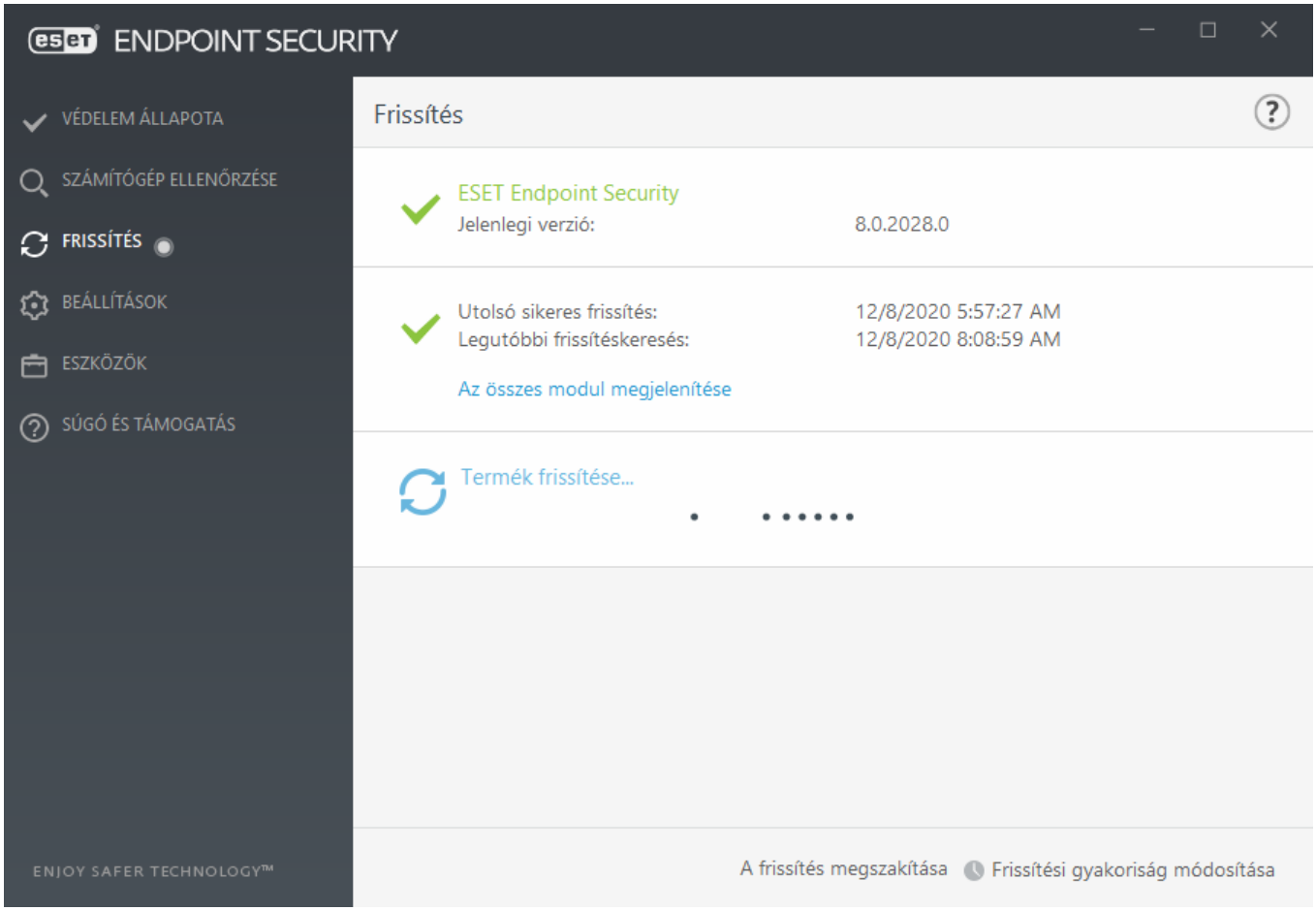
Utolsó sikeres frissítés – Itt látható a legutóbbi sikeres frissítés dátuma és időpontja. Ennek közelmúltbeli dátumnak kell lennie, ugyanis ez jelzi, hogy a keresőmotor naprakész.

Legutóbbi frissítéskeresés – Itt látható a legutóbbi sikeres modulfrissítési kísérlet dátuma és időpontja.

Az összes modul megjelenítése – A hivatkozásra kattintva megnyithatja a telepített modulok listáját és ellenőrizheti az adott modul verzióját.

A frissítési folyamat

A **Frissítések keresése** gombra kattintást követően elindul a letöltési folyamat. Megjelenik a letöltési folyamatjelző sáv, illetve látható a letöltésből hátralévő idő. A frissítést **A frissítés megszakítása** gombra kattintva megszakíthatja.

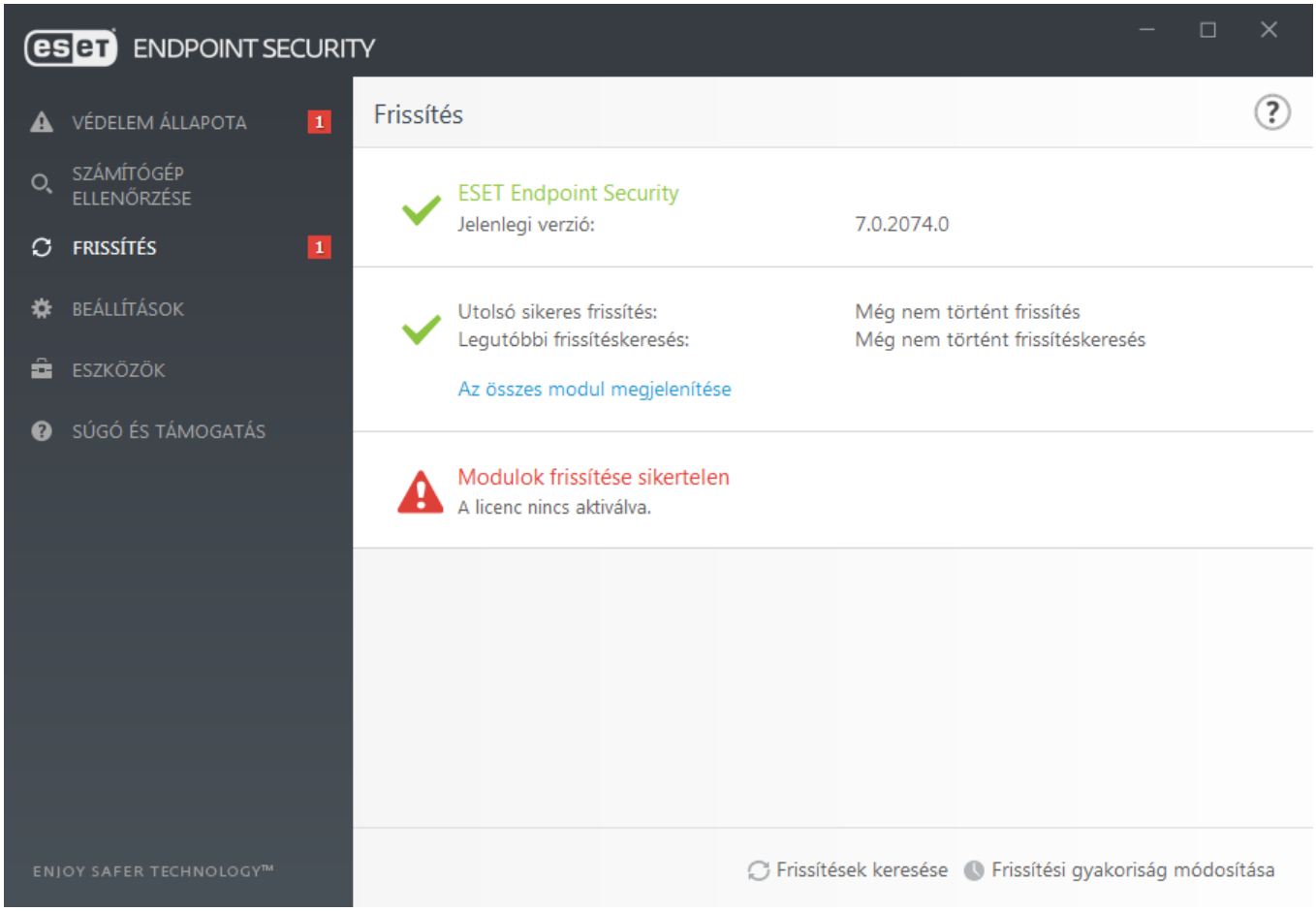


Szokásos körülmények között a modulok frissítése naponta többször is megtörténik. Ellenkező esetben ugyanis a program elavult, és sokkal sérülékenyebb a fertőzésekkel szemben. Ilyenkor a lehető leghamarabb frissítse a modulokat.

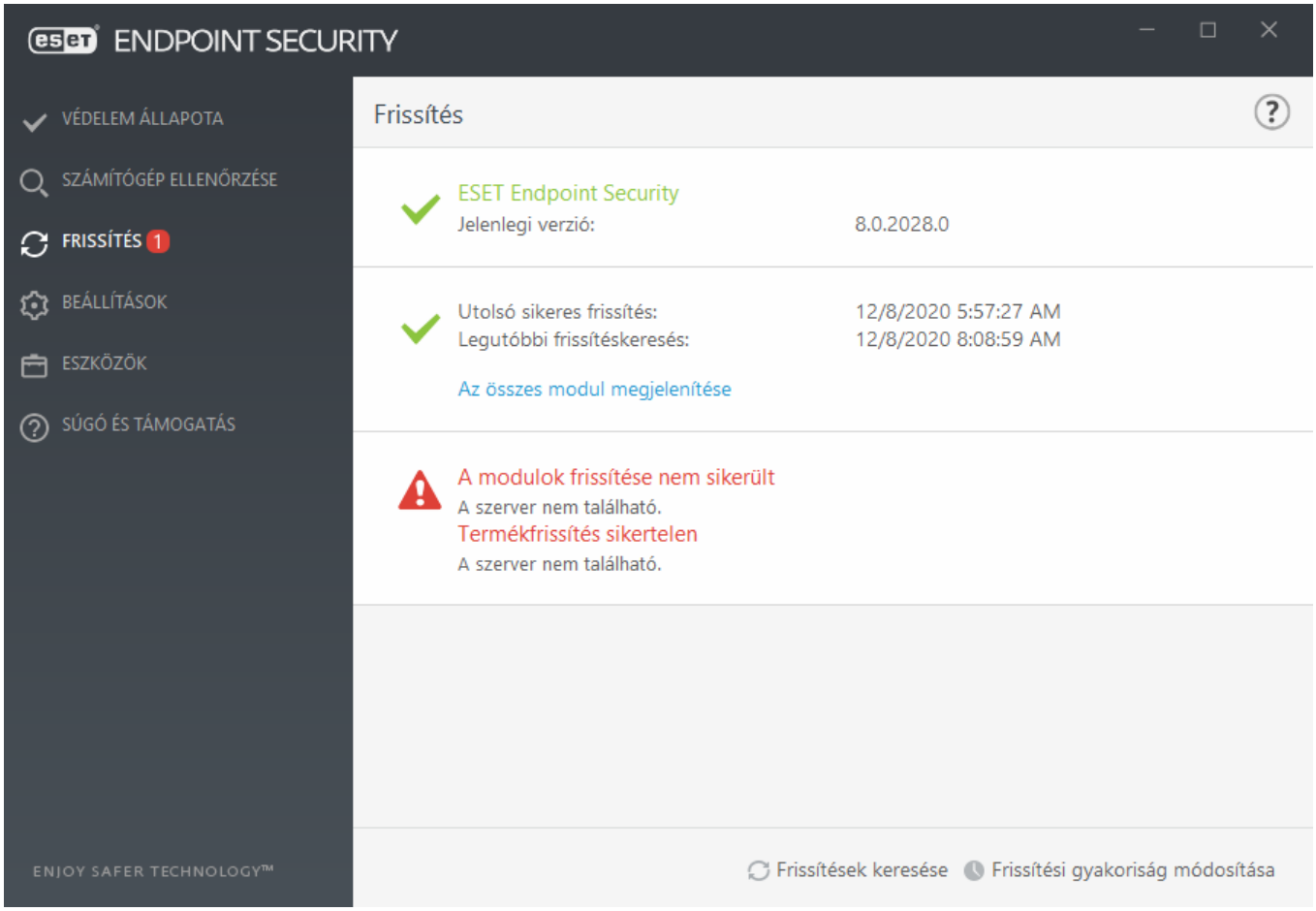
A keresőmotor elavult – Ez a hibaüzenet a modulok frissítésére tett több sikertelen kísérletet követően jelenik meg. Javasoljuk, hogy ellenőrizze a frissítési beállításokat. A hiba leggyakoribb oka a helytelenül megadott hitelesítési adatok, illetve a kapcsolati beállítások nem megfelelő konfigurációja.

Az előző értesítés az alábbi két sikertelen frissítésre vonatkozó üzenethez kapcsolódik (**A modulok frissítése nem sikerült**):

1. **Érvénytelen licenc** – Helytelenül adta meg a licenckulcsot a frissítési beállítások között. Javasoljuk, hogy ellenőrizze a hitelesítési adatokat. 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. Új licenckulcs megadásához a főmenüben kattintson a **Súgó és támogatás** > **Licenc módosítása** parancsra.



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



További információt az ESET e tudásbáziscikkében talál.

Frissítési beállítások

A frissítési beállítások az F5 billentyűvel megnyitható **További beállítások** fastruktúra **Frissítés** csoportjában érhetők el. Ebben a csoportban adhatja meg a frissítés forrásának beállításait, például a használatban lévő frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat.

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 HTTPS-kommunikációt).

Általános

Az aktuálisan használatban lévő frissítési profil az **Alapértelmezett frissítési profil kiválasztása** legördülő menüben látható.

Ha új profilt szeretne hozzáadni, tekintse meg a Profilok című részt.

Automatikus profilváltás – Frissítési profil hozzárendelése a Tűzfalban lévő Ismert hálózatok szerint. Az Automatikus profilváltás lehetővé teszi profil módosítását az adott hálózatnak megfelelően a Feladatütemezőben lévő beállításoktól függően. További információkért tekintse meg a súgóoldalakat.

Frissítési értesítések konfigurálása – A Szerkesztés elemre kattintva kiválaszthatja a megjeleníteni kívánt alkalmazásértesítéseket. Ezenkívül választhat a Megjelenítésének az asztalon és a Küldés e-mailben beállítás

közül.

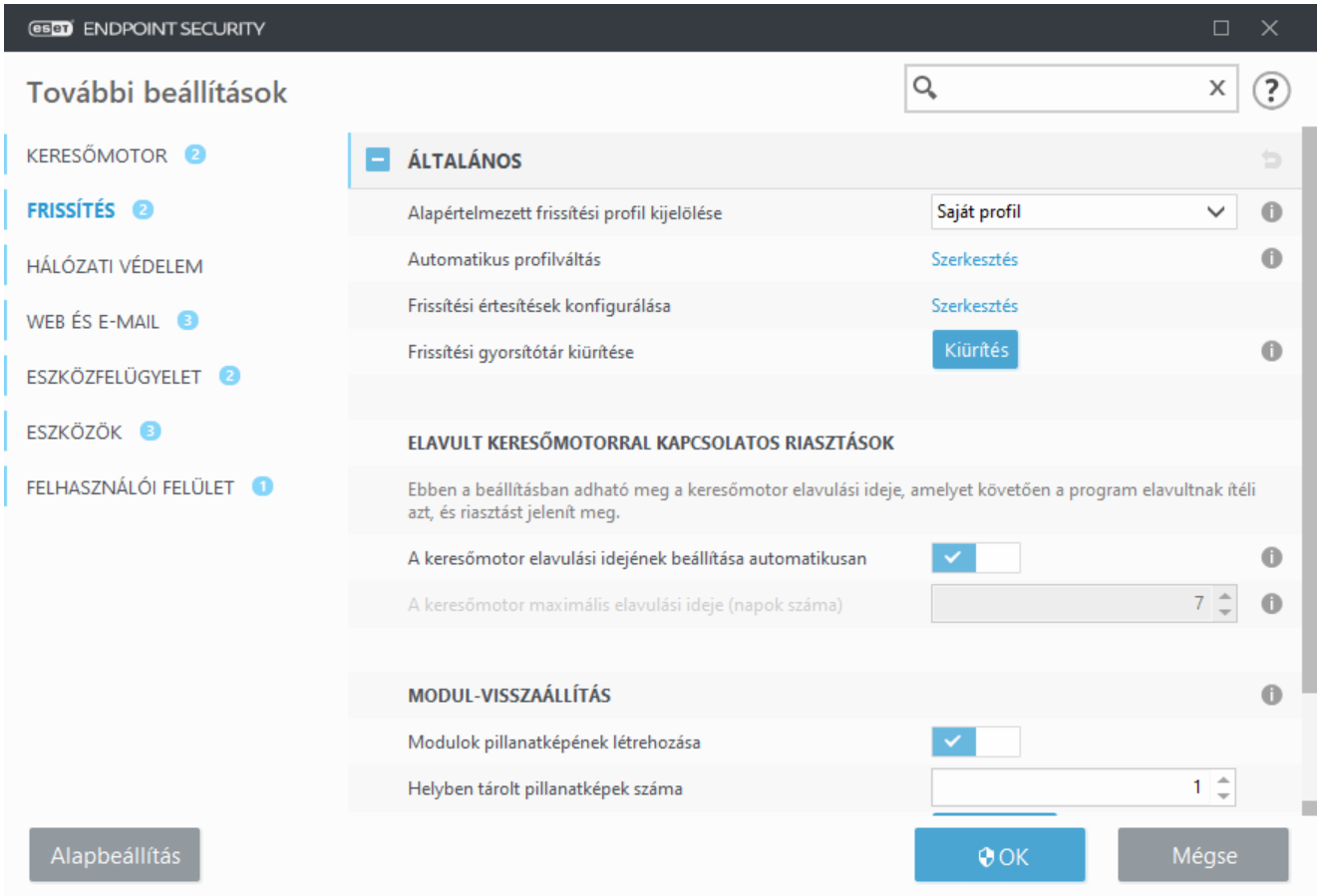
Ha a modulfrissítések letöltése során problémát tapasztal, a **Frissítési gyorsítótár kiürítése** felirat melletti **Kiürítés** gombra kattintva törölje az ideiglenes frissítési fájlokat/ürítse ki a gyorsítótárat.

Elavult keresőmotorral kapcsolatos riasztások

A keresőmotor elavulási idejének beállítása automatikusan – Ez az opció lehetővé teszi a maximális időtartam megadását (napokban), amely után a keresőmotort elavultként fogja jelenteni. **A keresőmotor maximális elavulási idejének (napok száma)** alapértelmezett értéke 7.

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.



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

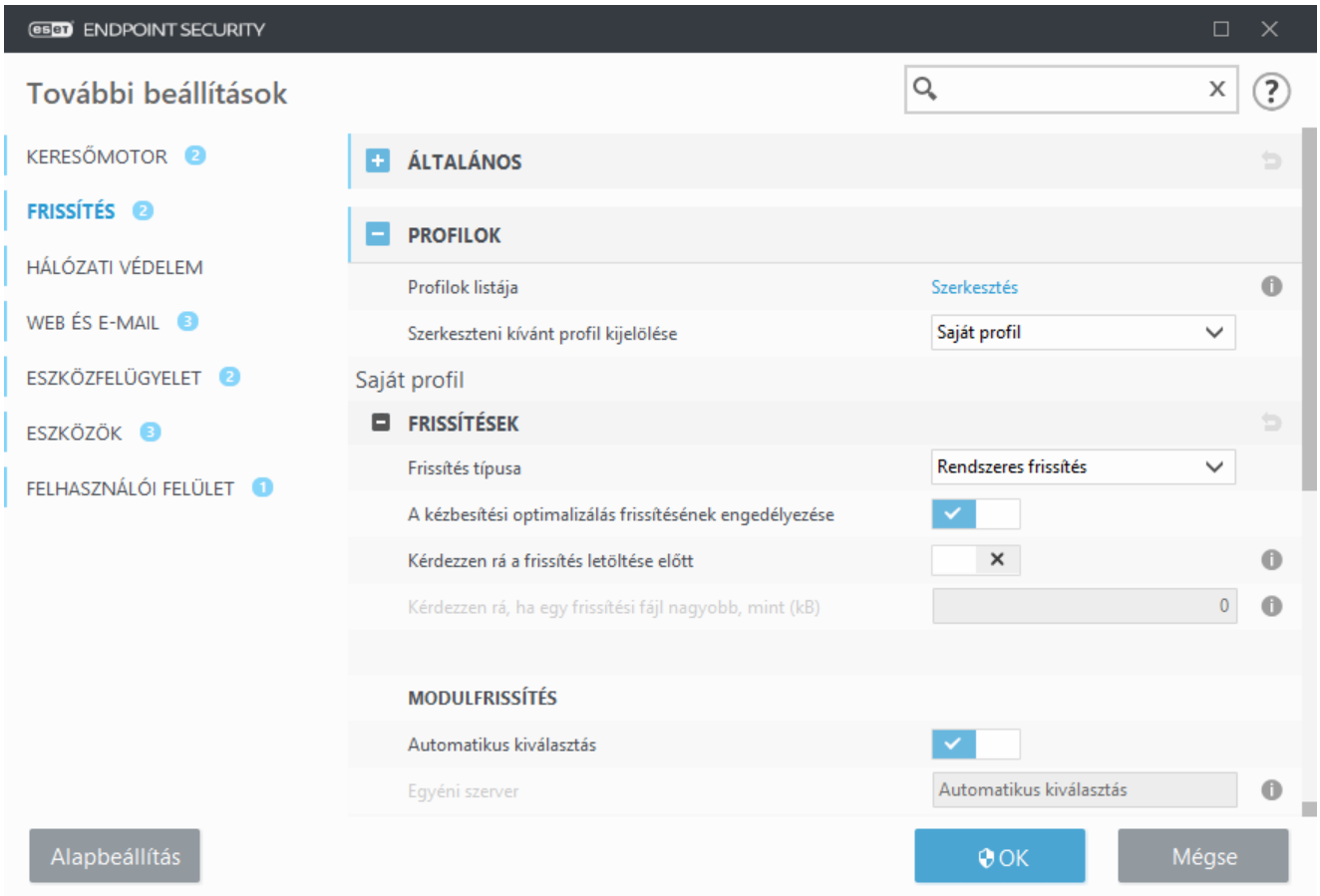
a **Profil neve** mezőbe, és kattintson a **Hozzáadás** elemre.

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. A Késleltetett frissítés lehetővé teszi a vírusdefiníciós adatbázisok új verzióit tartalmazó speciális frissítési szerverekről történő frissítést legalább X órás késleltetéssel (vagyis az adatbázisok valós környezetben teszteltek, ezért stabilnak tekinthetők).

A kézbesítési optimalizálás frissítésének engedélyezése – Ha engedélyezve van, a frissítőfájlok egy CDN (Content Delivery Network) kiszolgálóról töltődhetnek le. A beállítás letiltása szakadásokat és lassulásokat eredményezhet a letöltésben, ha az ESET dedikált frissítési kiszolgálói túlterheltek. A letiltás akkor hasznos, ha a tűzfal csak az ESET frissítési kiszolgáló IP-címeinek elérésére van korlátozva, vagy ha nem lehet kapcsolódni a CDN szolgáltatásokhoz.

Kérdezzen rá a frissítés letöltése előtt – A program megjelenít egy értesítést, és megerősítheti, illetve elutasíthatja a frissítési fájlok letöltését. Ha a frissítési fájl mérete nagyobb a Kérdezzen rá, ha egy frissítési fájl nagyobb mint (kB) mezőben megadott értéknél, a program megjeleníti a megerősítést kérő párbeszédpanelt. Ha a frissítési fájl 0 kB-ra van beállítva, a program mindig megjeleníti a megerősítést kérő párbeszédpanelt.



Modulfrissítés

Az **Automatikus kiválasztás** beállítás az alapértelmezett. Az **Egyéni szerver** a frissítési fájlokat tartalmazó helyi

vagy internetes szerver. Ha ESET frissítési szervert használ, tanácsos meghagynia az alapértelmezett beállítást.

Vírusdefiníciók gyakrabban történő frissítésének engedélyezése – A program gyakrabban fogja frissíteni a vírusdefiníciókat. A funkció letiltása negatív hatással lehet az észlelési arányra.

Modulfrissítések engedélyezése cserélhető adathordozókról – Lehetővé teszi a frissítést a cserélhető adathordozóról, ha az létrehozott tükröt tartalmaz. Az Automatikus beállítás választásakor a frissítés a háttérben fut. Ha meg szeretné jeleníteni a frissítési párbeszédpaneleket, válassza a Mindig rákérdez lehetőséget.

Helyben létrehozott frissítési szerver alkalmazása esetén – ezt tükörnek is nevezik – a frissítési szervert a következőképpen kell beállítani:
http://számítógép_neve_vagy_IP-címe:2221

Helyben létrehozott HTTP-szerver SSL használatával történő alkalmazása esetén a frissítési szervert a következőképpen kell beállítani:
https://számítógép_neve_vagy_IP-címe:2221

Helyben létrehozott megosztott mappa használata esetén a frissítési szervert a következőképpen kell beállítani:
*számítógép_neve_vagy_IP-címe**megosztott_mappa*

> A fenti példában is látható HTTP-szerverportszámot annak megfelelően kell kiválasztani, hogy a HTTP/HTTPS-szerver melyik portot figyeli.

Termékfrissítések

Lásd: Termékfrissítések.

Kapcsolati beállítások

Lásd a Kapcsolati beállítások című részt.

Frissítési tükör

Lásd: Frissítési tükör.

Frissítési fájlok visszaállítása

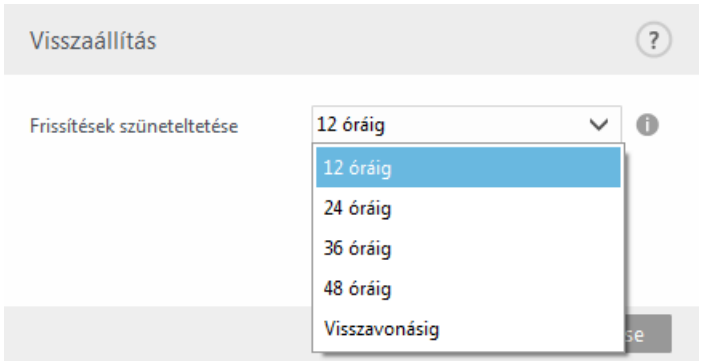
Ha a keresőmotor egyik frissítése vagy a programmodulok feltehetően nem stabilak, illetve sérültek, visszaállhat az előző verzióra, és átmenetileg letilthatja a frissítéseket. Másik lehetőségként engedélyezheti a korábban letiltott frissítéseket, ha bizonytalan időre elhalasztotta őket.

Az ESET Endpoint 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 Endpoint Security visszaállítja a keresőmotor és a programmodulok frissítési verzióját a legrégebbi pillanatfelvételre.

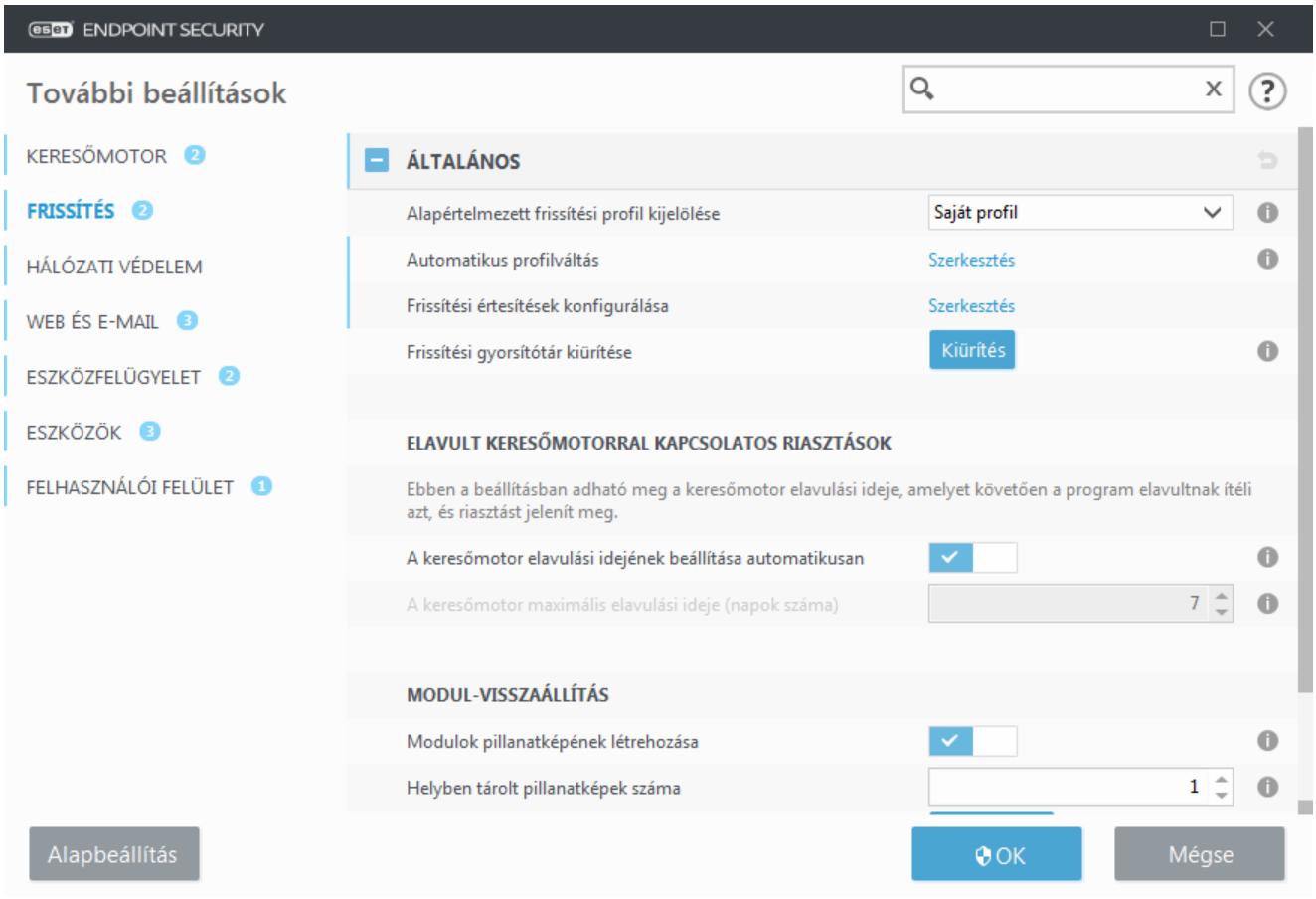
Ki kell választania egy időintervallumot az **Időtartam** legördülő menüben, ha a **Visszaállítás** elemre kattint

(**További beállítások** (F5) > **Frissítés** > **Általános** > **Modul-visszaállítás**).



A **Visszavonásig** beállítással határozatlan időre elhalaszthatja a szokásos frissítéseket, amíg kézzel vissza nem állítja a frissítési funkciót. Mivel biztonsági kockázatot jelent, nem javasoljuk 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.

Termékfrissítések

A **Termékfrissítések** szakaszban találhatók a termékfrissítésekhez kapcsolódó beállítások. Megadható, hogy miként viselkedjen a program abban az esetben, ha új termékfrissítés érhető el.

A termékfrissítések révén új szolgáltatások válnak elérhetővé, vagy módosulnak a korábbi verziókban is rendelkezésre álló szolgáltatások. Automatikusan, felhasználói beavatkozás nélkül is végrehajtható, de a frissítésekről értesítés is kérhető. Termékfrissítés telepítése után a rendszer újraindítására lehet szükség.

Automatikus frissítések – A frissítési profilok automatikus frissítésének szüneteltetésével ideiglenesen letilthatja az automatikus termékfrissítéseket, miközben más hálózatokkal vagy díjas kapcsolatokkal csatlakozik az internethez. Engedélyezze ezt a beállítást, hogy folyamatosan hozzáférhessen a legújabb funkciókhoz és a lehető legmagasabb szintű védelemhez. Az automatikus frissítésekről a következő részben olvashat részletesen:Automatikus frissítések – Gyakori kérdések.

Alapértelmezés szerint a termékfrissítések az ESET-adattárszerverekről töltődnek le. Nagy méretű vagy offline környezetben eloszthatóa forgalom a termékfájlok belső gyorsítótárazása érdekében.

Egyéni szerver megadása a programösszetevők frissítéséhez

1. Az **Egyéni szerver** mezőben megadhatja az elérési utat a termékfrissítésekhez.
Lehet HTTP(S)-hivatkozás, SMB hálózati megosztási útvonal, illetve egy helyi vagy cserélhető meghajtó elérési útvonala. Hálózati meghajtó esetén a csatlakoztatott meghajtó betűjele helyett használjon UNC elérési utat.
2. Szükség esetén hagyja üresen a **Felhasználónév** és a **Jelszó** mezőt.
Szükség esetén adja meg itt a megfelelő hitelesítési adatokat az egyéni webszerveren való HTTP-hitelesítéshez.
3. Erősítse meg a módosításokat, majd az ESET Endpoint Security szokásos frissítésével tesztelje, hogy rendelkezésre áll-e termékfrissítés.

A beállításokat az adott munkaállomástól függően kell kiválasztani. Érdemes figyelembe venni a munkaállomások és szerverek közötti különbségeket (jelentős károkat okozhat a vállalatnak például, ha egy termékfrissítést követően automatikusan indítja újra a szervert).

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.

Proxyszerver

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 Endpoint Security frissítéséhez nem használ proxyszervert, a **Proxyszerver használatának mellőzése**

választógombot jelölje be.

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

- Az ESET Endpoint 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 Endpoint Security azonban a frissítések beszerzése érdekében proxyszerverhez kapcsolódik.
- A számítógépe proxyszerveren keresztül csatlakozik az internetre. A beállításokat a program telepítés közben böngésző 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.

Windows-megosztások

Amikor egy, a Windows NT egyik verzióját futtató helyi szerverről végez frissítést, alapértelmezés szerint minden hálózati kapcsolatot hitelesíteni kell.

Az ilyen fiókok beállításához válasszon a **Kapcsolódás a helyi frissítési szerverhez** legördülő listából:

- **Rendszerfiókkal (alapbeállítás)**;
- **Aktuális felhasználóként**;
- **Megadott felhasználóként**.

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

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

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

A **Felhasználónév** és a **Jelszó** beállítás opcionális.

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

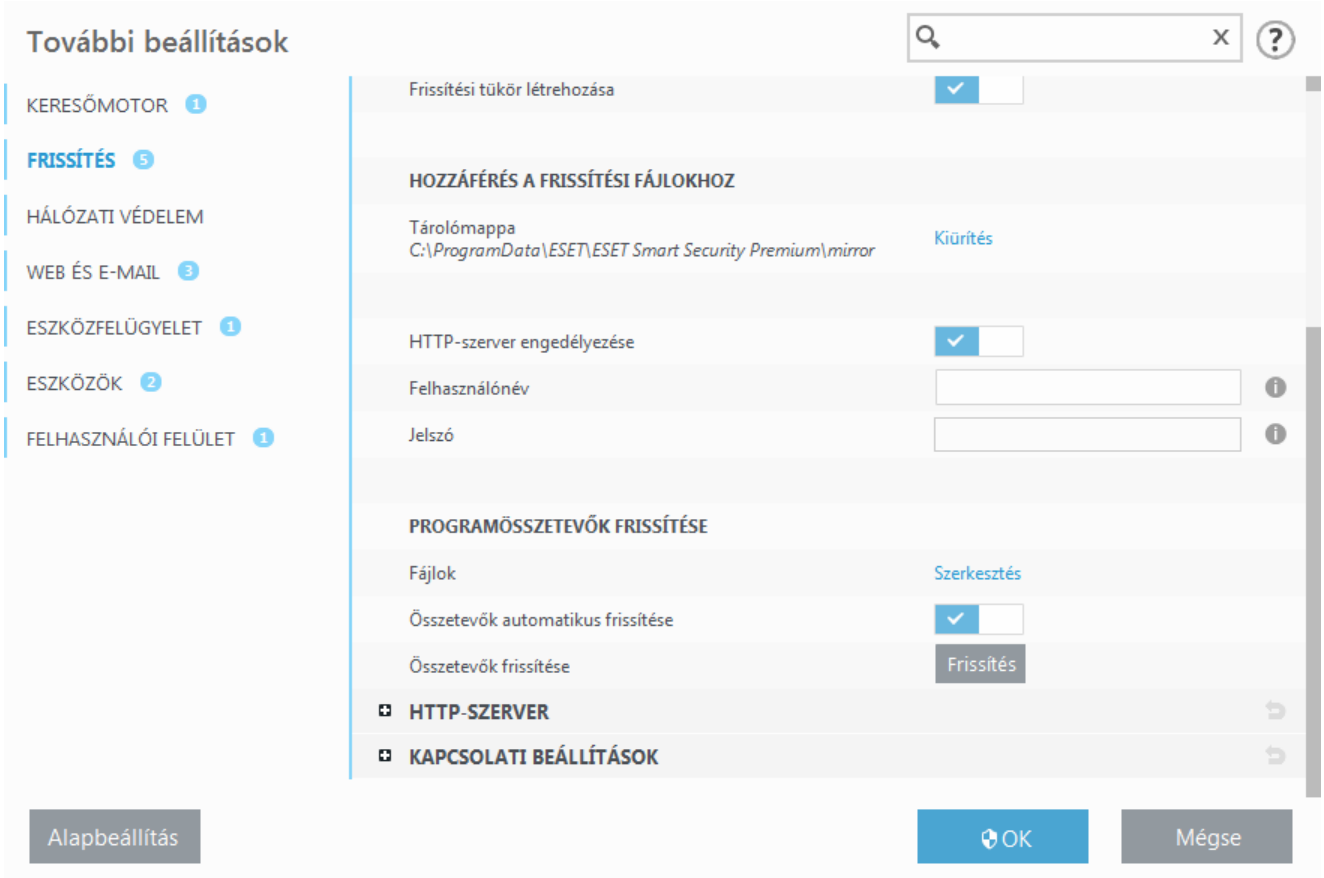
Jelölje be a **Kapcsolat** bontása a frissítés után jelölőnégyzetet, ha azt szeretné, hogy a számítógép bontsa a kapcsolatot a helyi frissítési szerverrel, ha a szerver egyik kapcsolata a frissítések letöltését követően is aktív marad.

Frissítési tükör

Az ESET Endpoint Security alkalmazásban a felhasználók másolatot (tükröt) készíthetnek a frissítési fájlokról, és ezekkel is frissíthetik a hálózaton levő többi munkaállomást. A tükör a frissítési fájlok helyi hálózati környezetben létrehozott másolata, amely azért hasznos, mert így a frissítési fájlokat nem kell minden egyes munkaállomásnak újra és újra letöltenie a gyártó frissítési szerveréről. A frissítések letöltődnek a helyi tükörszerverre, majd a rendszer szétosztja őket az egyes munkaállomásokra, így nyújtva védelmet a hálózati túlterhelés ellen. A munkaállomások tükörből történő frissítése javítja a hálózati terheléselosztást, és internetes sávszélességet szabadít fel.

> **i** Annak érdekében, hogy minimális legyen az internetforgalom azokon a hálózatokon, ahol az ESET PROTECT nagy számú kliens kezelésére szolgál, azt javasoljuk, hogy az Apache HTTP-proxyt használja ahelyett, hogy tükörként konfigurálna egy klienset. Az Apache HTTP-proxy az ESET PROTECT segítségével telepíthető az univerzális telepítővel, vagy önálló összetevőként. Az Apache HTTP-proxyról, a tükrözési eszközről és a közvetlen kapcsolatról, illetve a különbségekről az ESET PROTECT online súgóoldalunkon talál további információkat.

A helyi tükörszerver további beállításai a **Frissítés** csoporton belüli További beállítások csoportban érhetők el. A csoport megnyitásához az **F5** billentyűt lenyomva nyissa meg a További beállítások párbeszédpanelt, kattintson a **Frissítés** > **Profilok elemre,** és válassza a **Tükör frissítése** fület.



Ha egy kliens-munkaállomáson szeretne tükröt létrehozni, engedélyezze a **Frissítési tükör létrehozása** opciót. Ezzel aktiválhatja a többi tükrözési beállítást, például megadhatja a frissítési fájlok elérésének módját vagy a

tükrözött fájlok elérési útját.

Hozzáférés a frissítési fájlokhoz

HTTP-szerver engedélyezése – Ha engedélyezi ezt az opciót, a fájlok hitelesítési adatok megadása nélkül is elérhetők lesznek HTTP protokollon keresztül.

A tükörszerver elérésének módszereit a Frissítés tükörből című témakör ismerteti részletesen. A tükör két alapvető módszerrel érhető el: a frissítési fájlokat tartalmazó mappa beállítható megosztott hálózati mappaként, illetve az ügyfelek hozzáférhetnek a tükörhöz egy HTTP-szerveren.

A tükör frissítési fájljainak tárolására szánt mappa a **Tükrözött fájlok tárolómappája** csoportban adható meg. Ha másik mappát szeretne választani, a **Törlés** elemre kattintva törölje az *C:\ProgramData\ESET\ESET Endpoint Security\mirror* előre megadott mappát, és a **Szerkesztés** lehetőségre kattintva keressen egy mappát a helyi számítógépen vagy a megosztott hálózati mappában. Ha a megadott mappához hitelesítés szükséges, a **Felhasználónév** és a **Jelszó** mezőben adja meg a hitelesítő adatokat. Ha a választott mappa egy Windows NT, 2000 vagy XP operációs rendszert futtató hálózati számítógép lemezén található, a megadott felhasználónévhez tartozó fióknak írási jogosultsággal kell rendelkeznie a választott mappában. A felhasználónevet *Tartomány/felhasználó* vagy *Munkacsoport/felhasználó* formában kell megadni. A helyes működéshez a jelszó megadása is szükséges.

HTTP-szerver és SSL a tükörhöz

A **Tükrözés** lap **HTTP-szerver** csoportjában a **Szerverport** mezőben adja meg azt a szerverportot, amelyen keresztül a HTTP-szerver a frissítést szolgáltatja, illetve a szerver által használt **hitelesítés** típusát. Alapértelmezés szerint a szerverport értéke **2221**.

Hitelesítés – Megadja a frissítési fájlok eléréshez használt hitelesítés típusát. A választható lehetőségek az alábbiak: **Nincs**, **Általános** és **NTLM**. Az **Általános** hitelesítés base64-kódolást használ egyszerű felhasználónév- és jelszóalapú hitelesítéssel. Az **NTLM** beállítás biztonságos titkosítási metódust nyújt. A hitelesítéshez pedig a tükörszerveren létrehozott felhasználót használja. Az alapértelmezett beállítás a **Nincs**, amellyel a frissítési fájlok hitelesítés nélkül is elérhetők.

A hitelesítési adatok, például a **Felhasználónév** és a **Jelszó** csak a tükör HTTP-kiszolgáló elérésére szolgálnak. Csak akkor töltse ki ezeket a mezőket, ha felhasználónév és jelszó szükséges.

Fűzze hozzá a **tanúsítványlánc fájlját** (vagy hozzon létre egy önaláírt tanúsítványt), ha HTTPS (SSL) támogatású HTTP-szervert szeretne futtatni. A választható **tanúsítványtípusok** az alábbiak: ASN, PEM és PFX. További védelemként használja a HTTPS protokollt a frissítési fájlok letöltéséhez. A protokoll használata szinte lehetetlenné teszi az adatátvitelek és a bejelentkezési hitelesítő adatok nyomon követését. A **Titkosítókulcs típusa** beállítás alapértelmezett értéke az **Integrált** (ezért a **Titkosítókulcs-fájl** opció alapértelmezés szerint le van tiltva). Ez azt jelenti, hogy a titkos kulcs a kiválasztott tanúsítványláncfájl része.

Önaláírt tanúsítványok HTTPS-tükörhöz
Ha HTTPS-tükörszervert használ, importálnia kell a tanúsítványát a megbízható gyökértárolóba minden kliensgépen. Lásd: A megbízható főtanúsítvány telepítése a Windows rendszerben.

Frissítés tükörből

Kétféle általános módszerrel állíthat be tükröt, amely lényegében egy olyan tárház, ahol a kliensek frissítési fájlokat tölthetnek le. A frissítési fájlokat tartalmazó mappa megosztott hálózati mappaként és HTTP-szerverként is beállítható.

A tükör elérése belső HTTP-szerveren keresztül

Az előre definiált programkonfigurációban ez a beállítás az alapértelmezett. A tükör HTTP-szerveren keresztüli eléréséhez nyissa meg a **További beállítások** > **Frissítés** > **Profilok** > **Frissítési tükör** lapot, és jelölje be a **Frissítési tükör létrehozása** opciót.

A **Tükrözés** lap **HTTP-szerver** csoportjában a **Szerverport** mezőben adja meg azt a szerverportot, amelyen keresztül a HTTP-szerver a frissítést szolgáltatja, illetve a szerver által használt **hitelesítés** típusát. Alapértelmezés szerint a szerverport értéke **2221**.

Hitelesítés – Megadja a frissítési fájlok eléréshez használt hitelesítés típusát. A választható lehetőségek az alábbiak: **Nincs**, **Általános** és **NTLM**. Az **Általános** hitelesítés base64-kódolást használ egyszerű felhasználónév- és jelszóalapú hitelesítéssel. Az **NTLM** beállítás biztonságos titkosítási metódust nyújt. A hitelesítéshez pedig a tükörszerveren létrehozott felhasználót használja. Az alapértelmezett beállítás a **Nincs**, amellyel a frissítési fájlok hitelesítés nélkül is elérhetők.

A HTTP-szerveren keresztül elért frissítési fájlokat tároló tükörmappa csak az azt készítő ESET Endpoint Security alkalmazáspéldányt futtató számítógépen található mappa lehet.

Az **Érvénytelen a felhasználónév és/vagy a jelszó** hiba jelenik meg a főmenü Frissítés ablaktábláján a tükörből való frissítés néhány sikertelen kísérletét követően. Javasoljuk, hogy keresse meg a **További beállítások** > **Frissítés** > **Profilok** > **Tükrözés** lapot, és ellenőrizze a felhasználónevet és a jelszót. A hiba leggyakoribb oka a helytelenül megadott hitelesítési adat.

A tükörszerver konfigurálása után hozzá kell adnia az új frissítési szervert a munkaállomásokon. Ehhez tegye az alábbiakat:

- Nyissa meg a **További beállítások** (F5) párbeszédpanelt, és kattintson a **Frissítés** > **Profilok** > **Frissítések** > **Modulfrissítések** fülre.
- Letiltás ki az **Automatikus kiválasztás** opciót, és a **Frissítési szerver** mezőben az alábbi formátumokat használva vegyen fel egy új szervert:
  http://szerver_IP_címe:2221
  https://szerver_IP_címe:2221 (SSL használata esetén)

A tükör elérése megosztásokon keresztül

Először hozzon létre egy megosztott mappát egy helyi vagy hálózati eszközön. A tükörmappa létrehozásakor írási jogot kell adnia annak a felhasználónak, aki a frissítési fájlokat a mappába menti, és olvasási jogot az összes olyan felhasználónak, aki a tükörmappából fogja frissíteni az ESET Endpoint Security programot.

Ezután a **További beállítások** > **Frissítés**> **Profilok**> **Frissítési tükör** lapon az **HTTP-szerver engedélyezése** beállítás letiltásával állítsa be a tükör elérési módját. A jelölőnégyzet jelölésének törlésével kapott beállítás egyben a telepítőcsomagbeli alapértelmezés is.

Ha a tükrözéshez kijelölt megosztott mappa másik számítógépen van, a számítógép eléréséhez meg kell adni a hitelesítő adatokat. A hitelesítő adatok megadásához az **F5** billentyűt lenyomva nyissa meg az ESET Endpoint Security **További beállítások** párbeszédpaneljét, majd kattintson a **Frissítés** > **Profilok** > **Frissítések** > **Kapcsolati beállítások** > **Windows-megosztások** > **Kapcsolódás a helyi frissítési szerverhez** elemre. Ez megegyezik a Csatlakozás a helyi frissítési szerverhez című témakörben használt frissítési beállítással.

A tükrözési mappa eléréséhez ugyanabban a fiókba kell bejelentkezni, mint amelyben a tükrözés létrejött. Ha számítógép egy tartományban található, a „tartomány\felhasználó” felhasználónevet kell használni. Ha a számítógép nem egy tartományban található, az „IP_szerver_neve\felhasználó” vagy az „állomásnév\felhasználó” felhasználónevet kell használni.

A tükrözés beállításának befejeztével állítsa be a szervert a munkaállomásokon *UNC**ELÉRÉSI ÚT* formátumban.

1. Nyissa meg az ESET Endpoint Security **További beállítások** párbeszédpaneljét, és kattintson a **Frissítés** > **Profilok** > **Frissítések** elemre.
2. Letiltás ki a **Modulfrissítések** felirat melletti **Automatikus kiválasztás** opciót, és a **Frissítési szerver** mezőben az *UNC**PATH* formátumot használva vegyen fel egy új szervert.

A frissítések megfelelő működése érdekében a tükörmappát UNC formátumú elérési útként kell megadni. Előfordulhat, hogy csatlakoztatott hálózati meghajtóról nem sikerül a frissítés.

A tükör létrehozása a tükrözési eszközzel
A tükrözési eszköz nem olyan mappaszerkezetet hoz létre, mint a végponttükör. Mindegyik mappában egy termékcsoport frissítési fájljai találhatók. Meg kell adnia a teljes elérési utat a megfelelő mappához a tükröt használó termék frissítési beállításaiban.
Például az ESET PROTECT tükörből való frissítéséhez adja meg a következőt a Frissítési szerver beállításnál (a HTTP-szerver gyökérhelye szerint):
`http://your_server_address/mirror/eset_upd/era6`

Az utolsó csoport a programösszetevőket szabályozza. Alapértelmezés szerint a letöltött programösszetevők elő vannak készítve a helyi tükör másolására. Ha be van kapcsolva a **Termékfrissítések** funkció, nem kell a **Frissítés** elemre kattintani, mert amikor elérhetővé válnak, a program automatikusan a helyi tükörre másolja a fájlokat. A termékfrissítésekről a Frissítési mód című fejezetben olvashat bővebben.

A tükrözésből történő frissítéssel kapcsolatos hibaelhárítás

A legtöbb esetben a tükörszerverről való frissítés közbeni problémákat a következők okozzák: a tükörmappa beállításainak helytelen megadása, nem megfelelő hitelesítési adatok használata, a tükörből letölteni próbáló munkaállomások hibás beállításai vagy mindezek együttesen. Az alábbiakban áttekintheti a leggyakoribb problémákat, amelyek a tükrözésből történő frissítéskor adódhatnak.

Az ESET Endpoint Security hibát jelez, miközben a tükörszerverhez próbál csatlakozni – A hiba oka valószínűleg a munkaállomás által használandó frissítési szerver adatainak helytelensége (nem megfelelő hálózati elérési út vagy tükörmappa). A mappa ellenőrzéséhez kattintson a Windows **Start** menüjének **Futtatás** parancsára, írja be a mappa nevét, és kattintson az **OK** gombra. Megfelelő beállítások esetén a mappa tartalma jelenik meg.

Az ESET Endpoint Security felhasználónév és jelszó megadását kéri – A jelenséget a frissítési beállítások között megadott hitelesítő adatok (felhasználónév és jelszó) helytelensége okozhatja. A felhasználónév és a jelszó biztosítja a hozzáférést a helyi tükörszerverhez, ahonnan a program frissíteni tudja magát. Ellenőrizze, hogy a

megadott hitelesítési adatok helyesek-e, és a megfelelő formátumban vannak-e megadva. Például tartomány\felhasználónév vagy munkacsoport\felhasználónév alakban –, az ahhoz tartozó jelszóval együtt. Ne feledje, ha a tükörszerver elérhető a Mindenki csoport által, az még nem jelenti azt, hogy mindenki megfelelő hozzáférési jogosultsággal rendelkezik. A Mindenki csoportnak ugyanis nem tagjai a nem hitelesített felhasználók; ez a csoport csupán a tartományi felhasználókat tartalmazza. Így a frissítési beállításoknál akkor is meg kell adni a felhasználónevet és a jelszót, ha a mappa „Mindenki” számára elérhető.

Az ESET Endpoint Security hibát jelez, miközben a tükörszerverhez próbál csatlakozni – A tükör HTTP-verziójának eléréséhez megadott porton valami gátolja a kommunikációt.

Az **ESET Endpoint Security hibát jelez frissítési fájlok letöltésekor** – A hiba oka valószínűleg az, hogy helytelenül van beállítva (hálózati elérési út a Tükör mappához) az a frissítési szerver, amelyről a helyi munkaállomások letöltik a frissítéseket.

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. Ha ütemezett feladatot szeretne beállítani, az **Eszközök** lapon válassza a **Feladatütemező** eszközt. Az ESET Endpoint Security programban alapértelmezés szerint az alábbi feladatok aktívak:

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

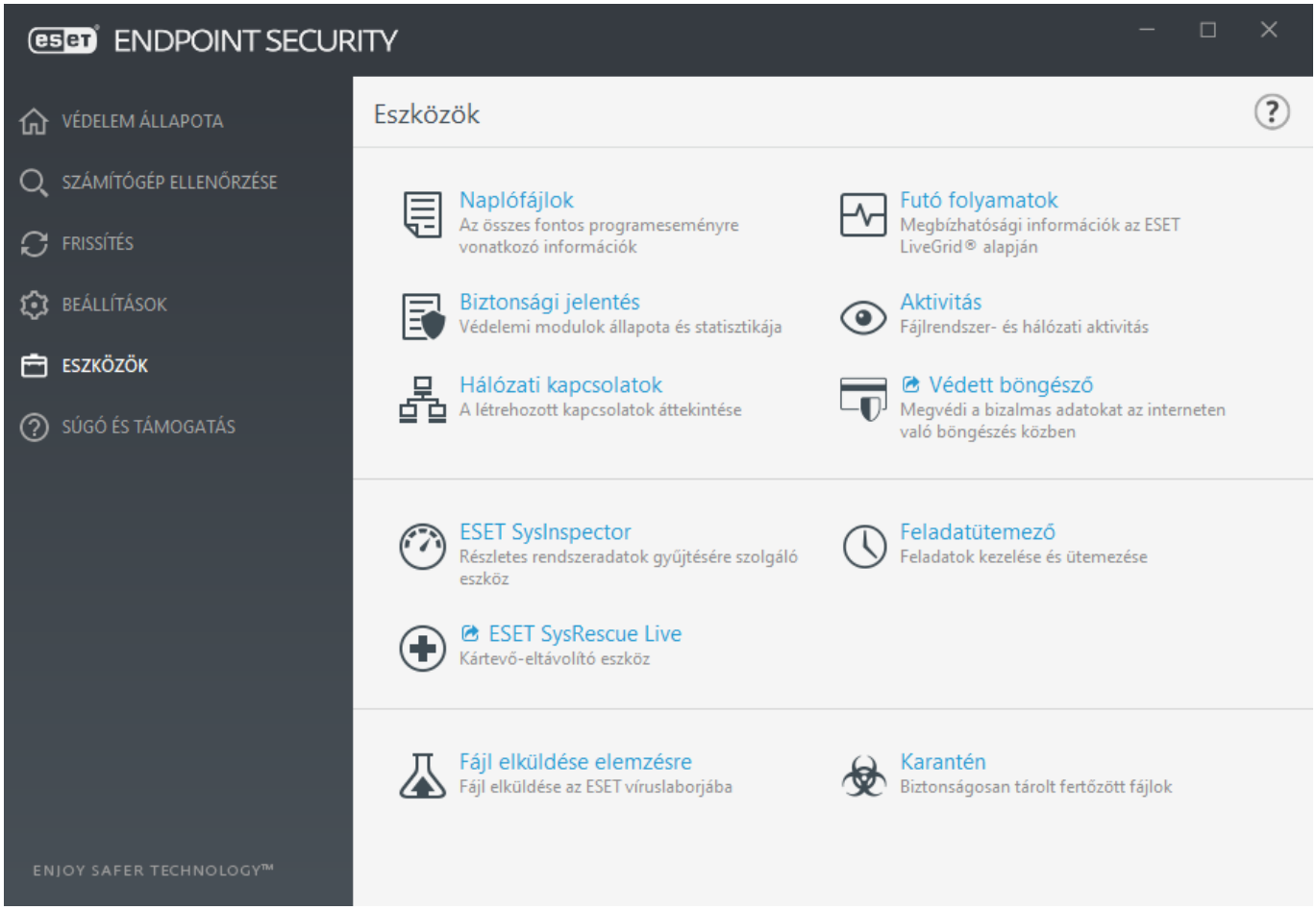
Minden frissítési feladat módosítható az igényeinek megfelelően. Az alapértelmezett frissítési feladatok mellett a felhasználó által definiált konfigurációjú új feladatok is létrehozhatók. A frissítési feladatok létrehozásáról és beállításáról a Feladatütemező című fejezet nyújt részletes tájékoztatást.

Eszközök

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

A lapon az alábbi eszközök láthatók:

- Naplófájlok
- Futó folyamatok (ha az ESET LiveGrid® engedélyezve van az ESET Endpoint Security alkalmazásban)
- Biztonsági jelentés (nem felügyelt végpontok esetén)
- Hálózati kapcsolatok (ha a Tűzfal engedélyezve van az ESET Endpoint Security alkalmazásban)
- Védett böngésző (alapértelmezés szerint letiltva az ESET Endpoint Security alkalmazásban)
- ESET SysInspector
- Feladatütemező
- ESET SysRescue Live – Átirányítja az ESET SysRescue Live webhelyre, ahol letöltheti az ESET SysRescue Live .iso CD-/DVD-képet.
- 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 naplók fontos szerepet töltenek be a rendszerelemzésben, az észlelésben és a hibaelhárításban. A program a naplózást a háttérben aktívan, felhasználói beavatkozás nélkül végzi. Az információkat az aktuális naplórészletességi beállításoknak megfelelően rögzíti. A szöveges üzeneteket és naplókat közvetlenül az ESET Endpoint Security környezetéből tekintheti meg. A naplófájlok archiválására is van lehetőség.

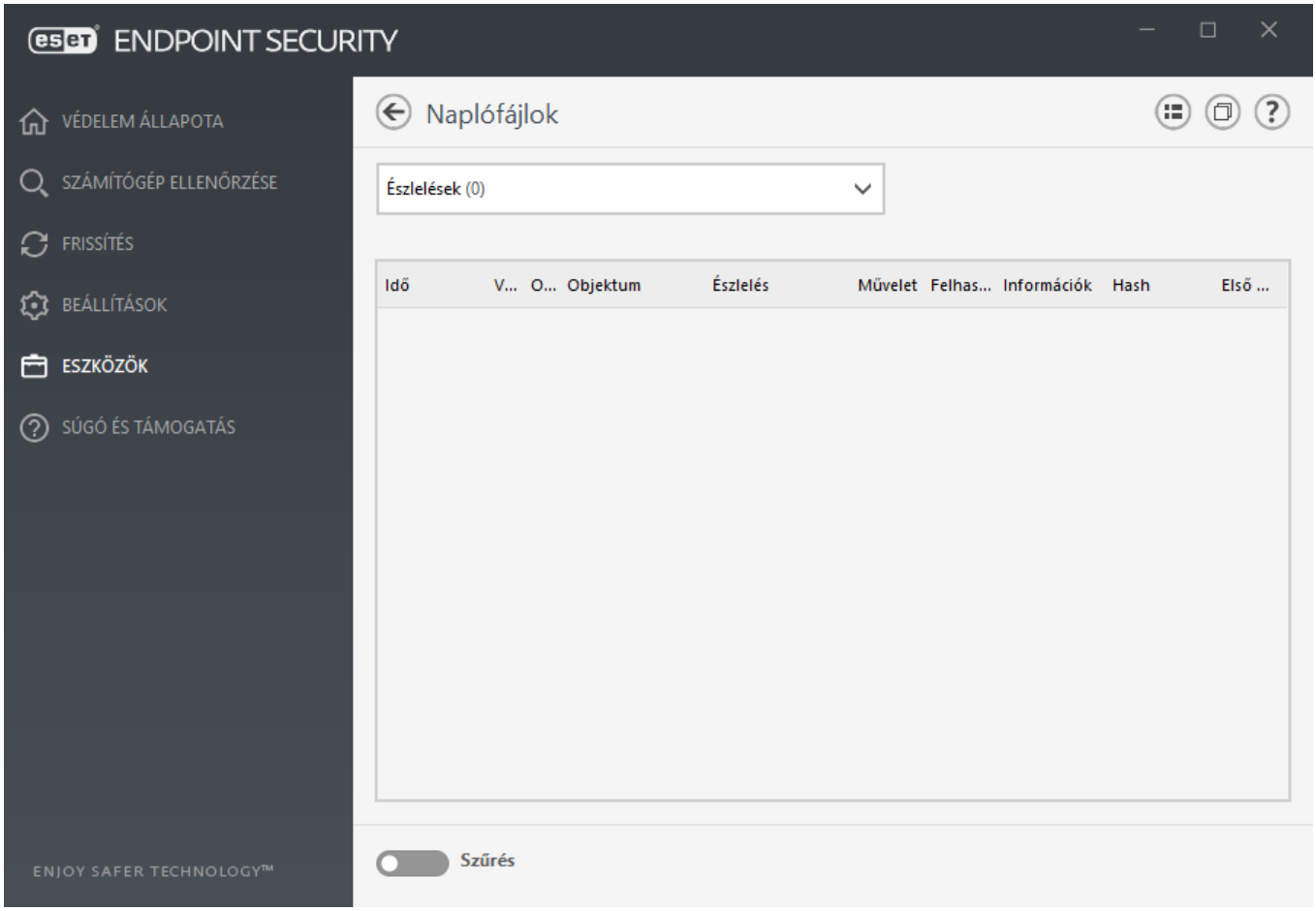
A naplófájlok a fő programablak **Eszközök** > **Naplófájlok** lehetőségére kattintva érhetők el. A **Napló** legördülő menüben válassza ki a kívánt naplótípust. A választható naplók az alábbiak:

- **Észlelések** – Ez a napló részletes információkat szolgáltat az ESET Endpoint Security moduljai által észlelt kártevőkről és fertőzésekről. A naplózott információ tartalmazza az észlelés idejét, a kártevő nevét és helyét, a végrehajtott műveletet és annak a felhasználónak a nevét, aki a fertőzés észlelésének idején be volt jelentkezve. A naplóbejegyzésre duplán kattintva külön ablakban megjelennek az adatai. 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 Endpoint 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** – Ebben az ablakban minden ellenőrzési eredmény megjelenik. Minden sor egy-egy számítógép-ellenőrzésnek felel meg. Az egyes bejegyzésekre duplán kattintva megjelenítheti az adott ellenőrzés részletes adatait.

- **Letiltott fájlok** – Azokról a letiltott fájlokról tartalmaz rekordokat, amelyeket nem lehetett elérni az ESET Enterprise Inspector szolgáltatáshoz kapcsolódva. A protokoll megjeleníti az okot és a forrásmodult, amely letiltotta a fájlt, valamint a fájlt végrehajtó alkalmazást és felhasználót. További információkért tekintse meg az ESET Enterprise Inspector online felhasználói útmutatóját.
- **Elküldött fájlok** – Az ESET LiveGrid®, illetve az ESET LiveGuard számára elemzésre elküldött fájlok listáját tartalmazza.
- **Auditálási naplók** – Mindegyik napló tartalmazza a módosítás dátumát és időpontját, a módosítás típusát, a leírást, a forrást, és a felhasználót. További információkért tekintse meg az Auditálási naplók című részt.
- **Behatolásmegelőző rendszer** – A bejegyzésre megjelölt adott szabályok bejegyzéseit tartalmazza. A protokoll megjeleníti a műveletet meghívó alkalmazást, az eredményt (a szabály engedélyezett vagy letiltott volt-e) és a létrehozott szabály nevét.
- **Hálózati védelem** – A tűzfal naplója megjeleníti a Hálózati támadások elleni védelem és a Tűzfal 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. Adott hálózati támadásokról az IDS és további beállítások című fejezetben olvashat bővebben.

- **Szűrt webhelyek** – Ebben a listában láthatók a webhozzáférés-védelem vagy a webfelügyelet által letiltott webhelyek. Ezekben a naplókban látható az idő, az URL-cím, a felhasználó és az adott webhely felé kapcsolatot megnyitó alkalmazás.

- **Levélszemétszűrő** – A levélszemétként megjelölt e-mail e-mailekhez tartozó bejegyzéseket tartalmazza.
- **Webfelügyelet** – Megjeleníti a letiltott vagy engedélyezett URL-címeket és a kategóriákkal kapcsolatos részletes információkat. A végrehajtott műveleteket megjelenítő oszlopban látható a szűrési szabályok alkalmazásának módja.
- **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. Itt láthatók bizonyos adatok, többek között az eszköz típusa, a sorozatszám, a gyártó neve és az adathordozó mérete (ha van).



Jelölje ki egy tetszőleges napló tartalmát, majd a `Ctrl + C` **billentyűkombinációval másolja a vágólapra**. Több bejegyzést a `Ctrl + Shift` billentyűkombinációt 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 bejegyzés(eke)t vagy az összes megjelenített bejegyzést. A művelet végrehajtásához rendszergazdai jogosultságokra van szükség.
- **Exportálás** – Ezzel XML formátumban exportálhatja a bejegyzésekre vonatkozó információkat.
- **Minden exportálása** – Ezzel XML formátumban exportálhatja a bejegyzésekre vonatkozó információkat.
- **Keresés/Következő keresése/Előző keresése** – Miután erre az opcióra kattintott, a Napló szűrése ablakban megadhatja az adott naplóbejegyzések szűrési feltételeit.
- **Kivétel létrehozása** – Létrehozhat egy új észlelési kivételt egy varázsló segítségével (nem áll rendelkezésre kártevőkészlelések esetén).

Napló szűrése

Kattintson a  **A szűréshez** az **Eszközök** > **Naplófájlok** lapon adhatja meg a szűrési feltételeket.

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 Endpoint 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 beépített tűzfallalstb.).

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 opciót engedélyezve a naplófájlok optimalizálása automatikusan megtörténik, ha a fölösleges bejegyzések száma meghaladja a **Ha a fölösleges bejegyzések száma több mint (%)** mezőben megadott százalékos értéket.

Az **Optimalizálás** gombra kattintva elkezdheti a naplófájlok töredezettségmentesítését. A teljesítmény és a naplók feldolgozási sebességének javítása érdekében a program eltávolítja az összes üres naplóbejegyzést. A teljesítményjavulás különösen a nagyszámú bejegyzést tartalmazó naplófájloknál látványos.

A **Szöveges protokoll engedélyezése** beállítással engedélyezheti a naplók tárolását a naplófájloktól eltérő fájlformátumban:

- **Célkönyvtár** – Válassza ki a naplófájlok tárolására szolgáló könyvtárat (csak szöveges/CSV-fájlokra vonatkozik). Másolhatja az elérési utat, vagy kiválaszthat másik könyvtárat a **Kiürítés** gombra kattintva. Az egyes naplószakaszokhoz saját, előre megadott nevű fájl tartozik (például a *virlog.txt* a naplófájlok **Észlelt kártevők** 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 konfigurációmódosítások nyomon követésének engedélyezése az Auditálási naplóban – A konfigurációs módosításokról tájékoztat. Az Auditálási napló című részben bővebben tájékozódhat erről.

> 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.

Auditálási naplók

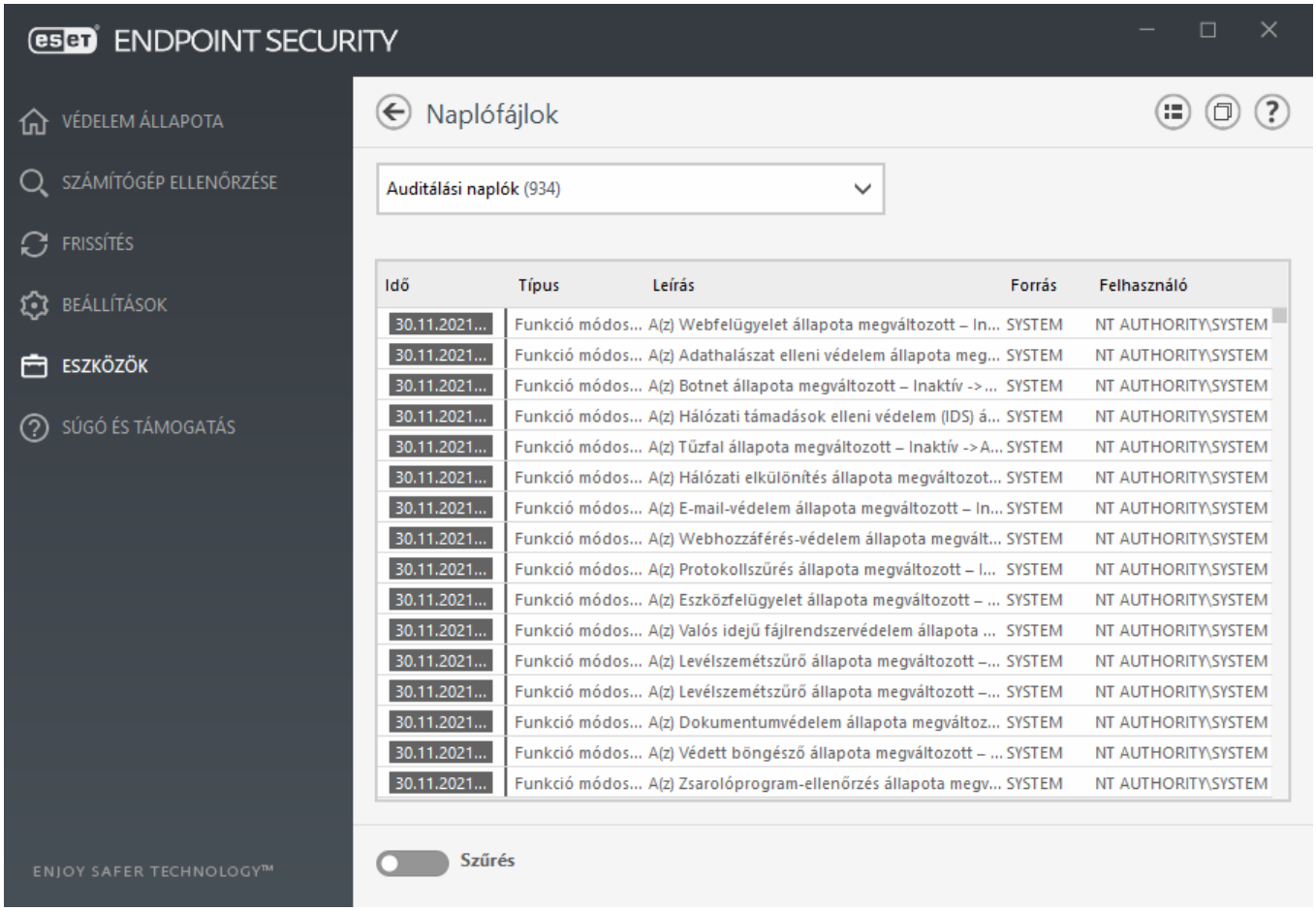
Vállalati környezetben általában több felhasználó rendelkezik végpontok konfigurálását lehetővé tevő hozzáférési jogosultsággal. Mivel a termékkonfiguráció módosítása drámai hatással lehet a termék működésére, rendkívül fontos, hogy a rendszergazdák nyomon kövessék a felhasználók által végrehajtott módosításokat, mert így lehetőségük nyílik a problémák gyors beazonosítására és elhárítására, valamint annak megakadályozására is, hogy a későbbiekben ugyanolyan vagy hasonló problémák fellépjenek.

Az Auditálási napló az ESET Endpoint Security 7.1-es verziójától rendelkezésre álló új típusú naplózás, amelynek segítségével megállapítható a problémák eredete. Az Auditálási napló nyomon követi a konfigurációban és a védelmi állapotban végrehajtott módosításokat, és pillanatképeket rögzít későbbi felhasználásra.

Az **Auditálási napló** megtekintéséhez a főmenüben kattintson az **Eszközök** elemre, majd kattintson a **Naplófájlok** elemre, és válassza ki a **Naplófájlok** menüpontot a legördülő menüben.

Az Auditálási napló a következőkről tartalmaz információkat:

- Idő – A módosítás végrehajtásának időpontja
- Típus – A módosított beállítás vagy funkció típusa
- Leírás – Annak ismertetése, hogy pontosan mi módosult, a beállítás mely részét módosították, és hány módosítást hajtottak végre
- Forrás – A módosítás forrásának helye
- Felhasználó – A módosítást végrehajtó személy



A Naplófájlok ablakban kattintson a jobb gombbal az auditálási napló bármely **Beállítások módosítva** típusára, majd a helyi menüből válassza ki a **Módosítások megjelenítése** menüpontot a végrehajtott módosításokkal kapcsolatos részletes információk megjelenítéséhez. Vissza is állíthatja a módosított beállítást a helyi menü **Visszaállítás** menüpontját kiválasztva (nem áll rendelkezésre az ESET PROTECT által felügyelt termékekben). Ha a helyi menüben a **Minden törlése** menüpontot választja ki, létrejön az adott műveletet ismertető napló.

Ha a **Naplófájlok automatikus optimalizálása** funkció engedélyezve van a **További beállítások** > **Eszközök** > **Naplófájlok** lapon, akkor az auditálási naplók optimalizálása is automatikusan megtörténik a többi naplóhoz hasonlóan.

Ha **Az ennél régebbi naplóbejegyzések törlése (nap)** funkció engedélyezve van a **További beállítások** > **Eszközök** > **Naplófájlok** lapon, akkor a megadott számú napnál régebbi naplóbejegyzések automatikusan törlődnek.

Feladatütemező

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

A Feladatütemező az ESET Endpoint Security fő programablakából érhető el az **Eszközök** > **Feladatütemező** elemre kattintva. A **Feladatütemező** valamennyi ütemezett feladat és beállított tulajdonságainak (például előre definiált dátum, időpont és ellenőrzési profil) összesített listáját tartalmazza.

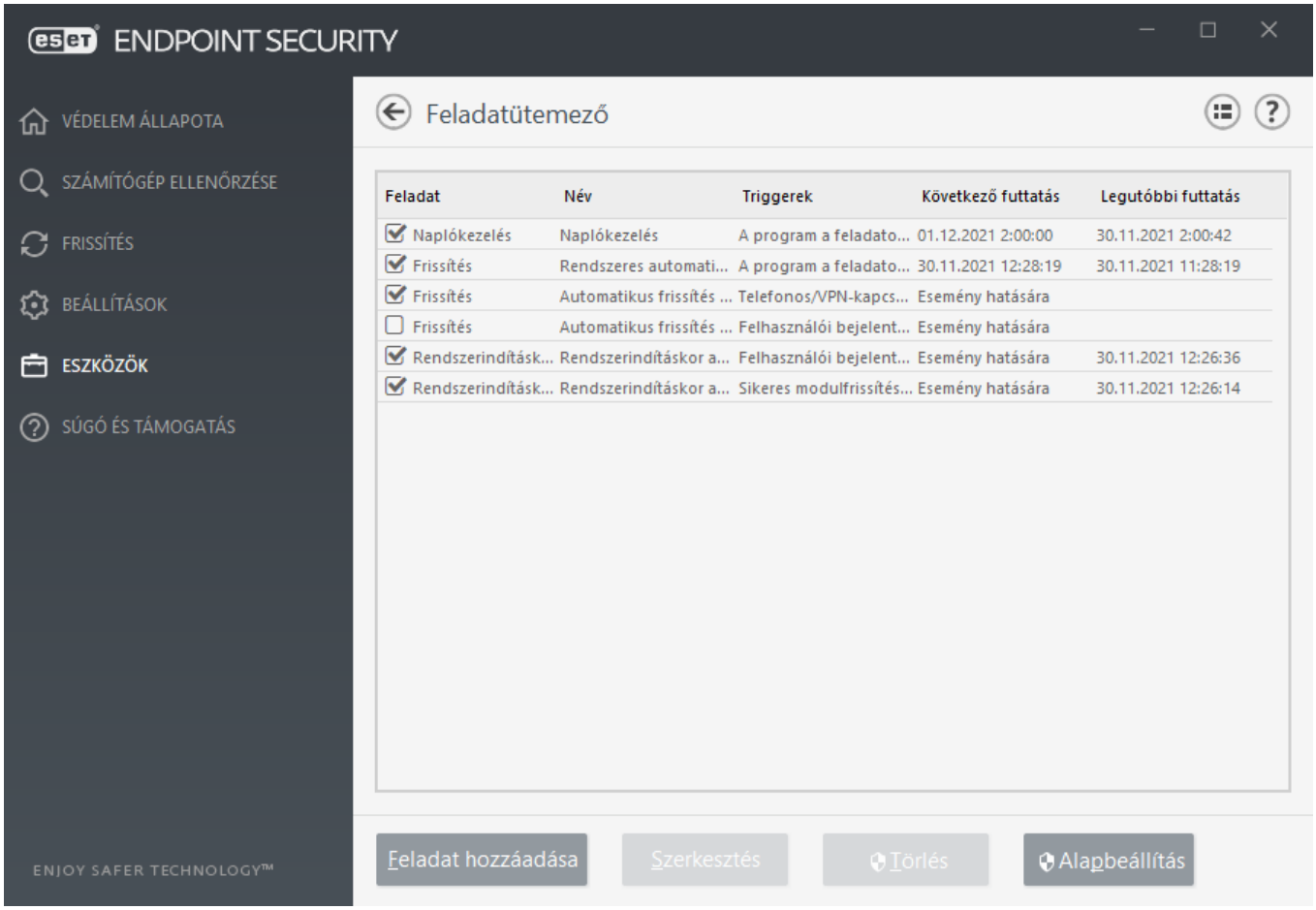
A feladatütemező a következő feladatok időzített végrehajtására alkalmas: keresőmotor frissítése, ellenőrzési feladatok, rendszerindításkor automatikusan futtatott fájlok ellenőrzése és naplókezelés. A Feladatütemező főablakából közvetlenül hozzáadhat vagy törölhet feladatokat. (Kattintson az ablak alján lévő **Feladat hozzáadása**

vagy **Törlés** gombra.) 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 sikeres modulfrissítés után)

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



Új feladat hozzáadása

1. Kattintson az ablak alján található **Feladat hozzáadása** gombra.
2. Adja meg a feladat nevét.
3. Válassza ki a kívánt feladatot a legördülő menüben:

- **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 keresőmotor és a programmodulok frissítésére.

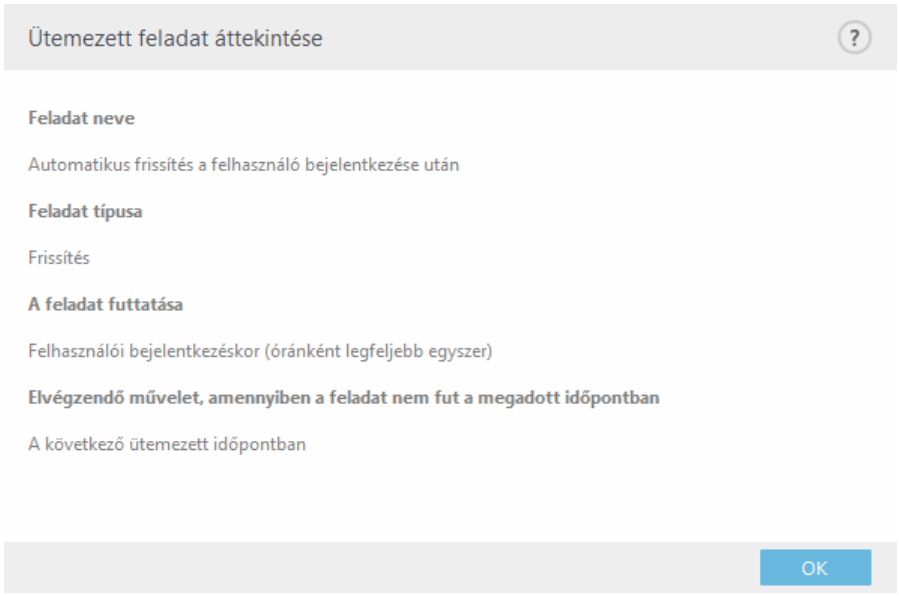
4. Kapcsolja be az **Engedélyezve** kapcsolót, ha aktiválni szeretné a feladatot (ezt később az ütemezett feladatok listájában található jelölőnégyzet bejelölésével/jelölésének törlésével teheti meg), kattintson a **Tovább** gombra, és válasszon egyet az alábbi időzítési beállítások közül:

- **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** (az időtartam az **Utolsó futtatás óta eltelt idő** görgetődobozban adható meg)

Az ütemezett feladat áttekintéséhez kattintson a jobb gombbal, és válassza a **Feladat részleteinek megjelenítése** parancsot.



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. Tekintse meg az ESET SysInspector online felhasználói útmutatóját is.

A SysInspector ablaka a létrehozott naplók alábbi adatait jeleníti meg:

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

A választható műveletek az alábbiak:

- **Megjelenítés** – A létrehozott napló megnyitása. A jobb gombbal kattinthat egy adott naplófájlra, és a helyi menüben választhatja a **Megjelenítés** parancsot.
- **Létrehozás** – Új napló létrehozása. Mielőtt megkísérelné a napló elérését, várja meg, hogy az ESET SysInspector elkészüljön (a napló állapota **Létrehozva** lesz).
- **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).
- **Létrehozás** – Új napló létrehozása. Mielőtt megkísérelné a napló elérését, várja meg, hogy az ESET SysInspector elkészüljön (a napló állapota **Létrehozva** lesz).
- **Törlés** – A kijelölt napló törlése.
- **Minden törlése** – Az összes napló törlése.
- **Exportálás** – A napló exportálása .xml vagy tömörített .xml fájlba.

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.

Három lehetőség közül választhat:

1. lehetőség: 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.

2. lehetőség: 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. Ez az információ tartalmazhatja a kártevőt magában foglaló fájl mintáját vagy másolatát, a fájl elérési útját és nevét, a dátumot és az időt, azt a folyamatot, amelynek során a kártevő megjelent a számítógépen, valamint a számítógép operációs rendszerére vonatkozó adatokat.

Az ESET Endpoint 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.

3. lehetőség: Az ESET LiveGrid® engedélyezésének mellőzése

A szoftver funkciói megmaradnak, bizonyos esetekben azonban előfordulhat, hogy az ESET LiveGrid® engedélyezése esetén az ESET Endpoint Security a keresőmotor frissítésénél gyorsabban reagál az új kártevőkre.

> 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 Endpoint Security alkalmazásban.

Felhőalapú védelmi konfiguráció a További beállításokban

Az ESET LiveGrid® beállításainak megnyitásához nyomja le az **F5** billentyűt, és a megjelenő További beállítások párbeszédpanelen bontsa ki a **Keresőmotor** > **Felhőalapú védelem csomópontot**.

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.

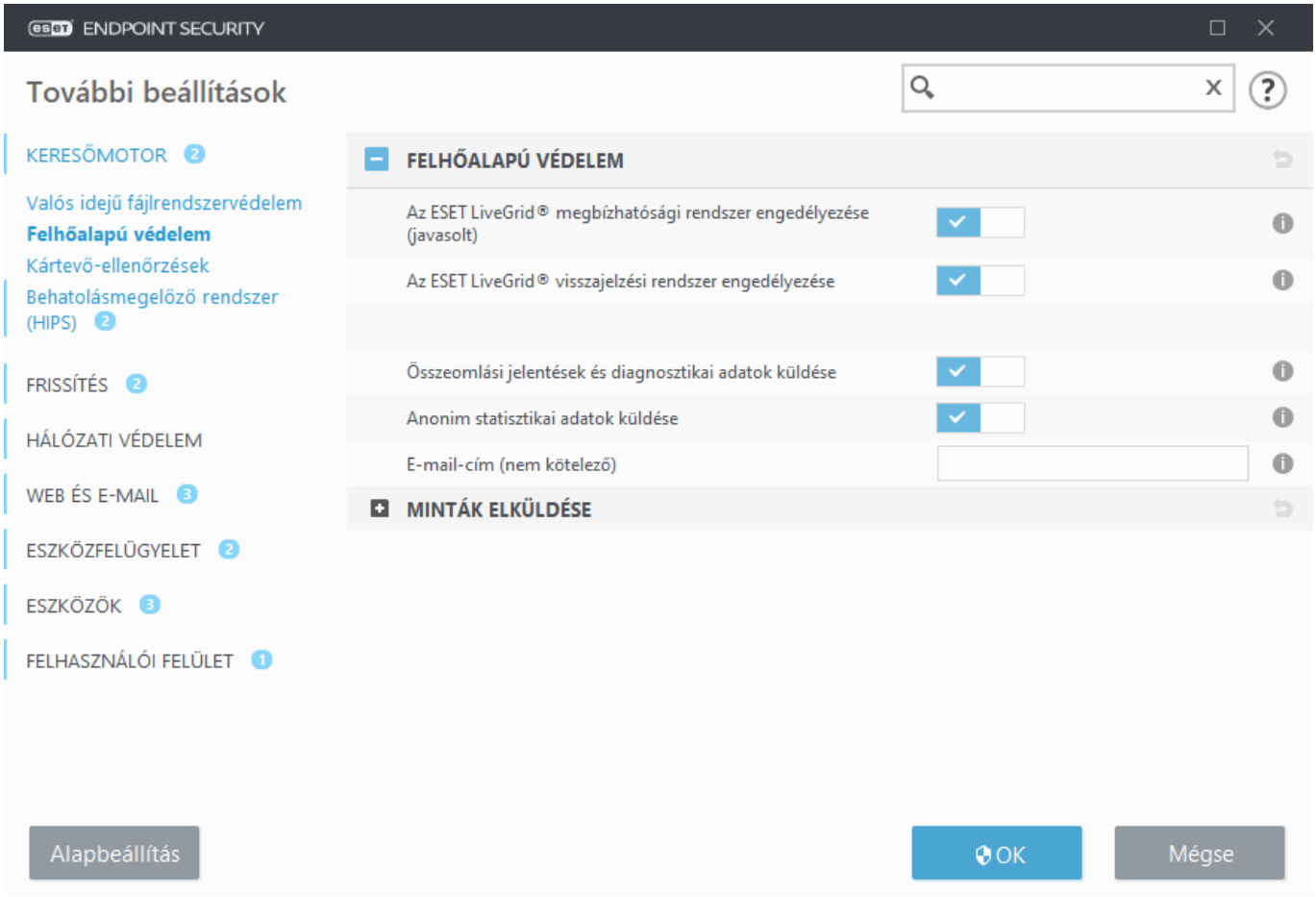
Az ESET LiveGuard engedélyezése (nem látható az ESET Endpoint Security termékben) – Az ESET LiveGuard az ESET által biztosított fizetős szolgáltatás. Egy olyan védelmi réteget biztosít, amelynek célja kifejezetten az újonnan megjelent kártevők által keltett kockázatok minimalizálása. A gyanús fájlok automatikusan bekerülnek az ESET-felhőbe. A felhőben elemzi őket a fejlett kártevőészlelő motorunk. A mintát biztosító felhasználó összegző jelentést kap a megfigyelt minta viselkedéséről.

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 azonban csak akkor keresik fel, ha a gyanús fájlokkal kapcsolatban további információra van szükségük.



Minták elküldése

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

Az észlelt vírusminták automatikus elküldése

Válassza ki, hogy milyen típusú mintákat szeretne elküldeni az ESET-nek elemzésre és a jövőbeli észlelés javítása céljából. A választható lehetőségek az alábbiak:

- **Az összes észlelt minta** – Az összes olyan objektum, amelyet észlelt a kereső motor (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 Endpoint Security védelmi moduljainak egyike gyanúsnak vagy zavaros viselkedésűnek találja a mintákat.

- **Végrehajtható fájlok** – Például a következő fájlok: .exe, .dll, .sys
- **Tömörített fájlok** – Például a következő fájltípusok: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

- **Tömörített fájlok** – Például a következő fájltípusok: .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** > **Felhőalapú védelem** > **Minták elküldése** > **Kizárások** elemre, majd adja hozzá a *download.domain.com* kizárást.

ESET LiveGuard

Ha az ESET LiveGuard szolgáltatást kliensgépen szeretné engedélyezni az ESET PROTECT Webkonzol segítségével, tekintse meg az ESET Endpoint Security ESET LiveGuard-konfigurációja című részt.

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.

Kivételszűrő a Felhőalapú védelemhez

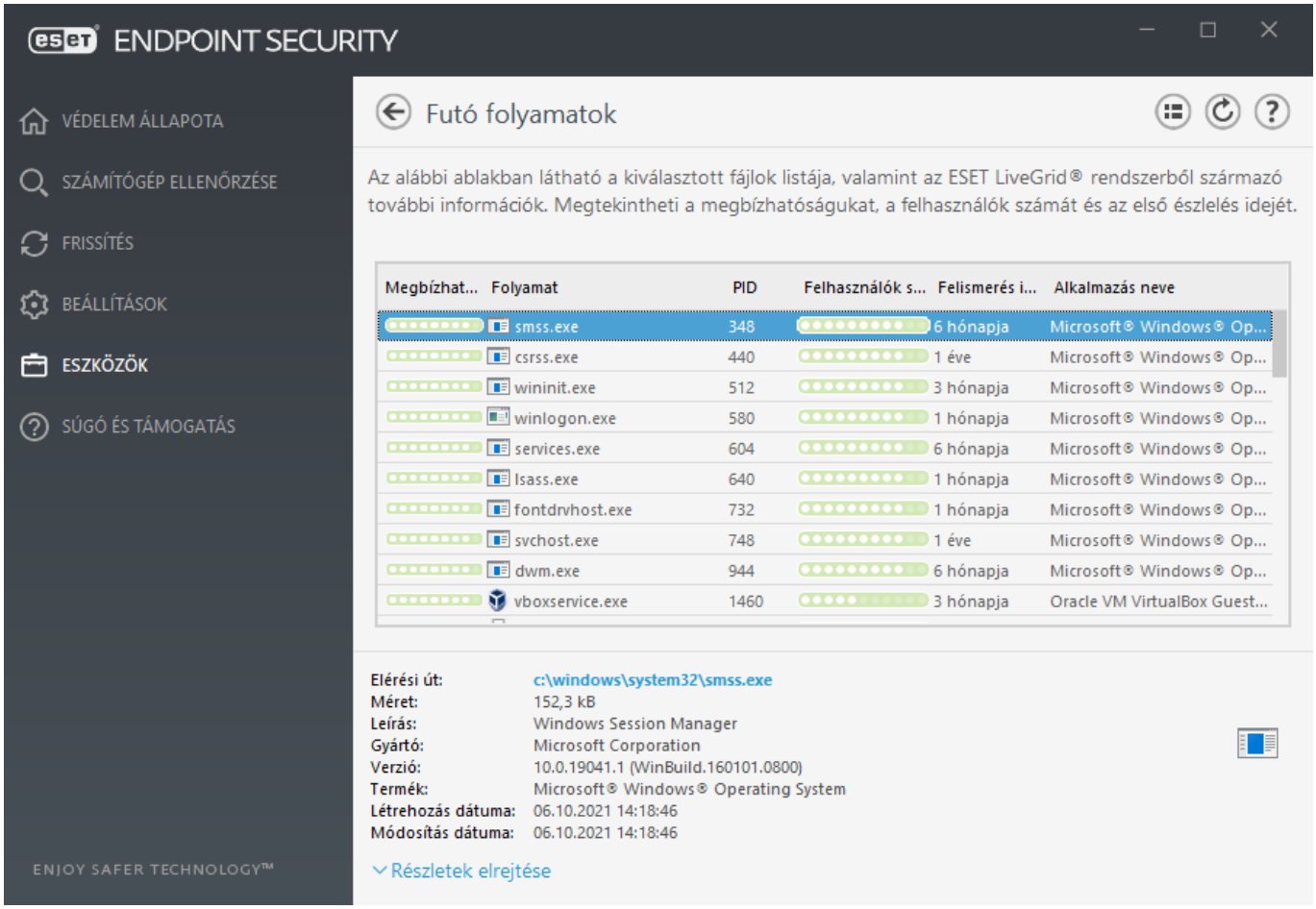
A Kivételszűrő segítségével megadhatja, hogy mely fájlokat vagy mappákat ne küldjön el a rendszer elemzésre. Az itt felsorolt fájlokat a rendszer még abban az esetben sem küldi el az ESET víruslaborjába elemzésre, ha azok gyanús kódot tartalmaznak. A gyakori fájltípusok (többek között a .doc stb.) alapértelmezés 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** > **Felhőalapú védelem** > **Minták elküldése** > **Kizárások** elemre, majd adja hozzá a *download.domain.com* kizárást.

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 Endpoint Security részletes adatokat szolgáltat a futó folyamatokról, amelyek segítségével az engedélyezett ESET LiveGrid® technológia biztosítja a felhasználók védelmét.



Megbízhatóság – A legtöbb esetben az ESET Endpoint 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 heurisztikai szabályok alapján az objektumok megbízhatósági szintje a 9 – Legmegbízhatóbb (zöld) és a 0 – Legmegbízhatatlanabb (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.

PID – A Windows operációs rendszereken futó folyamatok azonosítója.

> A zöld kockázati szintű ismert alkalmazások egészen biztosan nem fertőzöttek (engedélyezőlistán vannak), ezért a szűrésből kizártak, ami növeli a kézi indítású ellenőrzések és a valós idejű fájlrendszervédelem sebességét.

Felhasználók száma – Egy adott alkalmazást használó felhasználók száma. Ezt az információt az ESET LiveGrid® technológia gyűjti.

Felismerés ideje – Az időtartam, amióta az ESET LiveGrid® technológia észlelte az alkalmazást.

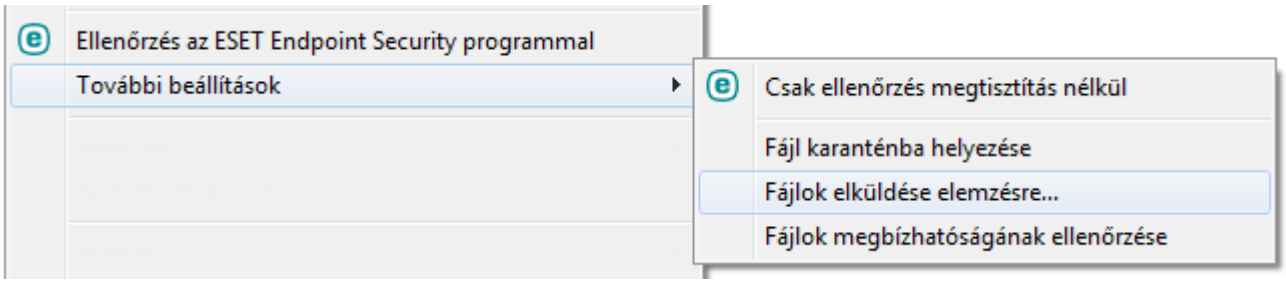
> Az alkalmazás nem feltétlenül kártékony szoftver, ha a jelölése Ismeretlen (narancsszínű)biztonsági szintű. Ezek rendszerint csak újabb alkalmazások. Ha kétségei vannak egy ilyen fájl biztonságosságát illetően, a Fájl elküldése elemzésre elemre kattintva elküldheti a fájlt elemzésre az ESET víruslaborjába. Ha a fájl egy kártékony alkalmazás, bekerül a keresőmotor valamelyik későbbi frissítésébe.

Alkalmazás neve – Egy programnak vagy folyamatnak adott név.

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

- **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 dátuma** – Az alkalmazás létrehozásának dátuma és időpontja.
- **Módosítás dátuma** – Az alkalmazás legutóbbi módosításának dátuma és időpontja.

> Nem csak a futó programok és folyamatok megbízhatósága ellenőrizhető a fájlokon – jelölje ki az ellenőrizni kívánt fájlokat, kattintson rájuk a jobb gombbal, és válassza a helyi menü **További beállítások** > **Fájlok megbízhatóságának ellenőrzése az ESET LiveGrid®** rendszerrel parancsát.



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 webfelügyelet alatt álló weboldalak – A webfelügyelet letiltott weboldalak számát jeleníti meg.

Észlelt kéretlen alkalmazások – A kéretlen alkalmazások számát jeleníti meg.

Észlelt levélszemét – Az észlelt levélszemét számát jeleníti meg.

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.

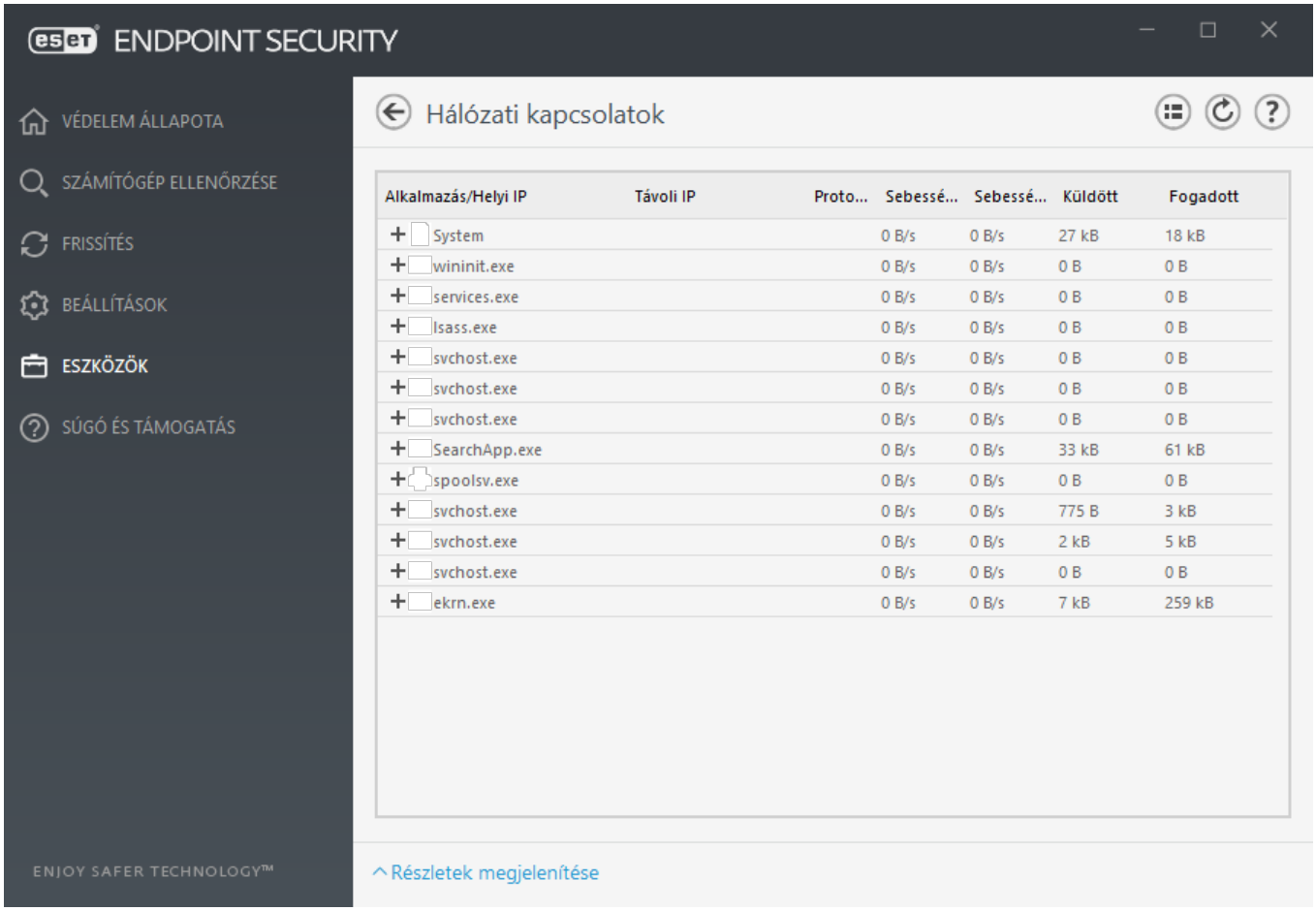
A jobb felső sarokban található fogaskerékre kattintva **engedélyezheti/letilthatja a biztonsági jelentésekről szóló értesítéseket**, vagy válassza ki, hogy az adatok az elmúlt 30 napból vagy a termék aktiválása óta jelenjenek meg. Ha az ESET Endpoint Security telepítése kevesebb, mint 30 napja történt 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** lapon.

Hálózati kapcsolatok

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



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

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.

Jelöljön ki egy alkalmazást vagy IP-címet a hálózati kapcsolatok képernyőjén, és kattintson rá a jobb gombbal az alábbi struktúrájú helyi menü megnyitásához:

Állomásnevek feloldása – Ha bejelöli a jelölőnégyzetet, 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 – A jelölőnégyzet bejelölése esetén a rendszer azokat a kapcsolatokat is megjeleníti, amelyekben a távoli oldal a helyi rendszer (a localhost tartománynévvel azonosított állomás).

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

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

Frissítési sebesség – Az aktív kapcsolatok frissítési gyakorisága.

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

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

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

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

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

Minták elküldése 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).

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 minták leadására szolgáló űrlap az **Eszközök** > **Minta elküldése elemzésre** lapon található.
2. A fájlt e-mailben is elküldheti. Ha inkább ezt a megoldást választja, tömörítse a fájlt WinRAR/ZIP 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 Webfelügyelet modul által helytelenül kategorizált webhelyek bejelentéséhezez az ESET-tudásbáziscikk nyújt segítséget.

A megnyitott **Minta kiválasztása elemzésre** lapon válassza ki az üzenetének leginkább megfelelő leírást **A fájl elküldésének oka** legördülő menüben:

- **Gyanús fájl**
- **Gyanús webhely** **(valamilyen kártevővel fertőzött webhely)**,
- **Tévesen jelentett fájl** (fertőzöttként észlelt, de nem fertőzött fájl)
- **Tévesen jelentett webhely**
- **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.

> 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 miként 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.

Karantén

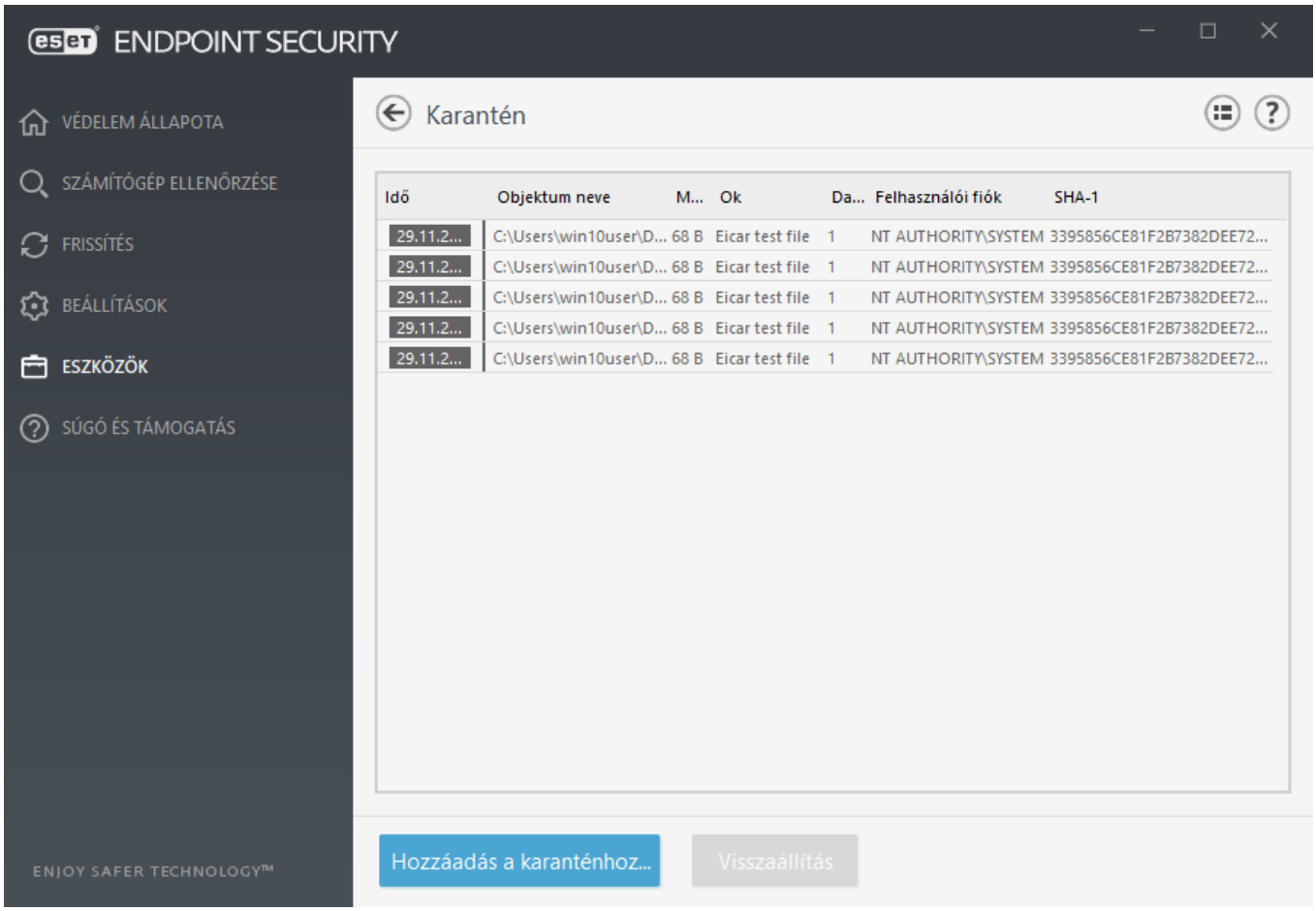
A karantén fő funkciója a jelentett objektumok (például kártevő, fertőzött fájlok vagy kéretlen alkalmazások) biztonságos tárolása.

A karantén az ESET Endpoint Securityfő programablakából érhető el az **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).

- Én kezelem távolról a karantént a kliensszámítógépeken



Fájlok karanténba helyezése

Az ESET Endpoint 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 Endpoint 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 **Hozzáadás a karanténhoz** gombra a program főablakában.

c. 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.

> Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
> - A karantén kezelése az ESET PROTECT szolgáltatásban
> - Az ESET-termékem észlelésről értesített – mit tegyek?

A proxyszerver beállításai

Nagyméretű helyi 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 Endpoint 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 Endpoint 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,

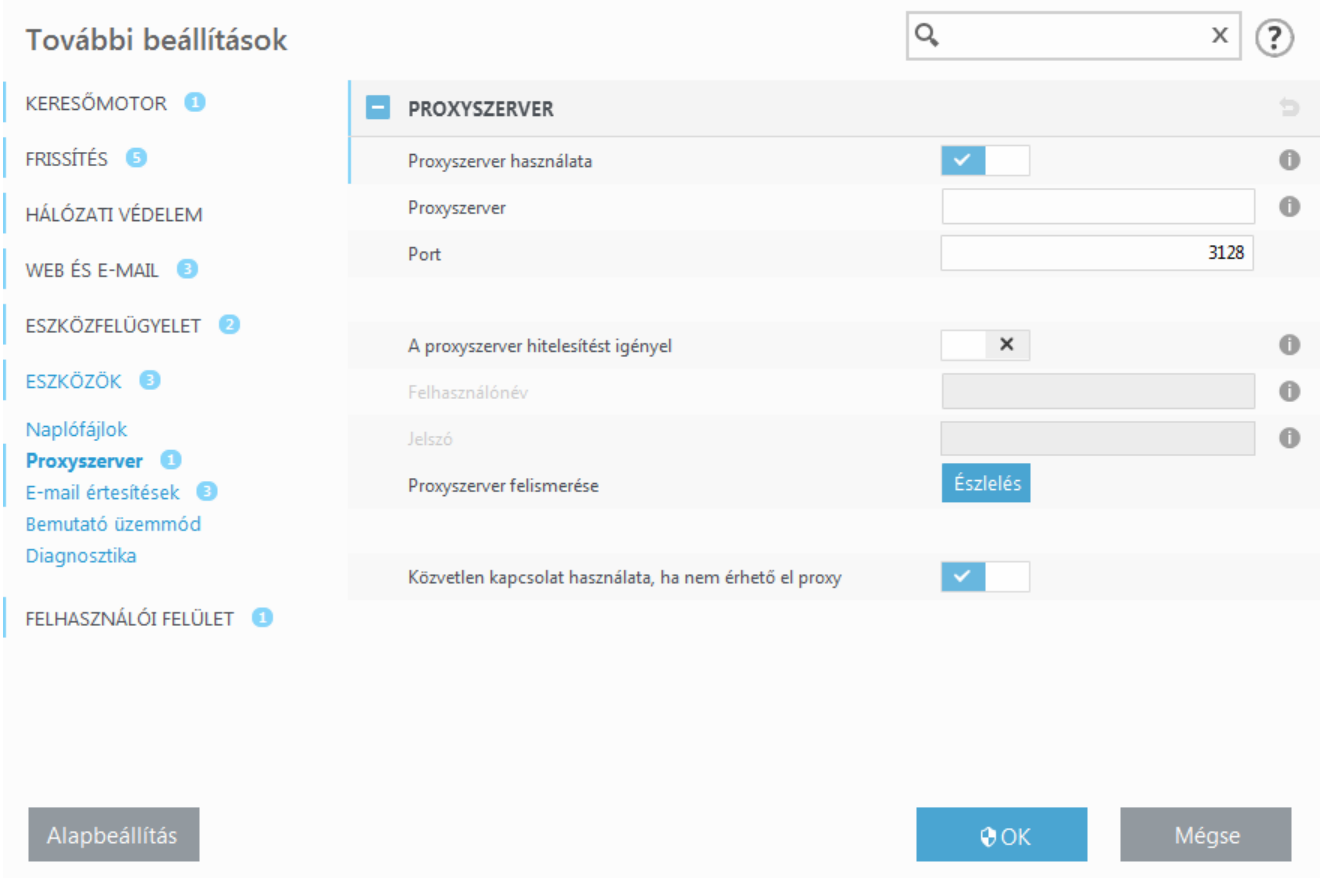
majd írja be a proxyszerver címét a **Proxyszerver** mezőbe, a portszámot pedig a **Port** mezőbe.

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. A program átmásolja az operációs rendszer megadott paramétereit. Az operációs rendszeren lévő proxybeállítások megkereséséhez nyomja meg a **Windows + I** billentyűkombinációt, majd kattintson a **Hálózat és internet** > **Proxy** elemre.

Felhasználónevét és jelszavát manuálisan kell megadnia a **Proxyszerver** beállításai között.

Közvetlen kapcsolat használata, ha nem érhető el proxy – Ha az ESET Endpoint Security proxy használatára van konfigurálva, és a proxy nem érhető el, az ESET Endpoint Security kihagyja a proxyt, és közvetlenül az ESET-szerverekkel kommunikál.

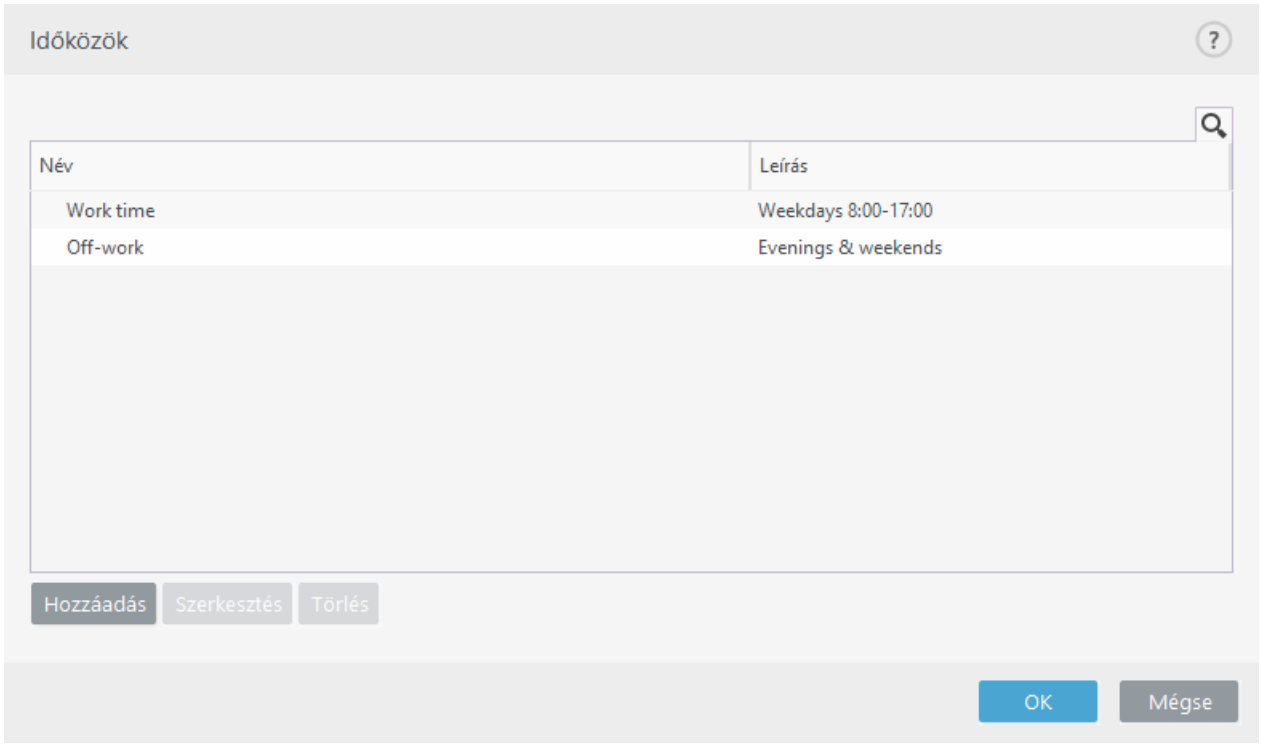
A proxyszerver-beállítások létrehozhatók a további frissítési beállításokban is (a **További beállítások** > **Frissítés** > **Profilok** > **Frissítések** > **Kapcsolódási beállítások** lapon válassza ki a **Kapcsolódás proxyszerveren keresztül** menüpontot a **Proxy mód** legördülő menüben). Ez a beállítás adott frissítési profilra vonatkozik, és laptopok esetén javasolt, mivel azok a keresőmotor-frissítéseket gyakran távoli helyekről kapják. Erről a beállításról a További frissítési beállítások című témakörben talál további információt.



Időközök

Létrehozásuk után az időközök az **Eszközfelügyelet** és a **Webfelügyelet** szabályaihoz rendelhetők hozzá. Az **Időközök** beállítás a **További beállítások** > **Eszközök** lapon találhatók. A beállítással általánosan használt időközök definiálhatók (pl munkaidő, hétvége stb.), és egyszerűen újra felhasználhatók anélkül, hogy az időtartományokat újra definiálni kellene mindegyik szabály esetén. Bármilyen releváns, időalapú felügyeletet támogató

szabálytípushoz alkalmazható időköz.



Időköz létrehozásához hajtsa végre a következőket:

1. Kattintson a **Szerkesztés** > **Hozzáadás** elemre.
2. Írja be a nevet, majd az időköz **leírását**, végül pedig kattintson a **Hozzáadás** gombra.
3. Adja meg a napot és az időköz kezdetét és végét, vagy válassza ki az **Egész nap** beállítást.
4. Az **OK** gombra kattintva erősítse meg a beállítást.

Egy időköz egy vagy több időtartománnyal határozható meg napok és időpontok alapján. A létrehozása után az időköz az **Alkalmazás a következő során** legördülő menüben lesz megtalálható az Eszközfelügyeleti szabályok szerkesztője ablakban vagy a Webfelügyeleti szabályok szerkesztője ablakban.

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 Endpoint 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.

Licenc intervallum-ellenőrzése

Az ESET Endpoint Security szolgáltatásnak automatikusan kell csatlakoznia az ESET szervereihez. Ha ezt a beállítást módosítani szeretné, lépjen a **További beállítások (F5)** > **Eszközök** > **Licenc** lapra. Alapértelmezés szerint az **Intervallum-ellenőrzés** funkciónál az **Automatikus** beállítás van megadva, így az ESET licencszerverei óránként néhány alkalommal ellenőrzik a terméket. Nagyobb hálózati forgalom esetén adja meg a **Korlátozott** beállítást a túlzott terhelés csökkentése érdekében. Ha a **Korlátozott** beállítás van kiválasztva, az ESET Endpoint Security naponta csak egyszer, illetve a számítógép újraindulásakor ellenőrzi a licencszervert.

Ha az **Intervallum-ellenőrzés** funkciónál a **Korlátozott** beállítás van megadva, akkor akár egy napot is igénybe vehet az ESET Business Account/ESET MSP Administrator segítségével végrehajtott licenccel kapcsolatos módosítások ESET Endpoint Security-beállításokra való alkalmazása.

Felhasználói felület

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

A Felhasználói felület elemei eszközzel módosíthatja a program vizuális megjelenését és a használt hatásokat.

A biztonsági szoftver maximális védelmének biztosításához a Hozzáférési beállítások eszközzel megakadályozhatja a jogosulatlan módosításokat.

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

Ha úgy dönt, hogy bizonyos értesítések ne jelenjenek meg, azok a **Felhasználói felület elemei** > **Alkalmazásállapotok** részen tekinthetők meg. Itt ellenőrizheti az állapotukat vagy más módon megakadályozhatja az értesítések megjelenítését.

Az egyes objektumokra a jobb gombbal kattintva az Integrálás a helyi menübe parancs jelenik meg. Ezzel az eszközzel az ESET Endpoint Security vezérlőelemei a helyi menübe integrálhatók.

A Bemutató üzemmód hasznos azoknak a felhasználóknak, akik nem szeretnék, ha tevékenységüket előugró ablakok, ütemezett feladatok, illetve processzor- és memóriaigényes összetevők zavarnák meg.

Tekintse meg a következőt is: Az ESET Endpoint Security minimalista felhasználói felületének beállítása (felügyelt környezetben hasznos).

Felhasználói felület elemei

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

A **Felhasználói felület elemei** csoportban módosíthatja a munkakörnyezetet. Az **Indítási mód** legördülő menüben válasszon az alábbi kezdő üzemmódok közül:

Teljes – A teljes grafikus felhasználói felület megjelenik.

Minimális – A grafikus felhasználói felület fut, de csak értesítések jelennek meg a felhasználónak.

Kézi – A grafikus felhasználói felület nem indul el automatikusan a bejelentkezéskor. Bármely felhasználó elindíthatja manuálisan.

Néma – Értesítések és riasztások nem jelennek meg. A grafikus felhasználói felületet csak a rendszergazda indíthatja el. Ez az üzemmód felügyelt környezetben, illetve olyan esetekben lehet hasznos, amikor meg kell őriznie a rendszererőforrásokat.

Miután a grafikus felhasználói felülethez kiválasztotta a Minimális kezdő üzemmódot és újraindította a számítógépet, értesítések megjelennek, a grafikus felhasználói felület azonban nem. Ha vissza szeretné állítani a teljes grafikus felhasználói felületet, rendszergazdaként futtassa azt a Start menü **Minden program** > **ESET** > ESET Endpoint Security pontjából. Az ESET PROTECT segítségével, házirendet használva is elvégezheti ezt.

Az ESET Endpoint Security nyitóképernyőjének letiltásához törölje a **Nyitóképernyő megjelenítése indításkor** jelölőnégyzet bejelölését.

Ha azt szeretné, hogy az ESET Endpoint Security hanggal jelezze az ellenőrzések során bekövetkező fontos eseményeket, például egy kártevő felismerését vagy az ellenőrzés befejezését, jelölje be a **Hangjelzés használata** jelölőnégyzetet.

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

Állapotok

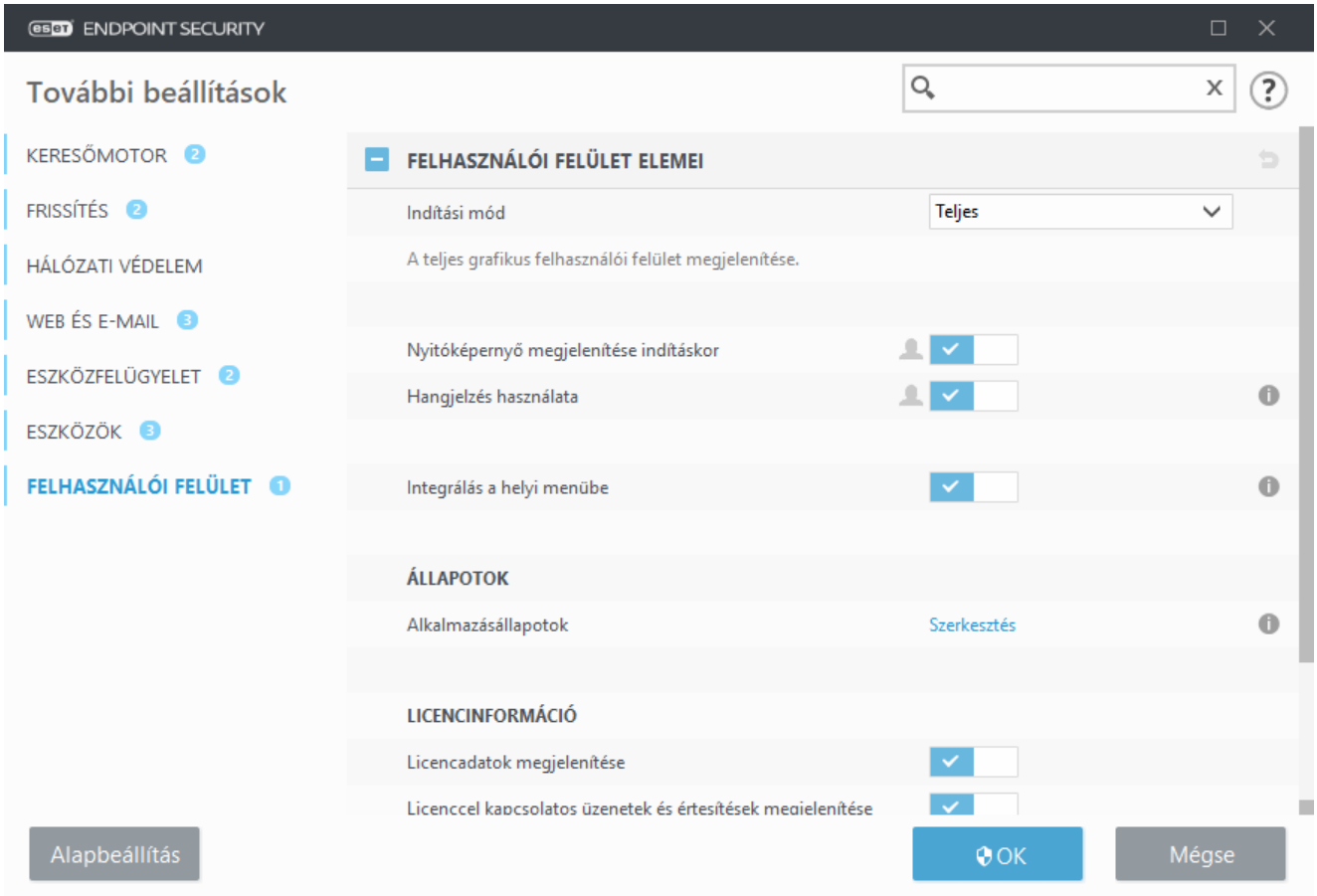
Alkalmazásállapotok – A **Szerkesztés** gombra kattintva kezelheti (letilthatja) a főmenü **Védelem állapota** ablaktáblájában megjelenített állapotokat.

Licencadatok

Licencadatok megjelenítése – Ha le van tiltva, a licenc lejárati dátuma a **Védelem állapota** és a **súgó és támogatás** képernyőn nem jelenik meg.

Licenccel kapcsolatos üzenetek és értesítések megjelenítése – Ha le van tiltva, csak a licenc lejártakor jelennek meg értesítések és üzenetek.

A licencadatok beállításai érvényesek, de nem érhetők el MSP-licenccel aktivált ESET Endpoint Security esetén.



Hozzáférési beállítások

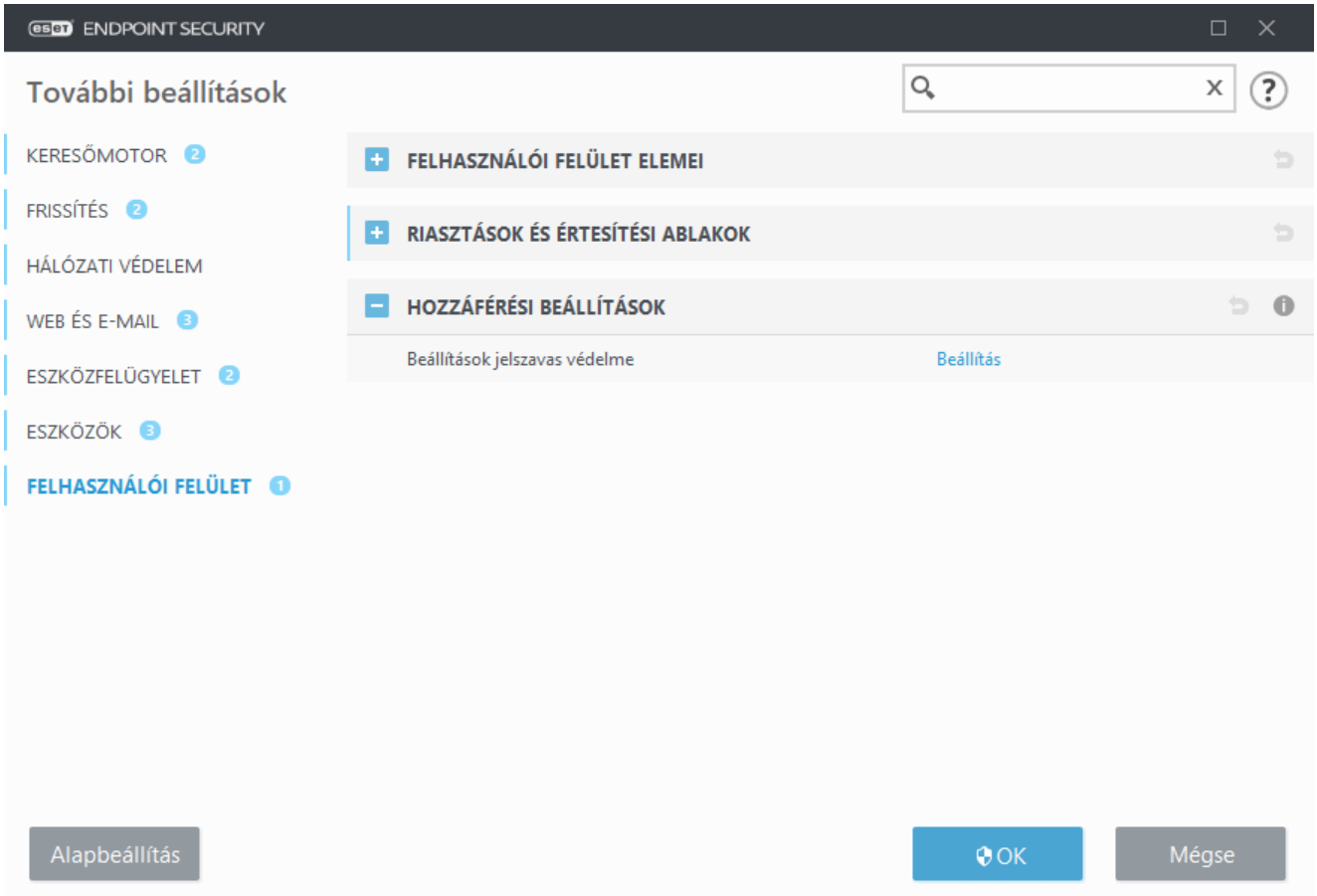
A rendszer maximális biztonsága érdekében fontos, hogy az ESET Endpoint Security megfelelően legyen konfigurálva. A nem hozzáértő módosítások akár a lényeges adatok elvesztéséhez is vezethetnek. A jogosulatlan módosítások elkerülése érdekében az ESET Endpoint Security beállításai jelszóval védhetők.

Felügyelt környezetek

A rendszergazda egy házirend létrehozásával megvédheti jelszóval az ESET Endpoint Security beállításait a csatlakoztatott kliensszámítógépeken. Ha új házirendet szeretne létrehozni, tekintse meg a Jelszóval védett beállítások című részt.

Nem felügyelt

A jelszavas védelem konfigurációs beállításai a **További beállítások** (**F5**) párbeszédpanel **Felhasználói felület** > **Hozzáférési beállítások** lapján találhatók.



Beállítások jelszavas védelme – Jelszóbeállításokra vonatkozik. Rákattintva megnyithatja a Jelszó beállítása ablakot.

A beállítási paraméterek védelmére szolgáló jelszó megadásához vagy módosításához kattintson a **Beállítás** hivatkozásra.

Jelszó a További beállításokhoz

Ha az ESET Endpoint Security beállítási paramétereit szeretné megvédeni a jogosulatlan módosítások ellen, adjon meg egy új jelszót.

Felügyelt környezetek

A rendszergazda egy házirend létrehozásával megvédheti jelszóval az ESET Endpoint Security beállításait a csatlakoztatott kliensszámítógépeken. Ha új házirendet szeretne létrehozni, tekintse meg a Jelszóval védett beállítások című részt.

Nem felügyelt

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 Endpoint Security módosításakor.

Ha elfelejti a jelszavát, visszaállítható a további beállításokhoz való hozzáférés.

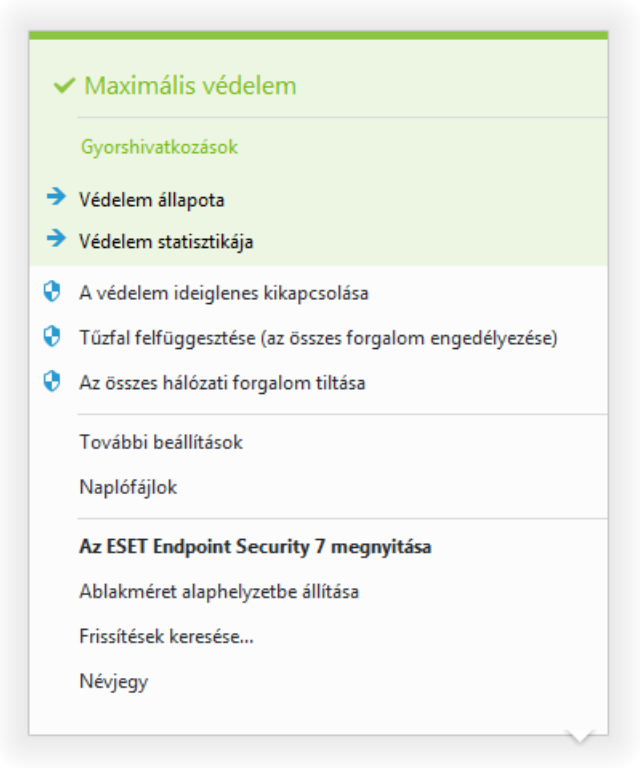
- Visszaállítás a „Jelszó visszaállítása” módszerrel (7.1-es és újabb verziók)
- Visszaállítás az ESET feloldási eszköz segítségével (7.0-s és régebbi verziók)

Olvasson itt további információkat, ha elfelejtette az ESET által biztosított licenckulcsot, a licenc lejárati dátumát vagy az ESET Endpoint Security egyéb licencelési adatait.

A rendszer tálcaikonja

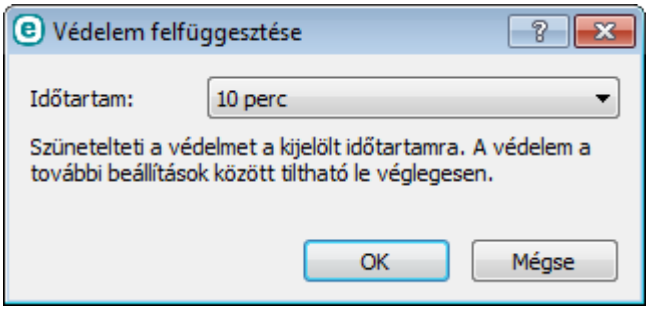
A legfontosabb beállítási lehetőségek és funkciók a rendszertálca ikonjára a jobb gombbal kattintva érhetők el.

> A rendszertálcán található menü eléréséhez győződjön meg arról, hogy a Felhasználói felület elemei indítási módnál a Teljes érték van beállítva.



A védelem ideiglenes kikapcsolása – Megjeleníti a fájlok, a webes tevékenységek és az elektronikus levelezés felügyeletén keresztül a rendszert a kártevőktől és támadásoktól védő Keresőmotort 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 – A parancsra kattintva a tűzfal minden bejövő és kimenő hálózati és internetes forgalmat blokkol. Az újbóli engedélyezéshez kattintson **Az összes hálózati forgalom tiltásának megszüntetése** elemre.

További beállítások – Ezt a lehetőséget választva megnyithatja a **További beállítások** fát. A További beállítások párbeszédpanel az F5 billentyűt lenyomva vagy a **Beállítások** > **További beállítások** elemre kattintva is elérhető.

Naplófájlok – A naplófájlok tájékoztatást nyújtanak a programban bekövetkezett minden fontos eseményről, illetve az észlelt veszélyekről.

Az ESET Endpoint Security megnyitása – Megnyílik az ESET Endpoint Security fő programablaka a tálcaikonról.

Ablakméret alaphelyzetbe állítása – Visszaállítja az ESET Endpoint Security ablakát az eredeti méretre és pozícióba.

Frissítések keresése – Elindítja a programmodulok frissítését, és így biztosítja a kártékony kódok elleni védelmi szintet.

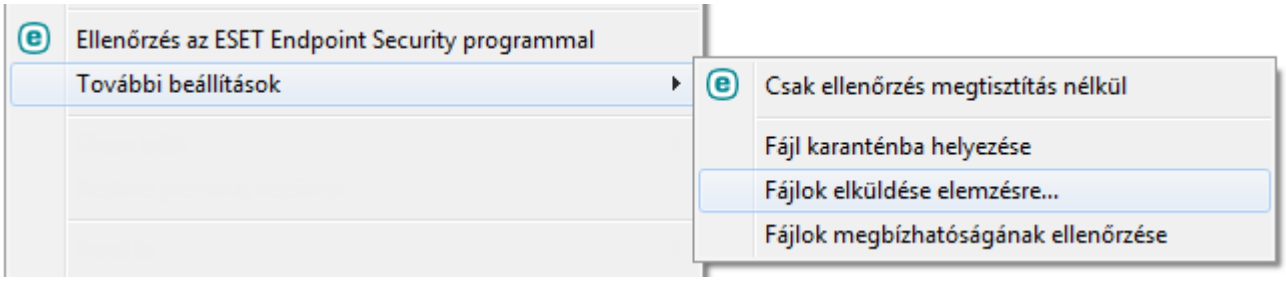
Névjegy – Megjeleníti a rendszer-információkat, köztük az ESET Endpoint Security telepített verziójának számát és a telepített programmodulok adatait, valamint a licenc lejárati dátumát. Az operációs rendszerrel és a rendszererőforrásokkal kapcsolatos információk az oldal alján találhatók.

Helyi menü

A helyi menü az egyes objektumokra (fájlokra) a jobb gombbal kattintva jelenik meg. A menüben az objektumokon végrehajtható összes művelet megtalálható.

Az ESET Endpoint Security vezérlőelemei a helyi menübe integrálhatók. A funkció beállításai a További beállítások párbeszédpanel beállításfájának **Felhasználói felület** > **Felhasználói felület elemei** csoportjában találhatók.

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



Súgó és támogatás

Az ESET Endpoint Security súgója hibaelhárítási eszközöket és támogatási információkat tartalmaz, amelyek segítséget nyújtanak a felmerülő problémák megoldásában.

Telepített termék

- **Az ESET Endpoint Security névjegye** – Információkat jelenít meg az ESET Endpoint Security példányáról.
- **Termék hibaelhárítása** – Erre a hivatkozásra kattintva megoldást találhat a leggyakrabban előforduló problémákra.
- **Licenc hibaelhárítása** – Erre a hivatkozásra kattintva megoldást találhat a licencmódosítással kapcsolatos problémákra.
- **Licenc módosítása** – Kattintson ide az aktiválási ablak elindításához és a licenc aktiválásához.

Súgóoldal – Kattintson erre a hivatkozásra az ESET Endpoint Security súgójának megnyitásához.

Műszaki terméktámogatás

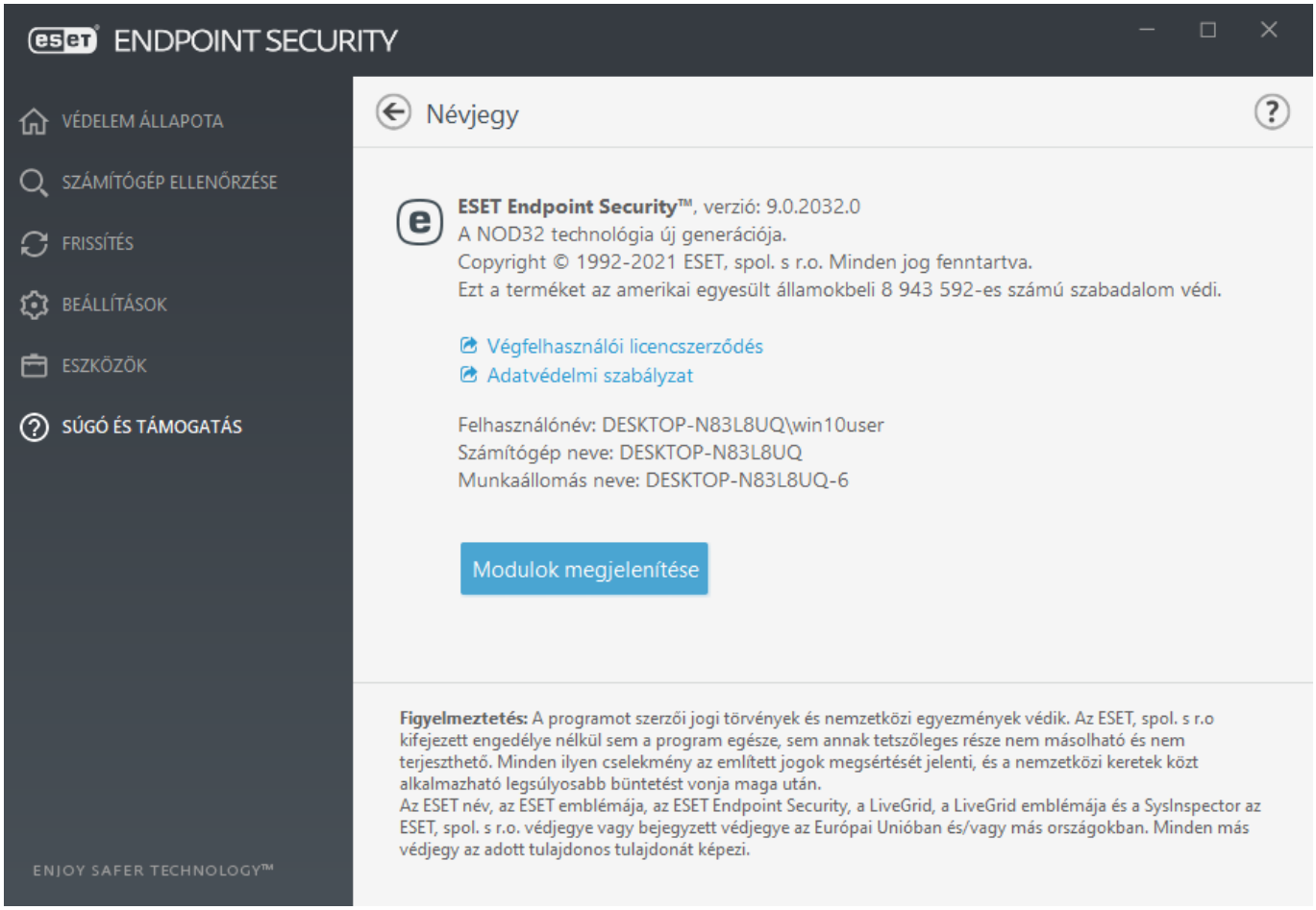
- **Terméktámogatási kérelem** – Ha nem talál megoldást a problémájára, az webhelyén megtalálható űrlapon keresztül gyorsan kapcsolatba léphet a Műszaki támogatási szolgálattal. A beállítások alapján megjelenik a rendszerkonfigurációs adatok elküldése ablak a webes űrlap kitöltése előtt.
- **Részletek a műszaki támogatási szolgálat számára** – Amikor a rendszer kéri, az adatokat (például a terméknevet, a termékverziót, az operációs rendszert és a processzor típusát) 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 információkért tekintse meg az ESET Log Collector online felhasználói útmutatóját.
- 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.

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 Endpoint Security névjegye

Az ablakban az ESET Endpoint Security telepített verziójának adatait, az operációs rendszert, illetve a rendszer-erőforrásokat tekintheti meg.

A **Modulok megjelenítése** elemre kattintva megtekintheti a telepített programmodulokkal és a verziójukkal kapcsolatos információkat. A **Másolás** elemre kattintva a vágólapra másolhatja a modulok adatait. Ez a hibakereséshez, illetve a terméktámogatási szolgálattal folytatott kommunikáció során lehet hasznos.



Rendszer-konfigurációs adatok küldése

A lehető leggyorsabb és legpontosabb segítségnyújtáshoz az ESET számára meg kell adnia az ESET Endpoint 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** opcióra 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

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

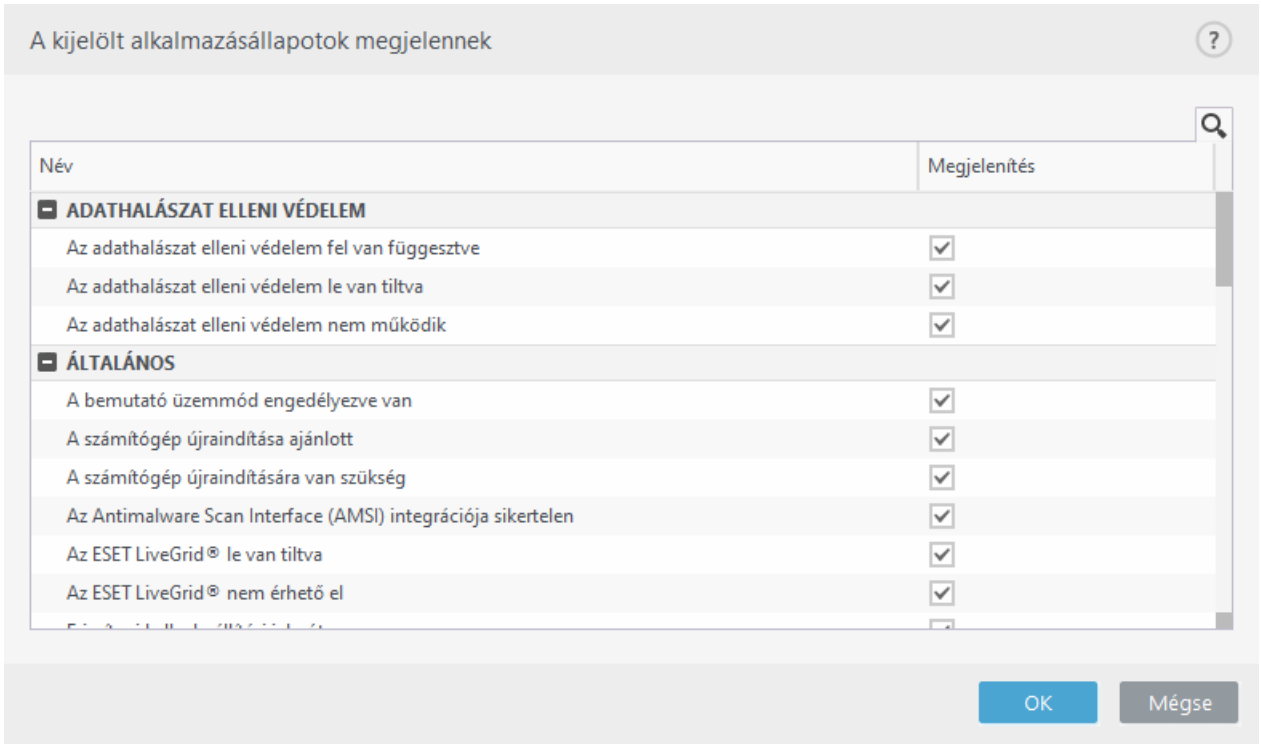
Az ESET Endpoint Security-értesítések kezeléséhez nyissa meg a **További beállítások** (F5) > **Értesítések** lapot. A következő típusú értesítéseket konfigurálhatja:

- Alkalmazásállapotok – Kattintson a **Szerkesztés** gombra annak kiválasztásához, hogy mely alkalmazásállapotok jelenjenek meg a program főablakának kezdő szakaszában.
- Asztali értesítések – Kis előugró ablakok a rendszertálca mellett.
- Az értesítések testreszabása – Egyéni üzenet adható meg például egy asztali értesítés esetén.
- 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

Annak konfigurálásához, hogy mely alkalmazásállapotok jelenjenek meg (ha például szünetelteti a vírus- és kémprogramvédelmet, vagy engedélyezi a játékos üzemmódot), nyissa meg a **További beállítások** (F5) > **Értesítések** lapot, majd a **Szerkesztés** gombra kattintva válassza ki, hogy mely alkalmazásállapotok jelenjenek meg a fő programablak kezdő szakaszában.

Akkor is megjelenik alkalmazásállapot, ha a termék nincs aktiválva, vagy ha lejárt a licenc. Ez a beállítás az ESET PROTECT házirendjein keresztül módosítható.



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. Ez az ESET Endpoint Security elsődleges eszköze a felhasználóval való kommunikációban: értesít 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 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** – A program csak a kritikus (például a vírusvédelem indításával vagy a fertőzött rendszerrel kapcsolatos) hibákat naplózza.

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 – Az értesítések képernyőfókuszt kapnak, és elérhetők lesznek az Alt+Tab billentyűkombinációval.

Párbeszédablak – asztali értesítések

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 az asztalon** jelölőnégyzetet.

Ha be szeretné állítani a **Fájl elemezve** és a **Fájl nincs elemezve** értesítést az ESET LiveGuard használatakor, akkor a Proaktív védelem esetén a **Végrehajtás tiltása az elemzés eredményének megkapásáig** beállítást kell megadni.

Az értesítések testreszabása

Ebben az ablakban testre szabhatja az értesítésekben használt üzeneteket.

Alapértelmezett értesítési üzenet – Az értesítések láblécén megjelenítendő alapértelmezett üzenet.

Észlelések

Ha engedélyezi **A kártevőre vonatkozó értesítések automatikus bezárásának mellőzése** beállítást, akkor a kártevőkről szóló értesítések a képernyőn maradnak, amíg manuálisan be nem zárják őket.

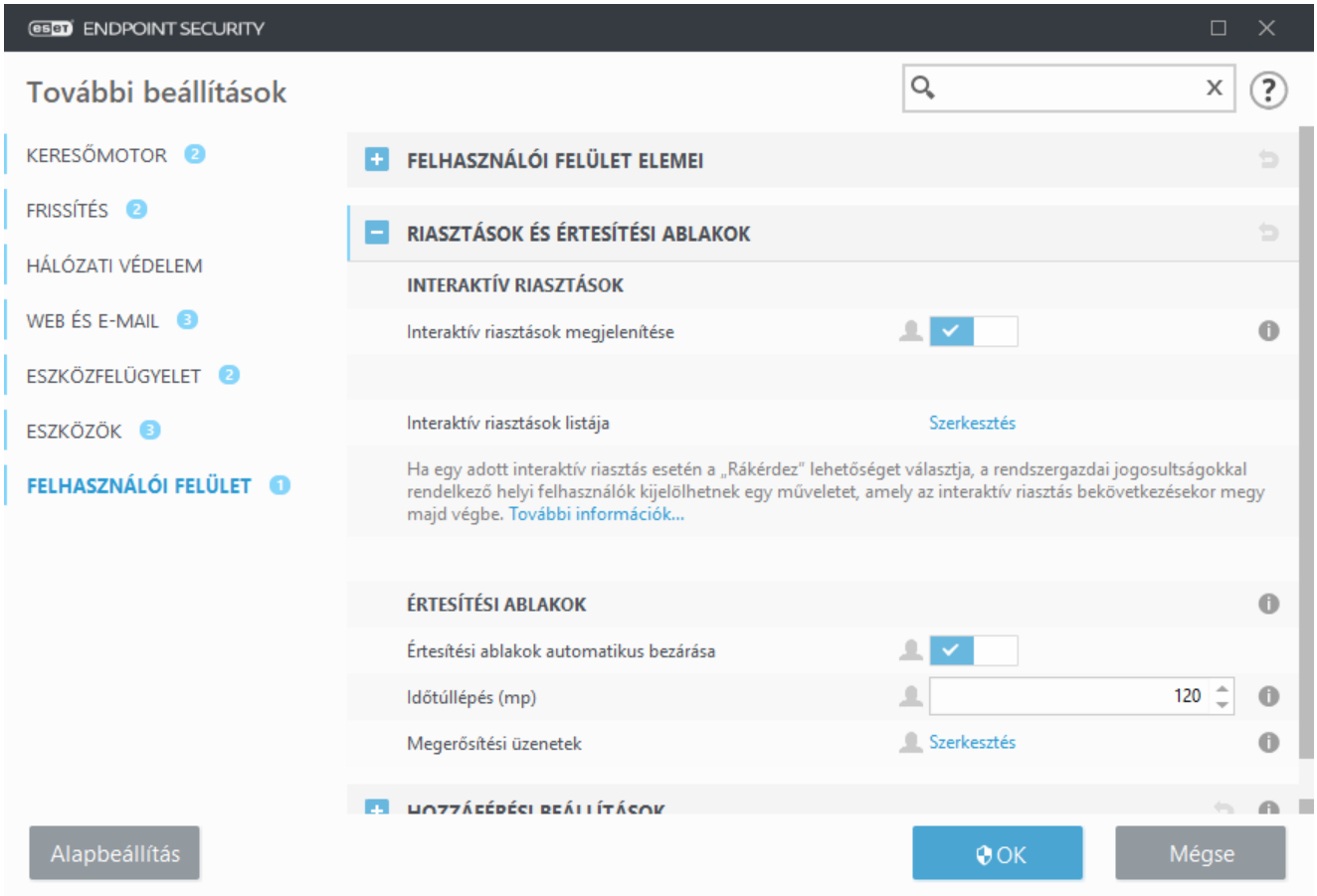
Tiltsa le az **Alapértelmezett üzenet használata** beállítást, és írja be saját üzenetét a **Értesítési üzenet észlelésről** mezőbe az egyéni értesítési üzenet használatához.

Interaktív riasztások

Gyakori riasztásokról és értesítésekről keres információkat?

- A program kártevőt talált
- A cím letiltva
- A licenc nincs aktiválva
- Frissítés elérhető
- A frissítési adatok nem egységesek
- A „Modulok frissítése sikertelen” üzenet hibaelhárítása
- „A fájl sérült” vagy „Nem sikerült a fájl átnevezése”
- A webhely tanúsítványát visszavonták
- Hálózati kártevő letiltva
- A fájl letiltva elemzés miatt

Az **Értesítések** részben található **Interaktív riasztások** szakasz segítségével beállítható, hogy az észlelt elemeket hogyan kezelje az ESET Endpoint Security, amikor a felhasználónak kell döntést hoznia (például potenciális adathalász webhelyek esetén).



Interaktív riasztások

Interaktív riasztásablakok jelennek meg, ha a rendszer kártevőt talál, vagy ha felhasználói beavatkozásra van szükség.

Interaktív riasztások megjelenítése

- Nem felügyelt felhasználók esetén azt javasoljuk, hogy maradjon meg az alapértelmezett beállítás (aktiválva).
- Felügyelt felhasználók esetén hagyja aktiválva a beállítást, és válasszon ki egy előre meghatározott műveletet a felhasználók számára az Interaktív riasztások listája szakaszban.

Az **Interaktív riasztások megjelenítése** funkció letiltásakor nem jelenik meg semmilyen riasztási ablak és böngészős párbeszédpanel. A program egy előre meghatározott alapértelmezett műveletet választ ki automatikusan (például a „potenciális adathalász webhely” üzenet nem jelenik meg).

Értesítési ablakok

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

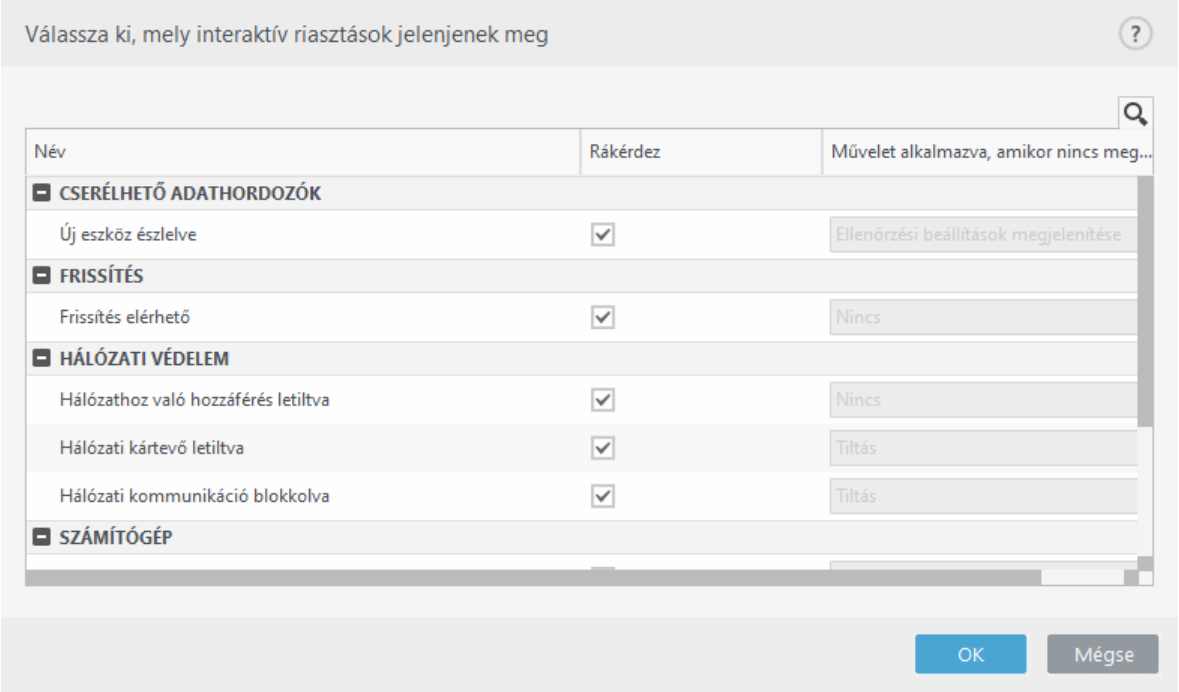
Megerősítési üzenetek – Az olyan megerősítési üzenetek listája, amelyek megjelenítését engedélyezheti és letilthatja.

Interaktív riasztások listája

Ez a szakasz bemutat több olyan interaktív riasztási ablakot, amelyet az ESET Endpoint Security megjelenít bármilyen művelet végrehajtása előtt.

A konfigurálható interaktív riasztások viselkedésének beállításához lépjen az **Értesítések** > **Interaktív riasztások** lapra az ESET Endpoint Security További beállítások fájában, majd kattintson a **Szerkesztés** elemre.

> Hasznos felügyelt környezetben, ahol a rendszergazda törölni tudja a **Rákérdez** jelölőnégyzetet mindenhol, és kiválaszthat egy előre meghatározott műveletet, amely interaktív riasztási ablakok megjelenésekor érvényesül.
> Tekintse meg a terméken belüli alkalmazásállapotokat is.



Tekintsen meg a kívánt interaktív riasztási ablak súgóoldalát is:

Cserélhető adathordozók

- Új eszköz észlelve

Védett böngésző

- Alapértelmezett böngészőben való folytatás engedélyezése

Hálózati védelem

- A Hálózathoz való hozzáférés letiltva riasztás akkor jelenik meg, ha aktiválódik a munkaállomás **Számítógép elkülönítése a hálózattól** kliensfeladata az ESET PROTECT felől.
- Hálózati kommunikáció blokkolva
- Hálózati kártevő letiltva

Webböngészős riasztások

- A program nemkívánatos tartalmat talált
- Webhely blokkolva adathalászat miatt

Számítógép

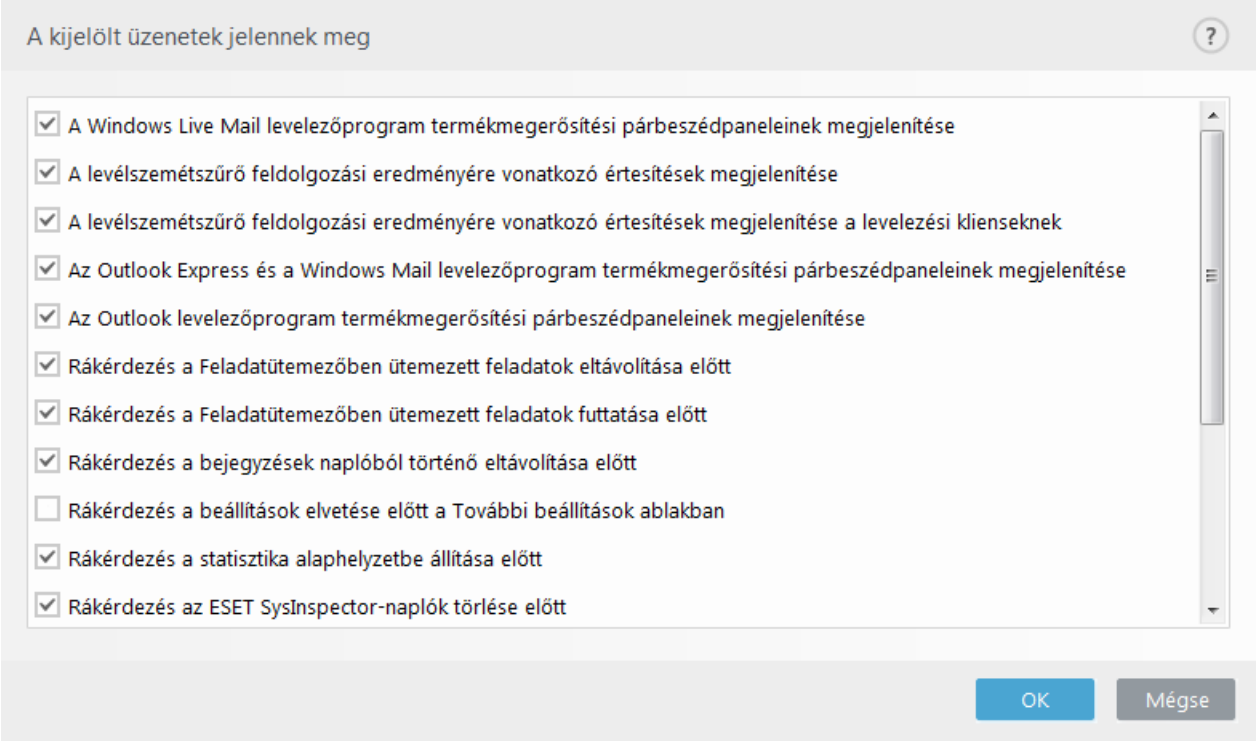
A következő riasztások narancs színűre változtatják a felhasználói felületet:

- Számítógép újraindítása (kötelező)
- Számítógép újraindítása (ajánlott)

> Az interaktív riasztások nem tartalmazzák a keresőmotor, a Behatolásmegelőző rendszer (HIPS) és a Tűzfal interaktív ablakait – ezek viselkedése külön konfigurálható az adott funkciónál.

Megerősítési üzenetek

A megerősítési üzenetek beállításához lépjen a **Felhasználói felület** > **Riasztások és értesítési ablakok** > **Megerősítési üzenetek** szakaszhoz az ESET Endpoint Security További beállítások fájában, majd kattintson a **Szerkesztés** elemre.



Ezen a párbeszédpanelen az ESET Endpoint 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

A további beállításokkal kapcsolatos ütközési hiba

Ez a hiba akkor fordulhat elő, ha valamely összetevő (pl. a behatolásmegelőző rendszer vagy a tűzfalés a felhasználó egyidejűleg interaktív vagy tanuló módban hozzák létre a szabályokat.

Saját szabályok létrehozásához javasoljuk, hogy változtassa a szűrési módot az alapértelmezett **Automatikus üzemmódra**. Bővebben lásd: Az ESET-tűzfal Tanuló módja. Bővebben lásd: A behatolásmegelőző rendszer és a szűrési üzemmódok.

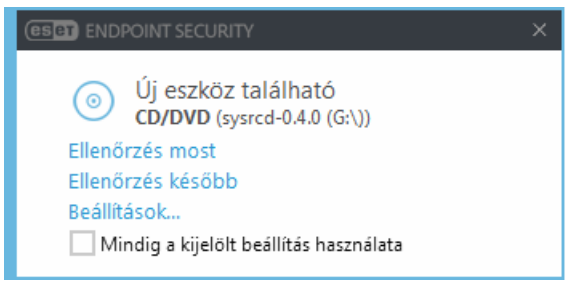
Alapértelmezett böngészőben való folytatás engedélyezése

Egy adott interaktív figyelmeztetés csak akkor jelenik meg, ha hiba történt a Védett böngésző megfelelő indításakor.

Cserélhető adathordozók

Az ESET Endpoint Security lehetővé teszi a cserélhető adathordozók (CD, DVD, USB stb.) automatikus ellenőrzését a számítógépbe való behelyezésük során. 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 Endpoint Security szolgáltatásban:



A párbeszédpanel beállításai:

- **Ellenőrzés most** – Erre a hivatkozásra kattintva elindíthatja a cserélhető adathordozó ellenőrzését.
- **Nincs ellenőrzés** – Nem lesz semmilyen művelet végrehajtva.

Az ESET Endpoint Security tartalmazza ezenkívül az Eszközfelügyelet funkciót, amellyel szabályokat határozhat meg külső eszközökhöz egy adott számítógépen. Az eszközfelügyeletről további tudnivalókat olvashat az Eszközfelügyelet című szakaszban.

A cserélhető adathordozók ellenőrzésére vonatkozó beállítások kezeléséhez nyissa meg a További beállítások (**F5**) > **Felhasználói felület** > **Riasztások és értesítési ablakok** > **Interaktív riasztások** > **Interaktív riasztások listája** > **Szerkesztés** > **Új eszköz észlelve** ablakot.

Ha a **Felhasználó megkérdezése** lehetőség nincs kiválasztva, válassza ki, hogy milyen művelet menjen végbe, amikor behelyeznek egy cserélhető adathordozót a számítógépbe:

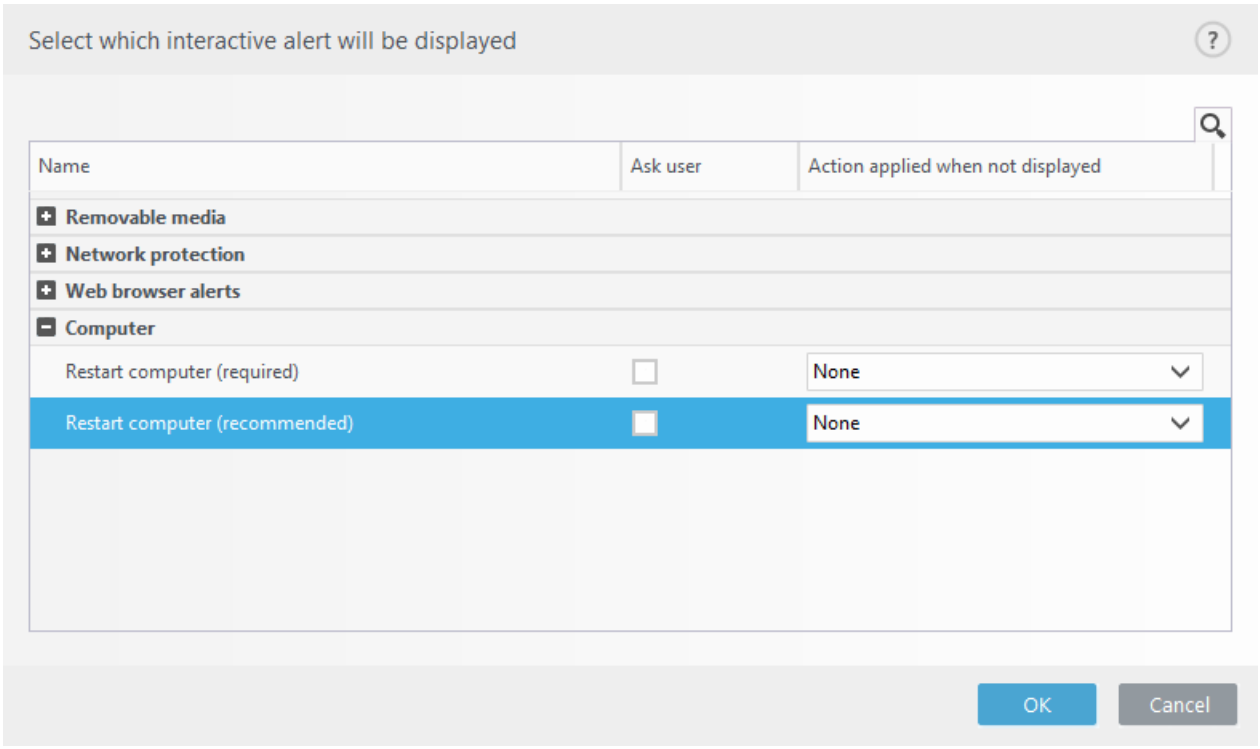
- **Nincs ellenőrzés** – Nincs művelet, és az **Új eszköz található** ablak nem nyílik meg.
- **Eszköz automatikus ellenőrzése** – A behelyezett cserélhető adathordozó eszköz ellenőrzése.
- **Kényszerített eszközellenőrzés** – Sor kerül a behelyezett cserélhető adathordozó eszköz ellenőrzésére, és nem szakítható meg a művelet.
- **Ellenőrzési beállítások megjelenítése** – Megnyitja az **Interaktív riasztások** beállítási szakaszt.

Újraindítás szükséges

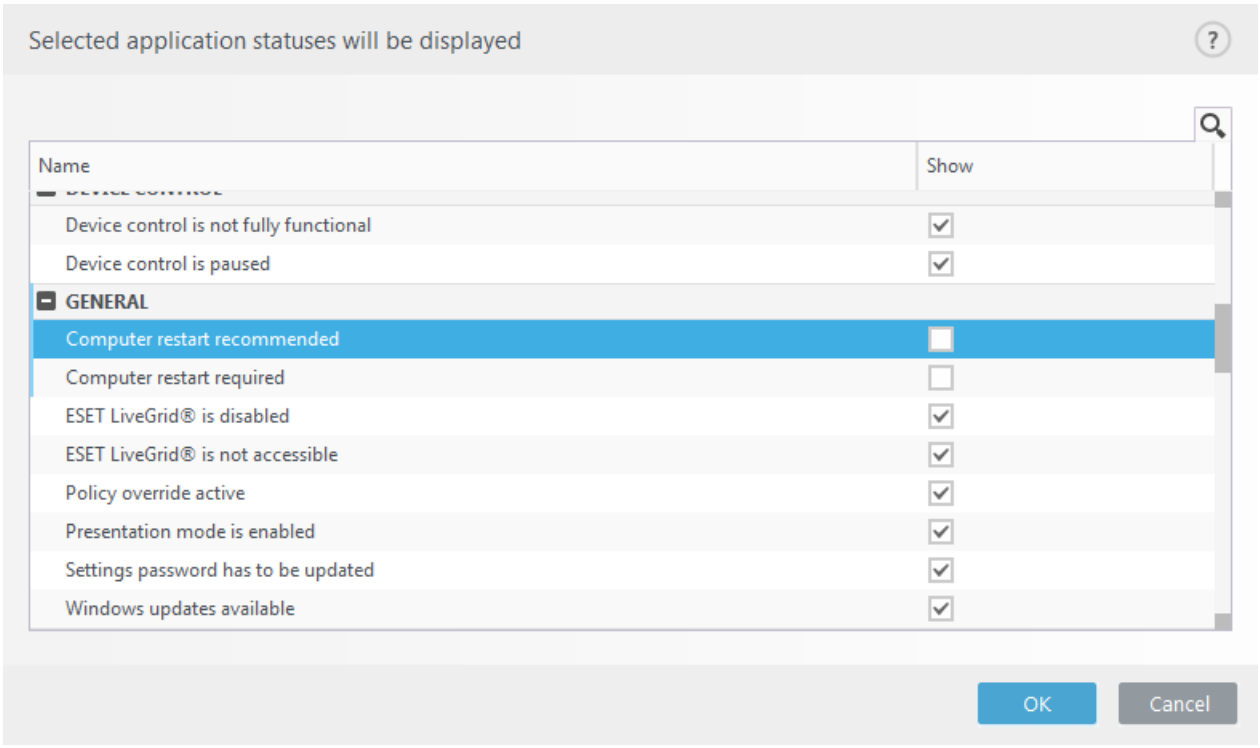
Ha végpontgépeken az „Újraindítás szükséges” vörös figyelmeztetés jelenik meg, letiltható a figyelmeztetések megjelenítése.

Az „Újraindítás szükséges” vagy az „Újraindítás javasolt” figyelmeztetés letiltásához kövesse az alábbi lépéseket:

1. Nyomja meg az **F5** billentyűt a További beállítások ablak megnyitásához, majd bontsa ki a **Riasztások és értesítési ablakok** szakaszt.
2. Kattintson a **Szerkesztés** elemre az **Interaktív riasztások listája** felirat mellett. A **Számítógép** szakaszban törölje a jelet a **Számítógép újraindítása (kötelező)** és a **Számítógép újraindítása (ajánlott)** jelölőnégyzetből.



3. Az **OK** gombra kattintva mentse a módosításokat mindkét megnyitott ablakban.
4. A figyelmeztetések ezután nem fognak megjelenni a végpontgépen.
5. (opcionális) Ha le szeretné tiltani az alkalmazásállapotokat az ESET Endpoint Security fő programablakában, az Alkalmazásállapotok ablakban törölje a jelet **A számítógép újraindítása szükséges** és **A számítógép újraindítása ajánlott** jelölőnégyzetből.

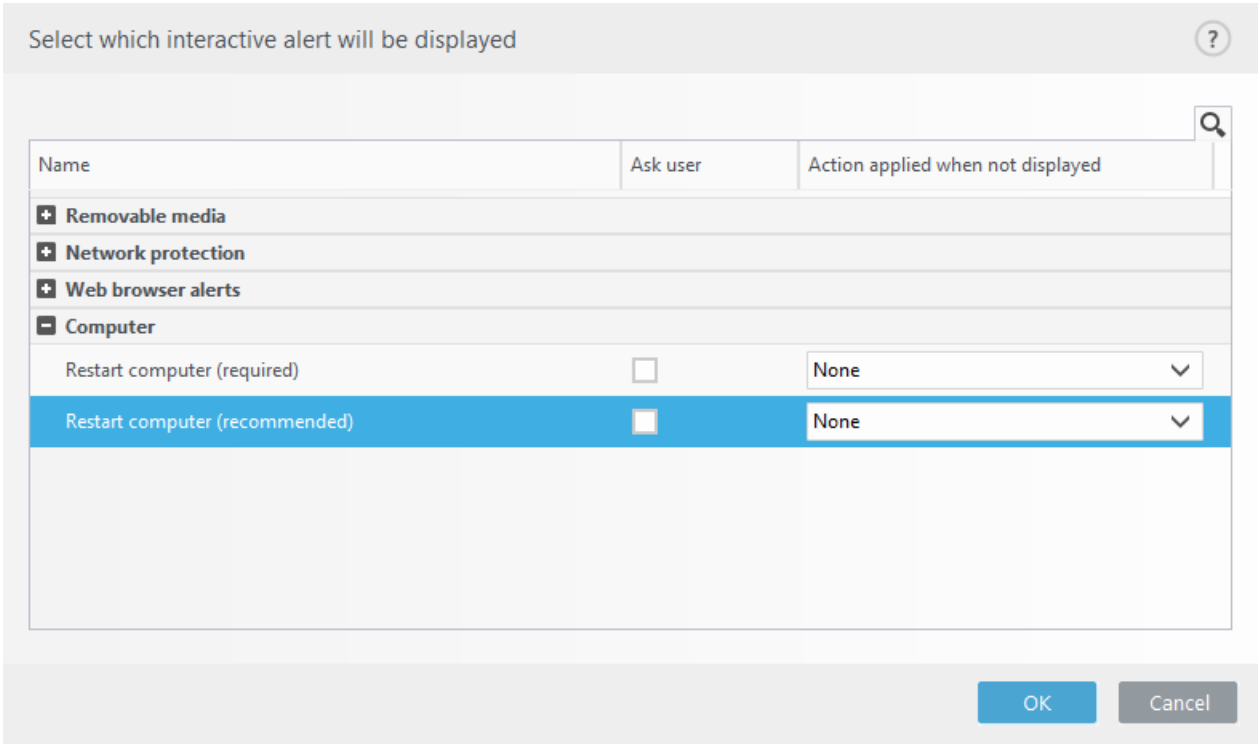


Újraindítás javasolt

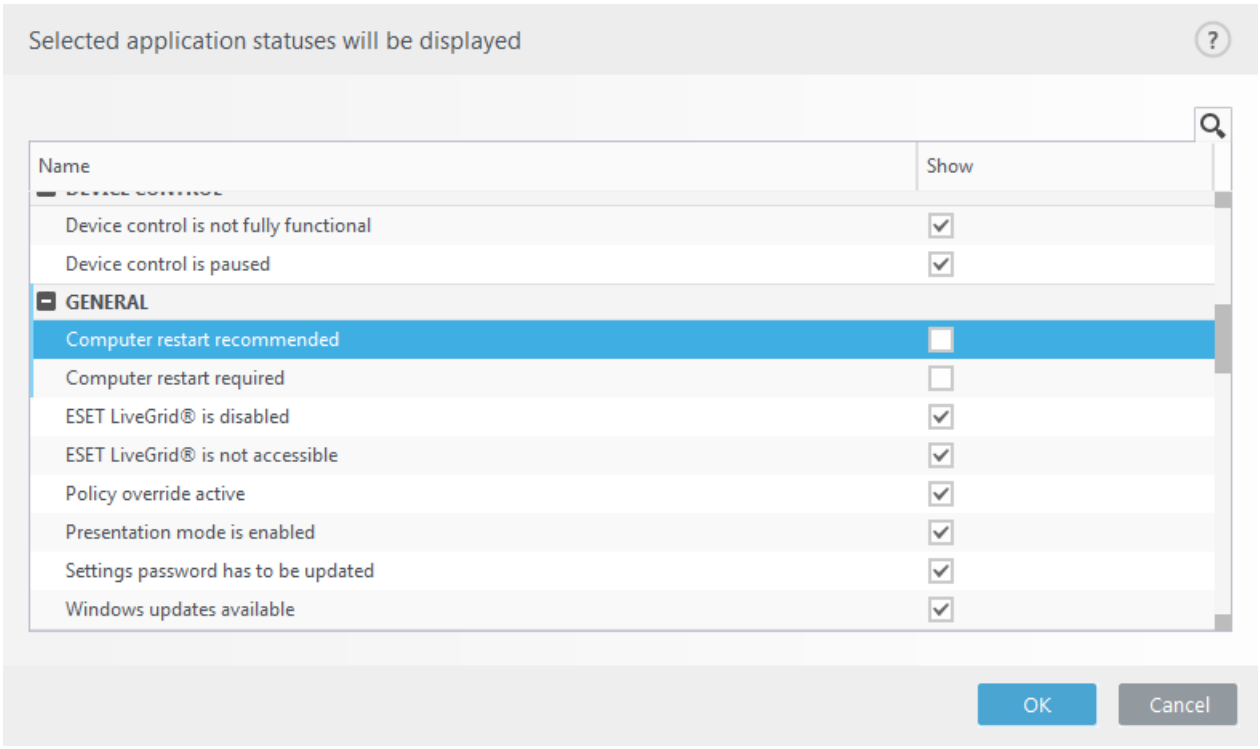
Ha végpontgépeken az „Újraindítás javasolt” sárga figyelmeztetés jelenik meg, letiltható a figyelmeztetések megjelenítése.

Az „Újraindítás szükséges” vagy az „Újraindítás javasolt” figyelmeztetés letiltásához kövesse az alábbi lépéseket:

1. Nyomja meg az **F5** billentyűt a További beállítások ablak megnyitásához, majd bontsa ki a **Riasztások és értesítési ablakok** szakaszt.
2. Kattintson a **Szerkesztés** elemre az **Interaktív riasztások listája** felirat mellett. A **Számítógép** szakaszban törölje a jelet a **Számítógép újraindítása (kötelező)** és a **Számítógép újraindítása (ajánlott)** jelölőnégyzetből.



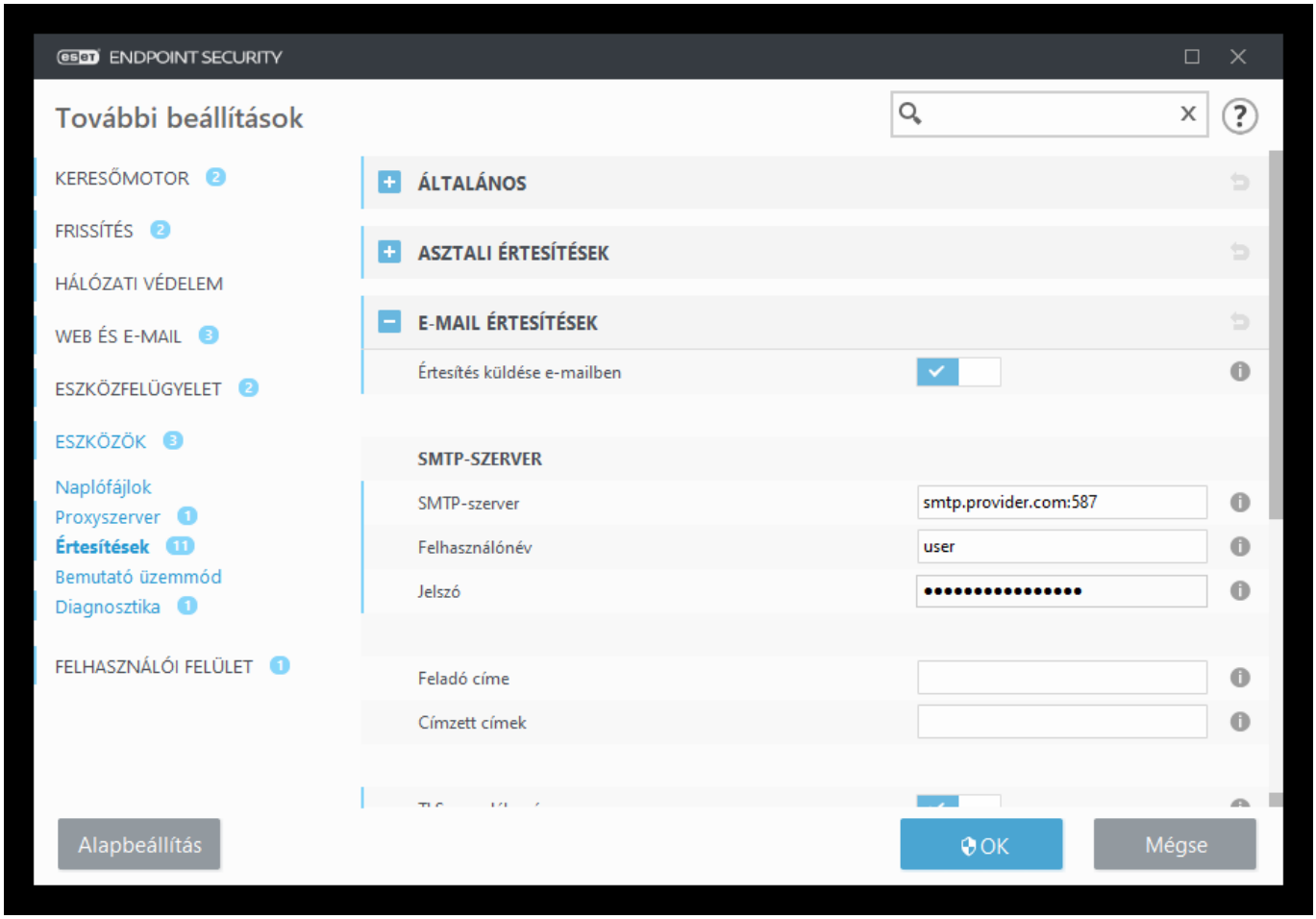
3. Az **OK** gombra kattintva mentse a módosításokat mindkét megnyitott ablakban.
4. A figyelmeztetések ezután nem fognak megjelenni a végpontgépen.
5. (opcionális) Ha le szeretné tiltani az alkalmazásállapotokat az ESET Endpoint Security fő programablakában, az Alkalmazásállapotok ablakban törölje a jelet **A számítógép újraindítása szükséges** és **A számítógép újraindítása ajánlott** jelölőnégyzetből.



Továbbítás

Az ESET Endpoint Security automatikusan értesítő e-maileket tud küldeni a kiválasztott részletességi szintű esemény előfordulása esetén. A **További beállítások** > **Értesítések** > **Továbbítás** > **Továbbítás e-mail címre** lapon engedélyezze az **Értesítések továbbítása e-mail címre** beállítást az e-mail-értesítések aktiválásához.

Továbbított értesítések – Válassza ki, hogy a szolgáltatás mely asztali értesítéseket továbbítsa az e-mail-címére.



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 Endpoint Security.

Felhasználónév és jelszó – Ha az SMTP-szerver hitelesítést igényel, írja be ezekbe a mezőkbe az eléréshez szükséges megfelelő felhasználónevet és jelszót.

Feladó címe – Ebben a mezőben megadhatja a feladó címét, amely az értesítő e-mailek fejlécében jelenik meg.

Címzett címe – Ebben a mezőben megadhatja a címzettek címeit, amelyek az értesítő e-mailek fejlécében jelennek meg. Több e-mail-cím elválasztásához használjon pontosvesszőt (;).

TLS engedélyezése – Engedélyezheti TLS titkosítású riasztások és értesítések küldését.

E-mail-beállítások

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** – A program csak a kritikus (például a vírusvédelem indításával vagy a fertőzött rendszerrel kapcsolatos) hibákat naplózza.

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 nagyszámú 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.

Üzenetformátum

A program és a távoli felhasználó vagy rendszergazda közötti kommunikáció e-mailek vagy (a Windows üzenetküldő szolgáltatásával továbbított) helyi hálózati üzenetek formájában történik. A riasztások és az értesítések alapértelmezett formátuma 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. Célszerű ezeket változatlanul hagyni. 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).

A tényleges információkat kulcsszavak (% jelekkel elválasztott karakterláncok) helyettesítik az üzenetekben. A következő kulcsszavak használhatók:

- **%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 vagy más objektum 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.

Profilkezelő

A profilkezelőt az ESET Endpoint Security programban két helyen használhatja: a **Kézi indítású számítógép-ellenőrzés** és a **Frissítés** csoportban.

Kézi indítású számítógép-ellenőrzés

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 **Vírusirtó** > **Kézi indítású számítógép-ellenőrzés** > **Szerkesztés** gombra a **Profilok listája** felirat mellett. A **Kiválasztott profil** legördülő lista tartalmazza a meglévő ellenőrzési profilokat. 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 **automatikus megtisztítást** 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 Endpoint Security programban:

Billentyűparancsok	Végrehajtott művelet
F1	a súgólapok megnyitása
F5	a További beállítások ablak megnyitása
Up/Down	navigálás a termékben elemeken keresztül
TAB	a kurzor mozgatása egy ablakban
Esc	az aktív párbeszédpanel bezárása
Ctrl+U	az ESET-licenccel és a számítógéppel kapcsolatos adatok megjelenítése (a terméktámogatási szolgáltatás számára)

Billentyűparancsok	Végrehajtott művelet
Ctrl+R	a termékablak visszaállítása az eredeti méretére és pozíciójába

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 Endpoint 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

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.

A számítógépes víruskereső részletes naplózásának engedélyezése – Rögzíthető az összes olyan esemény, amely akkor lép fel, amikor a Számítógép ellenőrzése, illetve a Valós idejű fájlrendszervédelem ellenőrzi a fájlokat és a mappákat.

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 - A termék és a Direct Cloud szerverei közötti összes termékkommunikáció rögzítése.

A Dokumentumvédelem speciális naplózásának engedélyezése – A Dokumentumvédelemben előforduló összes esemény rögzítése, amivel lehetővé válik a problémák diagnosztizálása és elhárítása.

Kernel részletes naplózásának engedélyezése – Az ESET-kernelszolgáltatásban (ekrn) fellépő összes esemény rögzítése, ami lehetővé teszi a problémák diagnosztizálását és megoldását (a 7.2-es és az újabb verziókban áll

rendelkezésre).

Licencelés speciális naplózásának engedélyezése – A termék ESET aktiválási szervereivel és az ESET Business Account-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 – Begyűjtésre kerülnek további információk 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.

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 diagnosztika és a problémamegoldás engedélyezéséhez.

A valós idejű fájlrendszervédelem részletes naplózásának engedélyezése – A Valós idejű fájlrendszervédelem során fellépő összes esemény rögzítése, ami lehetőséget ad a problémák diagnosztizálására és elhárítására.

Védett böngésző részletes naplózásának engedélyezése - Rögzítse a Védett böngészőben előforduló összes eseményt, mert ezzel lehetővé válik a problémák diagnosztizálása és elhárítása.

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.

Webfelügyelet speciális naplózásának engedélyezése – A Webfelügyelet modulban előforduló összes esemény rögzítése. Ez segíti a fejlesztőket a Webfelügyelet modullal kapcsolatos problémák felismerésében és javításában.

Naplófájl helye

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

Parancssori víruskereső

Az ESET Endpoint 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 Endpoint 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 Endpoint 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.

A speciális ecmd parancsok csak helyileg futtathatók. Az ecmd parancsok szüneteltetése csak a **Parancs futtatása** kliensfeladattal hajtható végre az ESET PROTECT segítségével.

Beállítások exportálása parancs:
```
ecmd /getcfg c:\config\settings.xml
```

Beállítások importálása parancs:
```
ecmd /setcfg c:\config\settings.xml
```

.xml konfigurációs fájl aláírása:

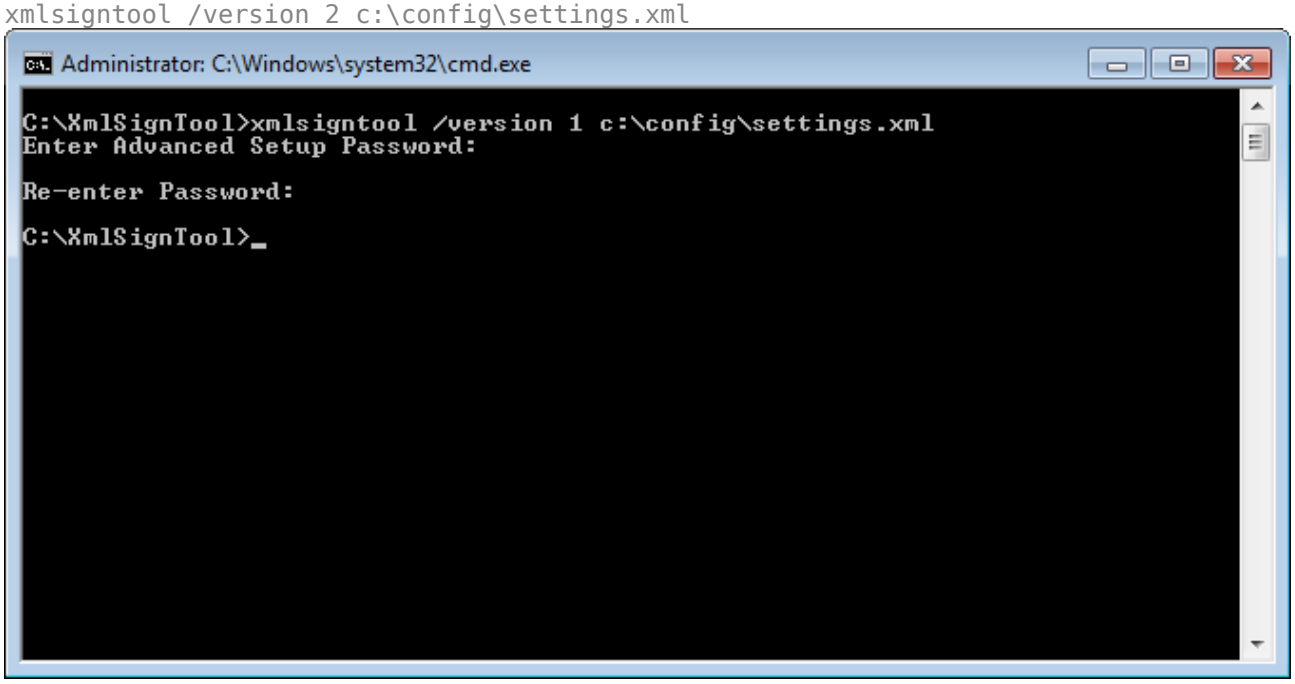
1. Töltse le az XmlSignTool végrehajtható fájlt.
2. Nyissa meg a Windows parancssori ablakát (cmd) a **Futtatás rendszergazdaként** paranccsal.
3. Lépjen oda, ahová az `xmlsigntool.exe` fájlt mentette.
4. Az *.xml* konfigurációs fájl aláírásához hajtson végre egy parancsot. Használat: `xmlsigntool /version 1|2 <xml_file_path>`

A `/version` paraméter értéke az ESET Endpoint Security verziójától függ. A 7-es és az újabb verziókhoz 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 Endpoint 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 Endpoint 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.

Az ecmd-parancsok listája

A Futtatás ESET PROTECT-kliensfeladattal engedélyezhetők és tilthatók le ideiglenesen egyéni biztonsági funkciók. A parancsok nem írják felül a házirend-beállításokat, és a szüneteltetett beállítások visszaállnak eredeti állapotukba a parancs végrehajtása után, illetve az eszköz újraindítása után. A funkció használatához adja meg, hogy a parancssor az azonos nevű mezőben fusson.

Az alábbiakban megtekintheti az egyes biztonsági funkciók parancsát:

Biztonsági funkció	Ideiglenes szüneteltetési parancs	Engedélyezési parancs
Valós idejű fájlrendszervédelem	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable

Biztonsági funkció	Ideiglenes szüneteltetési parancs	Engedélyezési parancs
Dokumentumvédelem	ecmd /setfeature document pause	ecmd /setfeature document enable
Eszközfelügyelet	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Bemutató üzemmód	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Anti-Stealth technológia	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Személyi tűzfal	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Hálózati támadások elleni védelem (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Botnet elleni védelem	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Webfelügyelet	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Webhozzáférés-védelem	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
E-mail védelem	ecmd /setfeature email pause	ecmd /setfeature email enable
Levélszemétszűrő	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Adathalászat elleni védelem	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

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:

- fut a képernyőkímélő;
- a számítógép zárolva van;
- egy felhasználó kijelentkezik.

Az üresjárat idején történő ellenőrzés eseményindítóinak engedélyezéséhez vagy letiltásához használhatja az egyes állapotok kapcsolóit.

Beállítások importálása és exportálása

Az ESET Endpoint Security testre szabott .xml konfigurációs fájlját a **Beállítások** menüből importálhatja, illetve exportálhatja.

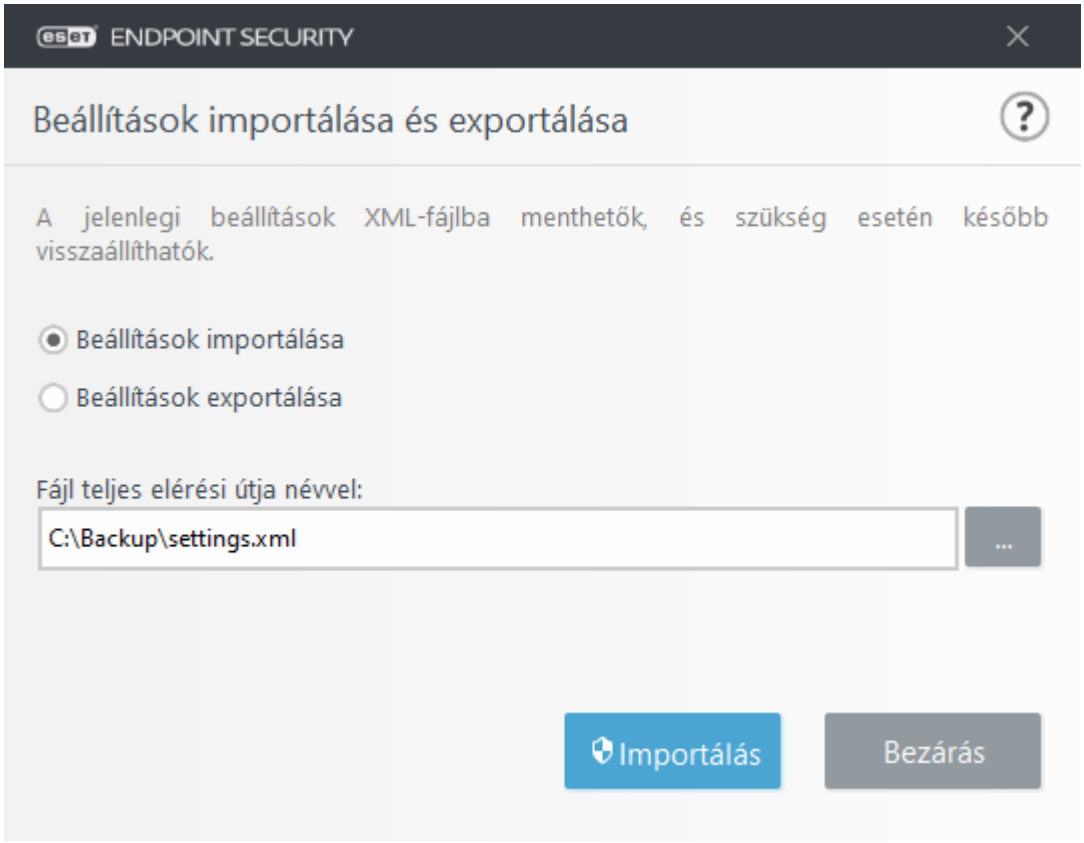
Mindkét művelet hasznos abban az esetben, ha az ESET Endpoint Security aktuális konfigurációjáról későbbi felhasználás céljából biztonsági másolatot szeretne készíteni. Az exportálási funkció emellett arra is alkalmas, hogy az .xml fájl importálásával a felhasználók egyszerűen átvihessék és más számítógépeken is beállíthassák a megfelelő konfigurációt.

A konfigurációk importálása igen egyszerű: A program főablakában válassza 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 fájlt.

A konfiguráció exportálásának lépései nagyon hasonlóak: A program főablakában kattintson a **Beállítások** > **Beállítások importálása és exportálása** lehetőségre. Jelölje be a **Beállítások exportálása** választógombot, és adja meg a konfigurációs fájl nevét (például *export.xml*). A tallózási funkcióval kijelölheti a fájl tárolására szánt mappát.

Ha nem rendelkezik megfelelő jogosultsággal az exportált fájl adott könyvtárba írásához, a beállítások exportálásakor hiba léphet fel.



Az összes beállítás visszaállítása alapértelmezettre

A További beállításokban (F5) található **Alapbeállítás** elemre kattintva visszaállíthatja az összes programbeállítást minden modul esetén. Az állapot áll vissza, amely egy új telepítést követően fennállna.

Tekintse meg a következőt is: Beállítások importálása és exportálása.

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.

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.

Távoli figyelés és kezelés

A Távoli figyelés és kezelés (RMM) a szoftverrendszerek felügyeletét és ellenőrzését jelenti egy helyileg telepített ügynök segítségével, amelyhez a felügyeleti szolgáltatók hozzáférhetnek.

ERMM – ESET beépülő modul az RMM-hez

- Az ESET Endpoint Security alapértelmezett telepítése tartalmazza az `ermm.exe` nevű fájlt a végpontalkalmazásban, a könyvtáron belül:
  C:\Program Files\ESET\ESET Security\ermm.exe
- Az `ermm.exe` egy parancssori segédprogram, amely megkönnyíti a végponttermékek felügyeletét és az esetleges RMM beépülő modullal való kommunikációt.
- Az `ermm.exe` adatokat cserél az RMM beépülő modullal, amely az RMM-szerverhez csatlakoztatott RMM-ügynökkel kommunikál. Alapértelmezés szerint az ESET RMM eszköz le van tiltva.

További segédanyagok

- Az ERMM-parancssor
- ERMM JSON-parancsok listája
- Távoli figyelés és kezelés aktiválásaESET Endpoint Security

ESET Direct Endpoint Management beépülő modulok külső gyártású RMM-megoldásokhoz

Az RMM-szerver egy külső szerveren fut szolgáltatásként. További információkért tekintse meg a következő ESET

Direct Endpoint Management online felhasználói útmutatókat:

- ESET Direct Endpoint Management beépülő modul a ConnectWise Automate szolgáltatáshoz
- ESET Direct Endpoint Management beépülő modul a DattoRMM szolgáltatáshoz
- ESET Direct Endpoint Management a Solarwinds N-Central szolgáltatáshoz
- ESET Direct Endpoint Management a NinjaRMM szolgáltatáshoz

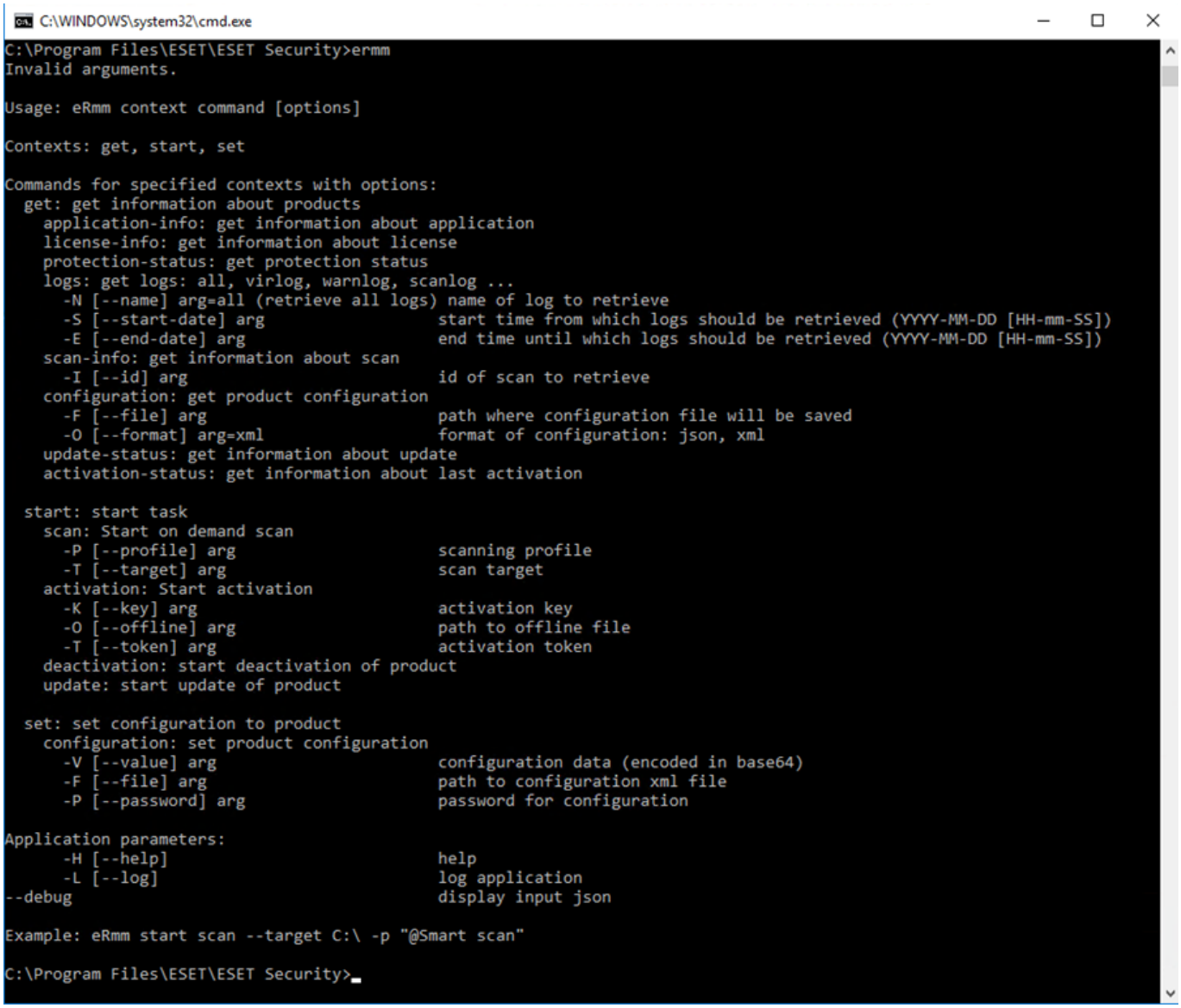
Az ERMM-parancssor

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update
	activation-status	Get information about last activation
start		**Start task**
	scan	Start on demand scan
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		**Set options for product**
	configuration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

ERMM JSON-parancsok listája

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status

- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call


```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```


result


```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```


get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"ANTISTEALTH32",
"description":"Anti-Stealth support module",
"version":"1106",
"date":"2016-10-17"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be {

success, running, failure }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

result


```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value

key	Activation key
offline	Path to offline file

Example

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

Gyakori kérdések

A fejezet néhány gyakori kérdést és problémát tekint át. Az adott probléma megoldási módjának megtekintéséhez kattintson a megfelelő témakör címére.

- Az ESET Endpoint Security frissítése
- Az ESET Endpoint Security aktiválása
- Új termék aktiválása az aktuális hitelesítő adatokkal
- Vírus eltávolítása a számítógépről
- Kommunikáció engedélyezése adott alkalmazás számára
- Új feladat létrehozása a feladatütemezőben
- Heti számítógép-ellenőrzés ütemezése
- Értesítések és interaktív riasztások kezelése
- A termék csatlakoztatása az ESET PROTECT alkalmazáshoz
  - A Felülbírálás mód használata
  - Ajánlott házirend alkalmazása az ESET Endpoint Security szolgáltatásra
- Tükrözés beállítása
- Frissítés Windows 10-re az ESET Endpoint Security programmal
- Távoli figyelés és kezelés aktiválása
- Hogyan akadályozható meg bizonyos fájltípusok letöltése az internetről?
- Az ESET Endpoint Security minimalista felhasználói felületének beállítása

Ha a megoldandó problémát nem találja a fenti listában, próbálja megkeresni az ESET Endpoint Security súgójában a problémához kapcsolódó kulcsszavak és kifejezések segítségével.

Ha a súgóban nem talál megoldást a problémájára vagy a kérdésére, keresse fel az ESET angol nyelvű tudásbázisát, ahol válaszokat találhat a gyakori kérdésekre és problémákra.

- Bevált eljárások a zsarolóprogramok elleni védekezéshez
- ESET Endpoint Security és ESET Endpoint Antivirus – gyakori kérdések
- Milyen címeket és portokat célszerű megnyitnom a külső tűzfalamon az ESET-termék teljes funkciókészletének engedélyezéséhez?

Ha szükséges, kérdésével vagy problémájával az online műszaki támogatási központunkat is megkeresheti. Az online kapcsolatfelvételi űrlap a program főablakának **Súgó és támogatás** ablaktáblájában található.

Automatikus frissítések – Gyakori kérdések

Az ESET Endpoint Security termékfrissítéseiről bővebben ebben az ESET-tudásbáziscikkünkben olvashat:
- Mik a különböző ESET-termékfrissítések és kiadási típusok?

A számítógépek automatikusan frissülnek? A frissítés az újraindítás előtt vagy után töltődik le?

A letöltés az újraindítás előtt történik, és a frissített fájlok előkészítése is ebben a szakaszban történik meg. Az újraindítás után is folyik a frissített fájlok használatra való előkészítése, és a jelenleg telepített verzió nyújt megszakítás nélküli védelmet. A módosítások az ESET Endpoint termék következő indítása után lesznek alkalmazva.

Körülbelül 3000 számítógépem van. Az összes számítógép egyszerre tölti le a frissítéseket? Használhatok proxyt ilyen sok számítógép automatikus frissítéséhez?

Az ESET a Tükrözési eszközt és a proxymegoldásokat kínálja a nagyobb hálózatokhoz, így a frissítéseket csak egyszer kell letölteni az internetről, és azután helyileg terjeszthetők. A frissítések kisebbek, jellemzően 5–10 MB-osak, és az ESET az elérhetőségük első néhány hetében szabályozza a frissítéseket. Ezért nem minden ügyfél egyszerre indítja a letöltést, amikor közvetlenül csatlakozik az ESET szervereihez.

Eldönthetem, hány számítógép vagy mely számítógépek frissüljenek automatikusan? Nem szeretnék tíznél több számítógépet letölteni óránként, vagy most csak tíz számítógépet szeretnék frissíteni, és néhány nap múlva egy újabb számítógépet.

A felügyelt környezetek automatikus frissítési házirenddel rendelkeznek, ahol megadhatja a legújabb kívánt verziót. Helyettesítő karaktereket (például 9.0.2032.*) is lehet használni. További információkért tekintse meg az Automatikus frissítések című fejezetet az ESET PROTECT vagy az ESET PROTECT Cloud online súgójában. Sajnos jelenleg nincs más lehetőség az automatikus frissítések korlátozására. Több házirendet is hozzárendelhet több csoporthoz.

Az automatikus frissítések csak a házirenden keresztül vannak konfigurálva? Letilthatom a házirendet, ha nem szeretnék frissíteni egy ESET-terméket?

Ha van egy biztonsági és stabilitási gyorsjavítás az ESET Endpoint termékhez, akkor a termék akkor is frissül, ha az automatikus frissítések le vannak tiltva, a vonatkozó végfelhasználói licencszerződésben meghatározott feltételek szerint. Az ESET biztonsági és stabilitási gyorsjavításokat alkalmaz a kritikus problémák elhárításához, valamint az ESET-termék maximális biztonságának és stabilitásának biztosításához.

Hozzárendelhet egy automatikus frissítési házirendet bármely végpontcsoporthoz, függetlenül a jelenlegi automatikus frissítési konfigurációjuktól. Nem felügyelt környezetekben a felhasználó helyileg konfigurálhatja az automatikus frissítéseket az ESET-végponttermék További beállítások képernyőjén.

Mi lenne akkor, ha a legkorábbi elérhető verzió használatára konfigurálnám a házirendet? Az ESET ekkor is frissítené a termékeimet?

A gyorsjavítások és a kritikus gyorsjavítások (biztonsági és stabilitási frissítések) kissé eltérő frissítési kategóriák. A felhasználói beállítások elfogadásakor a rendszeres gyorsjavítások szabványos prioritással rendelkező automatikus frissítésekhez rendelődnek. A kritikus gyorsjavítások kiemelt fontosságot kapnak a felhasználói beállításoktól függetlenül.

Hogyan fognak működni a frissítések offline forgatókönyvek esetén? Mikor használják a felhasználók az offline adattárat?

Az offline adattár is tartalmaz .dup és .fup fájlokat. Az adattárszakaszt a Tükrözési eszköznek kell letöltenie, nem a modulfrissítésnek. További információkért olvassa el ezt az ESET-tudásbáziscikket.

Honnan tudják az ESET termékei, hogy frissítésre van szükség? Az adattárból? Megkapnak bizonyos adatokat a szerverek? Ha az ESET egy hónappal a verziókiadás után tervez egy frissítést, akkor a szerverei tudják kezelni a világszerte történő kiadást?

Az ESET-termékek az adattárból töltik le az automatikus frissítéseket. A szerverek készen állnak erre, mivel a kritikus frissítések csupán néhány kilobájt méretűek. Az ESET nem alkalmaz szabályozást kritikus frissítések esetén az adattár szervereire. Van azonban egy lehetőség a szerverfrissítések szabályozására, ha az automatikus frissítések nagyobb méretűek. Az alábbi táblázatban példák láthatók a gyorsjavítások méretére eltérő automatikus frissítés esetén:

Előző verzió	Új verzió	Méret
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

Ha egy eltérő automatikus frissítés sikertelen, akkor az ESET-termék teljes körű frissítést kezdeményezhet. Ez továbbra is egy automatikus frissítés lenne funkcionalitási garanciával, viszont .dup fájl helyett .fup fájl fog letöltődni, ami nagyobb méretű fájl. A 9.0.2032.2-es verzió esetében 27 MB. Egy ilyen forgatókönyv azonban ritka.

Az ESET Endpoint Security/ESET Endpoint Antivirus frissítését szabályozással adják ki? Ha igen, meddig lesz szabályozva a frissítés a kiadás után?

Az ESET az új verziók kiadása utáni első néhány hétben szabályozza a frissítéseket, hogy ezzel csökkentse a szervereink terhelését és egyenletesen tudja terjeszteni az új verziót.

Az automatikus frissítések lesznek a frissítés egyik elsődleges módszere. Hogyan működik ez részleteiben?

Az ESET célja az, hogy a lehető legtöbb kliens frissüljön automatikus frissítések révén. Nehéz támogatást nyújtani, ha nagyon sok régebbi verzió érhető el. Az Automatikus frissítések funkció egyszerűen működik – a .dup fájlok letöltődnek az első modulfrissítési ellenőrzés során. A frissítési eljárás során a termék teljesen működőképes és védi a számítógépet. Az új verzió újraindítás után aktiválódik. Az ESET PROTECT (szerveroldali) szolgáltatásban egy házirend segítségével megadhatja a legújabb verziót, amelyre frissíteni szeretne, illetve helyettesítő karaktereket is használhat. További információkért tekintse meg az Auttomatikus frissítések című fejezetet az ESET PROTECT vagy az ESET PROTECT Cloud online súgójában.

Az igaz, hogy az automatikus frissítések 1/10 alapon működnek? Most az ESET Endpoint Security 8.0.2028.1-et használom. Az automatikus frissítések futtatása esetén ez milyen verzióra frissül?

A termékek automatikus frissítésekor késhet a frissítés az adattárszerverek szabályozása miatt. Ha a termékfrissítést szabályozással adjuk ki, akkor előfordulhat, hogy az automatikus frissítési ellenőrzések nem kapják meg azonnal. Ha a frissítés biztonságosnak és stabilnak tekinthető, a szabályozás csökkenthető vagy teljesen elhagyható, így az összes fennmaradó ügyfél megkapja a frissítést.

A szabályozási eljárás minden frissítésnél eltérő ideig tarthat. Attól függ, hogy hány ügyfél kéri a frissítést, mekkora a szervereink forgalma, valamint egyéb tényezőktől. Az eljárás folyamatosan fejlődik, és folyamatosan újításokra kerül sor. Továbbá, mivel az automatikus frissítési funkció új, a későbbiekben valószínűleg továbbfejlesztjük, ezzel is fokozva az ügyfélélményt.

Mikor indulnak el az automatikus frissítések, ha reggel 8:45-kor elindítok egy számítógépet, és délután 17:00 órakor kikapcsolom?

A következő sikeres ütemezett modulfrissítés során, legfeljebb egyszer 24 óránként.

Legközelebb mikor fog futni a frissítés, ha a számítógép akkor áll le, amikor az automatikus frissítések futnak?

A frissítés a következő beütemezett frissítési időszakban fog futni. Működésben van egy erőteljes hibamentes mechanizmus az automatikus frissítési (korábban uPCU) eljárás során. A frissítés letöltése és a számítógép újraindítása előtt még a frissített fájlok előkészítése folyik, és a jelenleg telepített verzió nyújt megszakítás nélküli védelmet. A módosítások az ESET Endpoint termék következő indítása után lesznek alkalmazva.

Hogyan futtathatom azonnal az automatikus frissítéseket anélkül, hogy 24 óránként megvárnám a normál kapcsolatot? Van más módja ennek azon kívül, hogy a Frissítések keresése gombra kattintok?

Csak akkor indíthatja el az automatikus frissítési eljárást manuálisan, ha megnyitja a fő programablakot, majd a **Frissítés** > **Frissítések keresése** elemre kattint. A modulfrissítések elindításának minden más módja a 24 órás Automatikus frissítési ütemező házirendet tükrözi. Jelenleg nem lehet távolról elindítani az automatikus frissítések letöltését. Ezt a funkciót a későbbiekben valósítjuk meg.

Az ESET Endpoint Security frissítése

Az ESET Endpoint 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. Az időköz módosításához lépjen az **Eszközök** > **Feladatütemező** lapra (további információk a feladatütemezőről).

Az ESET Endpoint Security aktiválása

A telepítés végeztével a rendszer kéri a szoftver licencének aktiválását.

A licenc számos módon aktiválható. Az aktiválási ablakban elérhető adott aktiválási lehetőség függ az országtól, valamint attól, hogy a telepítőfájl milyen formában érhető el (ESET weboldala, .msi vagy .exe telepítőtípus stb.).

Ha az ESET Endpoint Security licencét közvetlenül a programból szeretné aktiválni, nyissa meg az ESET Endpoint Security fő programablakát, és a főmenüben kattintson a **Súgó és támogatás** > **Termék aktiválása** vagy a **Védelem állapota** > **Termék aktiválása** elemre.

Az ESET Endpoint Security aktiválásához az alábbi lehetőségek közül választhat:

- **Licenckulcs megadása** – A licenctulajdonos azonosítására és a licenc aktiválására szolgáló egyedi, XXXX-XXXX-XXXX-XXXX-XXXX formátumú karakterlánc.
- **ESET Business Account** – Az ESET Business Account portálon a hitelesítő adatokkal (e-mail-cím és jelszó) létrehozott fiók. Ezzel a módszerrel több licencet kezelhet egyetlen helyről.
- **Kapcsolat nélküli licenc** – Egy automatikusan létrehozott, a licencadatok megadása végett az ESET-szoftverbe átvitt fájl. Ha egy licenc lehetővé teszi kapcsolat nélküli licencfájl (.lf) letöltését, az adott fájl használható a kapcsolat nélküli aktiválás végrehajtásához. A program kivonja a kapcsolat nélküli licencek számát a rendelkezésre álló licencek teljes számából. A kapcsolat nélküli fájlok létrehozásáról az ESET Business Account felhasználói útmutatójában olvashat részletesen.

Kattintson az **Aktiválás később** elemre, ha a számítógép egy felügyelt hálózat tagja, és a rendszergazda távoli aktiválást hajt végre az ESET PROTECT eszközzel. Akkor is használhatja ezt a lehetőséget, ha később szeretné aktiválni ezt a klienst.

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

⚠ Nem sikerült a termékaktiválás?

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. A **Névjegy** részen látható a felhasználónév, amelyen a számítógép regisztrálva van. A megnyitásához kattintson a jobb gombbal a rendszertálca ikonjára.

> ℹ Az ESET PROTECT 7.2 vagy ESET PROTECT 9 képes értesítés nélkül, a rendszergazda által elérhetővé tett licenceket használva aktiválni a kliensszámítógépeket. Ennek módját az ESET PROTECT online súgóban találja meg.

A licenckulcs megadása az aktiválás során

Az automatikus frissítések fontosak a biztonság szempontjából. Az ESET Endpoint Security csak akkor kapja meg a frissítéseket, ha aktiválva lett a **Licenckulcs** mezőben megadott licenckulccsal.

Ha nem adta meg a licenckulcsot a telepítés után, a termék aktiválása nem történik meg. A licencet a fő programablakban módosíthatja. Ehhez kattintson a **Súgó és támogatás** > **Licenc aktiválása** elemre, és a Licenc aktiválása ablakban adja meg az ESET biztonsági termékkel kapott licencadatokat.

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.

Bejelentkezés az ESET Business Account-fiókba

A biztonsági rendszergazdai fiók az ESET Business Account portálon az **e-mail-címével** és a **jelszavával** létrehozott fiók, amely minden munkaállomásonkénti hitelesítést lát. A biztonsági rendszergazdai fiók lehetővé teszi több licenc kezelését. Ha nem rendelkezik biztonsági rendszergazdai fiókkal, kattintson a **Fiók létrehozása** gombra, hogy a rendszer átirányítsa az ESET Business Account portálra, ahol a hitelesítő adatait használva regisztrálhat.

Ha elfelejtette a jelszavát, kattintson az **Elfelejtettem a jelszavam** hivatkozásra, hogy a rendszer átirányítsa az ESET Business Account portálra. Adja meg az e-mail címét, és a megerősítéshez kattintson a **Bejelentkezés** gombra. Ezután egy levelet kap a jelszava alaphelyzetbe állítására vonatkozó utasításokkal.

Újabb ESET-végponttermékek aktiválása régi típusú licenc hitelesítő adataival

Ha már van felhasználóneve és jelszava, és szeretne licenckulcsot beszerezni, keresse fel az ESET Business Account portált, ahol a hitelesítő adatait új licenckulccsá konvertálhatja.

Vírus eltávolítása a számítógépről

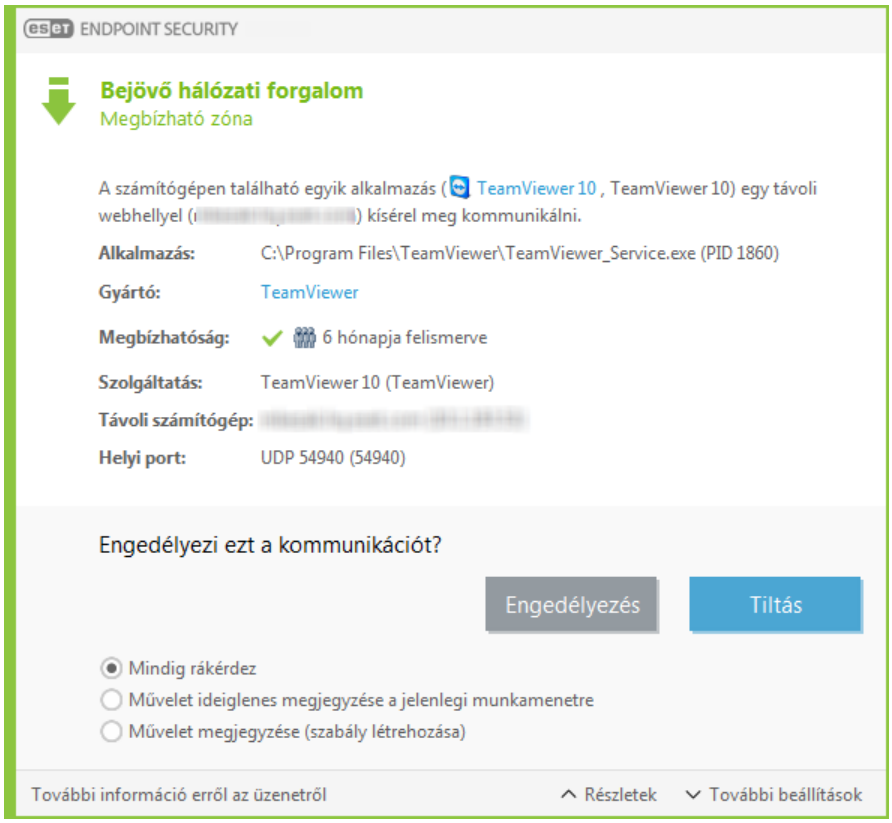
Ha a számítógép fertőzés jeleit mutatja, például lassabb vagy gyakran lefagy, ajánlott elvégezni az alábbiakat:

1. A program főablakában kattintson a **Számítógép ellenőrzése** lehetőségre.
2. A rendszer ellenőrzéséhez kattintson az **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 Endpoint 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 Endpoint Security észlelné az alkalmazásokat, új tűzfalszabályokat hozhat létre az alkalmazásokhoz a tűzfal beállítási ablakában. Nyissa meg a fő programablakot > **Beállítások** > **Hálózat** > **Tűzfal** > kattintson a fogaskerékre > **Konfigurálás** > **Speciális** > **Szabályok** a **Szerkesztés** gombra kattintva.

A szabály hozzáadásához kattintson a **Hozzáadás** gombra. A **Szabályok** 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.

Új feladat létrehozása a feladatütemezőben

Ha új feladatot szeretne létrehozni az **Eszközök** > **Feladatütemező** eszközben, kattintson a **Feladat hozzáadása** 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 modulfrissítésekre.

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** 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** > **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. Jelölje ki a legördülő lista **Kézi indítású számítógép-ellenőrzés** elemét.
3. Nevezze el a feladatot, és jelölje be a **Hetente választógombot**.

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.

Az ESET Endpoint Security csatlakoztatása az ESET PROTECT alkalmazáshoz

Ha telepítette az ESET Endpoint Security szolgáltatást a számítógépére, és az ESET PROTECT segítségével szeretne kapcsolódni, akkor telepítse az ESET Management Agentet is a kliensszámítógépekre. Minden olyan kliensmegoldás szerves részét képezi, amely az ESET PROTECT-szerverrel kommunikál.

- Az ESET Management Agent telepítése vagy központi telepítése kliensszámítógépekre

Lásd még:

- Távolról felügyelt végpontok dokumentációja
- A Felülbírálás mód használata
- Ajánlott házirend alkalmazása az ESET Endpoint Security szolgáltatásra

A Felülbírálás mód használata

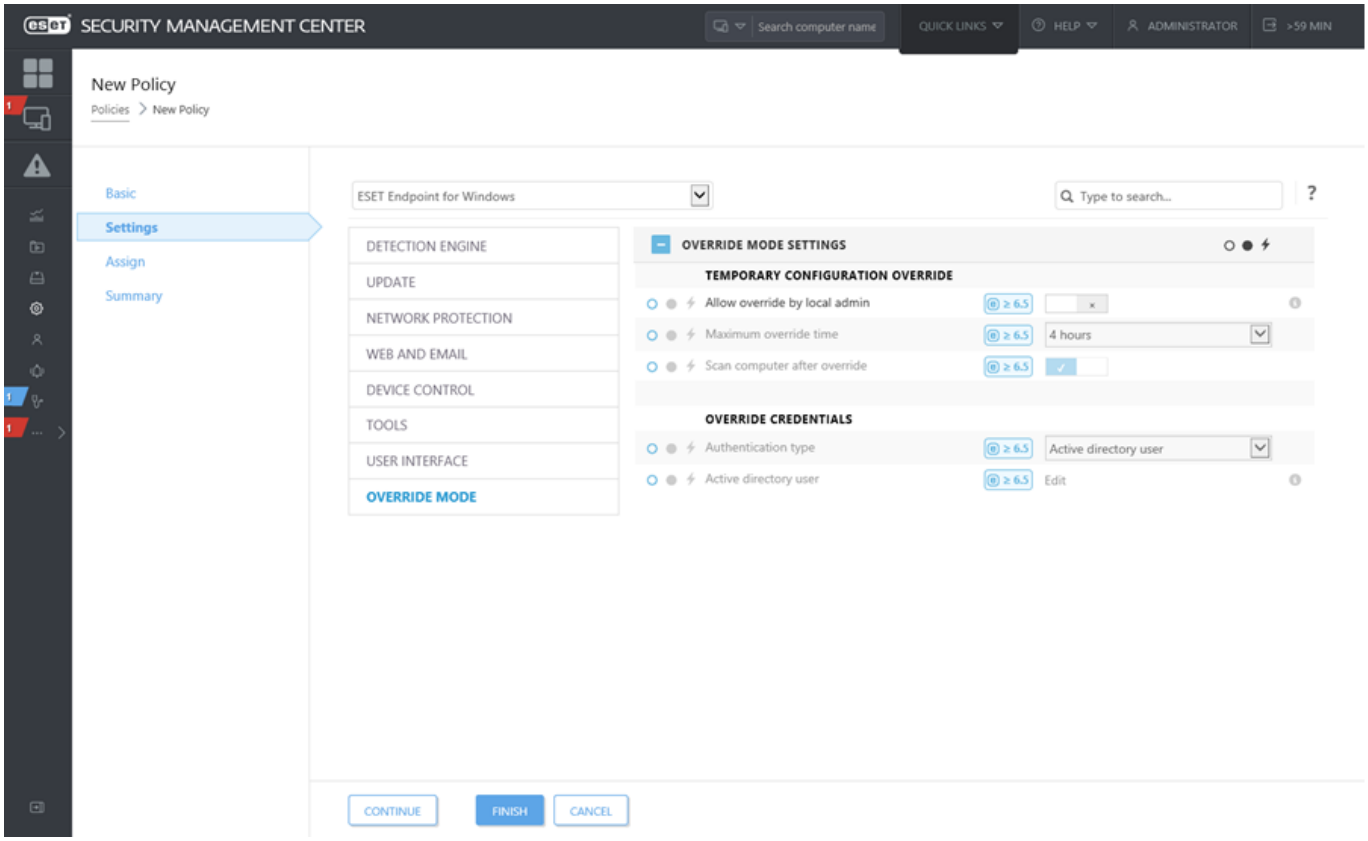
A Windows rendszerhez készült ESET Endpoint termékek (6.5-ös és újabb verziók) felhasználói használhatják a Felülbírálás módot. A Felülbírálás mód lehetővé teszi a felhasználóknak, hogy kliensszámítógép-szinten akkor is módosítsák a beállításaikat a telepített ESET szoftverben, ha a beállításokra házirend vonatkozik. A Felülbírálás mód bizonyos AD-felhasználókhoz engedélyezhető, illetve jelszóval védhető. A funkció egyszerre legfeljebb négy órára engedélyezhető.

⚠ • Az aktiválása után a Felülbírálás mód nem állítható le az ESET PROTECT Webkonzolban. A Felülbírálás mód automatikusan leáll, ha letelik a felülbírálási időszak. A kliensgépen is kikapcsolható.
• A Felülbírálás módot használó felhasználónak is Windows rendszergazdai jogosultságokkal kell rendelkeznie. Ellenkező esetben a felhasználó nem tudja menteni a módosításokat az ESET Endpoint Security beállításaiban.
• Active Directory-csoporthitelesítésre az ESET Endpoint Security 7.0.2100.4-es és újabb verziói esetén van lehetőség.

A **Felülbírálás mód** beállítása:

1. Lépjen a **Házirendek** > **Új házirend** lapra.
2. A **Basic** (Alapadatok) csoportban írjon be egy **nevet** és **leírást** a házirendhez.
3. A **Settings** (Beállítások) csoportban válassza az **ESET Endpoint for Windows** lehetőséget.
4. Kattintson az **Override mode** (Felülbírálás mód) lehetőségre, és adja meg a felülbírálás mód szabályait.
5. Az **Assign** (Hozzárendelés) csoportban válassza ki a számítógépet vagy a számítógépcsoportot, amelyre a házirendet alkalmazni szeretné.
6. Tekintse át a beállításokat a **Summary** (Összegzés) csoportban, és a házirend alkalmazásához kattintson a

Finish (Befejezés) elemre.



Ha *Jánosnak* problémája van az Endpoint beállításaival, amelyek letiltják egyes fontos funkciók működését vagy a webhozzáférést ezen a gépen, a rendszergazda engedélyezheti, hogy *János* felülírja a meglévő Endpoint-házirendet, és kézzel módosítja a beállításokat ezen a gépen. Ezután az ESET PROTECT lekérheti ezeket az új beállításokat, így a rendszergazda azok alapján létrehozhat egy új házirendet.
Ehhez végezze el az alábbi lépéseket:
1. Lépjen a **Házirendek** > **Új házirend** lapra.
2. Töltse ki a **Name** (Név) és a **Description** (Leírás) mezőt. A **Settings** (Beállítások) csoportban válassza az **ESET Endpoint for Windows** lehetőséget.
3. Kattintson az **Override mode** (Felülbírálás mód) lehetőségre, engedélyezze a Felülbírálás módot egy órára, és AD-felhasználóként válassza *Jánost*.
4. Rendelje a házirendet *János számítógépéhez*, és a házirend mentéséhez kattintson a **Finish** (Befejezés) lehetőségre.
5. *Jánosnak* engedélyeznie kell a **Felülbírálás módot** az ESET Endpoint szoftverében, és kézzel kell módosítania a beállításokat ezen a gépen.
6. Az ESET PROTECT webkonzolon keressen meg a **Computers** (Számítógépek) csoportot, válassza ki *János számítógépét*, és kattintson a **Show Details** (Részletek megjelenítése) elemre.
7. A **Configuration** (Konfiguráció) csoportban kattintson a **Request configuration** (Konfiguráció kérése) elemre, ha egy kliensfeladatot szeretne ütemezni a konfiguráció azonnali beolvasásához a kliensről.
8. Kis idő múlva megjelenik az új konfiguráció. Kattintson arra a termékre, amelynek a beállításait menteni szeretné, majd kattintson az **Open Configuration** (Konfiguráció megnyitása) lehetőségre.
9. Ekkor áttekintheti a beállításokat, majd a **Convert to policy** (Konvertálás házirendre) elemre kattinthat.
10. Töltse ki a **Name** (Név) és a **Description** (Leírás) mezőt.
11. A **Settings** (Beállítások) csoportban szükség szerint módosíthatja a beállításokat.
12. Az **Assign** (Hozzárendelés) csoportban hozzárendelheti ezt a házirendet *János számítógépéhez* (vagy másokhoz).
13. A beállítások mentéséhez kattintson a **Finish** (Befejezés) lehetőségre.
14. Ha már nincs rá szükség, távolítsa el a felülbírálási házirendet.

Ajánlott házirend alkalmazása az ESET Endpoint Security szolgáltatásra

Miután megtörtént az ESET Endpoint Security és az ESET PROTECT csatlakoztatása, a legcélszerűbb megoldás egy ajánlott vagy egyéni házirend alkalmazása.

Több beépített házirend is rendelkezésre áll az ESET Endpoint Security szolgáltatáshoz:

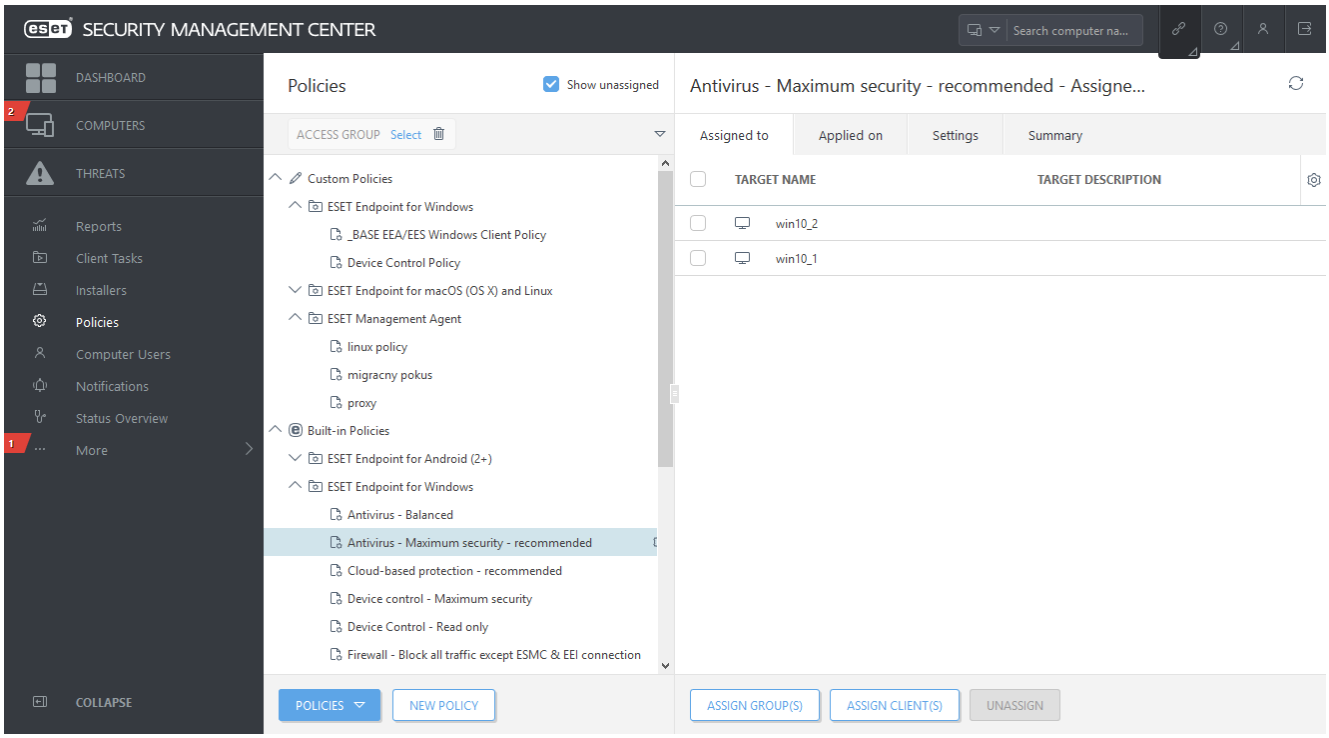
Házirend	Leírás
Vírusvédelem – Kiegyensúlyozott	Ez az ajánlott biztonsági konfiguráció a legtöbb telepítési mód esetén.
Vírusvédelem – Maximális biztonság	Kihasználja a gépi tanulás, a viselkedésalapú ellenőrzés és az SSL-szűrés előnyeit. Ez a veszélyes, kéretlen és gyanús alkalmazások észlelésére van hatással.
Felhőalapú megbízhatósági és visszajelzési rendszer	Engedélyezi az ESET LiveGrid® felhőalapú megbízhatósági és visszajelzési rendszert, amivel javítható a legújabb kártevők felismerése, és megoszthatók a rosszindulatú és ismeretlen potenciális kártevők a további elemzés elősegítése céljából.
Eszközfelügyelet – Maximális biztonság	Az összes eszközt blokkolja. Az eszközök csatlakoztatását a rendszergazdának kell engedélyeznie.
Eszközfelügyelet – Csak olvasható	Az összes eszközt csak olvasni lehet. Az írás nem engedélyezett.
Tűzfal – Minden forgalom tiltása az ESET PROTECT- és az ESET Inspect-csatlakozások kivételével	Minden forgalom tiltása, kivéve az ESET PROTECThez és az ESET Inspect Serverhez történő csatlakozást (csak az ESET Endpoint Security esetén).
Naplózás – Teljes diagnosztikai naplózás	Ez a sablon biztosítja, hogy a rendszergazdának szükség esetén minden napló a rendelkezésére álljon. Minden naplózva lesz egészen a minimális részletességtől kezdve, többek között a Behatolásmegelőző rendszer (HIPS) és a Threatsense paraméterei, illetve a tűzfal. A naplók 90 nap után automatikusan törlődnek.
Naplózás – Csak a fontos események naplózása	A figyelmeztetések, hibák és kritikus események naplózását biztosító házirend. A naplók 90 nap után automatikusan törlődnek.
Láthatóság – Kiegyensúlyozott	A láthatóság alapbeállításai. Engedélyezve vannak az állapotok és az értesítések.
Láthatóság – Láthatatlan mód	Le vannak tiltva az értesítések, a riasztások, a GUI és a helyi menübe történő integráció. Az egui.exe nem fog futni. A kizárólag az ESET PROTECT Cloud-ból történő felügyelet esetén megfelelő.
Láthatóság – Csökkentett interakció a felhasználóval	Az állapotok és az értesítések le vannak tiltva, de a GUI fut.

Kövesse az alábbi lépéseket a **Vírusvédelem – Maximális biztonság** elnevezésű házirend beállításához, amely több mint 50 ajánlott beállítást tartalmaz a számítógépekre telepített ESET Endpoint Security szolgáltatáshoz:

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:
• Ajánlott vagy előre megadott házirend alkalmazása az ESET Endpoint Security szolgáltatáshoz az ESET PROTECT segítségével

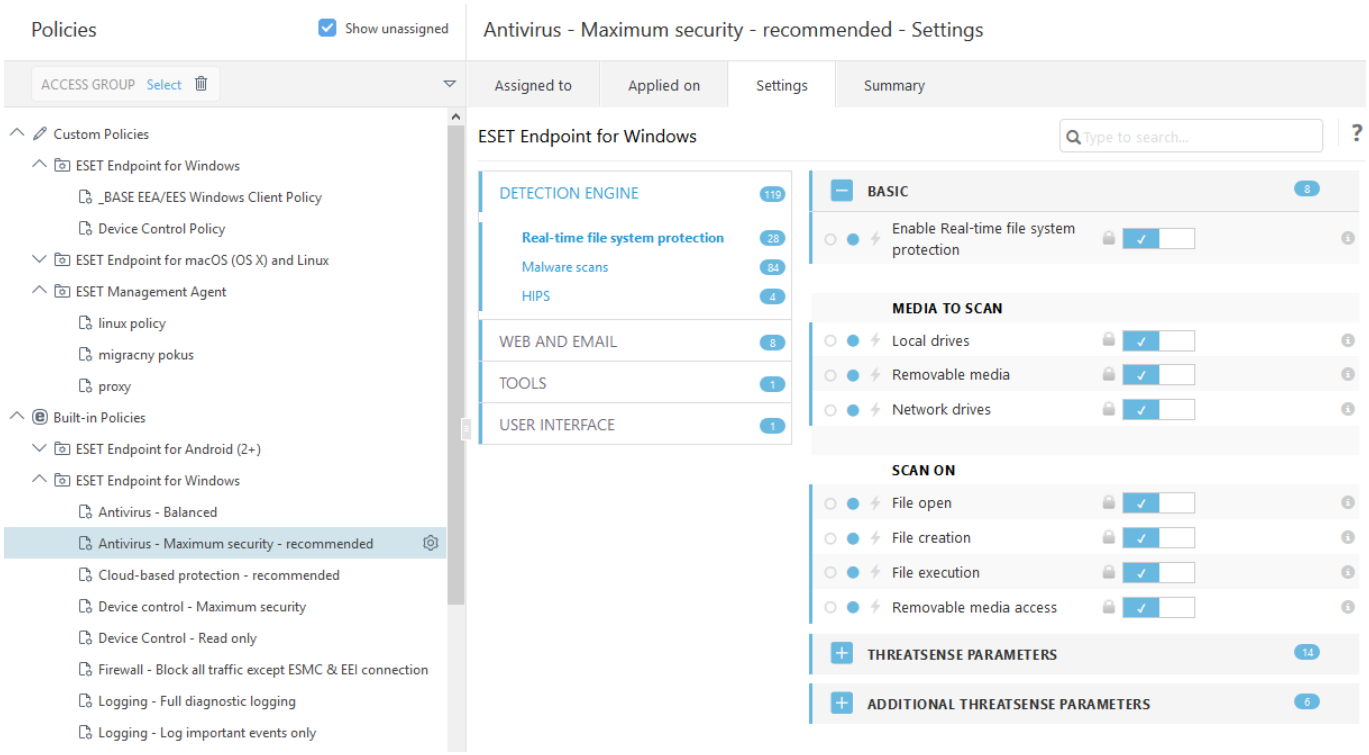
1. Nyissa meg az ESET PROTECT Webkonzolt.

2. Lépjen a **Házirendek** lapra, majd bontsa ki a **Beépített házirendek** > **ESET Végpont for Windows** szakaszt.
3. Kattintson a **Vírusvédelem – Maximális biztonság – javasolt** elemre.
4. A **Hozzárendelve ehhez:** lapon kattintson a **Kliens(ek) hozzárendelése** vagy a **Csoport(ok) hozzárendelése** elemre, majd válassza ki azokat a számítógépeket, amelyekre alkalmazni szeretné a házirendet.



Ha meg szeretné nézni, hogy mely beállítások vannak alkalmazva a házirendre, kattintson a **Beállítások** fülre, majd bontsa ki a További beállítások fát.

- A kék színű pont a házirend miatt módosított beállítást jelzi
- A kék színű keretben látható szám a házirend által módosított beállítások mennyiségét jelzi
- Itt bővebben olvashat az ESET PROTECT-házirendekről



Tükrözés beállítása

Az ESET Endpoint Security beállítható a keresőmotor-frissítési fájlok másolatának tárolására és a frissítések terjesztésére az ESET Endpoint Security vagy az ESET Endpoint Antivirus programot futtató más munkaállomásokra.

Az ESET Endpoint Security beállítása tükörszerverként a frissítések biztosításához belső HTTP-szerveren keresztül

1. Az **F5** billentyűt megnyomva nyissa meg a További beállítások párbeszédpanelt, majd kattintson a **Frissítés** > **Profilok** > **Frissítési tükör** elemre.
2. Bontsa ki a **Frissítések** csomópontot, és jelölje be az **Automatikus kiválasztás** jelölőnégyzetet a **Modulfrissítés** szakaszban.
3. Bontsa ki a **Frissítési tükör** csomópontot, és jelölje be az **Frissítési tükör létrehozása** és a **HTTP-szerver engedélyezése** jelölőnégyzetet.

További információkért tekintse meg a következőket:
- Frissítési tükör
- Frissítés tükörből

Tükörszerver beállítása frissítések biztosításához megosztott hálózati mappán keresztül

1. Megosztott mappa létrehozása helyi vagy hálózati eszközön. A mappának olvashatónak kell lennie az ESET biztonsági termékeit futtató összes felhasználó számára, a helyi RENDSZER fiókról pedig írhatónak kell lennie.
2. Aktiválja a **Frissítési tükör létrehozása** funkciót a **További beállítások** > **Frissítés** > **Profilok** > **Frissítési tükör** lapon.

3. Válassza ki a megfelelő **Tárolómappát** a **Kiürítés**, majd a **Szerkesztés** elemre kattintva. Keresse meg és válassza ki a létrehozott megosztott mappát.

Ha nem szeretne a belső HTTP-szerveren keresztül modulokat frissíteni, kapcsolja ki a **Frissítési tükör létrehozása** funkciót.

Frissítés Windows 10-re az ESET Endpoint Security programmal

Azt javasoljuk, hogy mielőtt frissítene a Windows 10 rendszerre, frissítse ESET-szoftverét a legújabb verzióra, majd töltse le a legújabb modulfrissítéseket. Ezzel biztosíthatja a maximális védelmet, és megőrizheti a program beállításait és a licencadatait a Windows 10-re történő frissítés során.

Verzió 7.x:

Az alábbi megfelelő hivatkozásra kattintva töltse le és telepítse a legújabb verziót, mielőtt Microsoft Windows 10-re frissítene:

A 32 bites ESET Endpoint Security 7 letöltése A 32 bites ESET Endpoint Antivirus 7 letöltése

A 64 bites ESET Endpoint Security 7 letöltése A 64 bites ESET Endpoint Antivirus 7 letöltése

Verzió 5.x:

Az 5-ös verziójú ESET Endpoint termékek jelenlegi állapota az Elérte az életciklus végét. Ez azt jelenti, hogy a buildek már nem érhetők el nyilvánosan letöltésre. Azt javasoljuk, mindenképpen frissítsen az ESET Endpoint termékek legújabb verziójára.

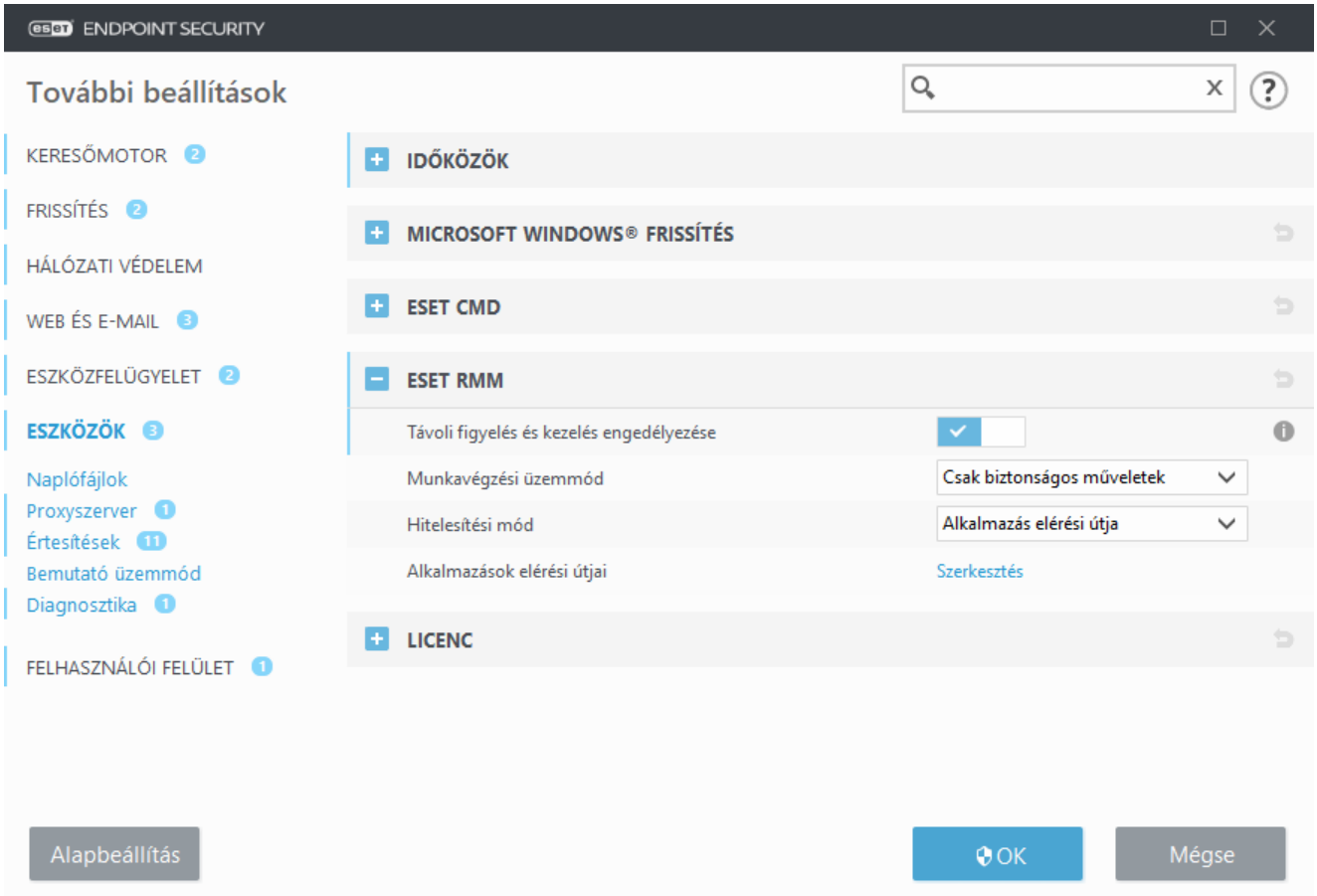
Más nyelvű verziók:

Ha az ESET Endpoint szoftver más nyelven kiadott verzióját keresi, látogasson el a letöltési lapunkra.

További információk az ESET üzleti termékek és a Windows 10 kompatibilitásáról.

Távoli figyelés és kezelés aktiválása

A Távoli figyelés és kezelés (RMM) a szoftverrendszerek felügyeletét és ellenőrzését jelenti (például asztali számítógépeken, szervereken és mobileszközökön) egy helyileg telepített ügynök segítségével, amelyhez a felügyeleti szolgáltatók hozzáférhetnek. Az RMM a 6.6.2028.0-s verziótól tudja felügyelni az ESET Endpoint Security szolgáltatást.



Az ESET RMM alapértelmezés szerint le van tiltva. Az ESET RMM engedélyezéséhez nyomja meg az **F5** billentyűt a további beállítások megnyitásához, kattintson az **Eszközök** elemre, bontsa ki az **ESET RMM** csomópontot, és kapcsolja be a **Távoli figyelés és kezelés engedélyezése** kapcsolót.

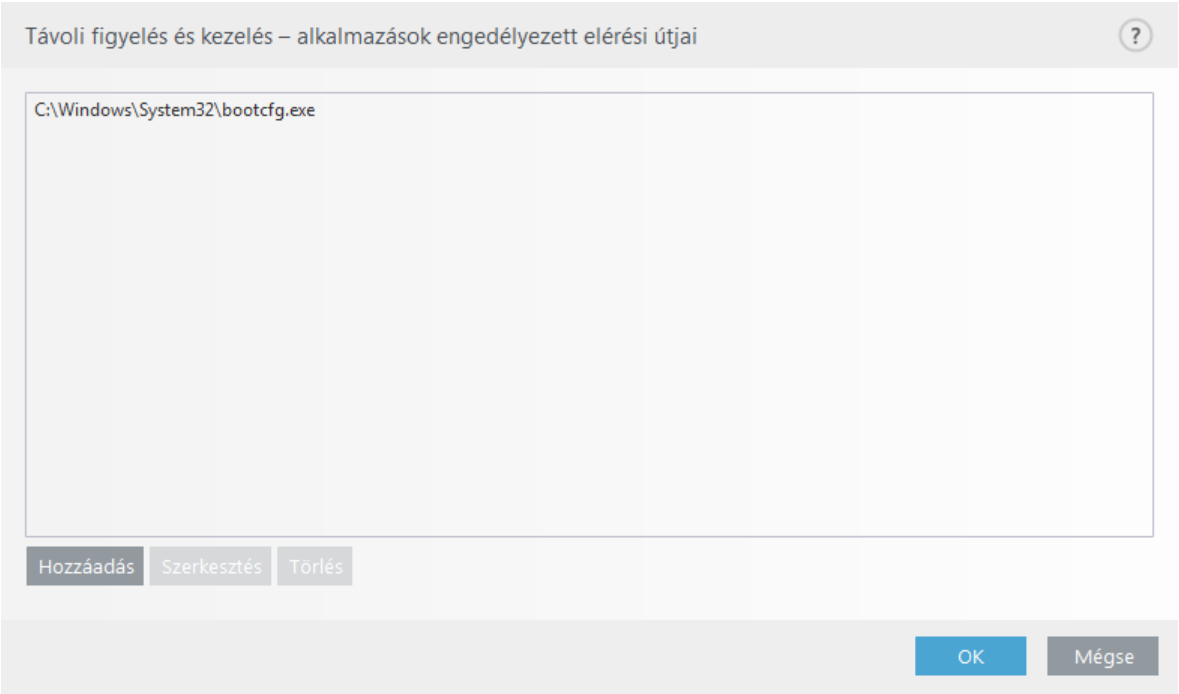
Munkavégzési üzemmód – Válassza a **Csak biztonságos műveletek** beállítást, ha a biztonságos és írásvédett műveletekhez szeretné engedélyezni az RMM felületét. A **Minden művelet** beállítást válassza, ha minden művelethez az RMM felületét szeretné használni.

Művelet	Mód: Csak biztonságos műveletek	Mód: Minden művelet
Get application-info	✔	✔
Get configuration	✔	✔
Licencinformációk megtekintése	✔	✔
Get logs	✔	✔
Védelmi állapot megtekintése	✔	✔
Frissítési állapot megtekintése	✔	✔
Set configuration		✔
Start activation		✔
Start scan	✔	✔
Start update	✔	✔

Hitelesítési mód – Adja meg az RMM hitelesítési módját. A hitelesítés használatához válassza a legördülő listából az **Alkalmazás elérési útja** lehetőséget, ellenkező esetben válassza a **Nincs** lehetőséget.

A Távoli figyelés és kezelés funkciónak engedélyezést használva meg kell akadályoznia, hogy a kártevő szoftverek letiltsák vagy megkerüljék az ESET Endpoint-védelmet.

Alkalmazások elérési útjai – Olyan alkalmazás, amelynek engedélye van az RMM futtatására. Ha az **Alkalmazás elérési útja** hitelesítési módot választotta, kattintson a **Szerkesztés** gombra a **Távoli figyelés és kezelés – alkalmazások engedélyezett elérési útjai** beállításablak megnyitásához.



Hozzáadás – Új engedélyezett alkalmazáselérési út létrehozása a Távoli figyelés és kezelés számára. Írja be az elérési utat, vagy kattintson a **…** gombra egy végrehajtható fájl kiválasztásához.

Szerkesztés – Meglévő engedélyezett elérési út módosítása. Amennyiben a végrehajtható fájl másik mappába került át, használja a **Szerkesztés** lehetőséget.

Törlés – Meglévő engedélyezett elérési út eltávolítása.

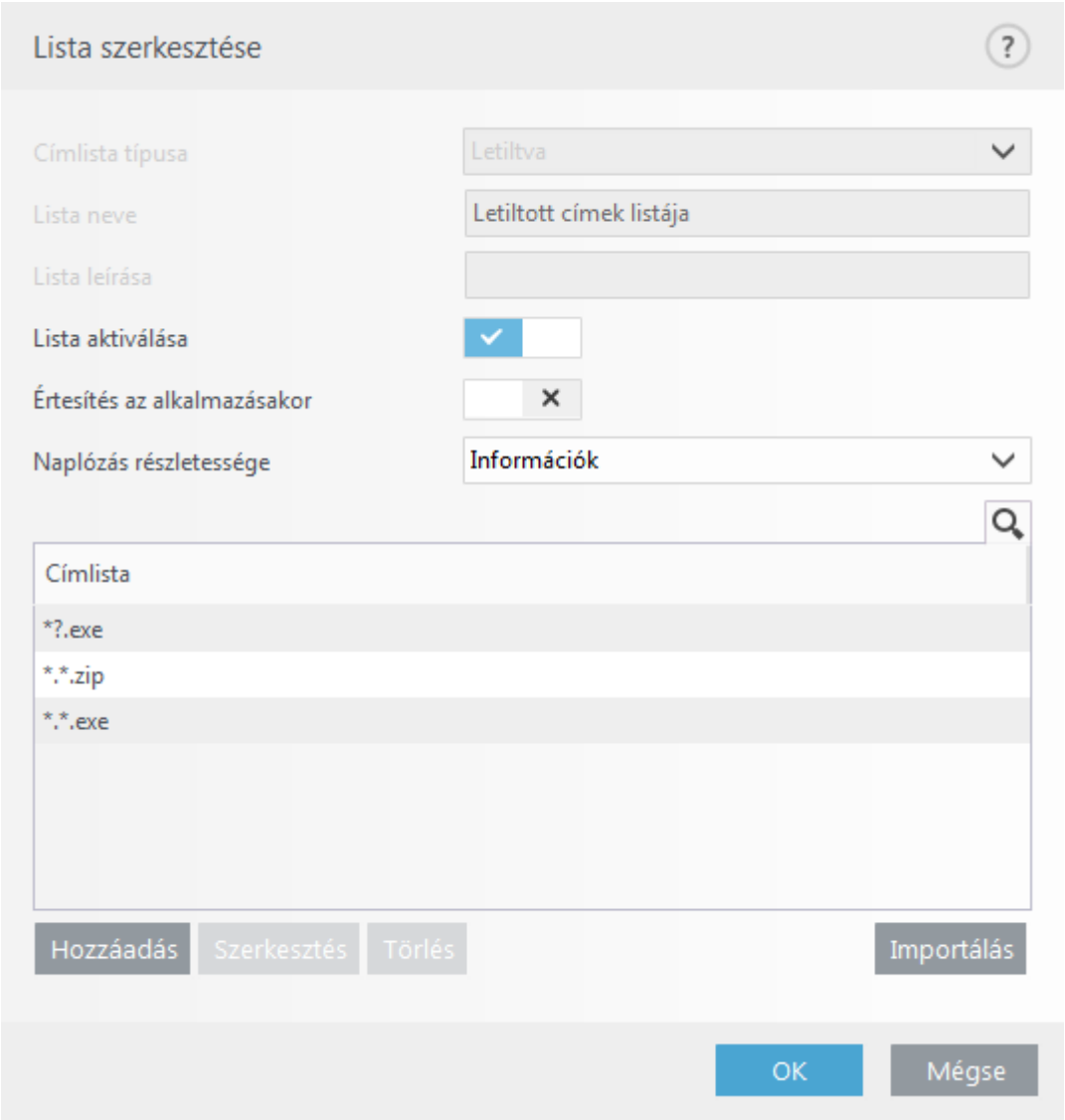
Az ESET Endpoint Security alapértelmezett telepítése esetén az ermm.exe az Endpoint alkalmazás alapértelmezett könyvtárában található (alapértelmezett elérési út C*:\Program Files\ESET\ESET Security*). Az ermm.exe az RMM beépülő moduljával cserél adatokat, amely egy RMM-szerverrel társított RMM-ügynökkel kommunikál.

- ermm.exe – az ESET által fejlesztett parancssori segédprogram, amely lehetővé teszi az Endpoint-termékek kezelését és a kommunikációt bármely RMM beépülő modullal.
- Az RMM beépülő modul egy harmadik fél által készített helyben futó alkalmazás az Endpoint Windows rendszeren. A beépülő modul egy adott RMM-ügynökkel (pl. csak Kaseya) és az ermm.exe programmal való kommunikációhoz készült.
- Az RMM-ügynök egy harmadik fél által készített helyben futó alkalmazás az Endpoint Windows rendszeren. Az ügynök az RMM beépülő modullal és az RMM-szerverrel kommunikál.

Hogyan akadályozható meg bizonyos fájltípusok letöltése az internetről?

Ha nem szeretné engedélyezni bizonyos fájltípusok (pl. exe, pdf vagy zip) internetről való letöltését, használja az URL-címek kezelése funkciót és helyettesítő karaktereket. Nyomja meg az F5 billentyűt a **További beállítások** ablak megnyitásához. Kattintson a **Web és e-mail** > **Webhozzáférés-védelem** elemre, majd bontsa ki az **URL-címek kezelése** szakaszt. Kattintson a **Szerkesztés** elemre a **Címlista** felirat mellett.

A **Címlista** ablakban válassza ki a **Letiltott címek listája** elemet, majd kattintson a **Szerkesztés** elemre, vagy a **Hozzáadás** elemre egy új lista létrehozásához. Ekkor megnyílik egy új ablak. Ha új listát hoz létre, válassza ki a **Letiltott** menüpontot a **Címlista típusa** legördülő menüből, és nevezze el a listát. Ha értesítést szeretne kapni az aktuális listában szereplő fájltípus elérésekor, aktiválja az **Értesítés az alkalmazásakor** csúszkát. Válassza ki a **naplózás részletességét** a legördülő menüből. A Remote Administrator **Figyelmeztetés** részletességű rekordokat tud gyűjteni.



A **Hozzáadás** gombra kattintva adjon meg egy olyan maszkot, amely a letöltésből kizárni kívánt fájltípusokat határozza meg. Adja meg a teljes URL-t, ha tiltani szeretné egy bizonyos fájl, bizonyos webhelyről való letöltését – például: *http://example.com/file.exe*. Helyettesítő karakterek használatával fájlcsoportokat is megadhat. A kérdőjel (?) egyetlen karaktert jelöl, a csillag (*) pedig nulla vagy annál több karaktert. Például a **/*.zip* maszk

letiltja az összes Zip-tömörítésű fájl letöltését.

Vegye figyelembe, hogy csak bizonyos típusú fájlok letöltése tiltható le ezzel a módszerrel, ha a fájlkiterjesztés a fájlok URL-címének részét képezi. Ha a weboldal fájlletöltési URL-címeket alkalmaz – például *www.example.com/download.php?fileid=42* –, akkor a linken található összes fájl letöltődik akkor is, ha letiltott kiterjesztésűek.

Az ESET Endpoint Security minimalista felhasználói felületének beállítása

Távoli felügyelet esetén alkalmazhat egy előre meghatározott „Láthatóság” házirendet.

Ha nem, manuálisan hajtsa végre a következőket:

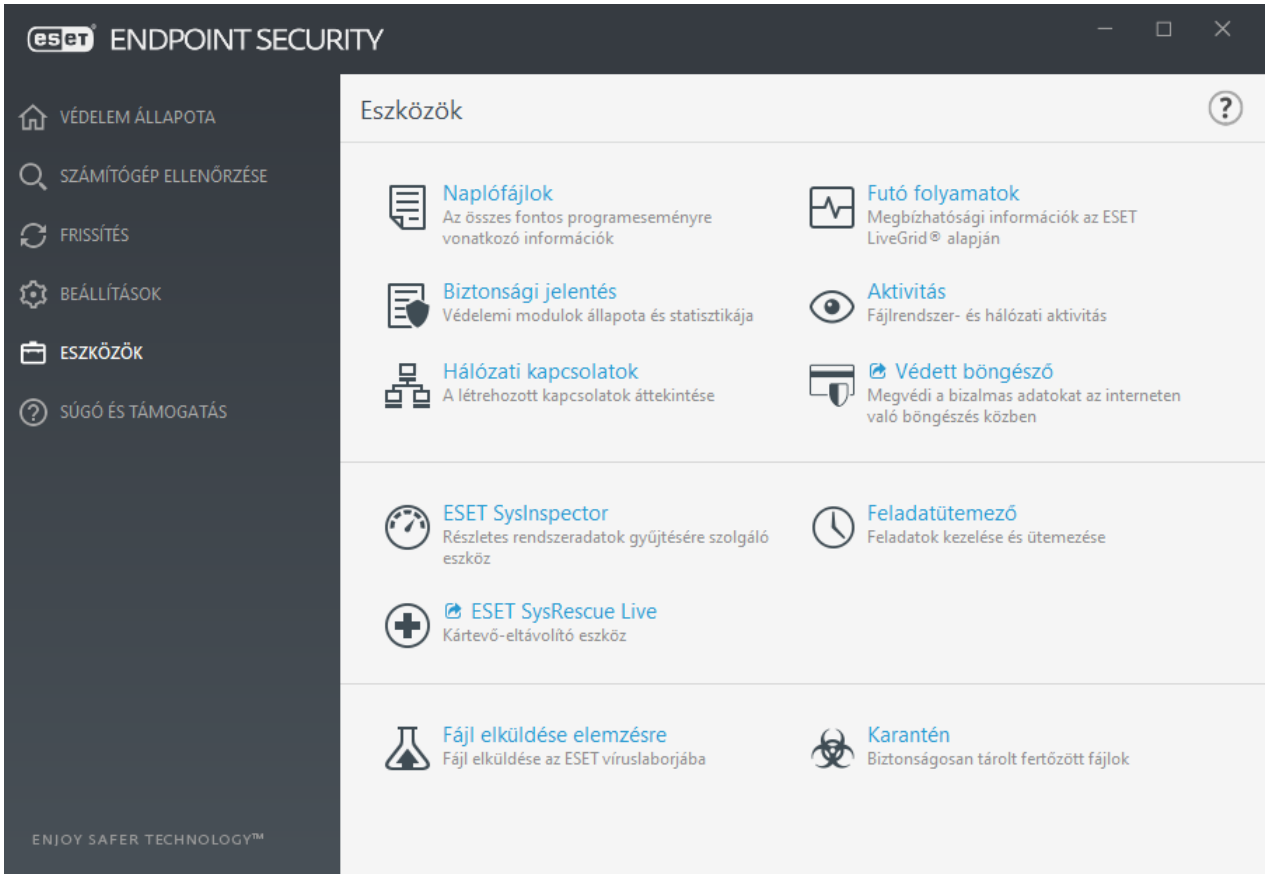
1. Az **F5** billentyűt lenyomva nyissa meg a További beállítások ablakot, majd bontsa ki a **Felhasználói felület** > **Felhasználói felület elemei** szakaszt.
2. Adja meg a kívánt értéket az **Indítási mód** beállításnál. További információk az indítási módokról.
3. Tiltsa le a **Nyitóképernyő megjelenítése indításkor** és a **Hangjelzés használata** funkciót.
4. Konfigurálja az értesítéseket.
5. Konfigurálja az alkalmazásállapotokat.
6. Konfigurálja a megerősítési üzeneteket.
7. Konfigurálja a riasztásokat és az értesítési ablakokat.

A következő hiba elhárítása: „A Védett böngésző átirányítása nem sikerült a kért weboldalra”

A hiba elhárításához kövesse az alábbi lépéseket:

Az egyes műveletek végrehajtása után ellenőrizze, hogy működik-e a Védett böngésző
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 Windows üzleti termék legújabb verzióját használja: Az ESET vállalati termékek legújabb verziójának ellenőrzése



3. Előfordulhat, hogy a külső gyártású biztonsági szoftver vagy tűzfal okoz problémát. Ellenőrizze, és szükség esetén távolítsa el a külső gyártású szoftvert a Programok telepítése/törlése ablakban. Kattintson az **Eszközök** > **Védett böngésző** elemre. Miután megnyílt a Védett böngésző ablak, folytassa a következő lépéssel.
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.
7. Ha nem frissítette az ESET-terméket az előző lépésekben, távolítsa el, majd telepítse újra az ESET-terméket. A számítógép újraindulása után tiltsa le a Védett böngészőt, és ismét indítsa újra a számítógépet. Engedélyezze újra a Védett böngészőt, és próbálja meg elindítani a Védett böngésző ablakát.

A Védett böngésző a védelem egy újabb rétege, amellyel megóvhatja pénzügyi adatait az online tranzakciók során.

A Védett böngésző az alapértelmezett böngészőjében nyílik meg, miután felkeresett egy ismert netbankos webhelyet. A védett böngésző közvetlen eléréséhez kattintson az **Eszközök** elemre az ESET Endpoint Security alkalmazásban, majd a  **Védett böngésző** elemre.

A Védett böngésző funkcióról az ESET alábbi tudásbáziscikkében talál további részleteket angol és néhány további nyelven:

- Hogyan használhatom az ESET Védett böngésző 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.

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_business 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.

EULAID: EULA-PRODUCT-LG; 3537.0

Adatvédelmi szabályzat

Az ESET, spol. s r. o. (székhelye: Szlovák Köztársaság, 851 01 Pozsony, Einsteinova 24; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B; cégjegyzékszám: 31333532) adatkezelőként („ESET” vagy „Mi”) átlátható módon szeretne eljárni a személyes adatok feldolgozása és ügyfelei adatvédelmének biztosítása során. Ezért közzétesszük a jelen Adatvédelmi szabályzatot azzal a céllal, hogy tájékoztassuk ügyfelünket („Végfelhasználó” vagy „Ön”) a következő témákról:

- A személyes adatok feldolgozása;
- Az adatok bizalmas kezelése;
- Az adatalany jogai

A személyes adatok feldolgozása

Az ESET által nyújtott és a termékeinkbe integrált szolgáltatások működését a Végfelhasználói szoftverlicenc-szerződés szabályozza, viszont néhány szolgáltatás különös figyelmet igényel. Szeretnénk további információkat biztosítani Önnek az adatgyűjtésről a szolgáltatásaink nyújtásával kapcsolatban. A Végfelhasználói szoftverlicenc-szerződésben és a termékdokumentációban leírtak szerint különböző szolgáltatásokat nyújtunk, például a következőket: frissítési/verzióváltási szolgáltatás, ESET LiveGrid®, védelem az adatokkal való visszaéléssel szemben, támogatás stb. A szolgáltatások működtetése érdekében a következő információkat kell gyűjtenünk:

- Frissítési és egyéb statisztikai adatok, amelyek 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.
- Kártevőkkel kapcsolatos egyirányú kivonatok, amelyek az ESET LiveGrid® megbízhatósági rendszer részét

képezik. A rendszer összeveti az ellenőrzött fájlokat a felhőben tárolt engedélyező- és tiltólistaelemek adatbázisával, ezáltal fokozva a kártevőirtó szoftvereink hatékonyságát.

• 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:

  okártevők, 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;

  oa helyi hálózathoz csatlakozó eszközökkel kapcsolatos információk, például az eszközök típusa, gyártója, modellszáma, illetve neve;

  ointernethasználattal kapcsolatos információk, például IP-cím és földrajzi adatok, IP-csomagok, URL-címek és Ethernet-keretek;

  oösszeomlási 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.

• Licencelési információkra, például licencazonosítóra és személyes adatokra – például név, vezetéknév, cím, e-mail-cím – szükséges számlázási célokra, a licenc eredetiségének ellenőrzéséhez, valamint a szolgáltatások biztosításához.

• Szervizelés, illetve segítségnyújtás biztosításához szükség lehet az Ön által leadott terméktámogatási kérelmekben foglalt elérhetőségekre és 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.

Az adatok bizalmas kezelése

Az ESET 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 információkat a Végfelhasználói licencszerződés teljesítése céljából, így például a szolgáltatások, a terméktámogatás és a számlázás biztosítása érdekében. Az Ön tartózkodási helye és a kiválasztott szolgáltatások alapján előfordulhat, hogy kötelességünk továbbítani az adatokat olyan országba, amely nem rendelkezik az Európai Bizottság megfelelőségi határozatával. Ilyen esetben is adatvédelmi jogszabályok szabályozzák az adatátvitelt, és csak szükség esetén kerül rá sor. Kivétel nélkül minden esetben általános szerződési feltételeket, kötelező erejű vállalati szabályokat vagy egyéb megfelelő védintézkedéseket kell alkalmazni.

Mindent megteszünk annak megakadályozása érdekében, hogy a szükségesnél hosszabb ideig történjen meg az adatok tárolása, amíg szolgáltatásokat nyújtunk a Végfelhasználói szoftverlicenc-szerződés szerint. A megőrzési időtartam hosszabb is lehet, mint az Ön licencének érvényessége, ami lehetőséget ad az egyszerű és kényelmes megújításra. Sor kerülhet a minimalizált és álnevesített statisztikai adatok, valamint az ESET LiveGrid® rendszerből származó egyéb adatok statisztikai célból történő további feldolgozására.

Az ESET megfelelő technikai és szervezeti intézkedésekkel biztosít a potenciális kockázatoknak megfelelő védelmi szintet. Mindent megteszünk azért, hogy a feldolgozó rendszerek és a szolgáltatások folyamatosan biztosítsák az

adatok bizalmas kezelését, az integritást, a hozzáférhetőséget és a terhelhetőséget. Ha azonban sor kerül az adatok megsértésére, ami veszélyezteti az Ön jogait és szabadságát, készen állunk értesíteni a felügyeleti hatóságot és az érintetteket. Ön mint adatalany jogosult panaszt benyújtani egy felügyeleti hatósághoz.

Az adatalany jogai

Az ESET vállalatra a szlovák törvények az irányadók, és az Európai Unió tagjaként kötelességünk betartani az adatvédelmi rendelkezéseket. A vonatkozó adatvédelmi törvényekben rögzített feltételek szerint Önt adatalanyként a következő jogok illetik meg:

- jogosult kérelmezni a személyes adataihoz való hozzáférést az ESET vállalattól;
- jogosult személyes adatai helyesbítésére, ha azok pontatlanok (arra is jogosult, hogy kiegészítse a hiányos személyes adatokat);
- jogosult személyes adatai törlését kérelmezni;
- jogosult személyes adatai feldolgozásának korlátozását kérelmezni;
- jogosult tiltakozni az adatfeldolgozás ellen
- jogosult panaszt emelni; valamint
- joga van az adathordozhatósághoz.

Hiszünk abban, hogy az általunk feldolgozott minden információ értékes és szükséges jogos érdekünk céljából, vagyis szolgáltatások és termékek biztosításához ügyfeleink számára.

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