

ESET Endpoint Antivirus

Felhasználói útmutató

[Ide kattintva megjelenítheti a dokumentum verzióját](#)

Copyright ©2024 – ESET, spol. s r.o.

Az ESET Endpoint Antivirus 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. 2024.04.12.

1 ESET Endpoint Antivirus 7	1
1.1 A 7-es verzió újdonságai	2
1.2 Rendszerkövetelmények	3
1.2 Támogatott nyelvek	4
1.3 Megelőzés	5
1.4 Súlytémakörök	6
2 Távolról felügyelt végpontok dokumentációja	8
2.1 Az ESET Security Management Center ismertetése	8
2.2 Az ESET PROTECT Cloud ismertetése	9
2.3 Jelszóval védett beállítások	9
2.4 Mik a házirendek?	11
2.4 Házirendek egyesítése	11
2.5 Hogyan működnek a jelzők?	12
3 Az ESET Endpoint Antivirus 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)	18
3.1 Telepítési mappa módosítása (.exe)	20
3.1 Telepítés (.msi)	21
3.1 Speciális telepítés (.msi)	23
3.1 Parancssori telepítés	24
3.1 Központi telepítés GPO vagy SCCM segítségével	29
3.1 Frissítés egy újabb verzióra	29
3.1 A telepítéssel kapcsolatos általános problémák	30
3.1 Nem sikerült az aktiválás	30
3.2 Licenc aktiválása	31
3.3 Számítógép ellenőrzése	31
3.4 Útmutató kezdő felhasználók számára	31
3.4 A felhasználói felület	32
3.4 Frissítési beállítások	35
4 Az ESET Endpoint Antivirus használata	36
4.1 Számítógép	39
4.1 Keresőmotor (7.2 és újabb)	40
4.1 A keresőmotor további beállításai	45
4.1 Keresőmotor (7.1 és korábbi)	45
4.1 A program fertőzést észlelt	46
4.1 Megosztott helyi gyorsítótár	49
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	52
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	58
4.1 Üresjárat idején történő ellenőrzés	58
4.1 Ellenőrzési profilok	59

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 Eszközcsoporthoz	62
4.1 Eszközfelügyeleti szabályok hozzáadása	63
4.1 Behatolásmegelőző rendszer	65
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	70
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	75
4.1 Kivételek	76
4.1 Teljesítménybeli kivételek	76
4.1 Teljesítménybeli kivételek felvétele vagy szerkesztése	78
4.1 Útvonalkivétel formátuma	80
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	85
4.1 Folyamatkivételek felvétele vagy szerkesztése	86
4.1 HIPS-kivételek	86
4.1 ThreatSense paraméterek	86
4.1 Megtisztítási szintek	89
4.1 Ellenőrzésből kizárt fájlkiterjesztések	91
4.1 További ThreatSense-paraméterek	92
4.2 Hálózat	92
4.2 Hálózati támadások elleni védelem	93
4.2 Speciális szűrési beállítások	93
4.2 IDS-kivételek	96
4.2 Lehetséges kártevő letiltva	97
4.2 Hálózati védelem hibájának elhárítása	98
4.2 IP-címek ideiglenes tiltólistája	98
4.2 Az ESET Tűzfallal kapcsolatos problémák megoldása	98
4.2 Hibaelhárítási varázsló	99
4.2 Naplózás és szabályok vagy kivételek létrehozása naplóból	99
4.2 Új szabály létrehozása naplóból	99
4.2 Kivételek létrehozása a személyi tűzfal értesítéseiből	100
4.2 Speciális PCAP-naplózás	100
4.2 Protokollszűrési problémák megoldása	100
4.3 Web és e-mail	102
4.3 Protokollszűrés	103
4.3 Kizárt alkalmazások	103
4.3 Kizárt IP-címek	104

4.3 SSL/TLS	105
4.3 Tanúsítványok	106
4.3 Titkosított hálózati forgalom	107
4.3 Ismert tanúsítványok listája	107
4.3 SSL/TLS szűrőű alkalmazások listája	108
4.3 E-mail védelem	109
4.3 Levelezési protokollok	110
4.3 E-mail-riasztások és értesítések	111
4.3 Integrálás a levelezőprogramokkal	112
4.3 Microsoft Outlook-eszköztár	112
4.3 Outlook Express- és Windows Mail-eszköztár	112
4.3 Megerősítés	113
4.3 Üzenetek újraellenőrzése	113
4.3 Webhozzáférés-védelem	113
4.3 A webhozzáférés-védelem haladó beállításai	115
4.3 Webprotokollok	116
4.3 URL-címek kezelése	116
4.3 URL-címlista	118
4.3 Új URL-címlista létrehozása	118
4.3 URL-maszk hozzáadása	119
4.3 Adathalászat elleni védelem	120
4.4 A program frissítése	121
4.4 Frissítési beállítások	125
4.4 Frissítési fájlok visszaállítása	128
4.4 Programösszetevők frissítése	129
4.4 Kapcsolati beállítások	130
4.4 Frissítési tükör	131
4.4 HTTP-szerver	133
4.4 Frissítés tükörből	133
4.4 A tükörzésből történő frissítéssel kapcsolatos hibaelhárítás	136
4.4 Frissítési feladatok létrehozása	136
4.5 Eszközök	137
4.5 Naplófájlok	138
4.5 Napló szűrése	140
4.5 Naplózási konfiguráció	141
4.5 Auditálási naplók	142
4.5 Feladatütemező	143
4.5 Védelem statisztikája	146
4.5 Aktivitás	147
4.5 ESET SysInspector	148
4.5 Felhőalapú védelem	149
4.5 Kivételiszűrő felhőalapú védelemhez	152
4.5 Futó folyamatok	153
4.5 Biztonsági jelentés	154
4.5 ESET SysRescue Live	156
4.5 Minták elküldése elemzésre	156
4.5 Minta kiválasztása elemzésre – Gyanús fájl	157
4.5 Minta kiválasztása elemzésre – Gyanús webhely	157
4.5 Minta kiválasztása elemzésre – Tévesen jelentett fájl	158
4.5 Minta kiválasztása elemzésre – Tévesen jelentett webhely	158
4.5 Minta kiválasztása elemzésre – Egyéb	158

4.5 Értesítések	158
4.5 Alkalmazásértesítések	160
4.5 Asztali értesítések	160
4.5 E-mail értesítések	161
4.5 Az értesítések testreszabása	163
4.5 Karantén	163
4.5 Proxyszerver beállítása	165
4.5 Időközök	166
4.5 Microsoft Windows® frissítés	167
4.5 Licenc intervallum-ellenőrzése	167
4.6 Felhasználói felület	168
4.6 Felhasználói felület elemei	168
4.6 Alkalmazásállapotok	170
4.6 Hozzáférési beállítások	171
4.6 Jelszó a További beállításokhoz	172
4.6 Riasztások és értesítési ablakok	172
4.6 Interaktív riasztások	174
4.6 Megerősítési üzenetek	176
4.6 A további beállításokkal kapcsolatos ütközési hiba	176
4.6 Újraindítás szükséges	176
4.6 Újraindítás javasolt	178
4.6 Cserélhető adathordozók	179
4.6 A rendszer tálcáikonja	180
4.6 Helyi menü	182
4.6 Súgó és támogatás	182
4.6 Az ESET Endpoint Antivirus névjegye	183
4.6 Rendszer-konfigurációs adatok küldése	184
4.6 Profilkezelő	184
4.6 Billentyűparancsok	185
4.6 Diagnosztika	185
4.6 Parancssori víruskereső	187
4.6 ESET CMD	189
4.6 Üresjárat idején történő ellenőrzés	191
4.6 Beállítások importálása és exportálása	192
4.6 Az összes beállítás visszaállítása alapértelmezettre	193
4.6 Az összes beállítás visszaállítása ezen a részen	193
4.6 Hiba a konfiguráció mentésekor	193
4.6 Távoli figyelés és kezelés	194
4.6 Az ERMM-parancssor	195
4.6 ERMM JSON-parancsok listája	197
4.6 get protection-status	197
4.6 get application-info	198
4.6 get license-info	201
4.6 get logs	201
4.6 get activation-status	203
4.6 get scan-info	203
4.6 get configuration	204
4.6 get update-status	205
4.6 start scan	206
4.6 start activation	207
4.6 start deactivation	208

4.6 start update	209
4.6 set configuration	210
5 Gyakori kérdések	210
5.1 Az ESET Endpoint Antivirus frissítése	211
5.2 Az ESET Endpoint Antivirus aktiválása	212
5.2 Bejelentkezés az ESET Business Account-fiókba	212
5.2 Újabb ESET-végponttermékek aktiválása régi típusú licenc hitelesítő adataival	213
5.3 Vírus eltávolítása a számítógépről	213
5.4 Új feladat létrehozása a feladatütemezőben	213
5.4 Heti számítógép-ellenőrzés ütemezése	214
5.5 Az ESET Endpoint Antivirus csatlakoztatása az ESET Security Management Center alkalmazáshoz	215
5.5 A Felülbírálat mód használata	215
5.5 Ajánlott házirend alkalmazása az ESET Endpoint Antivirus szolgáltatásra	217
5.6 Tükrözés beállítása	220
5.7 Frissítés Windows 10-re az ESET Endpoint Antivirus programmal	220
5.8 Távoli figyelés és kezelés aktiválása	221
5.9 Hogyan akadályozható meg bizonyos fájltypusok letöltése az internetről?	224
5.10 Az ESET Endpoint Antivirus minimalista felhasználói felületének beállítása	225
6 Végfelhasználói licencszerződés	225
7 Adatvédelmi szabályzat	232

ESET Endpoint Antivirus 7

Az ESET Endpoint Antivirus 7 egy újszerű megoldást jelentő integrált biztonsági programcsomag. A ThreatSense® keresőmotor legújabb verziója gyorsan és megbízhatóan védi számítógépét. Az eredmény egy olyan intelligens rendszer, amely szünet nélkül figyeli a számítógépet veszélyeztető támadási kísérleteket és kártevő szoftvereket.

Az ESET Endpoint Antivirus 7 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 Antivirus 7 elsősorban kisvállalati környezetben működő munkaállomásokhoz készült.

[Az ESET Endpoint Antivirus 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 Antivirus az ESET Security Management Center](#) 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 Antivirus 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 , rootkitek , 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-mail-es 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 Antivirus alkalmazásból ellenőrizheti.

Távoli felügyelet	Az ESET Security Management Center lehetővé teszi, hogy egyetlen központi helyről felügyeljen ESET-termékeket munkaállomásokon, szervereken és mobil eszközön hálózati környezetben. Az ESET Security Management Center Webkonzol (ESMC 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 7-es verzió újdonságai

Az ESET Endpoint Antivirus 7 megjelent, és [letölthető](#).

Újdonságok az ESET Endpoint Antivirus 7.0-s verziójában

- Új kialakítású grafikus felhasználói felület.
- Fájlok ellenőrzése húzással – Manuálisan ellenőrizheti a fájlokat vagy a mappákat, ha egyszerűen a megjelölt területre húzza az adott fájlt vagy mappát.
- Az ESET Endpoint Antivirus most már lehetővé teszi a [hálózati támadások elleni védelmet](#). További információkért tekintse meg a [Hálózati támadások elleni védelem](#) című részt.
- A Védelem állapota lapon található gyorsműveleti hivatkozás letiltható ESET Security Management Center-házirendben.
- Eszközfelügyeleti szabályok alkalmazhatók egy bizonyos ideig. További információkért olvassa el az [Időközök](#) című részt.

Újdonságok az ESET Endpoint Antivirus 7.1-es verziójában

- Új típusú naplózás – Most már rendelkezésre áll a haladó naplózás. További információkért tekintse meg az [Auditálási naplók](#) című részt.

Újdonságok az ESET Endpoint Antivirus 7.2-es verziójában

- A Speciális gépi tanulás egy fejlett védelmi réteg, amely hatékonyabbá teszi a gépi tanulás alapú észlelést. A [Szószedetben](#) bővebben olvashat erről a típusú védelemről. A [Keresőmotor beállításaiban](#) már nem található meg a BE/KI kapcsolók, mint a 7.1-es és korábbi verziókban. A BE/KI gombok helyett a következő négy küszöb található meg: „Mélyreható”, „Kiegyensúlyozott”, „Mérsékelt” és „Ki”.
- Lett lokalizálással bővült.
- Módosítások a [kivételek](#) területén. A Teljesítménybeli kivételek részen fájlokat és mappákat zárhat ki az ellenőrzésből. Az Észlelési kivételek részen objektumokat zárhat ki a tisztításból az észlelt elem neve, az objektum elérési útvonala vagy kivonata segítségével.

- A Behatolásmegelőző rendszer (HIPS) új programmodulja magában foglalja a Viselkedésalapú ellenőrzést, amely elemzi a számítógépen futó összes program viselkedését, és figyelmezteti, ha a folyamat gyanúsán viselkedik. [Súgóoldalainkon további információkat talál a Behatolásmegelőző rendszerről \(HIPS\).](#)
- A [konfigurálható interaktív riasztások](#) segítségével megadhatja a konfigurálható interaktív riasztások viselkedését (például letilthatja az „Újraindítás javasolt” riasztást végpontgépeken).

Újdonságok az ESET Endpoint Antivirus 7.3-es verziójában

- Ez a kisebb kiadás különböző hibajavításokat és teljesítménybeli fejlesztéseket tartalmaz.

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

- [Újdonságok az ESET Endpoint Antivirus 7-es verziójában](#)

Rendszerkövetelmények

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

Támogatott processzorok

32 bites (x86) processzor SSE2 utasításkészlettel vagy 64 bites (x64) processzor, 1 GHz-es vagy nagyobb

Operációs rendszerek

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8

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

A Windows XP és a Windows Vista [már nem támogatott a 7-es verzió esetén.](#)

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)

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.



Megjegyzés

- (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 naplók rekord 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 Antivirus 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
Kazak	kk-KZ	1087
Koreai	ko-KR	1042
Lett	lv-LV	1062
Litván	lt-LT	1063

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
*Vietnami	vi-VN	1066

*Az ESET Endpoint Antivirus 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 [kártévők](#) 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 töltsse 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.

Súgótemakörök

Üdvözli az ESET Endpoint Antivirus súgója! A súgóbeli információk segítenek a termék megismerésében és a számítógép biztonságosabbá tételében.

Első lépések

Mielőtt megkezdene az ESET Endpoint Antivirus használatát, vegye figyelembe, hogy termékünk [az ESET Security Management Center 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 Antivirus jelen verziójában bevezetett funkciókat. Az ESET Endpoint Antivirus alapvető beállításainak megadásához és testreszabásához rendelkezésre áll egy útmutató is.

Az ESET Endpoint Antivirus 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 Antivirus paraméternevein alapul. A különös jelentőséggel bíró témakörök kiemelésére emellett egy egységes szimbólumkészletet is használunk.



Megjegyzés

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



Fontos

Azt javasoljuk, hogy ne hagyja ki ezt a lépést. A megjegyzések általában nem kritikus, ám jelentős információkkal szolgálnak.



Figyelmeztetés

Ezek az információk különleges figyelmet és elővigyázatosságot igényelnek. A figyelmeztetések kifejezetten arra szolgálnak, hogy figyelembevételükkel elkerülhesse a potenciálisan kárt okozó hibákat. Kérjük, hogy figyelmesen olvassa el és értelmezze a figyelmeztetéseket, mivel azok a különösen érzékeny rendszerbeállításokra vagy valamilyen kockázatra hívják fel a figyelmet.



Példa

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.
<i>Dőlt formázás</i>	Az Ön által megadandó információk helyőrzője. A fájlnev 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 Antivirus távolról felügyelhetők kliensszámítógépeken, szervereken és mobilkészülékeken egy központi helyről a hálózati környezetben. A több mint 10 kliensszámítógépet felügyelő rendszergazdának 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 Antivirus az ESET Security Management Center, illetve az ESET PROTECT Cloud segítségével felügyelhető távolról.

- [Az ESET Security Management Center 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 Antivirus segítségével az ESET Security Management Centerhez](#)
- 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 Antivirus szolgáltatással elvégezhető felhasználói műveleteket

Útmutatók

- [A Felülbírálás mód használata](#)
- [Telepítés ESET Endpoint Antivirus GPO vagy SCCM segítségével](#)

Az ESET Security Management Center ismertetése

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

Az ESET Security Management Center (ESMC) egy új generációs távoli felügyeleti rendszer, amely jelentősen eltér az ESET Remote Administrator (ERA) korábbi verzióitól. Mivel teljesen eltérő architektúrával rendelkezik, az ESET

Security Management Center 7 csak részben kompatibilis az ERA 6-os verziójával, és visszamenőlegesen nem kompatibilis az ERA 5-ös verziójával. Az [ESET biztonsági termékek korábbi verzióival azonban kompatibilis](#).

Az ESET biztonsági megoldások portfóliójának teljes mértékű telepítéséhez a következő komponenseket kell telepíteni (Windows és Linux platformok):

- [ESMC Szerver](#)
- [ESMC Webkonzol](#)
- [ESET Management Ügynök](#)

A következő támogató komponensek opcionálisak. Azt javasoljuk, telepítse őket, hogy az alkalmazás optimális teljesítményt nyújtson a hálózaton.

- [Engedélyezetlen szerverek felismerésérzékelője](#)
- [Apache HTTP-proxy](#)
- [Mobile Device Connector](#)

Az ESET Security Management Center Webkonzol (ESMC Webkonzol) segítségével telepíthet ESET-megoldásokat, feladatokat kezelhet, [biztonsági irányelveket](#) érvényesíthet, felügyelheti a rendszerállapotot, és gyorsan reagálhat a távoli számítógépeken fellépő problémákra és fertőzésekre.



További információ

További információkat az [ESET Security Management Center online felhasználói útmutatójában](#) talál.

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 ESMC 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](#)

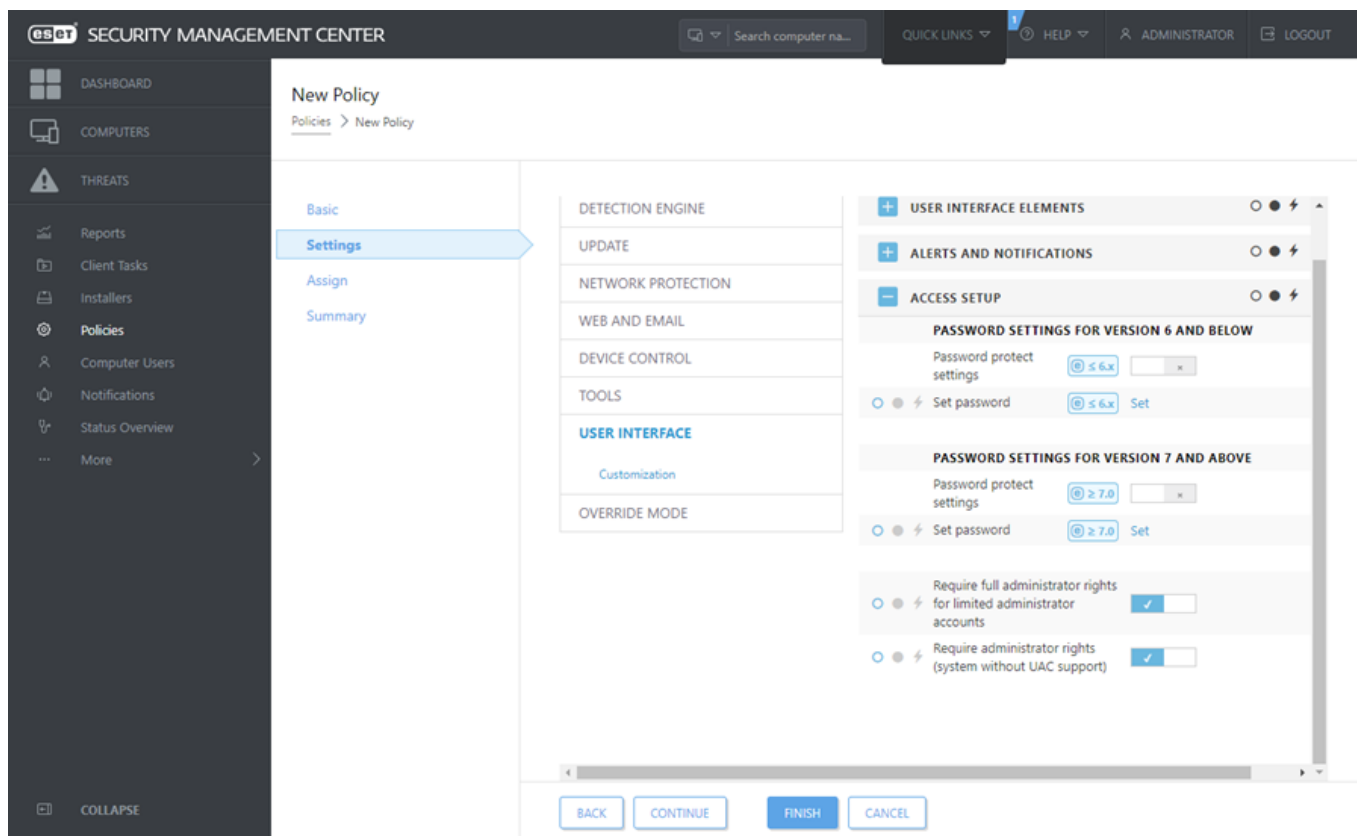
Jelszóval védett beállítások

A rendszer maximális biztonsága érdekében fontos, hogy az ESET Endpoint Antivirus 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 Antivirus speciális beállításait a csatlakoztatott kliensszámítógépeken. Új házirend létrehozása:

1. Az ESMC 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 Antivirus verziójának megfelelően a csúszkára kattintva engedélyezze a **Jelszó a beállítások védelméhez** funkciót. Vegye figyelembe, hogy az ESET Endpoint 7 fejlett védelmet nyújt. Ha az Endpoint-termékek 7-es és 6-os verziója is megtalálható a hálózaton, különböző jelszavakat adjon meg. Azt javasoljuk, hogy csak a 6-os verzió mezőjében adja meg a jelszót, mert ez esetben a biztonsági szint alacsonyabb lesz a 7-es verzió végpontjain.
7. Az előugró ablakban hozzon létre egy új jelszót, erősítse meg, majd kattintson az **OK** gombra. Kattintson a **Folytatás** 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 ESMC 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 Antivirus-felhasználó felül tudja írni az alsóbb csoportok házirendjeit. Az algoritmus magyarázata az [ESMC online súgójában](#) található.



Általánosabb házirendek hozzárendelése

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 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 Antivirus 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 [ESMC 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.




PÉLDA: Az összes házirend megtekintésének engedélyezése a felhasználóknak

Forgatókönyv: A *rendszergazda* szeretné engedélyezni *János* felhasználónak, hogy létrehozhasson és szerkeszthesen 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 **Házirendek**hez.
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 létrehozson 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 Antivirus használata önállóan

A felhasználói útmutató jelen szakasza és [Az ESET Endpoint Antivirus](#) használata című szakasza az ESET Endpoint Antivirus alkalmazást az ESET Security Management Center vagy ESET PROTECT Cloud nélkül használó felhasználóknak készült. A felhasználói fiók jogosultságaitól függően teljes mértékben elérhető az ESET Endpoint Antivirus összes szolgáltatása és funkciója.

Telepítési módszerek

Többféle módon telepíthetők az ESET Endpoint Antivirus 7.x verziói a kliensszámítógépekre, ha nem az [ESET Endpoint Antivirus segítségével távolról telepíti a kliensszámítógépekre az ESET Security Management Center vagy az ESET PROTECT Cloud](#) segítségével.

- [Kattintson ide, ha az ESET Endpoint Antivirus 6.6.x verzióját szeretné telepíteni, vagy ilyen verzióra szeretne frissíteni](#)

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 Security Management Center segítségével hajthatók végre.	64 bites letöltése 32 bites letöltése
Parancssori telepítés	Az ESET Endpoint Antivirus helyileg a parancssor segítségével telepíthető, illetve távolról az ESET Security Management Center 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 Antivirus 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 Antivirus a kliensszámítógépekre	N/A

Az ESET Endpoint Antivirus [több mint 30 nyelven áll rendelkezésre](#).

Telepítés az ESET AV Remover eszközzel

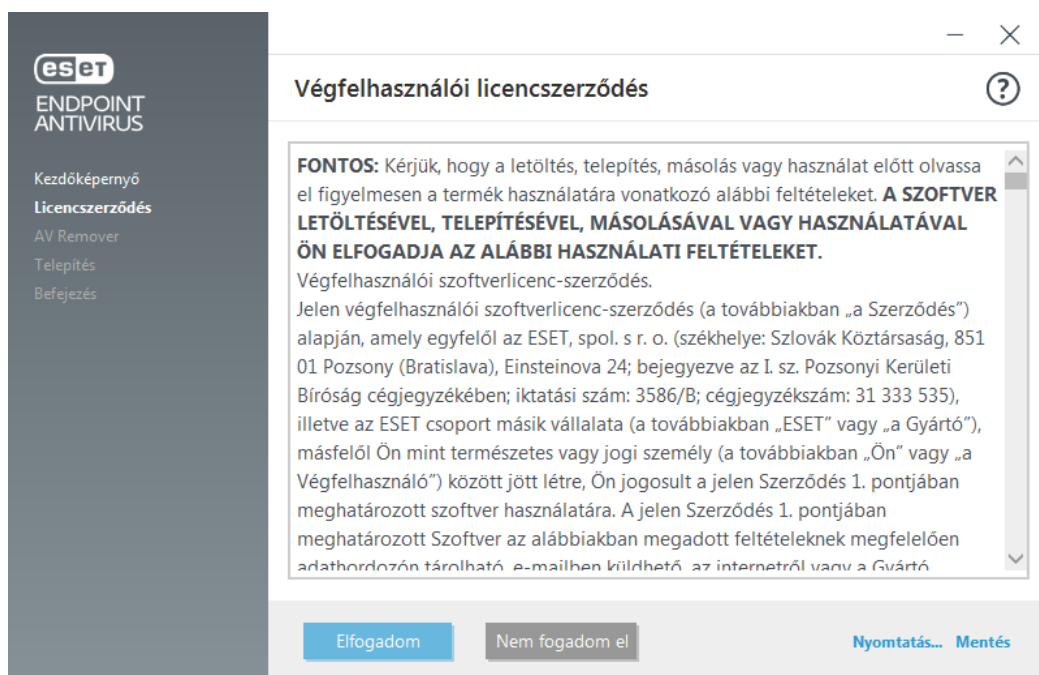
A telepítési folyamat folytatása előtt fontos eltávolítani minden meglévő biztonsági alkalmazást a számítógépről. Jelölje be az **El szeretném távolítani a nemkívánatos vírusirtó alkalmazásokat az ESET AV Remover** használatával jelölőnégyzetet ahhoz, hogy az ESET AV Remover ellenőrizze a rendszerét,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



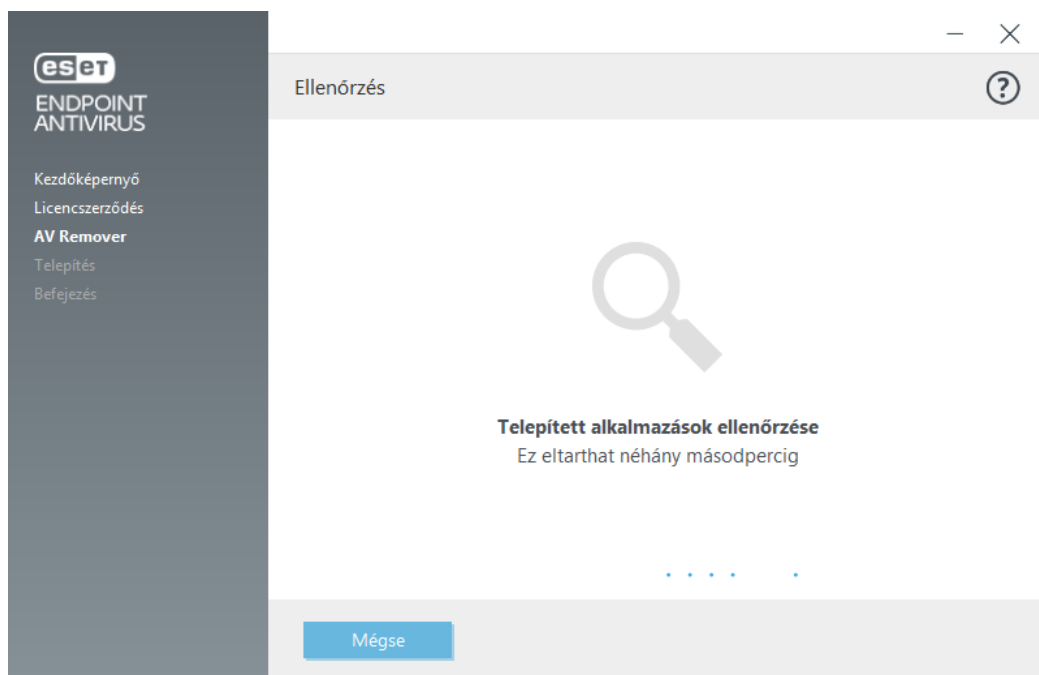
ESET AV Remover

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:

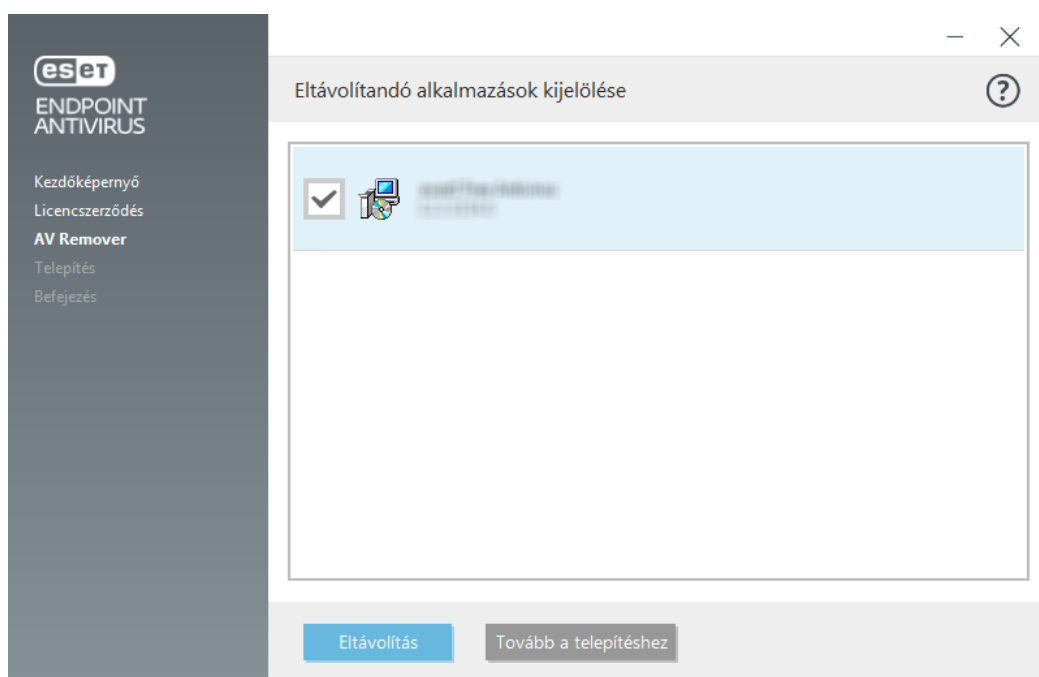
1. Az ESET AV Remover eszközzel eltávolítható víruskereső szoftverek listája az [ESET tudásbázisának cikkében található](#).
2. A végfelhasználói licencszerződés átolvasását követően az **Elfogadom** választógombot bejelölve jelezheti, hogy elfogadja a szerződésben foglaltakat. Ha a **Nem fogadom el**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



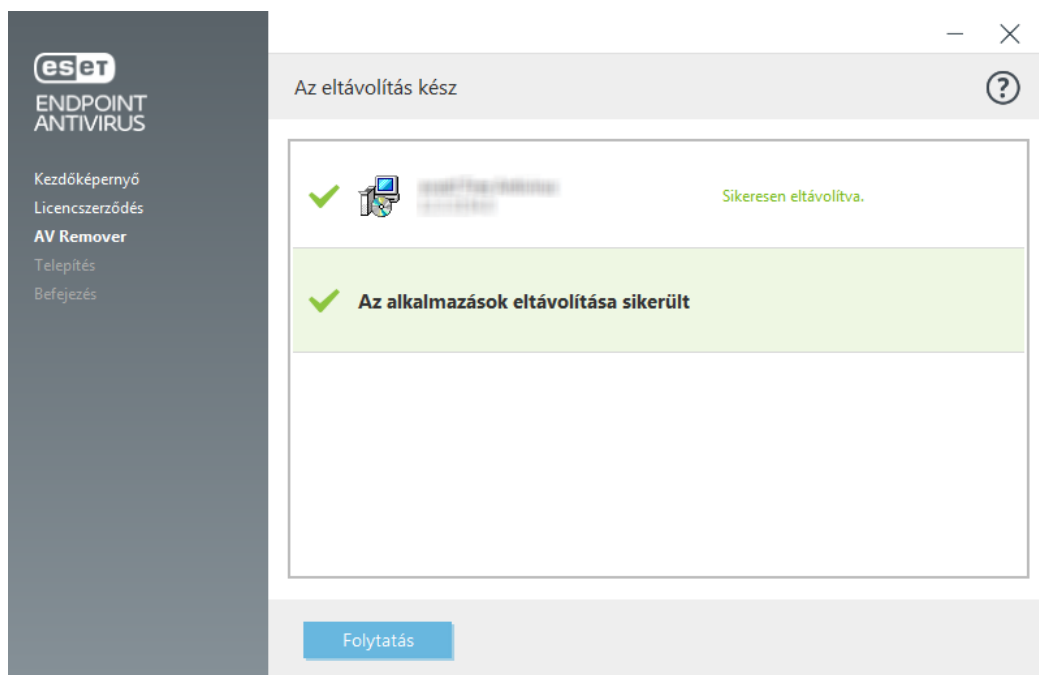
3. Az ESET AV Remover elkezdi a víruskereső szoftverek keresését a rendszerben.



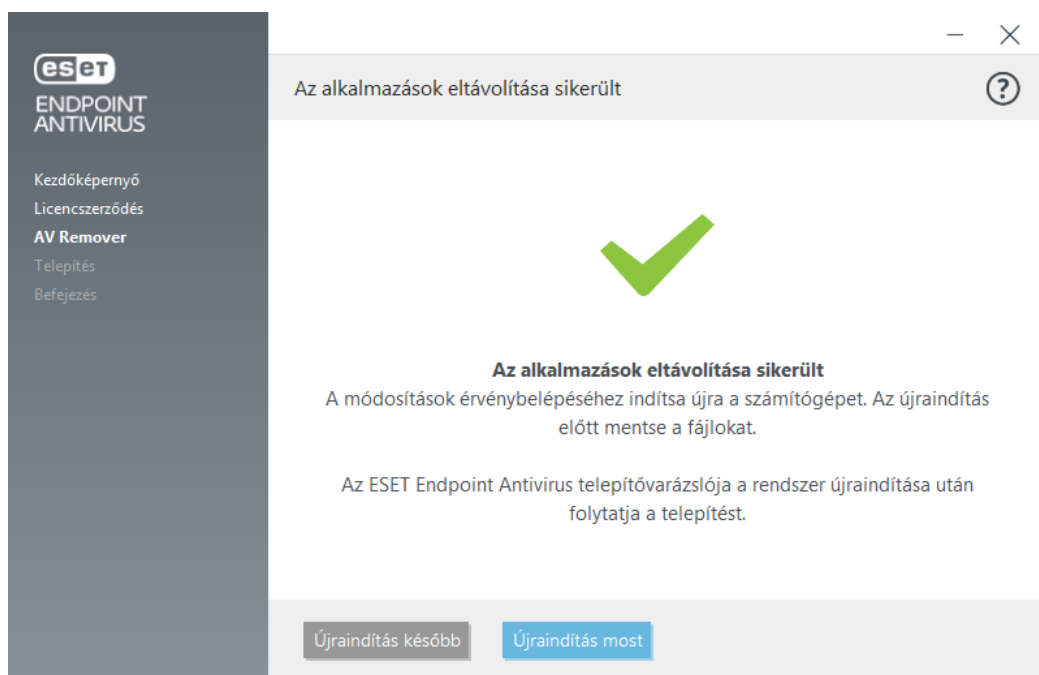
4. Jelölje ki bármelyik víruskereső alkalmazást a listában, és kattintson az **Eltávolítás** elemre. Az eltávolítás eltarthat kis ideig.



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



6. Indítsa újra a számítógépet a módosítások alkalmazásához és az ESET Endpoint Antivirus 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.

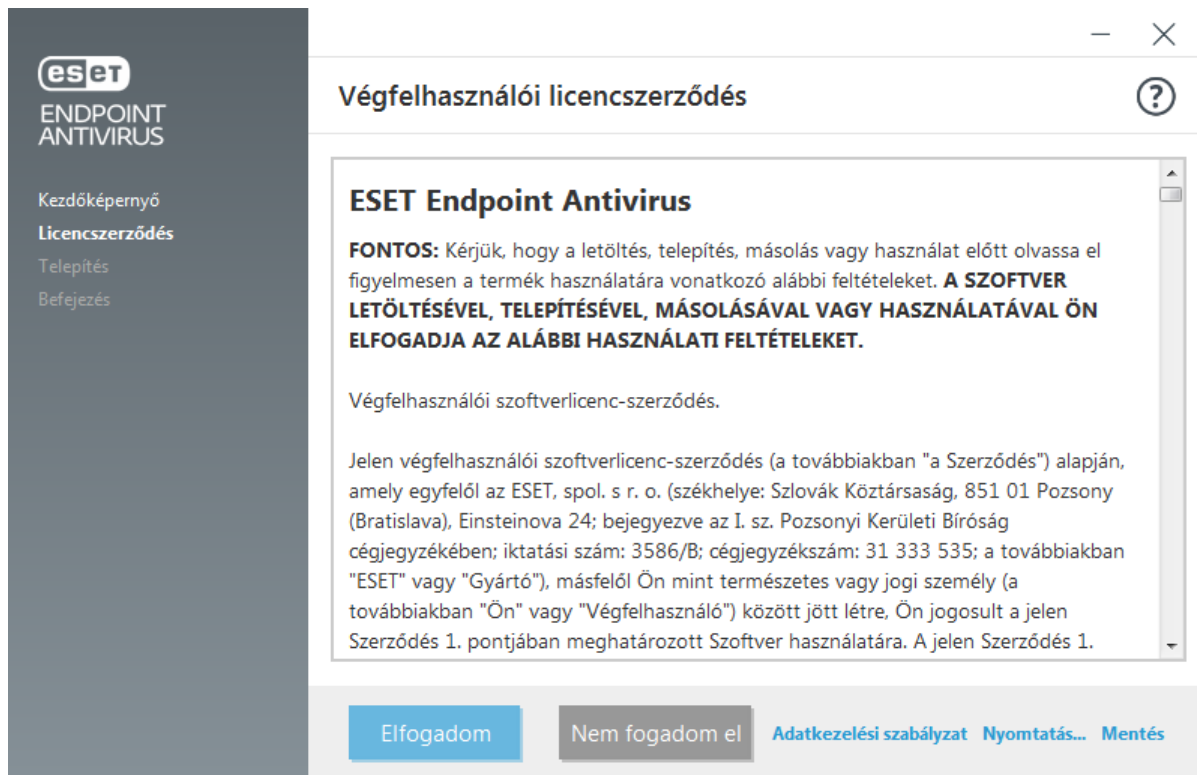


Fontos

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



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

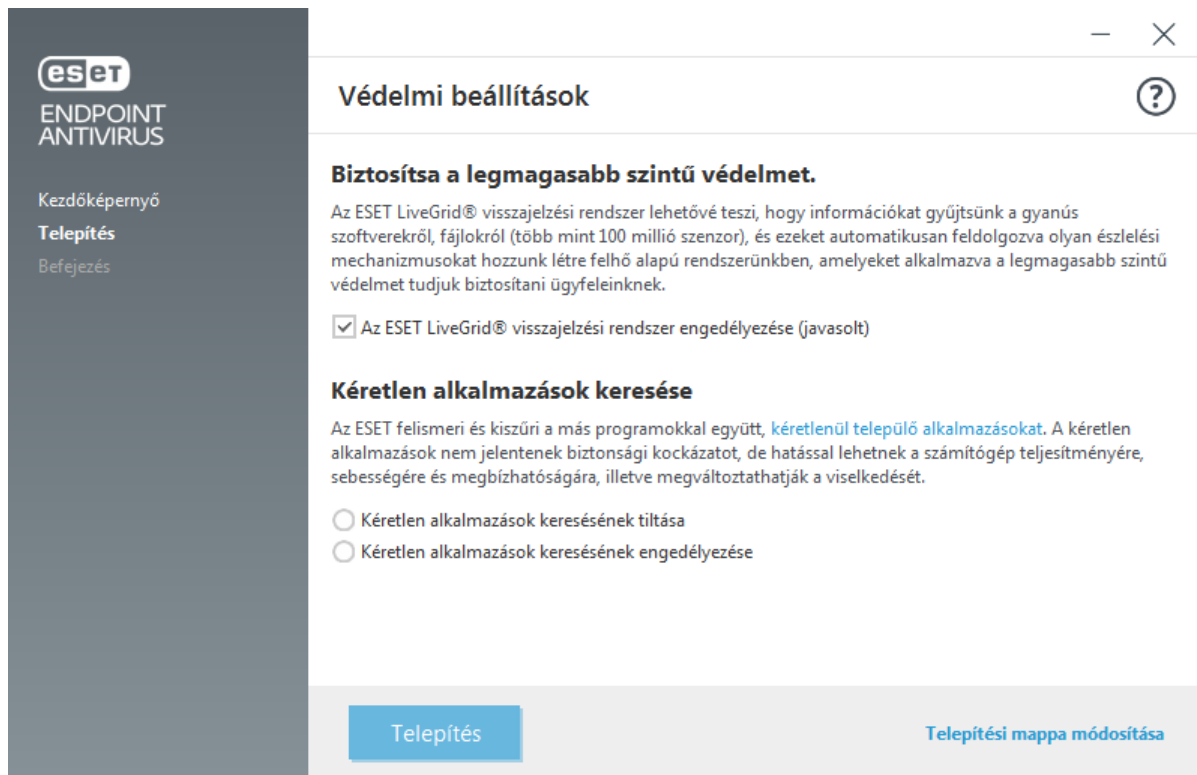


2. Adja meg, hogy engedélyezi-e az [ESET LiveGrid® visszajelzési rendszert](#). Az ESET LiveGrid® segítségével az ESET azonnal és folyamatosan értesül az új fertőzésekről, így biztosíthatja ügyfelei fokozottabb védelmét. A rendszer lehetővé teszi, hogy a felhasználó elküldje az új kártevőket az ESET víruslaborjába, ahol elemzik és feldolgozzák az adatokat, és felveszik azokat a keresőmotorba.

3. A következő telepítési lépés a kérietlen alkalmazások felismerésének beállítása. További tudnivalókat erről a [Kérietlen alkalmazások](#) című fejezetben talál.

Az ESET Endpoint Antivirus programot a [Telepítési mappa módosítása](#) gombra kattintva telepítheti egy adott mappába.

5. Utolsó lépésként a **Telepítés** gombra kattintva hagyja jóvá a telepítést. A telepítés befejeződése után felszólítást kap [az ESET Endpoint Antivirus](#) 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 Antivirus telepítési mappájának helyét. Alapértelmezés szerint a program telepítése az alábbi könyvtárba történik:

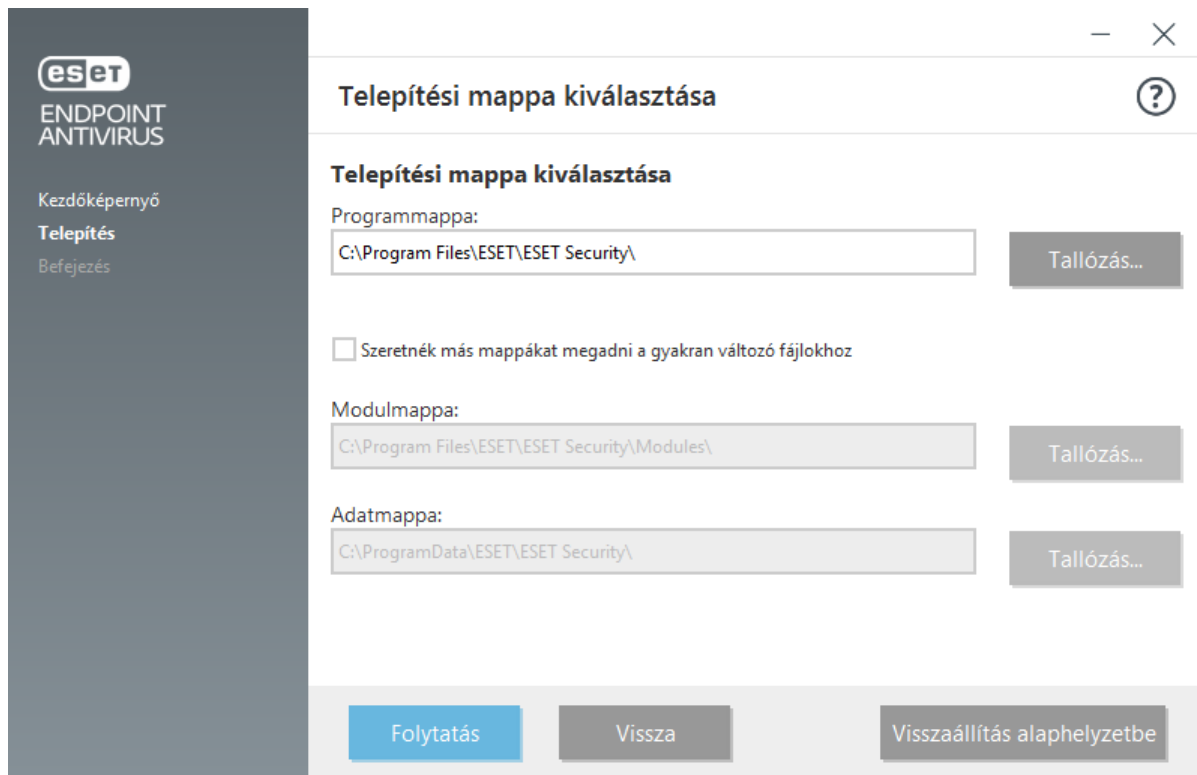
`C:\Program Files\ESET\ESET Security\`

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).



A telepítés elindításához kattintson a **Folytatás**, majd a **Telepítés** gombra.

Telepítés (.msi)

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



Az .msi telepítő rendeltetése

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



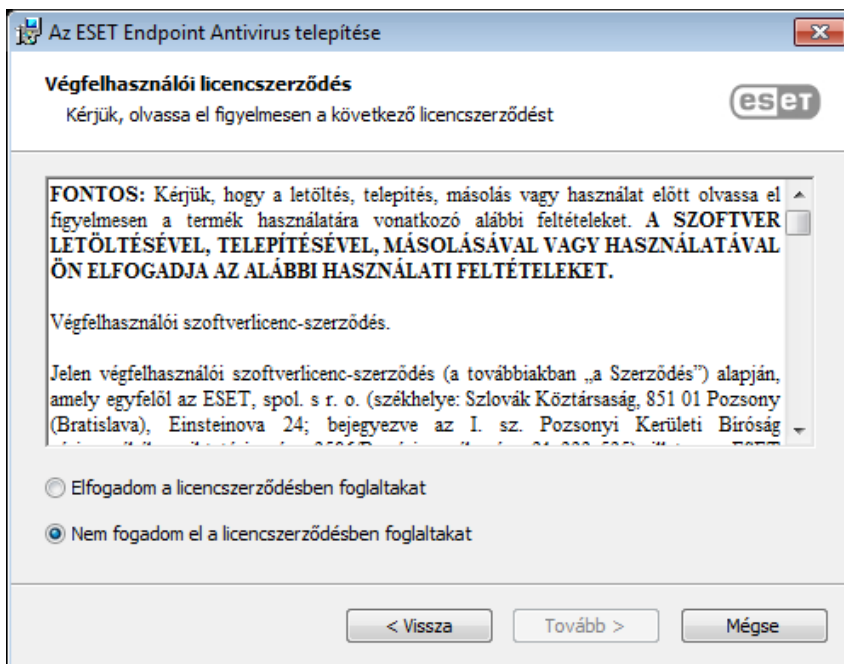
Fontos

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

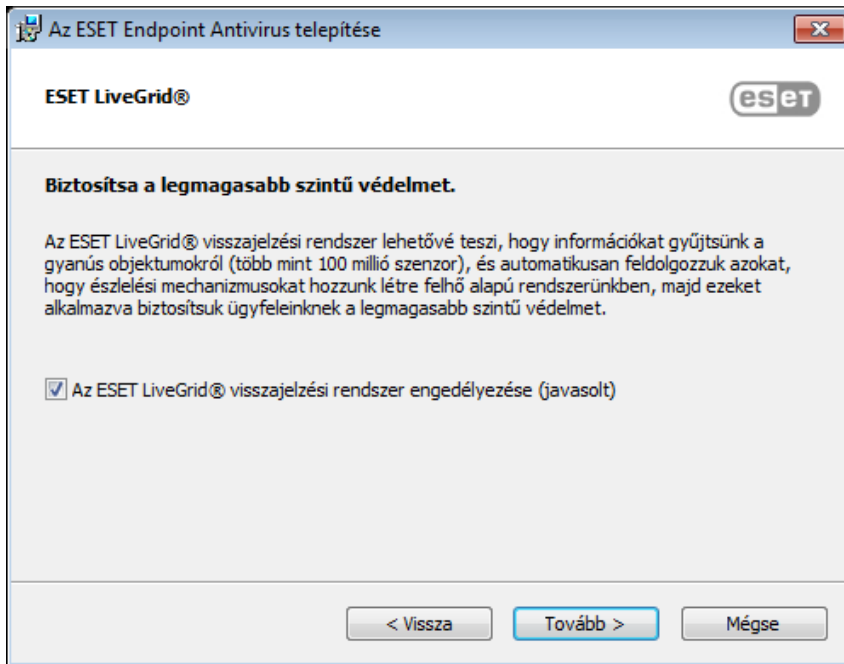
1. Válassza ki a kívánt nyelvet, majd kattintson a **Tovább** gombra.



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.

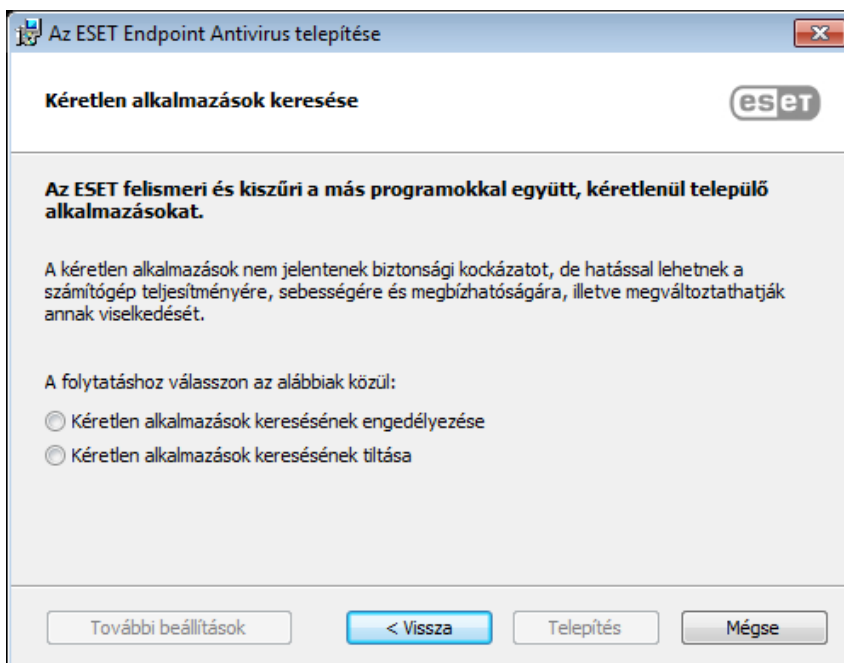


3. Adja meg, hogy engedélyezi-e az [ESET LiveGrid® visszajelzési rendszert](#). Az ESET LiveGrid® segítségével az ESET azonnal és folyamatosan értesül az új fertőzésekről, így biztosíthatja ügyfelei fokozottabb védelmét. A rendszer lehetővé teszi, hogy a felhasználó elküldje az új kártevőket az ESET víruslaborjába, ahol elemzik és feldolgozzák az adatokat, és felveszik azokat a keresőmotorba.



4. A következő telepítési lépés a kényszerű alkalmazások felismerésének beállítása. További tudnivalókat erről a [Kényszerű alkalmazások](#) című fejezetben talál.

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 Antivirus](#) aktiválására.

Speciális telepítés (.msi)

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

5. A [kényszerű alkalmazások](#) keresésére vonatkozó beállítások megadása és a **További beállítások** gombra kattintást követően a rendszer kéri, hogy válassza ki az ESET Endpoint Antivirus telepítési mappájának helyét.

Alapértelmezés szerint a program telepítése az alábbi könyvtárba történik:

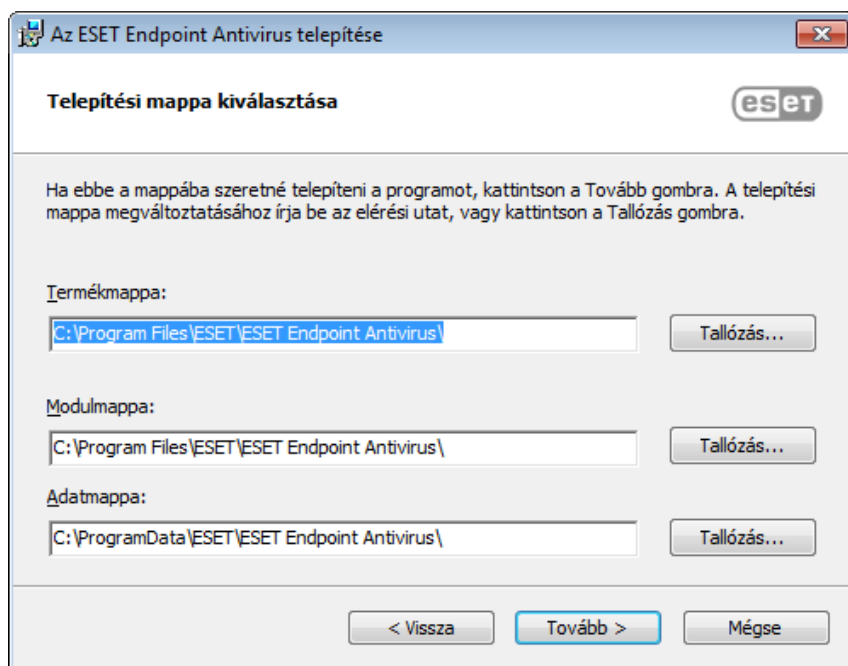
C:\Program Files\ESET\ESET Security

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).



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

Parancssori telepítés

Az ESET Endpoint Antivirus helyileg a parancssor segítségével, távolról pedig az ESET Security Management Centerben 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`



Megjegyzés

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

Lásd a megfelelő parancssori kapcsolóhoz 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



Megjegyzés

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 Antivirus funkciókészlete a következő:

Leírás	Funkció neve	Funkciószülő	Állapot
Alapvető programösszetevők	Computer		Helyőrző
Keresőmotor	Antivirus	Computer	Kötelező
Keresőmotor/Kártevő-ellenőrzések	Scan	Computer	Kötelező
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
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 / Levélszemétszűrő	Antispam	EmailClientProtection	Választható
Web és e-mail/Webfelügyelet	WebControl	WebAndEmail	Választható
Eszközök/ESET RMM	Rmm		Választható
Frissítés/Profilok/Frissítési tükör	UpdateMirror		Választható
ESET Enterprise Inspector beépülő modul	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 UPDITEMIRROR 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 paraméter t
FIRSTSCAN_ENABLE=	0 – Letiltva 1 – Engedélyezve	Számítógép-ellenőrzés ütemezése és futtatása a telepítés után
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=	<felhasználónév>	Felhasználónév hitelesítéshez
CFG_PROXY_PASSWORD=	<jelszó>	Jelszó hitelesítéshez
ACTIVATION_DATA=	Lásd lent	Termékaktiválás, licenckulcs vagy offline licencfájl
ACTIVATION_DLG_SUPPRESS=	0 – Letiltva 1 – Engedélyezve	Ha a beállítás „1”, akkor a licenctelepítési párbeszédpanel nem fog megjelenni az első alkalommal történő indítás után
ADMINCFG=	<elérési út>	Az exportált XML-konfiguráció elérési útja (alapértelmezett érték: <i>cfg.xml</i>)

[LiveGrid®](#) paraméter

Az ESET Endpoint Antivirus 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 Antivirus 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 .
--------------------	---

Példák parancssori telepítésre



Fontos

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



Példa

A **NetworkProtection** szakasz kizárása a telepítésből (meg kell adnia az összes gyermekvédelmi funkciót is):

```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```



Példa

Ha azt szeretné, hogy az ESET Endpoint Antivirus konfigurálása automatikusan megtörténjen a telepítést követően, a telepítési parancsban megadhat alapvető konfigurációs paramétereket. Az ESET Endpoint Antivirus telepítése úgy, hogy az ESET LiveGrid® engedélyezve legyen:

```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```



Példa

Telepítés nem az [alapértelmezett](#) könyvtárba, hanem egy másik alkalmazástelepítési könyvtárba:

```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```



Példa

Az ESET Endpoint Antivirus telepítése és aktiválása az ESET-licenckulccsal:

```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```



Példa

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
```



Példa

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 Antivirus nem csupán közvetlenül kliensszámítógépekre](#), illetve [szerverfeladat segítségével távolról az ESMC-ben](#), 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 Antivirus telepítését az ESET Security Management Center segítségével (ESMC). Az ESMC-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 ESMC-hez.
5. [Telepítse és aktiválja az ESET Endpoint Antivirus szolgáltatást a kliensszámítógépeken](#).



Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- [Az ESET Management Agent telepítése SCCM vagy GPO \(7.x\) segítségével](#)
- [Az ESET Management Agent telepítése GPO \(Group Policy Object\) segítségével](#)



Frissítés egy újabb verzióra

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

1. Automatikusan az ESET Security Management Center, az ESET Remote Administrator (csak a 6.x verziójú ESET-végponttermékek esetén) vagy az ESET PROTECT Cloud segítségével.
2. Manuálisan, egy [újabb verzió letöltésével és telepítésével](#) (az előző verzióra).

Javasolt frissítési eljárások

[Frissítés távolról](#)

Ha több, mint 10 ESET Endpoint terméket felügyel, akkor érdemes az ESET Security Management Center vagy az ESET PROTECT Cloud segítségével kezelni a frissítéseket. Tekintse meg a következő dokumentációt:

- [ESET Security Management Center | Infrastruktúra kiépítése és méretezése](#)

- [ESET Remote Administrator | Frissítési, áttelepítési és újratelepítési eljárások](#)
- [ESET Security Management Center | Frissítési, áttelepítési és újratelepítési eljárások](#)
- [Az ESET PROTECT Cloud ismertetése](#)

[Manuális frissítés kliensszámítógépen](#)

Ha manuálisan szeretné kezelni a frissítéseket az egyes kliensszámítógépeken:

1. Először ellenőrizze az ESET Endpoint Antivirus frissítésének előfeltételeit:

Frissítés erről:	Frissítés erre:	Frissítési előfeltételek
6.x	7.x	<ul style="list-style-type: none"> • Nincsenek előfeltételek • Megjegyzés: Az ESET Endpoint Antivirus 7-es verziója nem felügyelhető az ESET Remote Administrator segítségével
6.x	6.6.x	<ul style="list-style-type: none"> • Nincsenek előfeltételek
5.x	7.x	<ul style="list-style-type: none"> • Ellenőrizze, hogy az operációs rendszere támogatott-e. Például a Windows XP nem támogatott a 7-es verzió esetén. • Ellenőrizze, hogyan az adott ESET-végponttermékek támogatják-e az 5.x verzióról való frissítést.
4.x	7.x	<ul style="list-style-type: none"> • Ellenőrizze, hogy az operációs rendszere támogatott-e. • Távolítsa el az ESET NOD32 Antivirus Business Edition vagy az ESET Smart Security Business Edition szolgáltatást. Ne telepítse a 7-es verziót 4.x verzióra.

2. Töltsön le [egy újabb verziót, és telepítse](#) az előzőre.

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 Antivirus aktiválása nem sikerült, a leggyakoribb okok a következők:

- A licenckulcs már használatban van.
- Érvénytelen licenckulcs. Hiba történt a licenckiváltási úrlappal kapcsolatban.
- 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 szerverével

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 licenccel kapcsolatos gyakori kérdésekhez, hibákhoz és problémákhoz (angolul és néhány egyéb nyelven áll rendelkezésre).

- [Az ESET termékaktiválási hibaelhárítás indítása](#)

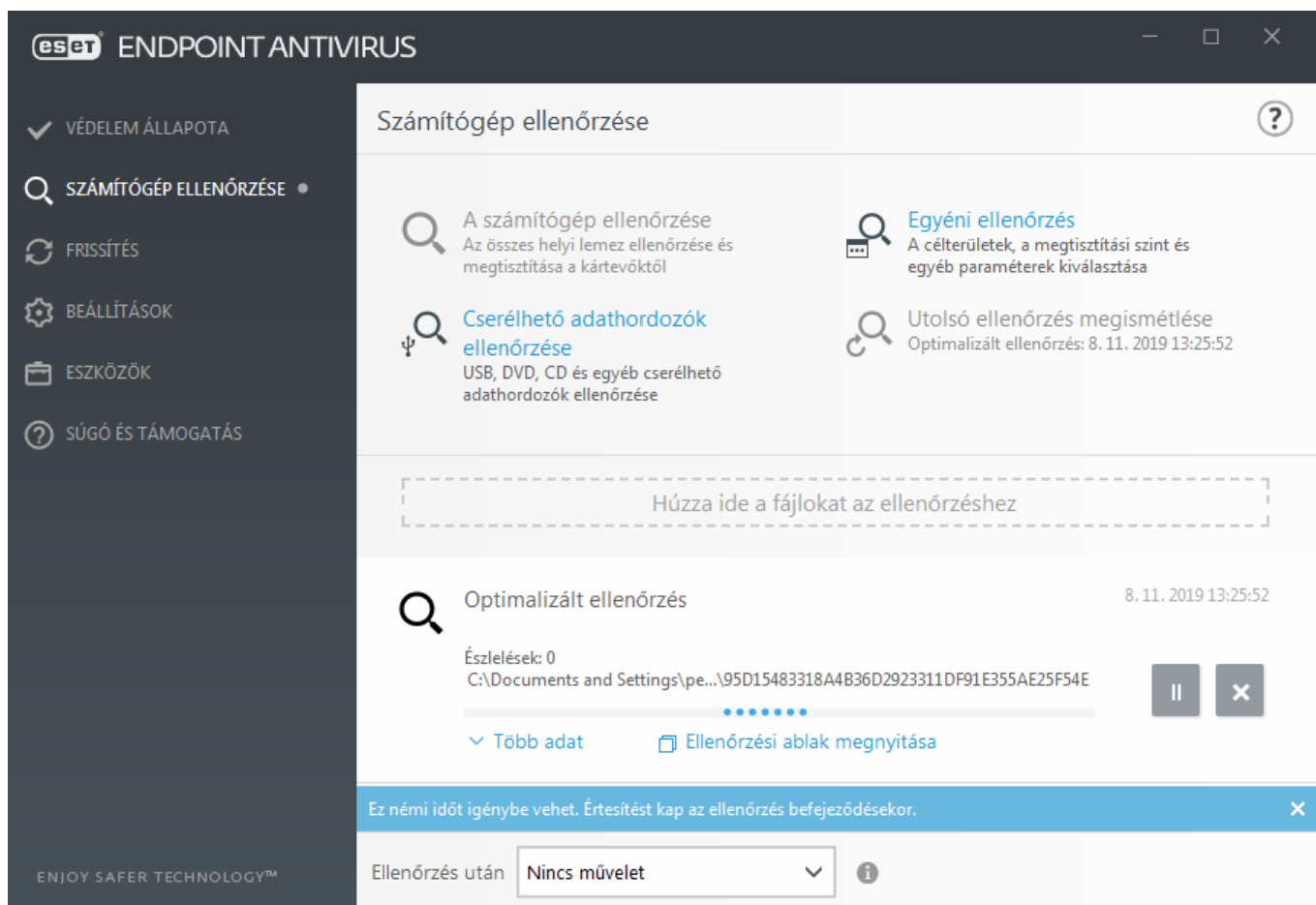
Licenc aktiválása

A telepítés végeztével a rendszer kéri a szoftver licencének aktiválását.

Az ESET Endpoint Antivirus licencének aktiválásához válasszon a rendelkezésre álló módok közül. További információt [Az ESET Endpoint Antivirus 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 **Optimalizált ellenőrzés** lehetőségre. A számítógép ellenőrzéséről a [Számítógép ellenőrzése](#) című témakörben olvashat részletesebben.



Útmutató kezdő felhasználók számára

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

A felhasználói felület

Az ESET Endpoint Antivirus 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 Antivirus védelmi állapotáról jelenít meg adatokat.

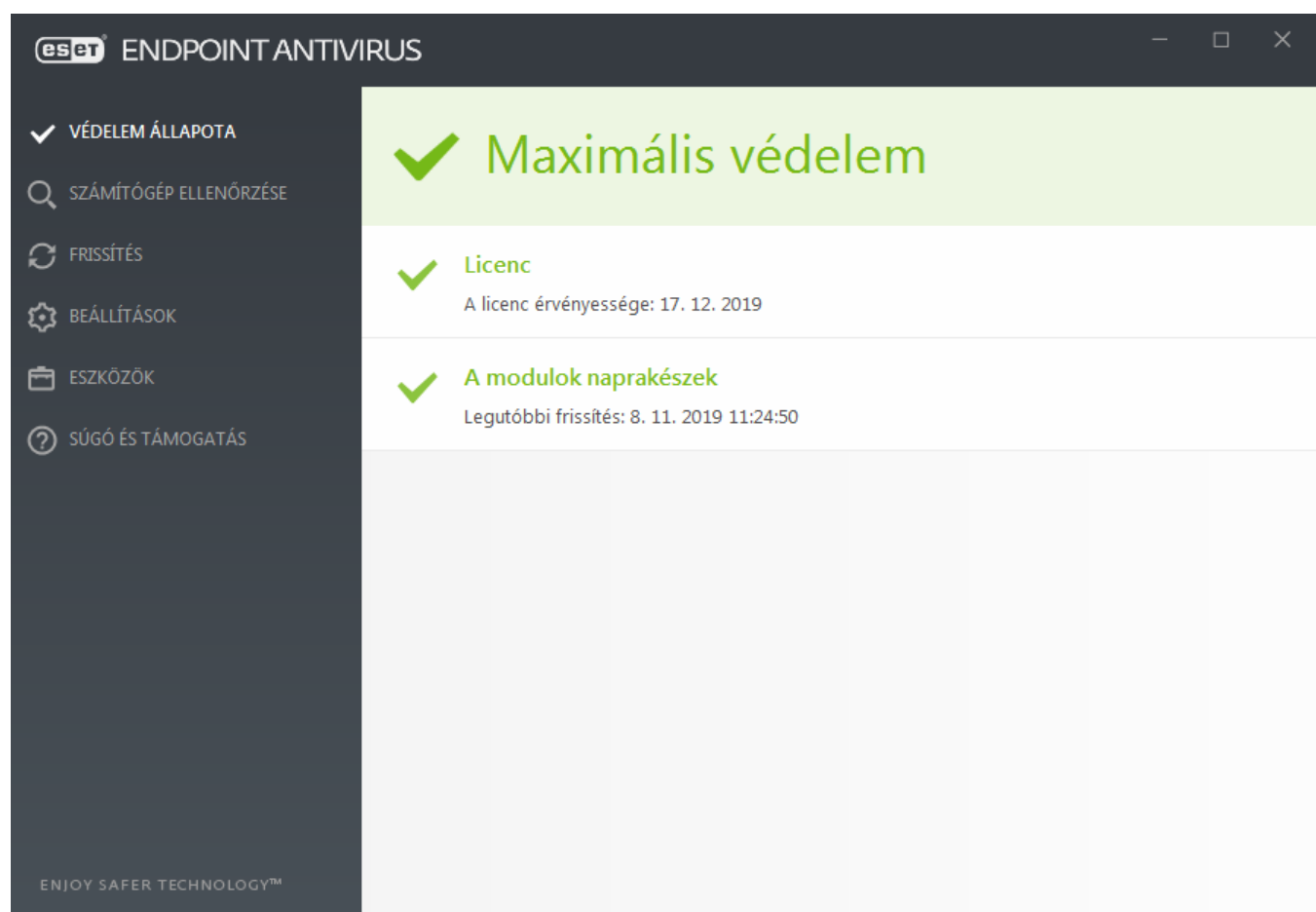
Számítógép ellenőrzése – Itt választhatja ki, hogy optimalizált vagy egyéni, illetve cserélhető adathordozón történő ellenőrzést szeretne-e beállítani vagy indítani. A legutóbb futtatott ellenőrzés megismétlésére is van lehetőség.

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

Beállítások – Ezt a lehetőséget választva módosíthatja a Számítógép 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, 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.



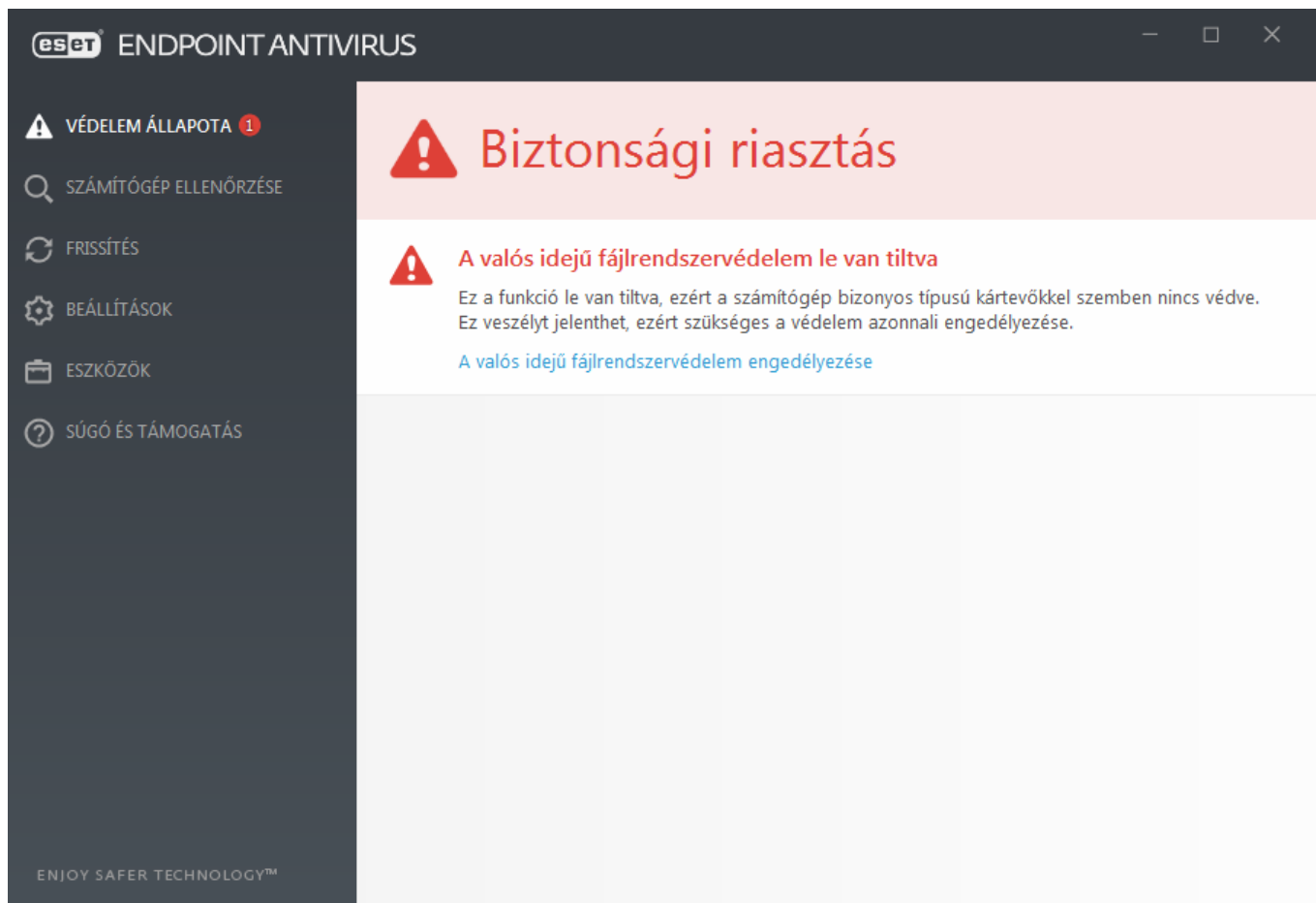
A **Védelem állapota** lap a számítógép biztonságáról és aktuális védelmi szintjéről nyújt tájékoztatást. A védelem

állapotát jelző zöld ikon azt jelöli, hogy biztosított a **maximális védelem**.

Az állapotablakban megtalálhatók továbbá az ESET Endpoint Antivirus 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 Antivirus legtöbb modulja nem működik megfelelően.
- **Az adathalászat elleni védelem nem működik** – Ez a funkció nem működik, mert más szükséges programmodulok nem aktívak.
- **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. Ennek a hibának a leggyakoribb oka a [hitelesítő adatok](#) téves megadása, illetve [csatlakozási beállítások](#) helytelensége.

- **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 Antivirus 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 ESMC 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 lejártá után a program nem frissül, és a védelmi állapot ikonja vörös lesz.
- **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 felülbíráltása 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 Felülbíráltás 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 Antivirus 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.



Megjegyzés

Ha egy állapot az ESMC 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.

eSET ENDPOINT ANTIVIRUS

✓ VÉDELEM ÁLLAPOTA

🔍 SZÁMÍTÓGÉP ELLENŐRZÉSE

🔄 FRISSÍTÉS

⚙️ BEÁLLÍTÁSOK

📁 ESZKÖZÖK

❓ SÚGÓ ÉS TÁMOGATÁS

Frissítés ⓘ

✓ **ESET Endpoint Antivirus**

Jelenlegi verzió: 7.2.2055.0

✓ Utolsó sikeres frissítés: 8. 11. 2019 11:24:50

Legutóbbi frissítéskeresés: 8. 11. 2019 12:25:08

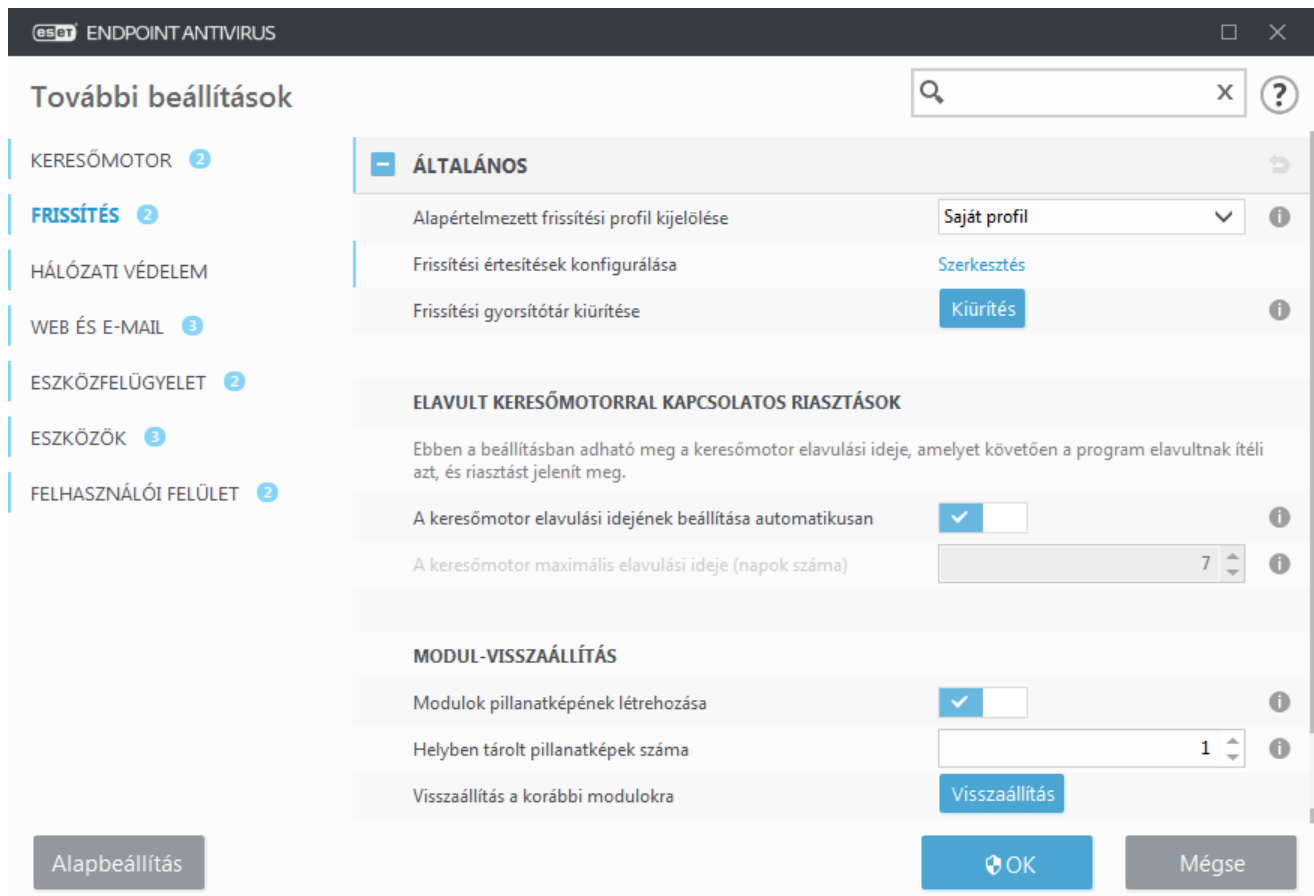
[Az összes modul megjelenítése](#)

ENJOY SAFER TECHNOLOGY™

🔄 Frissítések keresése ⌚ Frissítési gyakoriság módosítása

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 kapcsolatokat 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 Antivirus aktiválása](#) című témakörben található részletes információkat, és a **Licenc részletei** ablakban adja meg az ESET biztonsági termékkel együtt kapott hitelesítő adatokat.

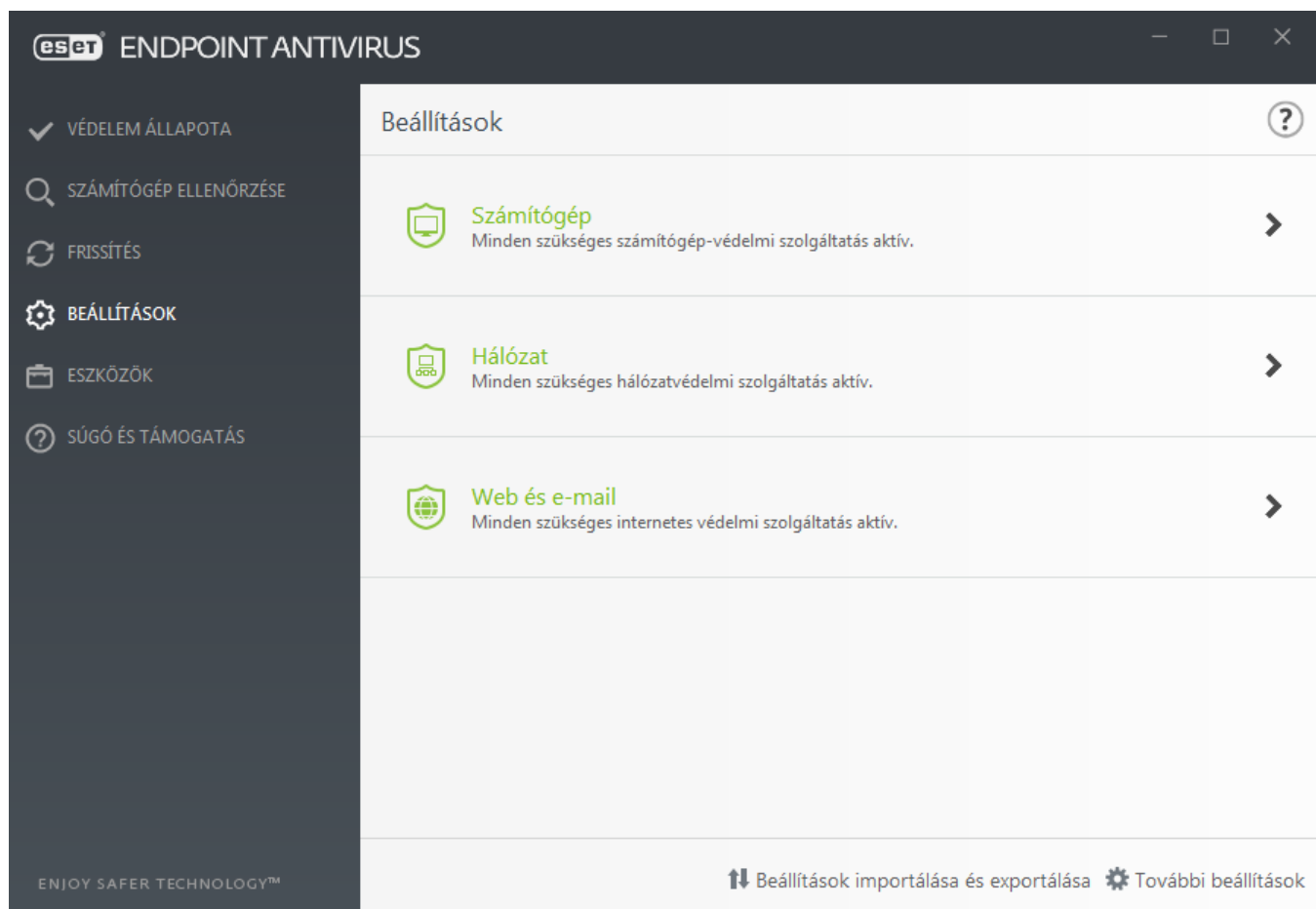
Az ESET Endpoint Antivirus használata

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



Megjegyzés

Amikor házirendet hoz létre az ESET Security Management Center 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 ESMC-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 szabálygyűttesek 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 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.
- **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 **Hálózati védelem** csoportban konfigurálhatja 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:

- **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.
- **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 ESMC/ERA házirend alkalmazásakor az adott összetevő mellett egy zár ikon  látható. Az ESET Security Management Center által alkalmazott házirend helyileg felülbírálnak a bejelentkezett felhasználó (pl. rendszergazda) hitelesítése után. További információt az [ESMC online súgójában](#) talál.



Megjegyzés

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


A biztonsági összetevők részletes beállításait az egyes összetevők melletti fogaskerék ikonra  kattintva érheti el.

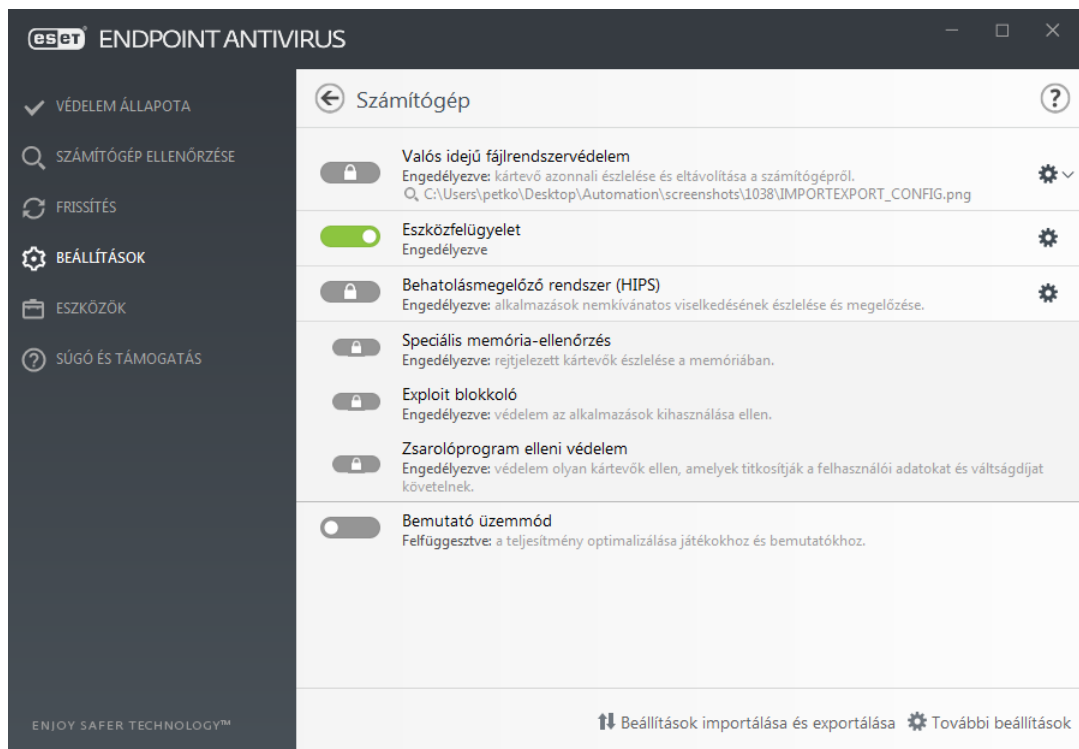
A beállítási ablak alsó részén további lehetőségek találhatók. Egy *.xml*/konfigurációs fájl segítségével betöltheti a beállítási paramétereket, illetve a **Beállítások importálása és exportálása** lehetőségre kattintva egy konfigurációs fájlba mentheti az aktuális beállítási paramétereket. Részletesebb 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 párbeszédpanel](#)t, ahol kizárhat fájlokat és mappákat az ellenőrzésből.



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 szabálygyűttesek 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 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.

- **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 (7.2 és újabb)

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 keresőmotor ellenőrzési konfigurációjának módosításai

A 7.2-es verziótól kezdve a Keresőmotor szakaszban nem található 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 „kárttevő” egy pontosabb kifejezés. A kártevőészlelést a keresőmotor végzi a gépi tanulás összetevővel együtt. Ezekről az alkalmazástípusokról a [Szószedetben](#) olvashat további információkat.

- **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.

Ezekről az alkalmazástípusokról a [Szószedetben](#) olvashat további információkat.

- **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).

Ezekről az alkalmazástípusokról a [Szószedetben](#) olvashat további információkat.

- A **gyanús alkalmazások** közé tartoznak a [tömörítőkkal](#) vagy védelmi modulokkal tömörített programok. Az észlelés alól kibúvókat kereső kártevőkészítők gyakran használnak ilyen típusú programokat.

eset ENDPOINT ANTIVIRUS

További beállítások

KERESŐMOTOR 2

Valós idejű fájlrendszervédelem

Felhőalapú védelem 1

Kártevő-ellenőrzések 2

Behatolásmegelőző rendszer (HIPS) 1

FRISSÍTÉS 2

HÁLÓZATI VÉDELEM

WEB ÉS E-MAIL 3

ESZKÖZFELÜGYELET 2

ESZKÖZÖK 3

FELHASZNÁLÓI FELÜLET 2

VALÓS IDEJŰ VÉDELEM ÉS GÉPI TANULÁS

Kártevők	Mélyreh...	Kiegyen...	Mérsékelt	Ki	i
Jelentés	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	i
Védelem	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	i
Kéretlen alkalmazások	Mélyreh...	Kiegyen...	Mérsékelt	Ki	i
Jelentés	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	i
Védelem	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	i
Gyanús alkalmazások	Mélyreh...	Kiegyen...	Mérsékelt	Ki	i
Jelentés	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	i
Védelem	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	i
Veszélyes alkalmazások	Mélyreh...	Kiegyen...	Mérsékelt	Ki	i
Jelentés	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	i
Védelem	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	i

Alapbeállítás

OK

Mégse



Nagyobb fokú védelem

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

Kártevő-ellenőrzések

Az ellenőrzési beállítások külön konfigurálhatók a valós idejű víruskereső és a [kézi indítású kereső](#) esetén. Alapértelmezés szerint a **Valós idejű védelmi beállítások használata** funkció aktiválva van. Ha aktiválva van, a vonatkozó kézi indítású keresési beállítások a **Valós idejű védelem és gépi tanulás** szakaszból öröklődnek.

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 Antivirus 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 KATEGÓRIAjelentés 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 Antivirus 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 Antivirus 7.2-es és újabb verzióiban áll rendelkezésre.

** Nem javasolt

[Termékverziók, programmodul-verziók és build dátumok meghatározása](#)

1. Kattintson a **Súgó és támogatás > Az ESET Endpoint Antivirus** névjegye elemre.
2. A **Névjegy** képernyőn a szöveg első sorában az ESET-termék verziószáma látható.
3. A **Telepített összetevők** elemre kattintva megtekintheti a különböző modulokkal kapcsolatos információkat.

Megjegyzések

Néhány megjegyzés a környezetnek megfelelő küszöb beállításához:

- A **Kiegyensúlyozott** a legtöbb telepítés esetén javasolt küszöb.
- A **Mérsékelt** küszöb az ESET Endpoint Antivirus 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 Antivirus programot és a moduljait naprakészen](#), mert így maximalizálható az észlelési arány teljesítményének és pontosságának, 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 ESMC házirend-átalakítási táblázata az ESET Endpoint Antivirus 7.1-es és korábbi verziói esetén](#)

Az ESMC 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 Antivirus 7.1-es és korábbi verziójában](#).

KATEGÓRIA küszöbállapota	Mélyreható	Kiegyensúlyozott	Mérsékelt	Ki
Alkalmazott KATEGÓRIA-kapcsoló	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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 munkahelyi gépekre [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 Antivirus 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 ESMC-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 [rootkitek](#)), amelyek képesek elrejtőzni az operációs rendszerben. Az elrejtőzés itt azt jelenti, hogy a szokásos vizsgálati eljárásokkal ezek a programok nem deríthetők fel.

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

Keresőmotor (7.1 és korábbi)

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

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



A keresőmotor ellenőrzési konfigurációjának módosítása
A 7.2-es verziótól kezdve a Keresőmotor szakasz [másképp néz ki](#).

Az összes védelmi modul (például Valós idejű fájlrendszervédelem, Webhozzáférés-védelem stb.) **víruskeresési beállításai** lehetővé teszik az alábbiak észlelésének engedélyezését vagy letiltását:

- **Kéretlen alkalmazások**– A „grayware” vagy kéretlen alkalmazás (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.
Ezekről az alkalmazástípusokról a [szószedetben](#) olvashat további információkat.

- A **veszélyes alkalmazások** csoportjába a kereskedelemben kapható, törvényes szoftverek tartoznak, amelyekkel kártékony célokból visszaélhetnek. Ilyenek például a távoli hozzáférést biztosító eszközök, a jelszófeltörő alkalmazások, valamint a billentyűzetfigyelők (a felhasználó minden billentyűleütését rögzítő programok). Ez a beállítás alapértelmezés szerint le van tiltva. Ezekről az alkalmazástípusokról a [szószedetben](#) olvashat további információkat.

- A **gyanús alkalmazások** közé tartoznak a [tömörítőkkkel](#) vagy védelmi modulokkal tömörített programok. Az észlelés alól kibúvókat kereső kártevőkészítők gyakran használnak ilyen típusú programokat.

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

A **kivételek** segítségével kizárhat objektumokat az ellenőrzésből. További információkért tekintse meg a [Kivételek](#) című részt.

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

További beállítások

KERESŐMOTOR 1

Valós idejű fájlrendszervédelem

Felhőalapú védelem

Kártevő-ellenőrzések

Behatolásmegelőző rendszer 3

FRISSÍTÉS 2

HÁLÓZATI VÉDELEM

WEB ÉS E-MAIL 3

ESZKÖZFELÜGYELET 1

ESZKÖZÖK 2

FELHASZNÁLÓI FELÜLET 1

ÁLTALÁNOS

VÍRUSKERESŐ BEÁLLÍTÁSAI

Kéretlen alkalmazások keresésének engedélyezése

☒

i

Veszélyes alkalmazások keresésének engedélyezése

☐

x

i

Gyanús alkalmazások keresésének engedélyezése

☒

i

ANTI-STEALTH

i

Az Anti-Stealth technológia engedélyezése

☒

FOLYAMATKIVÉTELEK

Ellenőrzésből kizárandó folyamatok

Szerkesztés

i

KIVÉTELEK

Ellenőrzésből kizárt fájlok és mappák

Szerkesztés

i

+ MEGOSZTOTT HFI VI GYORSÍTÓTÁR

Alapbeállítás

OK

Mégse

A program fertőzést észlelt

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

Szokásos viselkedés

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

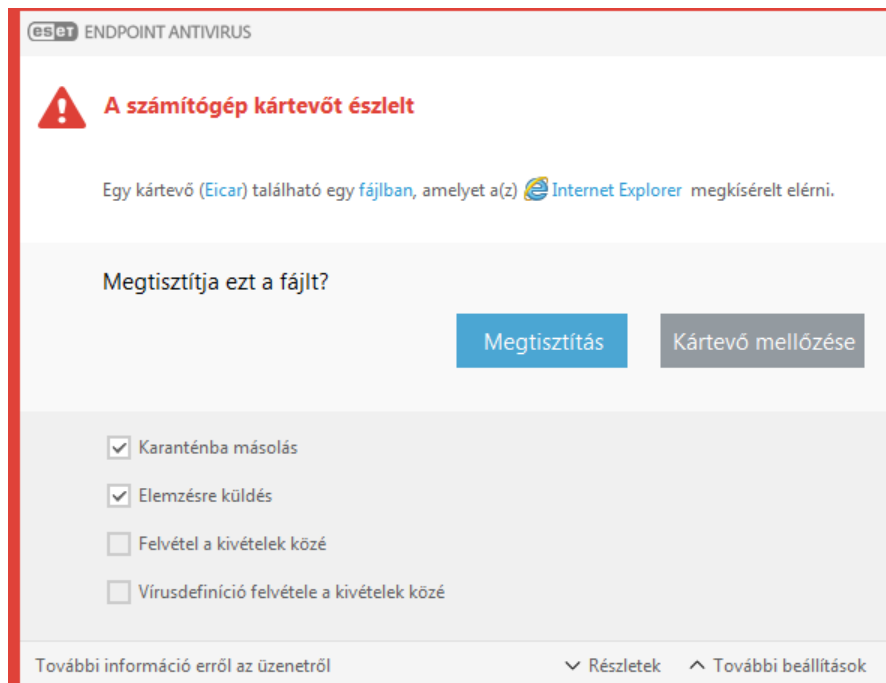
- [Valós idejű fájlrendszervédelem](#)
- [Webhozzáférés-védelem](#)
- [E-mail védelem](#)
- [Kézi indítású számítógép-ellenőrzés](#)

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. 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).

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 Antivirus programot, és kattintson a Számítógép ellenőrzése ikonra.
- Kattintson az **Optimalizált ellenőrzés** hivatkozásra (további információért lásd: [Számítógép ellenőrzése](#)).
- Az ellenőrzés befejeztével 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.

Megosztott helyi gyorsítótár

A megosztott helyi gyorsítótár javíthatja az izolált környezetek (például virtuális gépek) teljesítményét oly módon, hogy kiküszöböli az ismétlődő ellenőrzést a hálózatban. Ezzel biztosítható, hogy minden egyes fájlt csak egyszer ellenőrizzen a program, tárolásuk pedig a megosztott gyorsítótárban történjen.

Először végre kell hajtani az ESET Shared Local Cache telepítését és konfigurálását.

- [Az ESET Shared Local Cache letöltése.](#)
- További információkért tekintse meg a következőt: [Az ESET Shared Local Cache kézikönyve.](#)

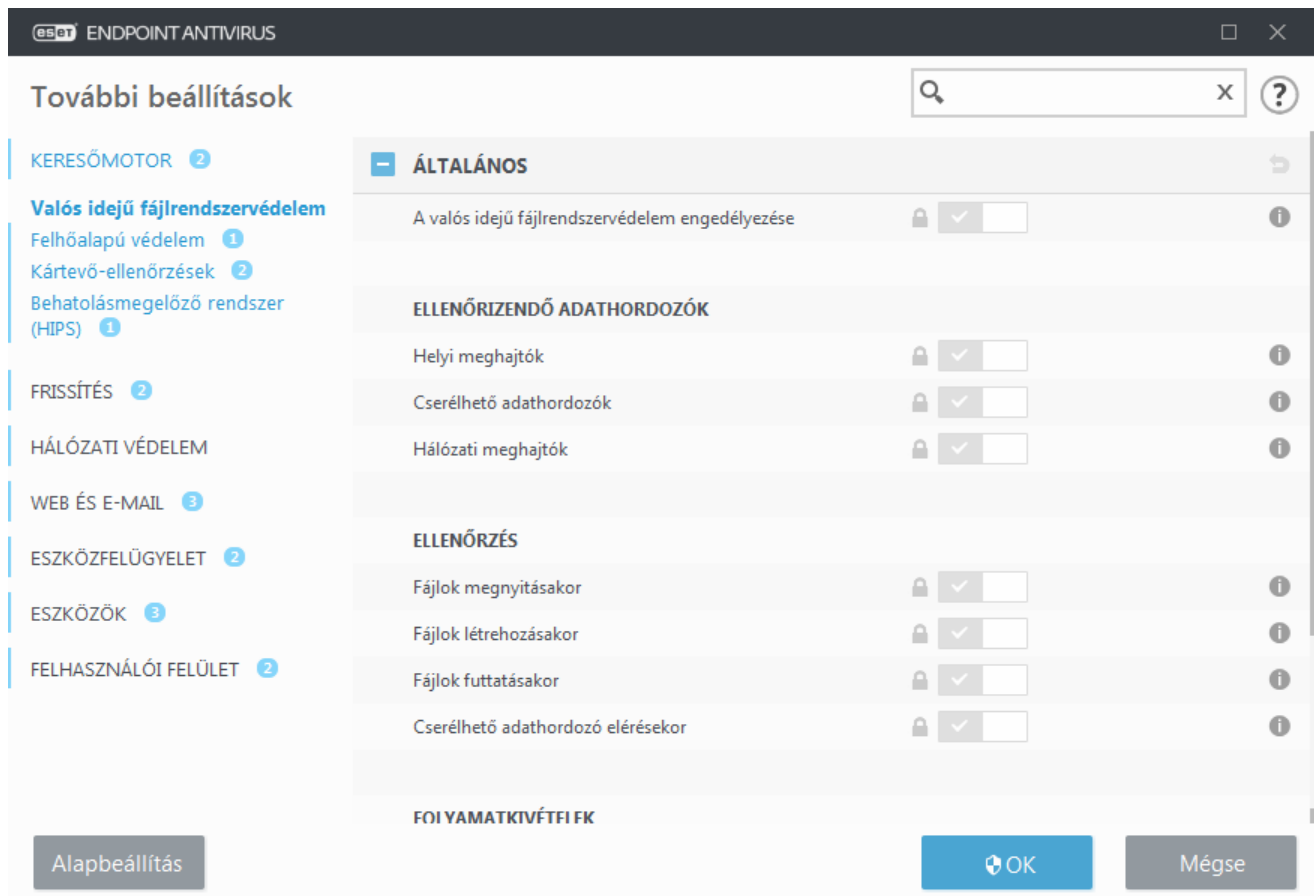
Ha bekapcsolja a **Gyorsítótárazási beállítás** kapcsolót, információkat menthet az ESET Shared Local Cache gyorsítótárba a hálózaton lévő fájlok és mappák ellenőrzéseiről. Új ellenőrzés végrehajtásakor az ESET Endpoint Antivirus megkeresi az ellenőrzött fájlokat az ESET Shared Local Cache gyorsítótárban. Ha talál egyezést, az egyező fájlokat kizárja az ellenőrzésből.

A **Gyorsítótárszerver** beállításai a következők:

- **Állomásnév** – Annak a számítógépnek az állomásneve vagy IP-címe, amelyen az ESET Shared Local Cache található.
- **Port** – A kapcsolathoz használt port száma (megegyezik az ESET Shared Local Cache beállítás értékével).
- **Jelszó** – Szükség esetén adja meg az ESET Shared Local Cache jelszavát.

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 indítása a rendszerindításkor történik, 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 Antivirus minden beállítást optimalizál, hogy a lehető legmagasabb szintű védelmet biztosíthassa 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 a valós idejű védelmet egy felhasználó akaratlanul letiltotta, akkor újra kell aktiválni. A valós idejű védelem újbóli aktiválásához a program főablakában kattintson a **Beállítások**, majd a **Valós idejű fájlrendszervédelem** lehetőségre.

Ha a valós idejű védelem nem indul el a rendszer indításakor, valószínűleg nincs bejelölve a **Valós idejű fájlrendszervédelem automatikus indítása** jelölőnégyzet. Az opció engedélyezéséhez nyissa meg a **További beállítások (F5)** párbeszédpanelt, és kattintson a **Keresőmotor > Valós idejű fájlrendszervédelem > Általános** elemre. Győződjön meg arról, hogy a **Valós idejű fájlrendszervédelem automatikus indítása** kapcsoló be van kapcsolva.

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

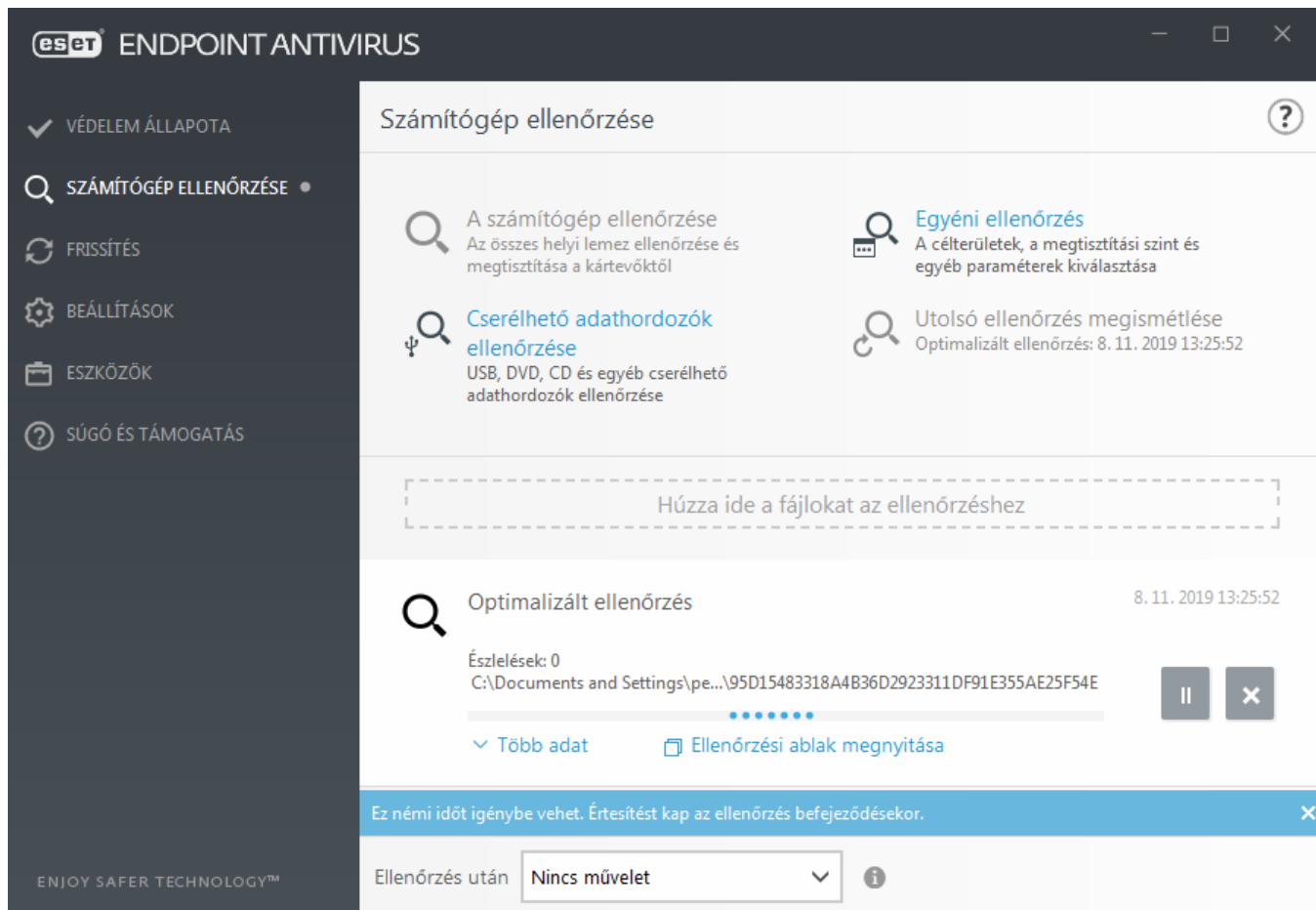
Győződjön meg arról, hogy a számítógépen nincs másik víruskereső program telepítve. Ha egyszerre két valós idejű védelmi szolgáltatást nyújtó eszköz van engedélyezve, azok ütközésbe kerülhetnek egymással. Javasoljuk, hogy az ESET telepítése előtt távolítsa el minden egyéb vírusvédelmi programot a rendszerről.

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 támogatási szolgálathoz.

Számítógép ellenőrzése

A kézi indítású víruskereső az ESET Endpoint Antivirus 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 ellenőrizi, 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**, a **Kikapcsolás**, illetve az **Újraindítás** lehetőséget az **Ellenőrzés után** 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 inaktíválhatja a kikapcsolást). A [További ellenőrzési beállítások](#) című rész bővebb információk tartalmaz erről.



Megjegyzés

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

Egyéni ellenőrzés indítása

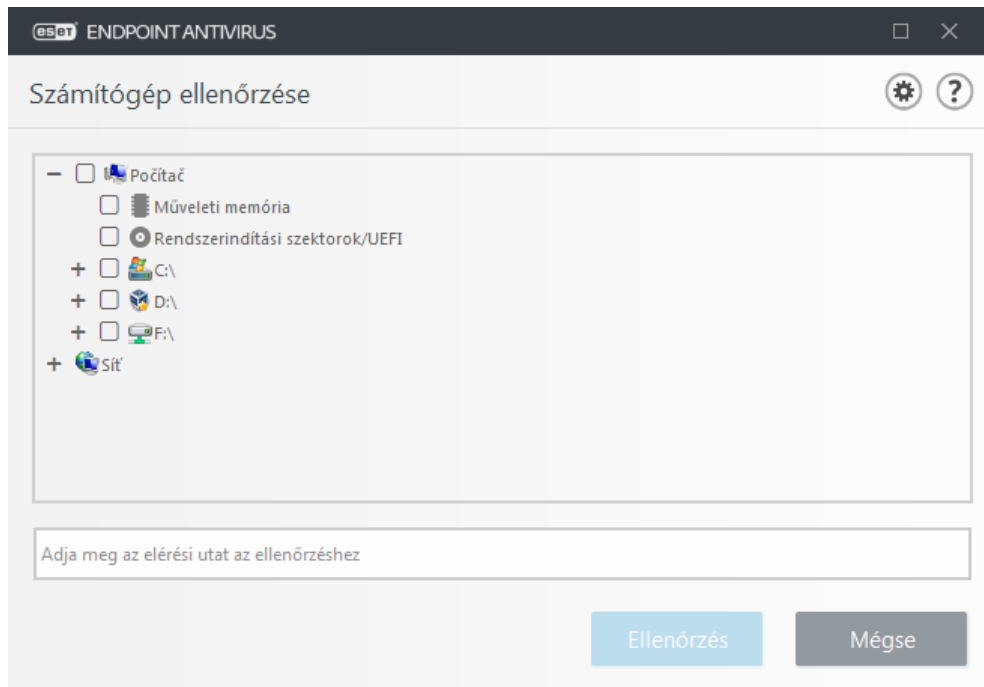
Ha csak egy adott célterületet szeretne ellenőrizni, használhatja az Egyéni ellenőrzés eszközt. Az ellenőrizendő célterületek kiválasztásához kattintson a **Számítógép ellenőrzése > Egyéni ellenőrzés** hivatkozásra, és válasszon egy területet az **Ellenőrizendő célterületek** legördülő listában, vagy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

Az Ellenőrizendő célterületek párbeszédpanelen definiálhatók azok a célterületek (memória, meghajtók, szektorok, fájlok és mappák), amelyeken vírusellenőrzést szeretne végrehajtani. Az ellenőrizendő objektumokat a

számítógépen rendelkezésre álló összes eszközt felsoroló, fa szerkezetű listából választhatja ki. Az **Ellenőrizendő célterületek** legördülő listában előre definiált célterületeket választhat ki.

- **Profilbeállítások alapján** – A kijelölt ellenőrzési profilban meghatározott célterületeket ellenőrzi.
- **Cserélhető adathordozó** – A hajlékonylemezeket, USB-tárolóeszközöket, CD és DVD lemezeket ellenőrzi.
- **Helyi meghajtók** – Kijelöli az összes helyi meghajtót.
- **Hálózati meghajtók** – Kijelöli az összes csatlakoztatott hálózati meghajtót.
- **Egyéni kiválasztás** – Lehetővé teszi a felhasználónak egyéni célterületek kiválasztását.

Ha gyorsan egy kiválasztott ellenőrizendő célterületre szeretne lépni, vagy hozzá szeretne adni egy célmappát vagy egy vagy több célfájlt, adja meg a célkönyvtárt a mappalista alatti üres mezőben. Ez csak akkor lehetséges, ha nem jelölt ki célterületet a fastruktúrák listából, és az **Ellenőrizendő célterületek** legördülő listában a **Nincs kiválasztás** elem van kiválasztva.



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 információszerezés céljából, megtisztítás nélkül szeretné ellenőrizni a rendszert, jelölje be a **Csak ellenőrzés megtisztítás nélkül** jelölőnégyzetet. Az ellenőrzéssel kapcsolatos információkat az ellenőrzési naplóba menti a program.

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**. Két további előre megadott ellenőrzési profil áll még rendelkezésre: **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 hozzáférésehez. Ne feledje, hogy ez a gomb nem érhető el akkor, ha az aktuális felhasználó nem hívhatja meg rendszergazdaként az UAC-műveleteket.



Megjegyzés

A számítógép-ellenőrzési naplót az ellenőrzés befejezésekor 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.

Optimalizált ellenőrzés

Talált kártevők: 0
C:\Documents and Settings\All Users\ESET\ESET Security\Installer\ees_nt64.msi

8/22/2018 10:02:58 AM

|| X

^ Kevesebb adat

Felhasználó: John-PC\John
Ellenőrzött objektumok: 721
Időtartam: 0:00:26

Víruskeresési napló

A keresőmotor verziószáma: 17923 (20180822) Dátum: 8/22/2018 Idő: 10:02:58 AM

Dátum: 8/22/2018 Idő: 10:02:58 AM

Ellenőrzött lemezek, mappák és fájlok: Műveleti memória; C:\Rendszerindítási szektorok\UEFI\C\

Műveleti memória = \\E:\wboxsn\VirtualBoxShare\Ranorex__EES\endpoint_65\endpoint_65\bin\Debug\Ranorex.Core.Resolver.dll - nem lehet megnyitni [4]

☒ Napló görgetése

Bezárás



Megjegyzés

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

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

Célterület – Az aktuálisan ellenőrzött objektum neve és helye.

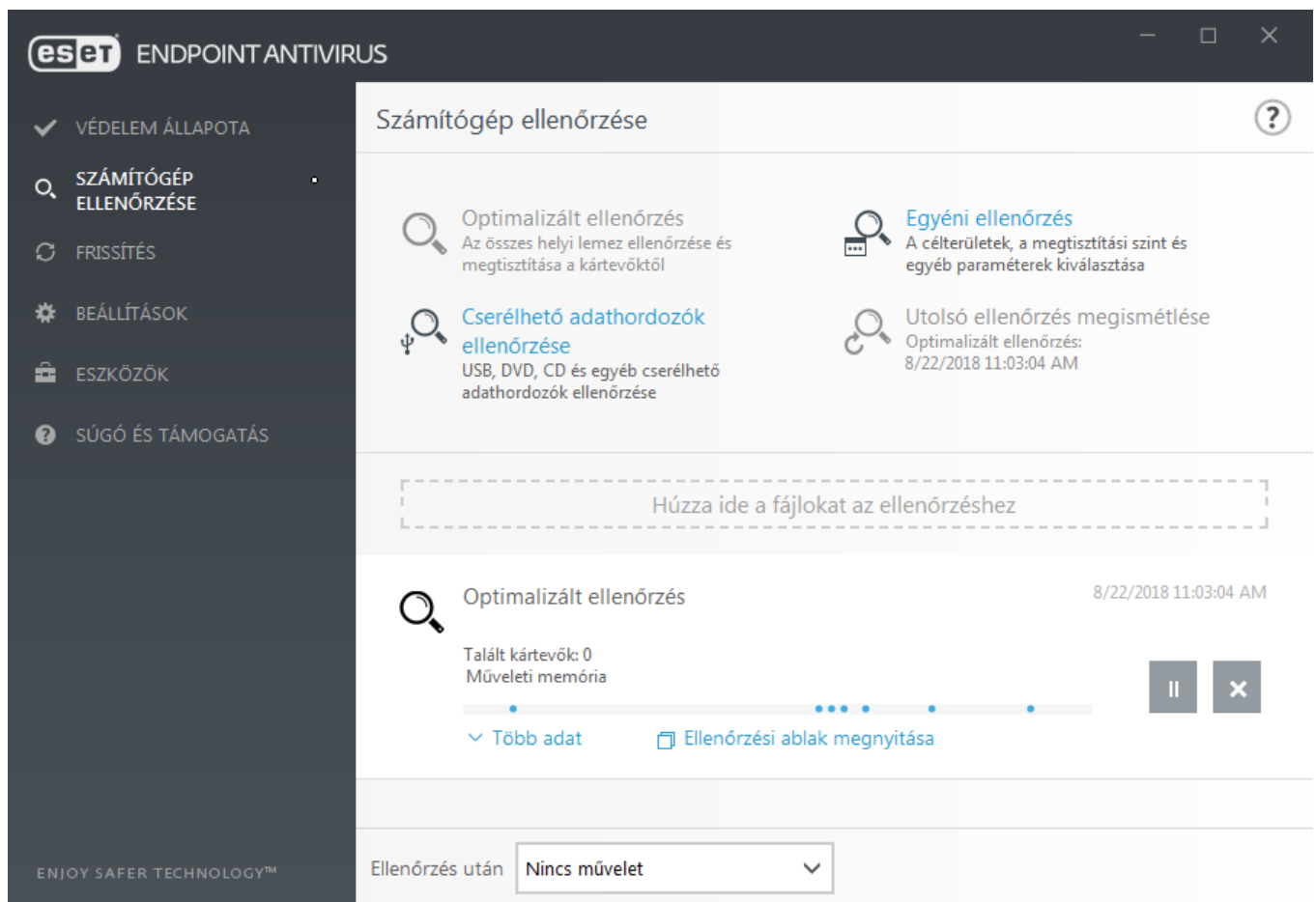
A víruskereső kártevőket talált – Itt látható a program által az ellenőrzés során észlelt kártevők száma.

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

Az előnyben részesített ellenőrzési paramétereket mentheti, és a későbbi ellenőrzésekhez használhatja. A rendszeresen használt ellenőrzésekhez ajánlott különböző 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, valamint 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.



Megjegyzés

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 párbeszédpanelen definiálhatók azok a célterületek (memória, meghajtók, szektorok, fájlok és mappák), amelyeken vírusellenőrzést szeretne végrehajtani. Az ellenőrizendő objektumokat a számítógépen rendelkezésre álló összes eszközt felsoroló, fa szerkezetű listából választhatja ki. Az **Ellenőrizendő célterületek** legördülő listában előre definiált célterületeket választhat ki.

- **Profilbeállítások alapján** – A kijelölt ellenőrzési profilban meghatározott célterületeket ellenőrzi.
- **Cserélhető adathordozó** – A hajlékonylemezeket, USB-tárolóeszközöket, CD és DVD lemezeket ellenőrzi.
- **Helyi meghajtók** – Kijelöli az összes helyi meghajtót.
- **Hálózati meghajtók** – Kijelöli az összes csatlakoztatott hálózati meghajtót.
- **Egyéni kiválasztás** – Lehetővé teszi a felhasználónak egyéni célterületek kiválasztását.

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.
- **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.



Megjegyzés

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 Antivirus 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 cserélhető lemez)
- CD/DVD
- USB-nyomtató
- FireWire tároló
- Bluetooth-eszköz
- Intelligenskártya-olvasó
- Képeszköz
- Modem

- LPT/COM port
- Hordozható eszköz
- Minden eszköztípus

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

Az **Integrálás a rendszerbe** jelölőnégyzet bejelölésével aktiválható az ESET Endpoint Antivirus 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 beszur egy meglevo szabaly 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 meglevo szabályait, és lehetővé teszi a felhasználók által a számítógéphez csatlakoztatott külső eszközök pontos vezérlését.


Név	Engedély...	Típus	Leírás	Művelet	Felhasználók	Részletesség	Időkö...
Block USB for User	<input checked="" type="checkbox"/>	Lemezes tár...		Letiltás	Összes	Mindig	Mindig
Rule	<input checked="" type="checkbox"/>	Bluetooth-es...		Olvasás/írás	Összes	Mindig	Mindig

Adott eszközök engedélyezhetők vagy letilthatók a felhasználójuk vagy a felhasználócsoporthoz, 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 Antivirus 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).

Ha kijelöl egy eszközt (az észlelt eszközök listájában), majd az **OK** gombra kattint, megjelenik egy szabályszerkesztésre használható ablak, előre megadott adatokkal (minden beállítás módosítható).

Eszközcsoportok



Figyelmeztetés

A számítógéphez 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 eszközlístával 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 számítógéphez 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 fájlból történő importálására szolgál.

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.



Példa

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.

Szabály szerkesztése

Név: Rule

Szabály engedélyezve: ☒

Alkalmazás a következő során: Mindig

Eszköz típusa: Bluetooth-eszköz

Művelet: Olvasás/írás

Feltételek típusa: Eszköz

Gyártó:

Típus:

Sorozatszám:

Naplózás részletessége: Mindig

Felhasználólista: Szerkesztés

OK

A **Név** mezőbe írt leírás segítségével a szabály 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 információkért kattintson [ide](#).

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 eszközzelkezelőjében 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 képfelolvasók és a fényképezőgépek. Mivel ezek az eszközök csak a saját műveleteikről adnak meg információkat, a felhasználókról nem, csak globálisan tilthatók le.



Megjegyzés

A modem-eszköz 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 hozzáférést 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 Eszközcsoporthoz vagy az Eszköz elem közül választhat.

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

- **Gyártó** – Szűrés a 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.



Megjegyzés

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



Megjegyzés

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 felhasználó csoportokra 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.



Megjegyzés

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

Behatolásmegelőző rendszer

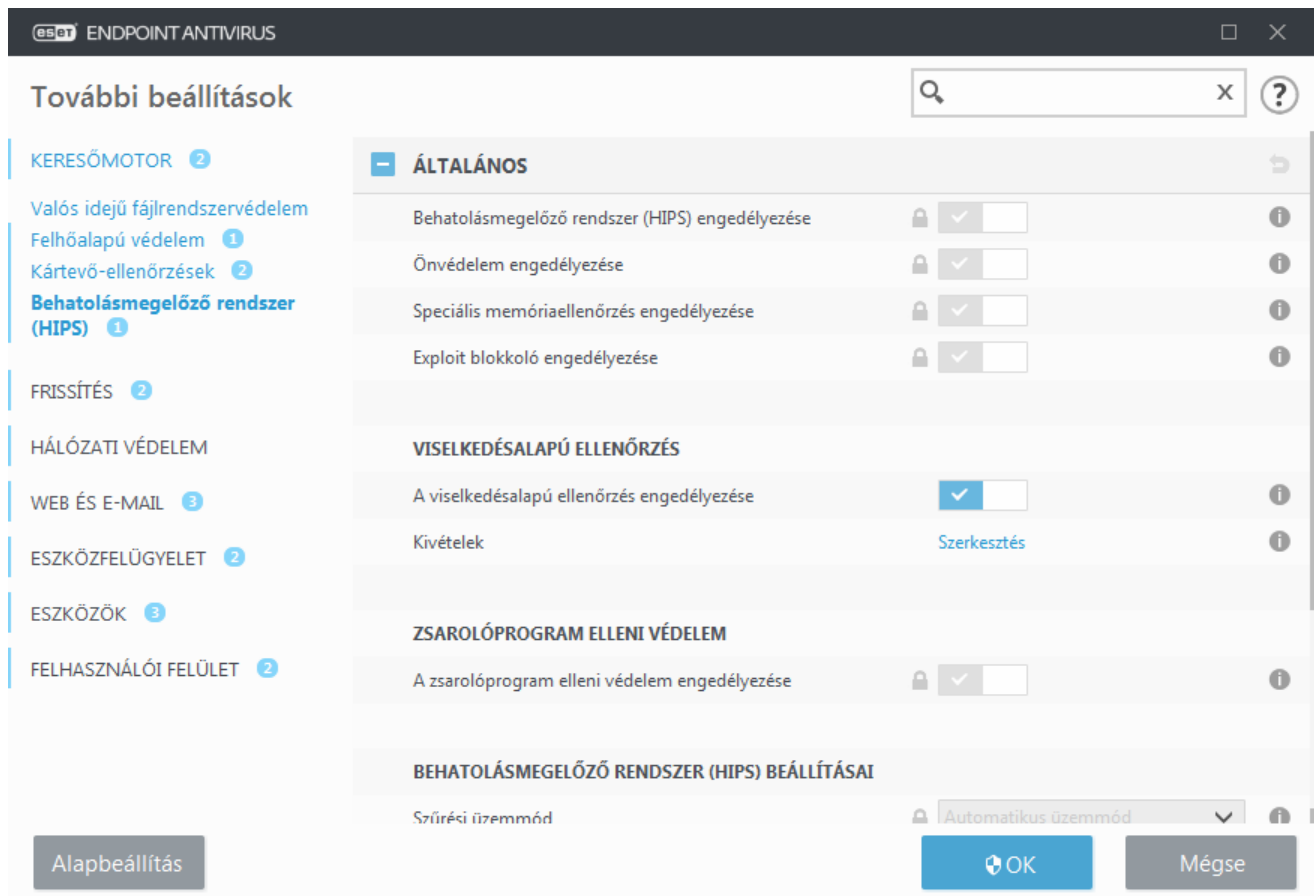


Figyelmeztetés

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

A **Behatolásmegelőző rendszer** 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 figyel.

A Behatolásmegelőző rendszer beállításainak megjelenítéséhez válassza a **További beállítások (F5) > Keresőmotor > Behatolásmegelőző rendszer > Általános** elemet. A Behatolásmegelőző rendszer állapota (engedélyezve/letiltva) az ESET Endpoint Antivirus fő programablakának **Beállítások > Számítógép** részén látható.



Általános

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

Önvédelem engedélyezése – Az ESET Endpoint Antivirus 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 folyamatokat, 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 Antivirus szolgáltatásban. Ez a funkció csak az ESMC és az ESET PROTECT Cloud 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.
Tanuló mód	A műveletek engedélyezettek, és mindegyikhez létrejön egy szabály. Az ebben a módban létrehozott szabályok megtekinthetők a Behatolásmegelőző rendszer szabályai ablakban, prioritásuk azonban alacsonyabb a manuálisan és az automatikus módban létrehozott szabályokénál. Ha kiválasztja a Tanuló mód lehetőséget a Szűrési üzemmód legördülő listában, a 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 (HIPS) által létrehozott szabályok szerkesztését. Választhat másik szűrési üzemmódot, vagy elhalaszthatja a döntést, és tovább használhatja a tanuló módot.

A tanuló mód lejáratát után beállított mód – Kiválaszthatja a tanuló mód lejáratát 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 hasonlóak a tűzfal szabályaihoz. A **Szabályok** felirat melletti **Szerkesztés** gombra kattintva megnyithatja a **Behatolásmegelőző rendszer szabálykezelési** 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 párbeszédpanel. További információkért tekintse meg a következő részt: [A Behatolásmegelőző rendszer szabályainak prioritása](#).

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

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

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

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

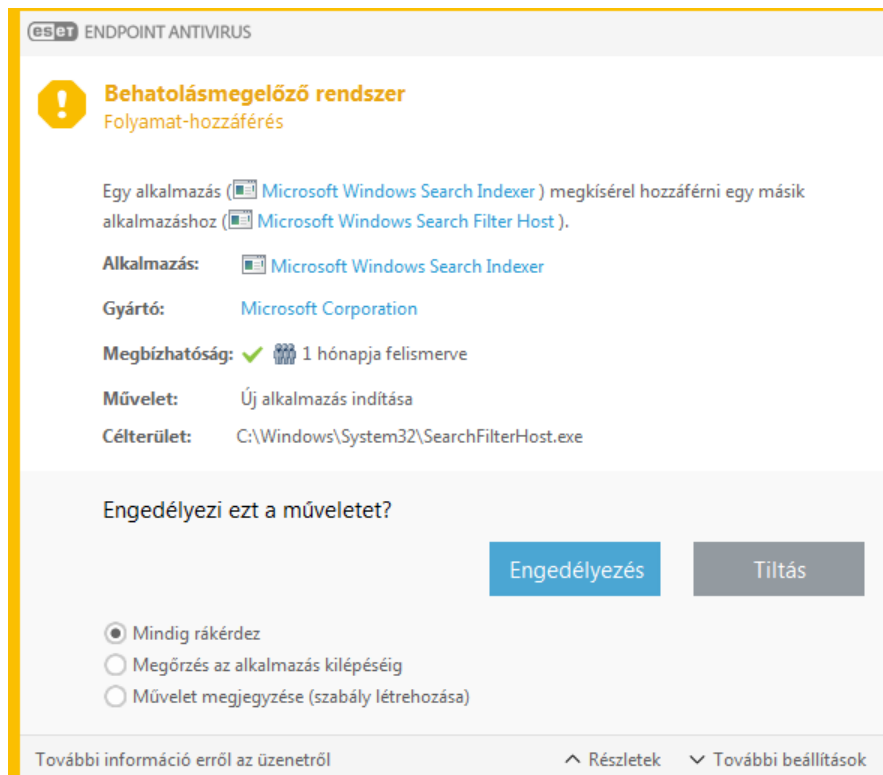
Részletesebb szabályok a **További beállítások** lapon adhatók meg. Az alábbi lehetőségek akkor állnak a rendelkezésére, ha kiválasztja a **Művelet megjegyzése (szabály létrehozása)** beállítást:

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



Túl sok értesítést küld a Behatolásmegelőző rendszer?


Ha nem szeretne értesítéseket kapni, módosítsa a szűrési módot **Automatikus üzemmódra** a **További beállítások (F5) > Keresőmotor > HIPS > Általános** lapon.



Lehetséges zsarolóprogram-viselkedés észlelve

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

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

**Fontos**
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 – Ha bekapcsolja ezt az opciót, a szabállyal kapcsolatos információkat a program bejegyzi a [Behatolásmegelőző rendszer 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.

- 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 felülrni 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 – Ha bekapcsolja ezt az opciót, a szabállyal kapcsolatos információkat a program bejegyzi a [Behatolásmegelőző rendszer 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.

Fájlok – A szabály alkalmazásához a műveletnek erre a célterületre kell vonatkoznia. A legördülő listában válassza az **Adott fájlok** elemet, és kattintson a **Hozzáadás** műveletre új fájlok vagy mappák hozzáadásához, illetve ha az összeset hozzá szeretné adni, a legördülő listában választhatja 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.



Megjegyzés

A Behatolásmegelőző rendszer által előre létrehozott speciális szabályok egyes műveletei alapértelmezés szerint engedélyezettek, és nem tilthatók le. Emellett a rendszer csak azokat a rendszerműveleteket figyeli, amelyek rendszerint nem biztonságosak.

Az alábbi szakaszok a fontosabb műveleteket ismertetik.

Fájlműveletek

- **Fájl törlése** – Az alkalmazás engedélyt kér a célfájlok törléséhez.
- **Írás fájlba** – Az alkalmazás engedélyt kér a célfájlok írásához.
- **Közvetlen hozzáférés lemezhez** – Az alkalmazás a Windows szokásos eljárásainak megkerülésével, nem normál módon próbálja meg olvasni vagy írni a lemezt. Ilyenkor nem alkalmazhatók a megfelelő szabályok, és ellenőrizetlenül módosulnak a fájlok. Ilyen műveleteket az észlelést kerülni próbáló kártevők, a lemezekről pontos másolatot készítő biztonsági mentési szoftverek, illetve a lemezkötetek átszervezését végző partíciókezelő szoftverek is végrehajthatnak.
- **Globális beavatkozási rutin telepítése** – Az MSDN Library SetWindowsHookEx függvényének hívása.
- **Illesztőprogram betöltése** – Illesztőprogramok betöltése és telepítése a rendszerben.

Alkalmazásműveletek

- **Másik alkalmazás hibakeresése** – Hibakereső csatlakoztatása a folyamathoz. Hibakeresés közben megfigyelhető és módosítható a tanulmányozott alkalmazás viselkedése, továbbá elérhetők az adatai is.
- **Események elfogása másik alkalmazásból** – A forrásalkalmazás megpróbálja elfogni a célalkalmazásnak szóló eseményeket (például egy keylogger így kaphatja el a böngésző eseményeit).

- **Másik alkalmazás megszakítása/felfüggesztése** – Egy folyamat felfüggesztése, folytatása vagy befejezése (közvetlenül a folyamatállóból 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.



Megjegyzés

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.



Megjegyzés

Helyettesítő karakterek használata

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.



Figyelmeztetés

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.

Behatolásmegelőző rendszer (HIPS) szabálybeállításai

Szabály neve: Névtelen

Művelet: Engedélyezés

Műveletek által érintett

Fájlok: ☐ X

Alkalmazások: ☐ X

Beállításjegyzék bejegyzései: ☐ X

Engedélyezve: ☒

Naplózás részletessége: Nincs

Felhasználó értesítése: ☐ X

Vissza | **Következő** | Mégse

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 – A jelölőnégyzet bejelölése esetén a program minden tiltott műveletet bejegyez a behatolásmegelőző rendszer naplójába.

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.



Megjegyzés

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 Antivirus 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.

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 az **Integrálás a rendszerbe** kapcsolóra.



Megjegyzés

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 játékal alkalmazások 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

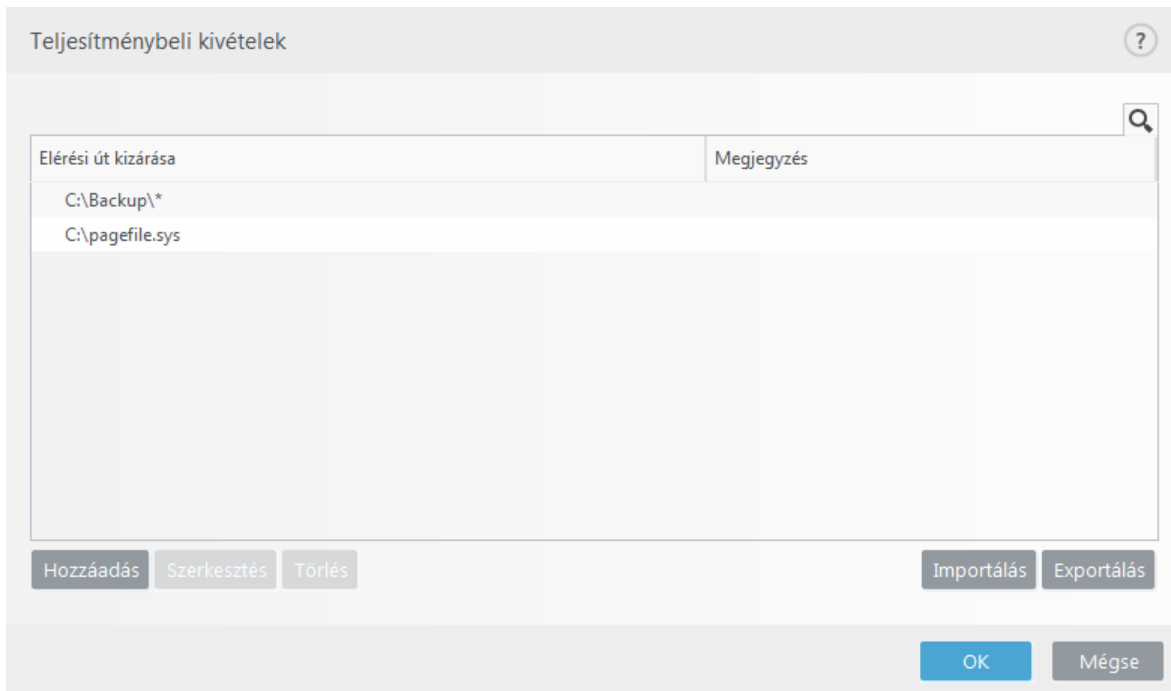
A Teljesítménybeli kivételek részen fájlokat és mappákat zárhat ki az ellenőrzésből.

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.



Megjegyzés

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":"7.2.2055","path":"plugins.01000600.settings.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.



Elérési út kiválasztása vagy manuális megadás

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

Kivétel szerkesztése

Elérési út: C:\Backup* ...

Megjegyzés:

OK Mégse

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



Kivételek formátuma

- Ha egy mappa összes fájlját 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).



Rendszerváltozók kivételekben

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

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

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

☐ [Bontsa ki a támogatott rendszerváltozók listáját](#)

A következő változók használhatók az útvonalkivétel formátumában:

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

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



Csillagot tartalmazó útvonalkivételek

Néhány további példa csillaggal jelzett kivételre:

`C:\Tools*` – Az elérési útnak fordított perjellel és csillaggal kell végződnie, ami azt jelzi, hogy a mappa és az összes almappájának kizárása a cél.

`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.

Kivétel teljesítménybeli kivételek alól:

`C:\Tools*. *` – Ugyanaz a viselkedés, mint a `C:\Tools*` esetén (nem összekeverendő azzal, hogy a `*.*` maszk csak a kiterjesztéssel rendelkező fájlokat zárja ki a `Tools` mappában).

Példa olyan kivételre, amelyet rosszul adtak meg manuálisan:

`C:\Tools` – A `Tools` mappa nem lesz kizárva. A víruskereső a `Tools` szót fájlnevként is kezelheti.

`C:\Tools\` – Ne felejtse el beírni a csillagot az elérési út végére: `C:\Tools*`



Helyettesítő karakterek az elérési út közepén

Azt javasoljuk, hogy semmiképpen se használjon helyettesítő karaktereket az elérési út közepén (például `C:\Tools*|Data|file.dat`), kivéve akkor, ha a rendszer miatt van erre szükség. 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
- Ha az ellenőrző modul megfelelt az első alkalmazandó szabálynak, a rendszer nem értékeli ki a második alkalmazandó szabályt
- Minél kevesebb a szabály, annál hatékonyabb lesz az ellenőrzés
- Ne hozzon létre párhuzamos szabályokat

Útvonalkivétel formátuma

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



Kivételek formátuma

- Ha egy mappa összes fájlját 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).



Rendszerváltozók kivételekben

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

- A Program Files mappa fenti rendszerváltozóval való kizáráshoz 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 működése

Az észlelési kivételek nem úgy zárnak ki fájlokat és mappákat az ellenőrzésből, mint a [Teljesítménybeli kivételek](#). Az észlelési kivételek csak akkor zárnak ki objektumokat, ha a keresőmotor észleli őket, és van egy megfelelő szabály a kizárási listában.

Ha például (lásd az első sort az alábbi képen) az észlelt objektum neve Win32/Adware.Optmedia, az észlelt fájl neve pedig C:\Recovery\file.exe. A második sorban a megfelelő SHA-1 kivonattal rendelkező fájl kizárása mindig megtörténik az észlelt elem nevétől függetlenül.

Észlelési kivételek

?

Objektumfeltételek

Észlelt elem kizárása

Megjegyzés

C:\Recovery*.*	Win32/Adware.Optmedia	
2723cb8ca015209528d3fbdcaa801124f40ad4	Bármilyen kártevő	SuperApi.exe

Hozzáadás

Szerkesztés

Törlés

Importálás

Exportálás

OK

Mégse

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.

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 fájl csak az adott elemet érintő ellenőrzésből van kizárva. Ha később egy másik kártevő is megfertőzi a fájlt, a rendszer ezt észlelni fogja. Ez a kizárástípus csak egyes fertőzéstípusok esetén használható, és a riasztási ablakban hozható létre (kattintson a **További beállítások megjelenítése**, majd a **Felvétel a kivételek közé** elemre), illetve úgy, hogy az **Eszközök > Karantén** elemre kattint, a jobb gombbal a karanténba helyezett fájltra kattint, majd a helyi menüben kiválasztja a **Visszaállítás és kizárás az ellenőrzésből** menüpontot).
- **Kivonat** – Fájl kizárása a megadott kivonat alapján (SHA1), 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":"7.2.2055","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}
```

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

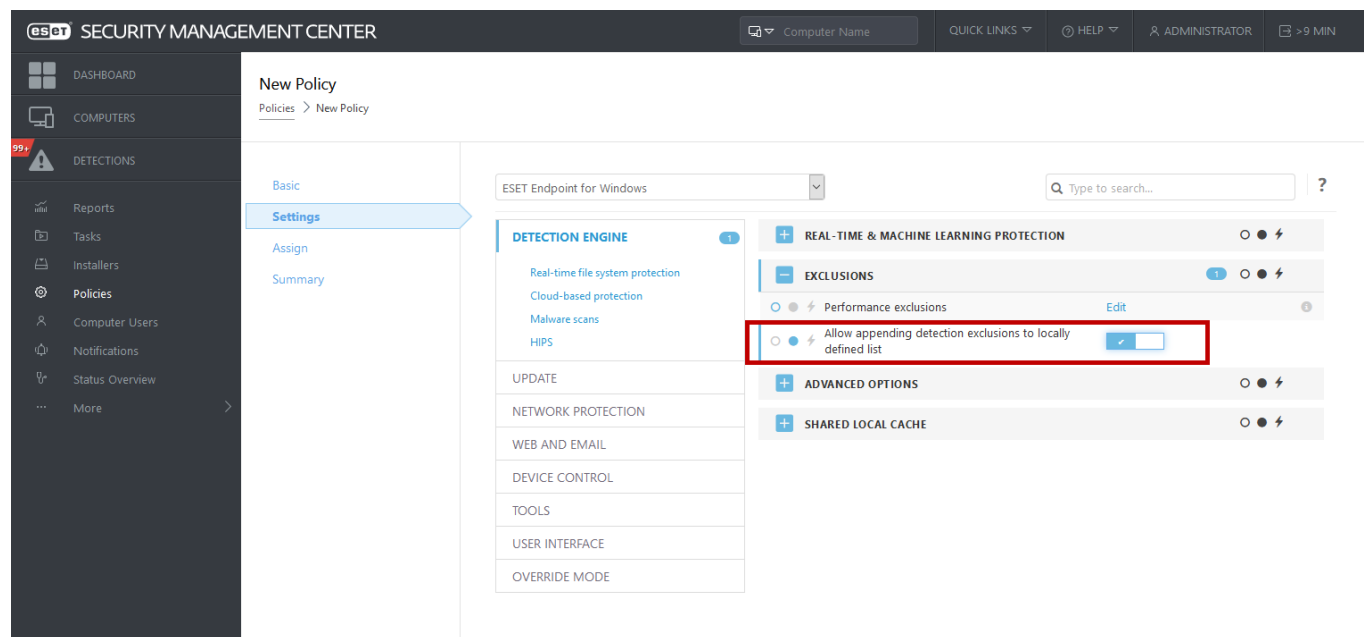
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

Az ESMC segítségével beállított észlelési kivételek

Az ESMC 7.1 [egy új varázslót tartalmaz az észlelési kivételek kezeléséhez](#) – létrehozhat egy észlelési kivételt, majd alkalmazhatja több számítógépre/csoportra.

A potenciális észlelési kivételek felülírása az ESMC 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 ESMC-ből.



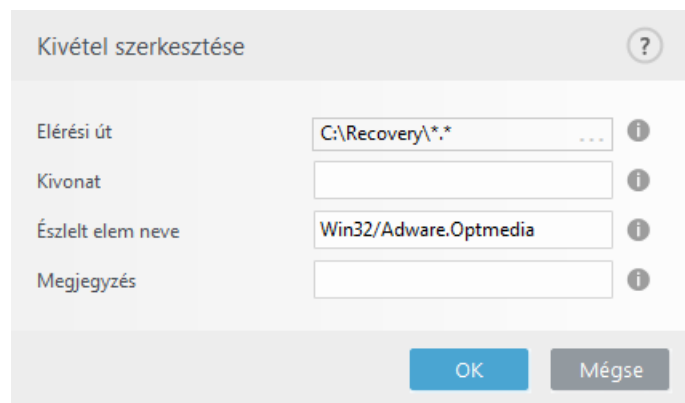
Észlelési kivétel felvétele vagy szerkesztése

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 Antivirus 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.

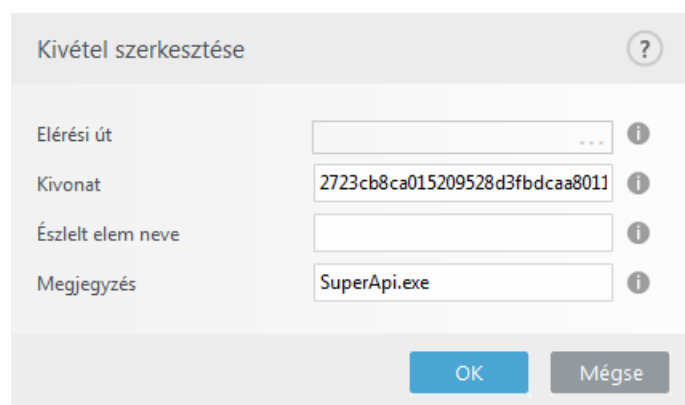
Tekintse meg az [Útvonal kivétel formátuma](#) című részt is.



Tekintse meg lent az [Észlelési kivételekről szóló példát](#).

Kivonat kizárása

Fájl kizárása a megadott kivonat alapján (SHA1), függetlenül a fájl típusától, tárolási helyétől, nevétől és kiterjesztésétől.



Kivételek a kártevő neve szerint

Ha ki szeretne zárni egy kártevőt, adjon meg érvényes kártevőnevet:

Win32/Adware.Optmedia

A következő formátumot is használhatja, amikor kizár egy fertőzést az ESET Endpoint Antivirus 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 kártevőkészletek 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.

Kivételek ?

Típus

Részletek

Elérési út: Leírás:	C:\Backup*.*
Elérési út: Leírás:	C:\pagefile.sys
Kártevő: Elérési út: Leírás:	@NAME=Win32/Adware.Optmedia C:\Recovery*.*
Kivonat: Leírás:	678C1422DE867141B947EA700E8A2D6114AFAE97 SuperApi.exe

Hozzáadás

Szerkesztés

Törlés

Mentés

Mégse

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 fájl szintű kártevővédelemben. Hasonló problémák léphetnek fel virtuális gépek élő áttelepítésekor. Az egyetlen hatékony módja ennek a két helyzetnek az elkerülésére a kártevőirtó szoftver inaktíválása. Bizonyos folyamatok kizárásával (például a biztonsági mentésre használt megoldás folyamatainak) a kizárt folyamat által végzett összes fájl műveletet 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.



Példa

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 Antivirus leállítja az adott folyamat felügyeletét, és nem ellenőrzi a folyamat által végrehajtott fájl műveleteket.



Fontos

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.



Megjegyzés

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.



Példa

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 Antivirus leállítja az adott folyamat felügyeletét, és nem ellenőrzi a folyamat által végrehajtott fájlműveleteket.



Fontos

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.

ThreatSense paraméterei

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.

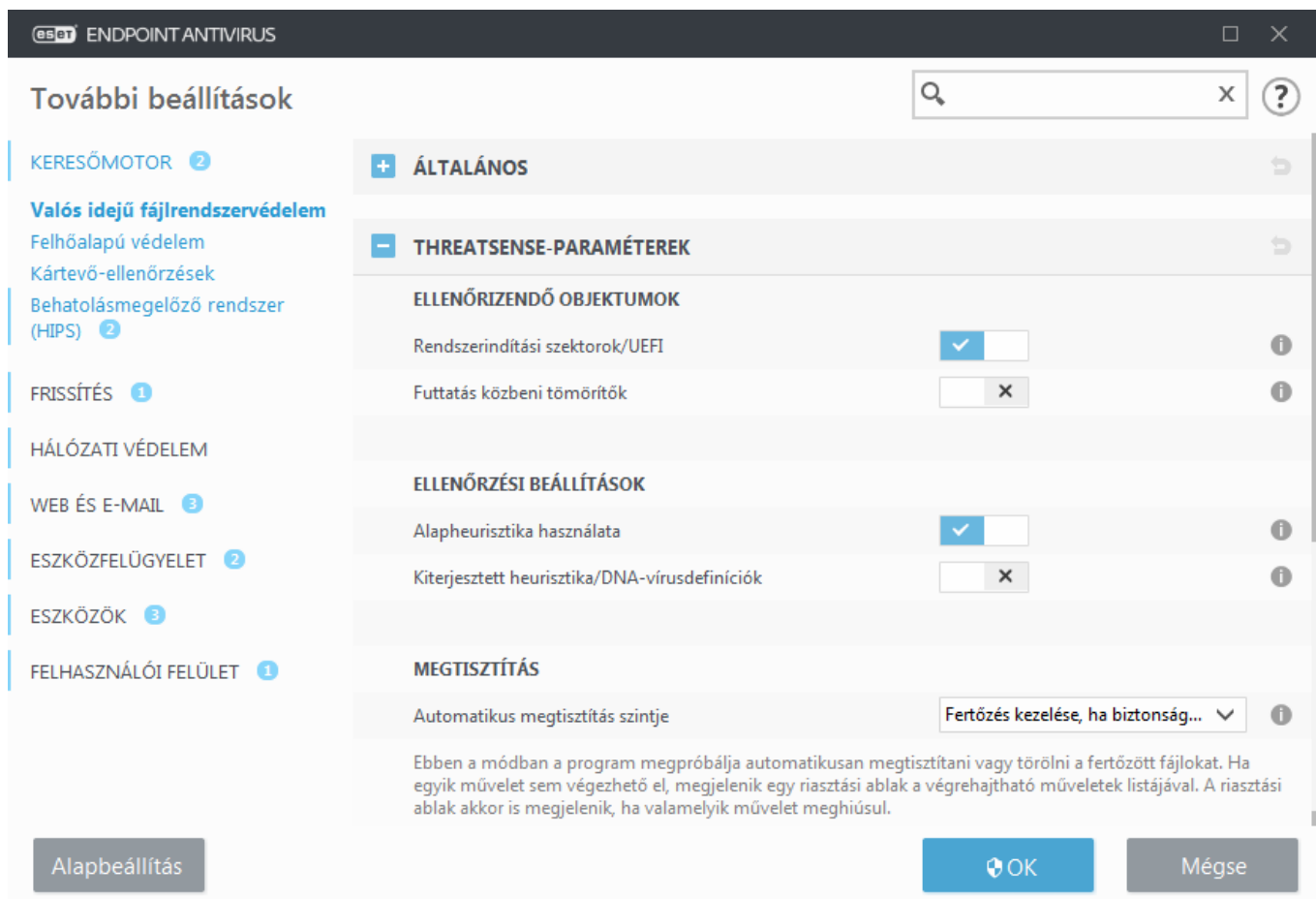
A ThreatSense motor beállítási lehetőségeivel több ellenőrzési paraméter megadható, többek között az alábbiak:

- Az ellenőrizendő fájltypusok 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 található-e kártevők. [További információk az UEFI-ről a szöszedetben.](#)

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 algoritmus. 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 Antivirus mit tegyen az objektumok megtisztítása során.

Kivételek

A kiterjesztés a fájlnev 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 leoptimálisabb beállításokat használja a leghatékonyabb ellenőrzési szint, ugyanakkor a leggyorsabb ellenőrzési sebesség biztosításához. A

különböző védelmi modulok intelligensen végzik az ellenőrzést, kihasználják és az adott fájl típusokhoz alkalmazzák a különböző ellenőrzési módszereket. Az optimalizálás letiltása esetén a program csak a felhasználók által az egyes modulok ThreatSense-alapbeállításában 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 az objektumok ellenőrzésének maximális időtartamát adhatja meg. Felhasználó által megadott érték esetén a víruskereső modul leállítja az objektum ellenőrzését, függetlenül attól, hogy az ellenőrzés befejeződött-e, vagy sem. 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. Alapértelmezett érték: korlátlan.



Megjegyzés

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 Antivirus 7.2-es és újabb verziójában

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.

ES

ENDPOINT ANTIVIRUS

További beállítások

KERESŐMOTOR 2

Valós idejű fájlrendszervédelem

Felhőalapú védelem

Kártevő-ellenőrzések

Behatolásmegelőző rendszer (HIPS) 2

FRISSÍTÉS 1

HÁLÓZATI VÉDELEM

WEB ÉS E-MAIL 3

ESZKÖZFELÜGYELET 2

ESZKÖZÖK 3

FELHASZNÁLÓI FELÜLET 1

ÁLTALÁNOS

THREATSENSE-PARAMÉTEREK

ELLENŐRIZENDŐ OBJEKTUMOK

Rendszerindítási szektorok/UEFI

☒

Futtatás közbeni tömörítők

☐

ELLENŐRZÉSI BEÁLLÍTÁSOK

Alapheurisztika használata

☒

Kiterjesztett heurisztika/DNA-vírusdefiníciók

☐

MEGTISZTÍTÁS

Automatikus megtisztítás szintje

Fertőzés kezelése, ha biztonság...

Ebben a módban a program megpróbálja automatikusan megtisztítani vagy törölni a fertőzött fájlokat. Ha egyik művelet sem végezhető el, megjelenik egy riasztási ablak a végrehajtható műveletek listájával. A riasztási ablak akkor is megjelenik, ha valamelyik művelet megghiúsul.

Alapbeállítás

OK

Mégse

Megtisztítási szintek az ESET Endpoint Antivirus 7.1-es és korábbi verziójában

Automatikus megtisztítás szintje	Leírás
----------------------------------	--------

90

Nincs megtisztítás	A program nem tisztítja meg automatikusan az észlelt elemeket, hanem megjelenít egy figyelmeztető ablakot, és a felhasználó választhat a műveletek közül. Ez a szint a tapasztalt felhasználóknak ajánlott, akik tisztában vannak azzal, hogy mi a teendő a fertőzések esetén.
Szokásos módon megtisztít	A program megkísérli az észlelt elemek automatikus megtisztítását vagy törlését egy előre megadott művelet alapján (a fertőzés típusától függően). Az észlelt elemek észlelését és törlését a program a képernyő jobb alsó sarkában megjelenő értesítéssel jelzi. Ha a megfelelő művelet automatikus kiválasztására nincs lehetőség, felkínál néhány utóműveletet. Ugyanez történik akkor is, ha az előre beállított műveletet nem lehet elvégezni.
Automatikusan megtisztít	A program megtisztítja vagy törli az összes észlelt elemet. A rendszerfájlok ez alól kivételt képeznek. Ha nem lehetséges a megtisztítás, a program egy figyelmeztető ablakban ajánl fel egy műveletet.

Az említett megtisztítási szint alkalmazására akkor kerül sor, amikor ESMC-házirendet állítanak be az ESET Endpoint Antivirus régebbi verzióhoz:

Megtisztítási szint az ESMC-házirendben	Alkalmazott megtisztítási szint
Mindig kezelje a fertőzést	Automatikusan megtisztít
Fertőzés kezelése, ha ez biztonságos. Egyéb esetben megtartás	Szokásos módon megtisztít
Fertőzés kezelése, ha ez biztonságos. Egyéb esetben rákérdezés*	Szokásos módon megtisztít
Mindig kérdezze meg a végfelhasználót	Nincs megtisztítás

*Az alapértelmezett érték a 7.2-es és újabb verzióra való frissítés során, amikor a **Szokásos módon megtisztít** beállítás van megadva az ESET Endpoint Antivirus termékben.

Ellenőrzésből kizárt fájlkiterjesztések

A kiterjesztés a fájlnev 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.



Megjegyzés

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.



Példa

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`).



Megjegyzés

Ha Windows operációs rendszerben meg szeretné nézni a fájlok pontos kiterjesztését (ha van), törölje az **Ismert fájl típusok kiterjesztéseinek elrejtése** opció bejelölését a **Vezérlőpult > Mappabeállítások > Nézet** (lap) beállításánál, 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 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.

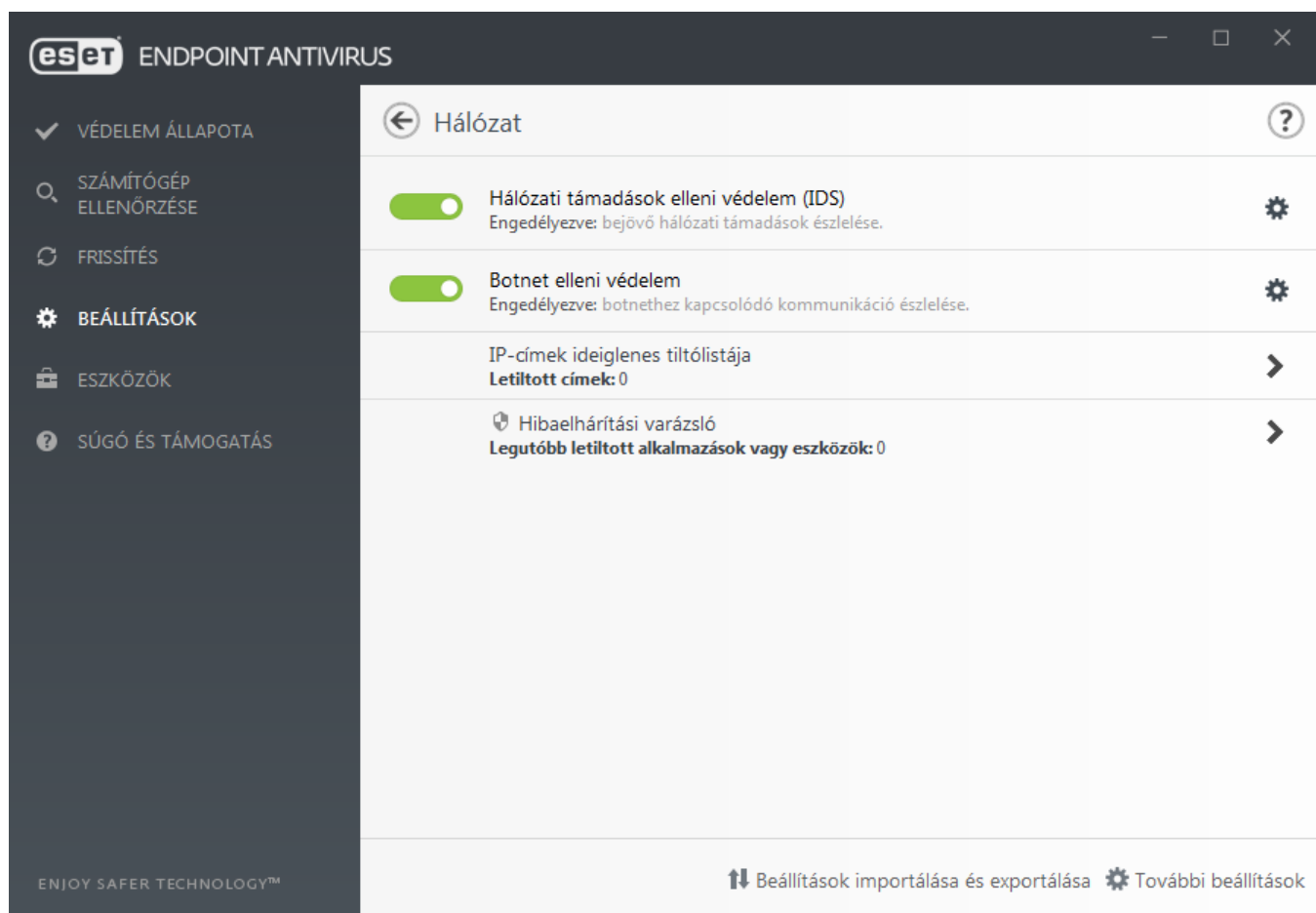
További ThreatSense-paraméterek a futtatott fájlokhoz – Alapértelmezés szerint a program [kiterjesztett heurisztikát](#) használ a fájlok futtatásakor. Ha be van jelölve, azt javasoljuk, hogy a rendszer teljesítményére gyakorolt hatás csökkentése végett tartsa meg az [optimalizálás](#) és az ESET LiveGrid®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

Hálózat

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

- **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 Antivirus 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).
- **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.



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 szöszedetben.](#)

IDS-kivételek – Ez a beállítás lehetővé teszi további szűrőbeállítások megadását a különböző típusú támadásokkal kapcsolatban.

Speciális szűrési beállítások

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



Értesítések és naplózás

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 különböző beállítások elérhetősége ezen a súgóoldalon

Az ESET-végponttermék és a tűzfalmodul típusától vagy verziójától, valamint az operációs rendszer verziójától függ, hogy a További beállítások (F5) > **Hálózati védelem** > **Hálózati támadások elleni védelem** lapon milyen beállítások állnak rendelkezésre. Előfordulhat, hogy néhányuk csak az ESET Endpoint Security szolgáltatáshoz áll rendelkezésre.

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 megnyitásokor** – Az MSRPC nevesített csövek megnyitásához használt ismert elkerülési technikák felismerése az SMB protokollban.
 - **Gyakori biztonsági rések és kitettségek felismerése** – Az SMB protokollon keresztülli 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 eljárásívási rendszerben.
- **RDP protokoll** – Észleli és letiltja a gyakori biztonsági réseket és kitettségeket az RDP protokollban (lásd fent).
- **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.
- **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** – Az MSRPC az elosztott számítógépes környezet (DCE) távoli eljárás hívtatási (RPC) mechanizmus megvalósítása a Microsoft által. Az MSRPC használhat továbbá az átvitelhez az SMB (hálózati fájl megosztási) protokollba továbbított nevesített csöveket (ncacn_np transport). Az MSRPC szolgáltatások a Windows rendszerek távoli hozzáférésehez 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).
- **TCP-kapcsolat állapotának ellenőrzése** – A jelölőnégyzet bejelölése esetén a program ellenőrzi, hogy minden TCP-csomag létező kapcsolathoz tartozik-e, és amelyik nem, azt elveti.
- **Inaktív TCP-kapcsolatok fenntartása** – Néhány alkalmazás működéséhez szükséges az általuk létrehozott TCP-kapcsolatok fenntartása, még ha esetleg inaktívak is. A jelölőnégyzet bejelölésével elkerülheti az inaktív TCP-kapcsolatok megszakítását.
- **TCP-protokolltúterhelés felismerése** – A módszer lényege, hogy a támadók nagyszámú kéréssel árasztják el a számítógépeket vagy szervereket (lásd még: [DoS, szolgáltatásmegtagadási támadások](#)).
- **ICMP-protokollüzenet ellenőrzése** – Az ilyen típusú támadások az ICMP protokoll gyenge pontjait használják ki (lásd még: [DoS, szolgáltatásmegtagadási támadások](#)).
- **Fedett adatok felismerése az ICMP-csomagokban** – A jelölőnégyzet bejelölése esetén a program ellenőrzi, hogy az ICMP protokollt nem adatátvitelre használják-e. Számos kártékony technika az ICMP protokollt használja a tűzfal kikerülésére.

A sűgóoldal frissített verzióját ebben az [ESET-tudásbáziscikkben](#) tekintheti meg.

IDS-kivételek

Bizonyos helyzetekben az [IDS \(Intrusion Detection Service\)](#) potenciális támadásként észleli a routerek és az egyéb belső hálózati eszközök közötti kommunikációt. Az IDS megkerüléséhez például hozzáadhatja az ismert biztonságos címet „Az IDS-észlelésből kizárt címek” listájához.



Ábrákkal ellátott útmutató


Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- [IDS-kivételek létrehozása munkaállomásokon az ESET Endpoint Antivirus alkalmazásban](#)
- [IDS-kivételek létrehozása munkaállomásokra az ESET Security Management Center alkalmazásban](#)

Oszlopok

- **Riasztás** – A riasztás 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/álhálózatok listája. A címeket vesszővel elválasztva kell megadni.
- **Tiltás** – Minden rendszerfolyamathoz saját alapértelmezett viselkedés és hozzárendelt művelet (tiltás vagy engedélyezés) tartozik. Ha felül szeretné bírálni az ESET Endpoint Antivirus 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 eseményeket [ESET Endpoint Antivirus naplófájlokba](#). A **Nem** beállítást válassza, ha nem szeretne eseményeket naplózni. A rendelkezésre álló lehetőségek az **Alapértelmezett/Igen/Nem**.

IDS-kivételek kezelése

- **Hozzáadás** – Új IDS-kivétel létrehozása.
- **Szerkesztés** – Meglévő IDS-kivétel szerkesztése.
- **Eltávolítás** – A kijelölt kivétel eltávolítása az IDS-kivételek listájáról.
-  **Tetejére/Fel/Le/Aljára** – A kivételek prioritási szintjének módosítása (a kivételek értékelése fentről lefelé történik).



Példa

Ha értesítést szeretne megjeleníteni, és naplózni szeretne minden alkalommal, amikor az esemény fellép:

- 1.A **Hozzáadás** gombra kattintva adja hozzá az új IDS-kivételt.
- 2.Válassza ki a kívánt riasztást a **Riasztás** legördülő menüben.
- 3.Kattintson a ... ikonra, majd válassza ki annak a fájlnek az elérési útvonalát, amelyre alkalmazni szeretné az értesítést.
- 4.Hagyja meg az **Alapértelmezett** beállítást a **Tiltás** legördülő menüben. Ezzel az ESET Endpoint Antivirus 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.



Példa

Ha nem szeretne ismétlődő értesítéseket kapni egy olyan típusú riasztás esetén, amelyet nem tart veszélyesnek:

- 1.A **Hozzáadás** gombra kattintva adja hozzá az új IDS-kivételt.
- 2.Válassza ki a kívánt riasztást a **Riasztás** legördülő menüben – például **Biztonsági bővítmények nélküli SMB-munkamenet**..
- 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-kivétel létrehozása a feltételezett kártevőhöz a kommunikáció engedélyezésére vonatkozó beállításokkal.

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



Megjegyzés

Az értesítési ablakban megjelenő információk az észlelt kártevő típusától függően eltérhetnek. A kártevőkről és a kapcsolódó fogalmakról a [Távrolról 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**.

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 Antivirus programból a **Beállítások > Hálózati védelem > IP-címek ideiglenes tiltólistája** lapra.

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 lejáratá 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.

Az ESET Tűzfallal kapcsolatos problémák megoldása

Ha a telepített ESET Endpoint Antivirus 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](#)
- [Speciális PCAP-naplózás](#)
- [Protokollszűrési problémák megoldása](#)

Hibaelhárítási varázsló

A Hibaelhárítási varázsló értesítések küldése nélkül figyeli a letiltott kapcsolatokat, és végigvezeti Önt a hibaelhárítási eljárás 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.

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-kivételt 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.



Megjegyzés

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 Antivirus 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 Antivirus 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.



Megjegyzés

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.

Speciális PCAP-naplózás

Ezzel a funkcióval összetettebb naplófájlok készülhetnek az ESET terméktámogatása számára. Mivel a funkció hatalmas naplófájlt hoz létre és lelassítja a számítógépet, csak az ESET terméktámogatásának kérésére használja.

1. A **További beállítások > Eszközök > Diagnosztika** részben kapcsolja be **protokollszűrés speciális naplózásának engedélyezése** beállítást.
2. Próbálja meg reprodukálni a tapasztalt problémát.
3. Tiltsa le a speciális PCAP-naplózást.
4. A PCAP-naplófájl ugyanabban a könyvtárban található, amelyben a diagnosztikai memóriakép létrejön:
 - Microsoft Windows Vista vagy újabb verzió

C:\ProgramData\ESET\ESET Security\Diagnostics

- Microsoft Windows XP

C:\Documents and Settings\All Users\...

Protokollszűrés 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-protokollszerűsítés, 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-protokollszerűsítést 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 protokollszerűsítésből (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 protokollszerűsítésből 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

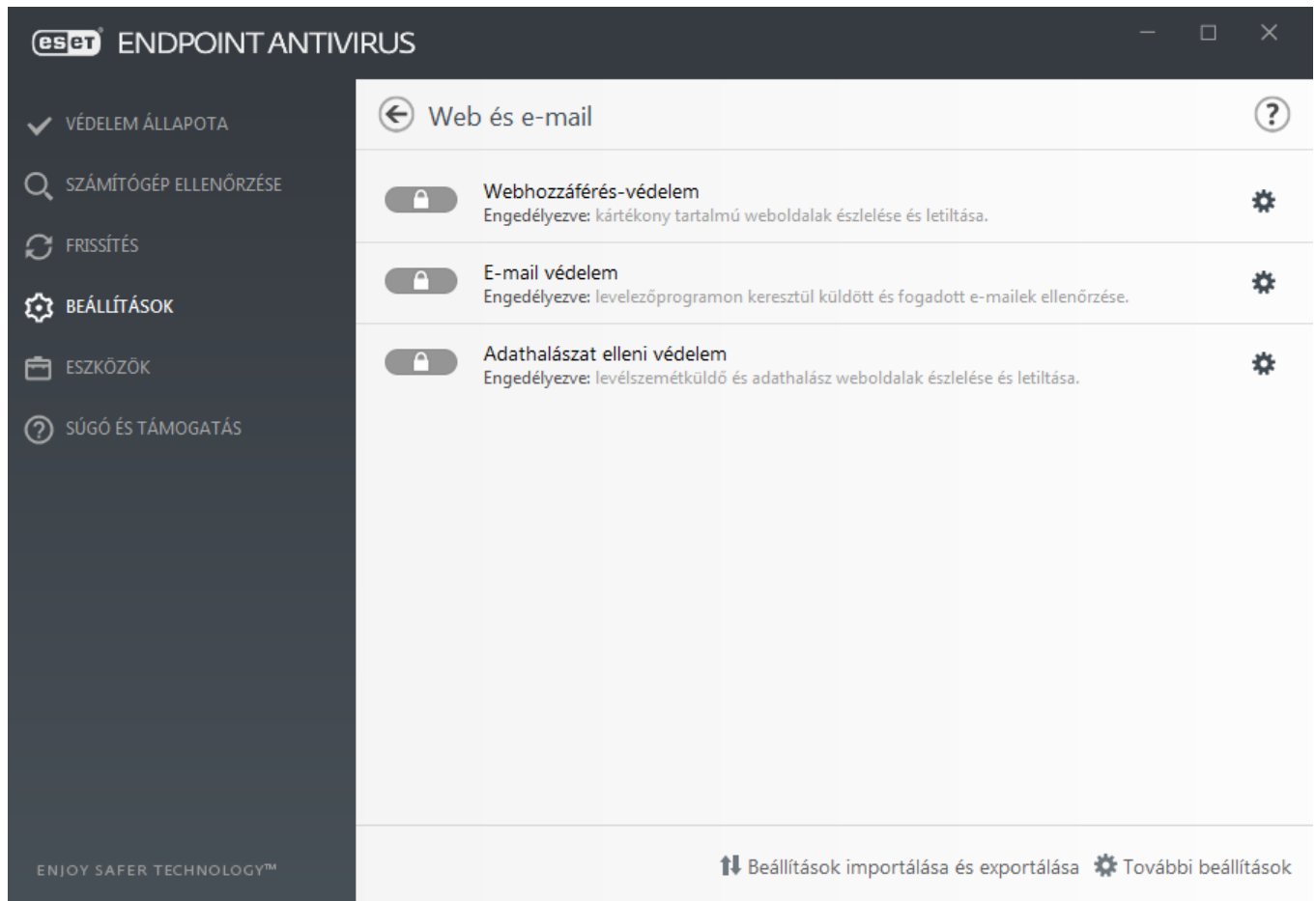
Az SSL-protokollszerűsítés engedélyezésekor az ESET Endpoint Antivirus meggyőződik arról, hogy a telepített alkalmazások megbíznak abban a módban, ahogyan a program az SSL-szűrést végzi. Ehhez egy tanúsítványt importál azok tanúsítványtárába. Egyes alkalmazások esetében ez nem lehetséges, amíg fut az 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 megghiúsult. Elsőként győződjön meg arról, hogy nem fut a fent említett alkalmazások egyike sem. Ezután tiltsa le, majd engedélyezze újra az SSL-protokollszerűsítést. 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.



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 Antivirus a levelezőprogramtól érkező minden kommunikáció ellenőrzésére képes.

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 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 Antivirus 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.



Példa kizárt IP-címekre

IPv4-cím és -maszk:

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

IPv6-cím és -maszk:

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

Kizárt alkalmazások

A rendszer nem végez 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 megjelennek, miután a **Hozzáadás** gombra kattintott.

Szerkesztés – A listában kijelölt bejegyzések szerkesztése.

Törlés – A kijelölt bejegyzések eltávolítása a listáról.

Kizárt alkalmazások

C:\Windows\System32\svchost.exe
C:\Program Files\Notepad++\notepad++.exe

Hozzáadás

Szerkesztés

Törlés

OK

Mégse

Kizárt IP-címek

A listában szereplő IP-címeken nem végez protokollsűrűst 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.

Kizárt IP-címek

10.1.2.3
10.2.1.1-10.2.1.10
192.168.1.0/255.255.255.0
fe80::b434:b801:e878:5975
2001:21:420::/64

Hozzáadás

Szerkesztés

Törlés

OK

Mégse

SSL/TLS

Az ESET Endpoint Antivirus 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	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 Antivirus viselkedésének testreszabását adott alkalmazásokhoz.

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



Megjegyzés

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

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

Ha a tanúsítvány érvénytelen vagy sérült – Ez azt jelenti, hogy a tanúsítvány vagy lejárt, vagy nem megfelelő az aláírása. Azt javasoljuk, hogy ilyen esetben hagyja bejelölve a **Tiltsa le a tanúsítványt használó kommunikációt** választógombot.



Ábrákkal ellátott példák

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, ön aláírt 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 egy tanúsítvány nem szerepel a megbízható legfelső szintű tanúsítványok listájában, az ablak színe piros lesz, ellenkező esetben zöld.

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

Az érvénytelen vagy sérült tanúsítványok lejártak, vagy helytelenül lettek ön aláírva. 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 Antivirus 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-protokollszűrés 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 Antivirus alkalmazásnak **mellőznie** kell az adott adatforgalmat ahhoz, hogy működőképes maradjon.



Ábrákkal ellátott példák

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- [Tanúsítványokkal kapcsolatos értesítések az ESET-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 Antivirus viselkedésének testreszabására adott SSL tanúsítványokhoz és olyan műveletek megjegyzésére, amelyeket akkor választ ki, ha az **SSL/TLS-protokollszűrés 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 Antivirus 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 – Az alkalmazás neve.

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.

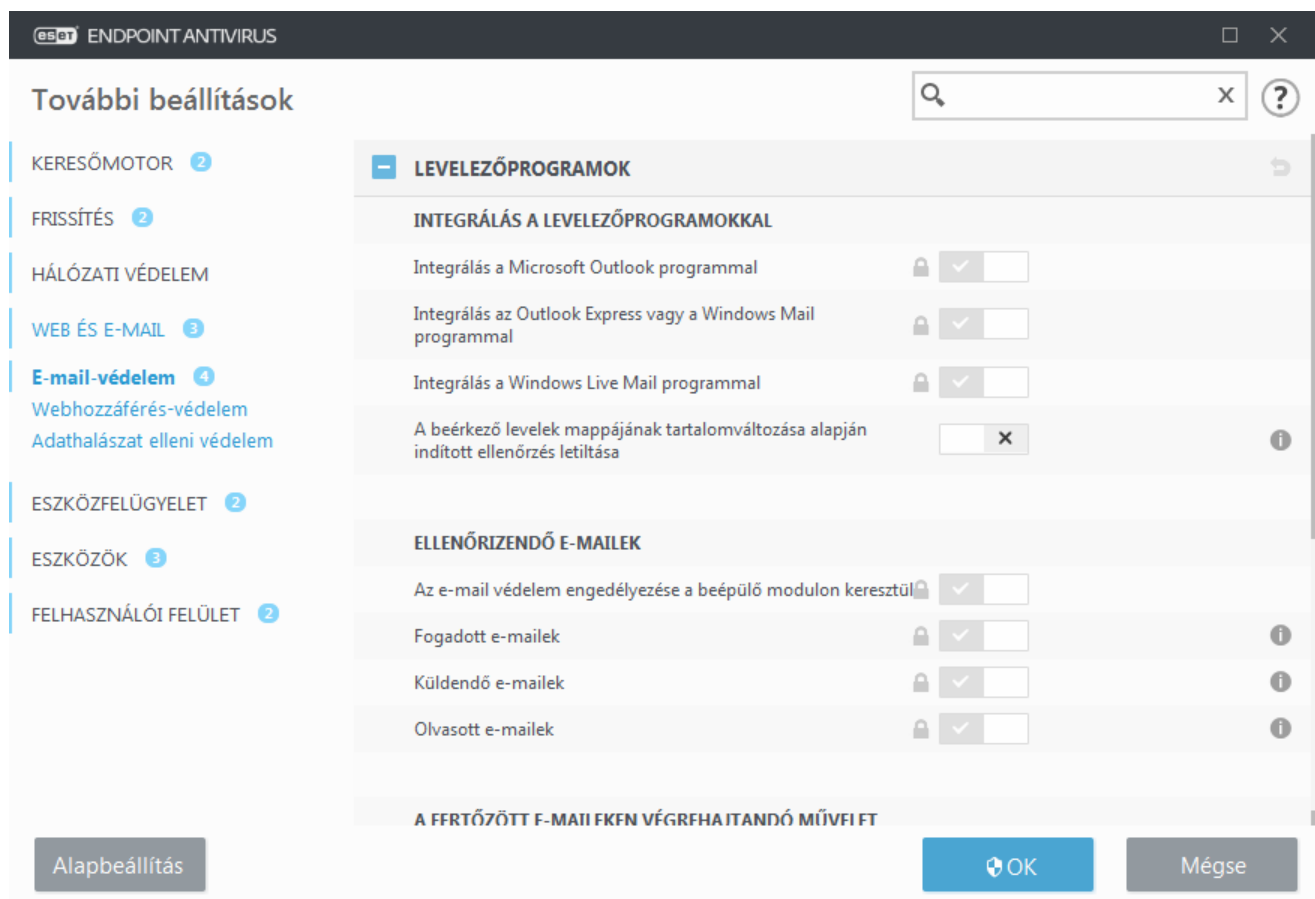
Törlés – Jelölje ki az eltávolítandó tanúsítványt, majd kattintson az **Eltávolítás** gombra.

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

kiléphet.

E-mail védelem

Az ESET Endpoint Antivirus levelezőprogrammal való integrálásával növelhető az e-mailekben terjesztett kártékony kódok elleni aktív védelem. A támogatott levelezőprogramok integrálása az ESET Endpoint Antivirus programban engedélyezhető. Ha integrálva van a levelezőprogramba, az ESET Endpoint Antivirus 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.



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 verziók teljes listáját az [ESET tudásbáziscikke](#) tartalmazza.

Ha az e-mailek beolvasásakor a rendszer lassulását tapasztalja, jelölje be **A beérkező levelek mappájának tartalomváltozása alapján indított ellenőrzés letiltása** jelölőnégyzetet.

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.



Megjegyzés

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, megválaszták, vagy törölték-e. A szabályozást biztosító védelmi modul automatikusan elindul a rendszer indításakor, majd ezután aktív marad a memóriában.

Az ESET Endpoint Antivirus 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.

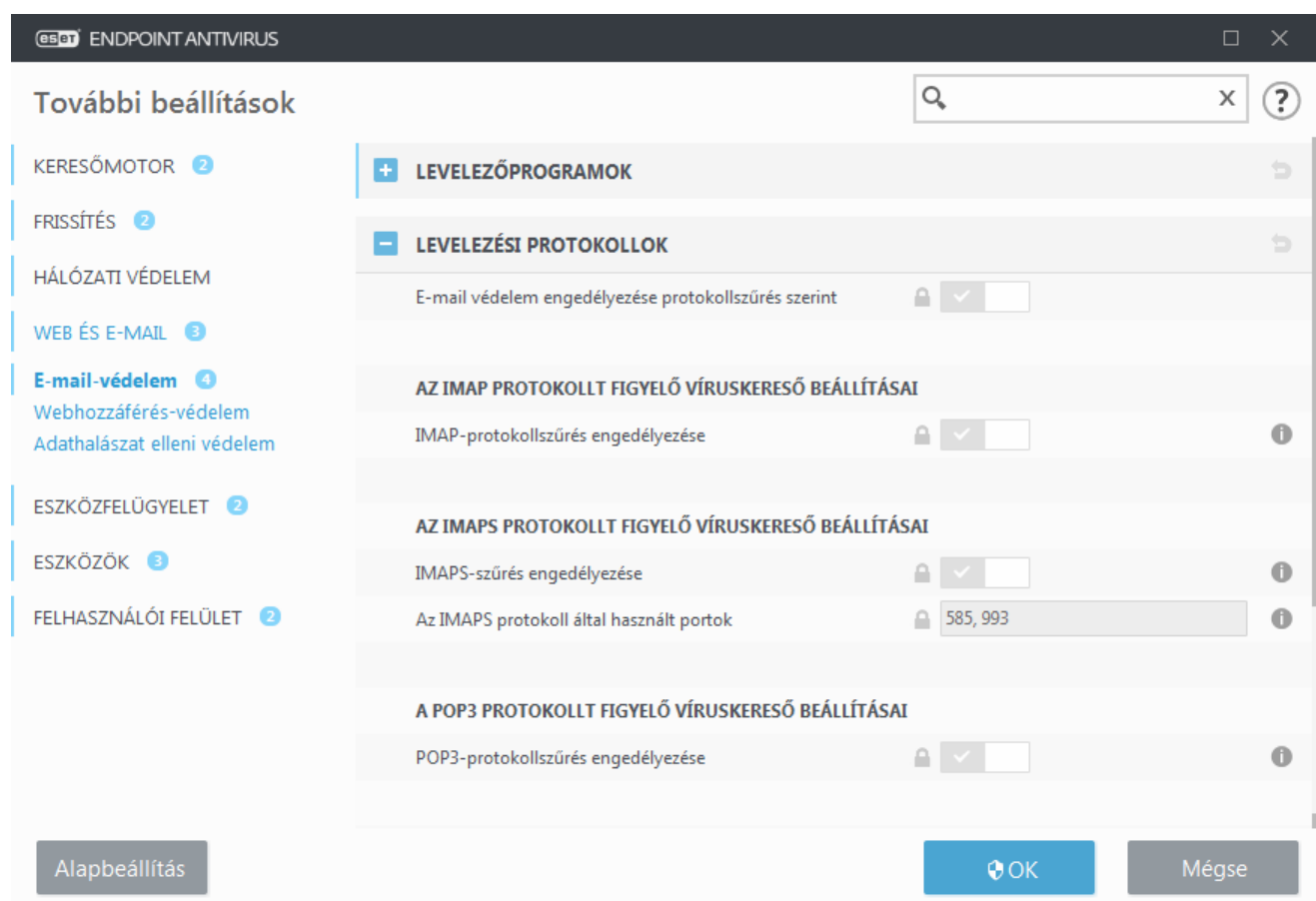
Az MAPI protokoll nem áll ellenőrzés alatt. A Microsoft Exchange szerverrel folytatott kommunikáció azonban ellenőriztethető az [integrációs modullal](#) az olyan levelezőprogramokban, mint a Microsoft Outlook.

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 Antivirus 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 Antivirus 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 az ellenőrzés további kommunikációs portokra is kiterjeszthető. Több portszámot vesszővel elválasztva kell megadni.

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-riasztások és értesítések

A funkció beállításai a **További beállítások** lapon találhatók a **Web és e-mail** > **E-mail védelem** > **Riasztások és értesítések** részen.

Miután a program ellenőrzi 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 verziók teljes listáját az [ESET tudásbázis](#) tartalmazza.

Microsoft Outlook-eszköztár

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

ESET Endpoint Antivirus – Az ikonra kattintva megnyithatja az ESET Endpoint Antivirus 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.

Outlook Express- és Windows Mail-eszköztár

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

ESET Endpoint Antivirus – Az ikonra kattintva megnyithatja az ESET Endpoint Antivirus 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.

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 Antivirus 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.

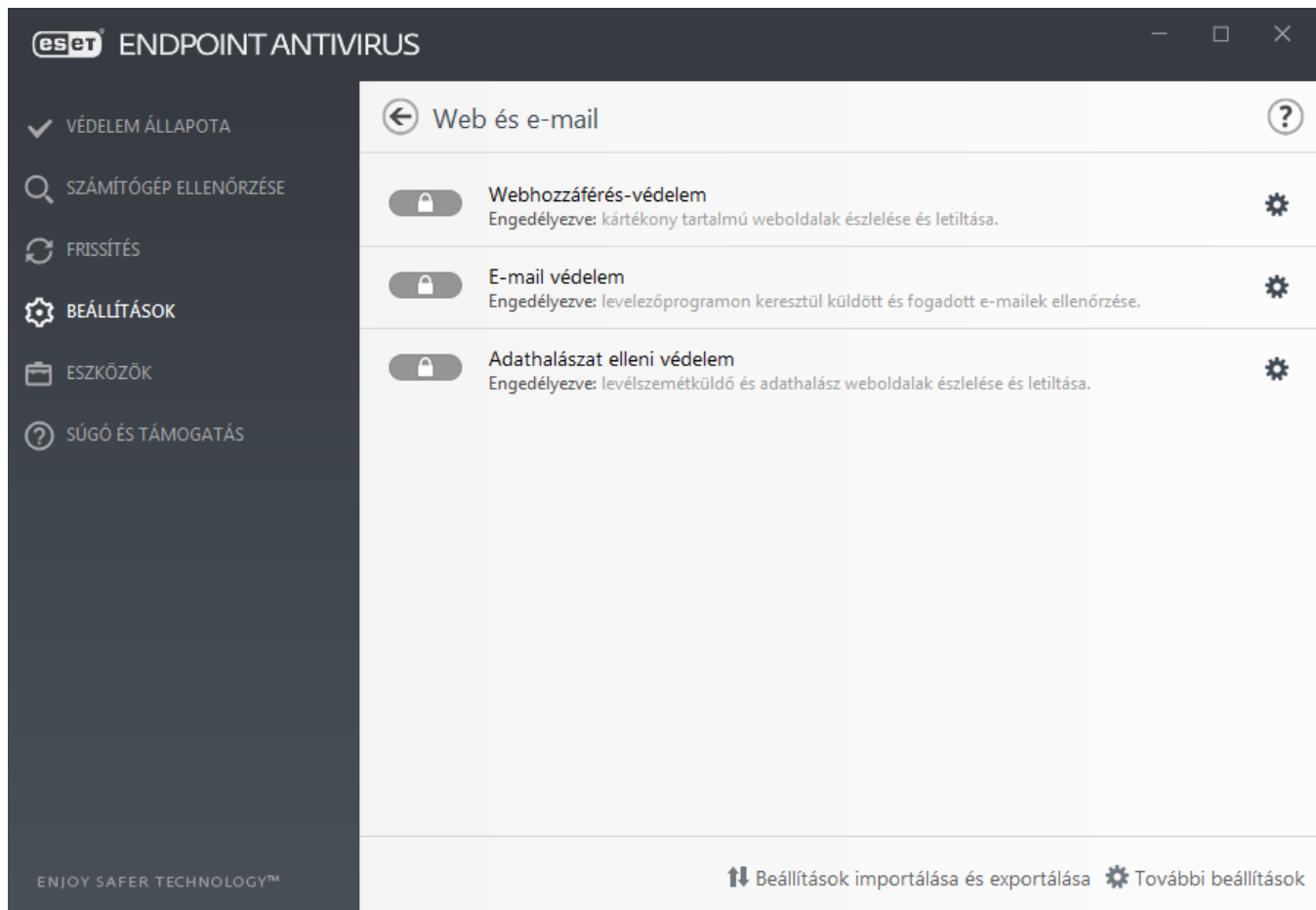
A már ellenőrzött üzenetek újraellenőrzése – A jelölőnégyzet bejelölése esetén újraellenőrizheti a korábban már ellenőrzött üzeneteket.

Webhozzáférés-védelem

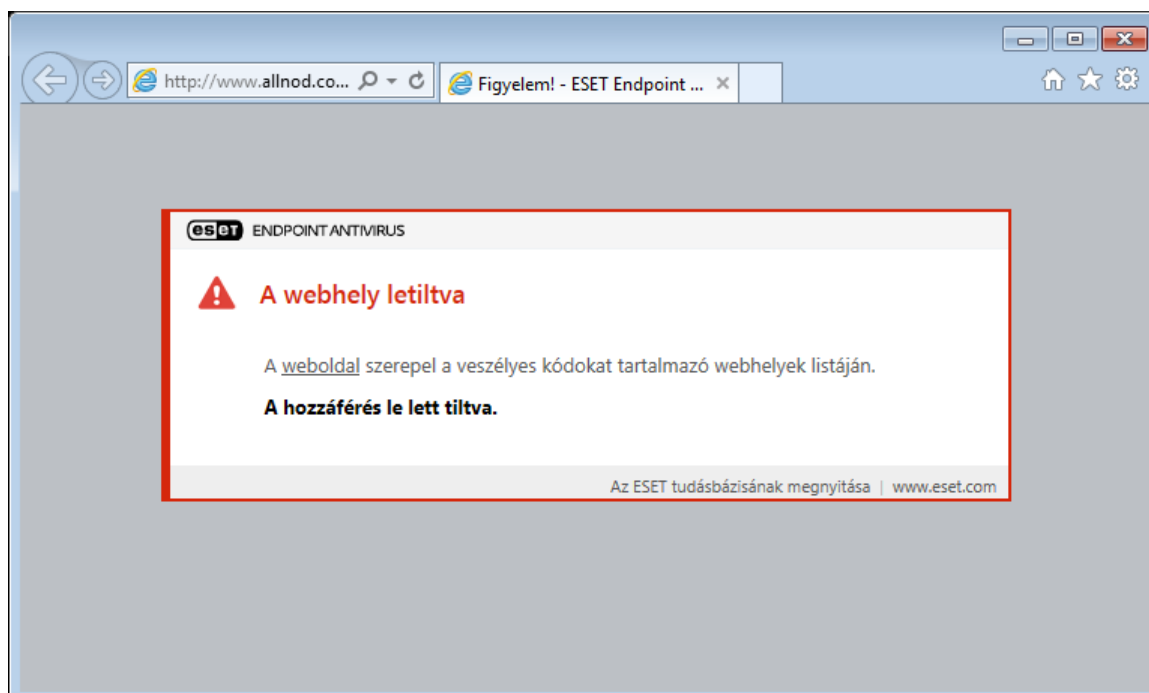
Az internetelérés a személyi számítógépek alapvető szolgáltatásaihoz tartozik. Sajnos a kártevők is ezt használják ki a terjedéshez. A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP és a HTTPS (titkosított kommunikáció) protokollon alapuló szabályokat.

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 Antivirus 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:





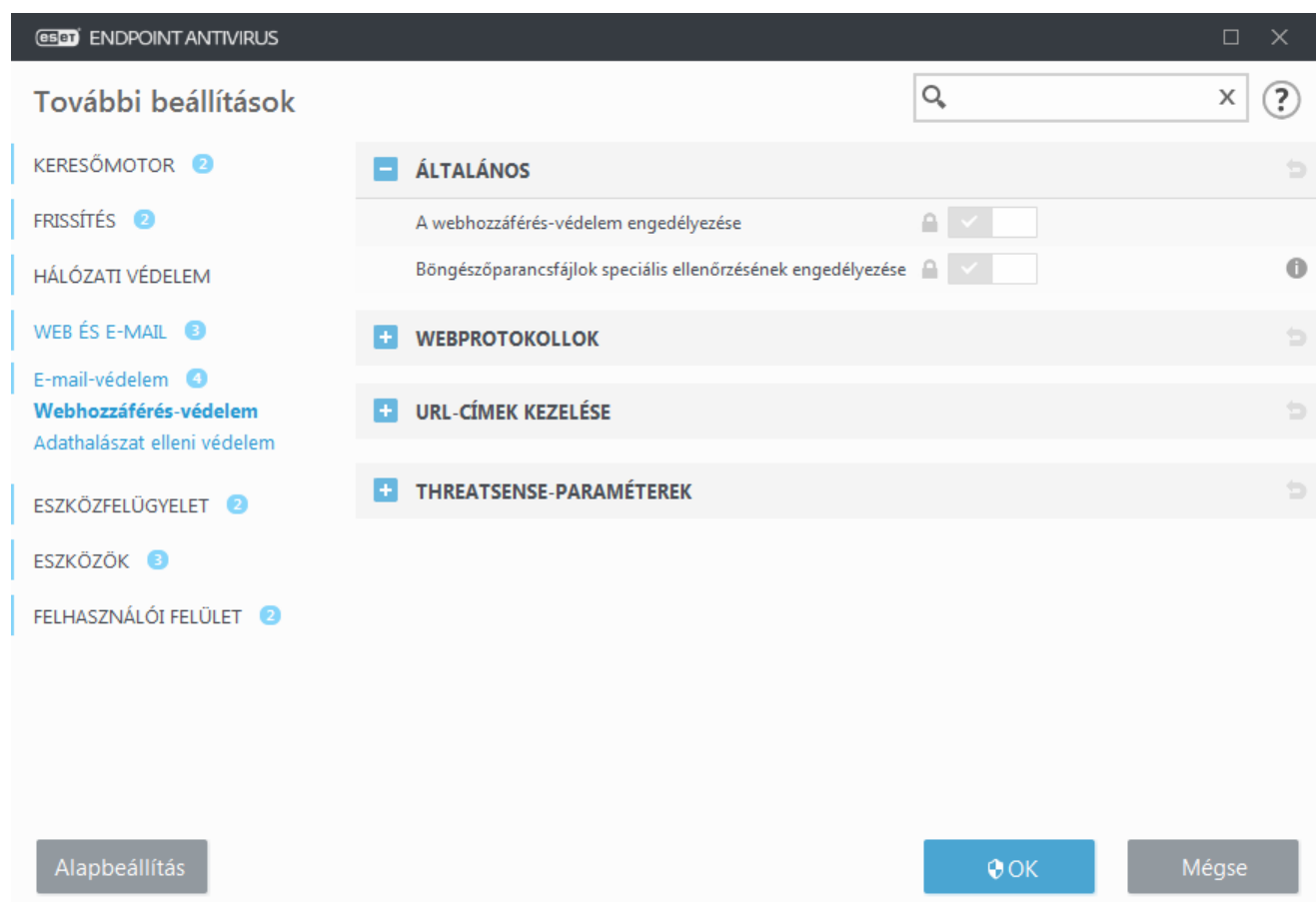
Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- [Biztonságos webhely feloldása önálló munkaállomáson az ESET Endpoint Antivirus programban](#)
- [Biztonságos webhely feloldása végponton az ESET Security Management Center segítségével](#)

A **További beállítások (F5) > Web és e-mail > Webhozzáférés-védelem** lehetőséget választva az alábbi beállítások érhetők el:

- **Általános** – A funkció engedélyezése vagy letiltása a További beállításokban.
- **Webprotokollok** – Segítségével konfigurálhatja azoknak a szabványos protokolloknak a figyelését, amelyeket a legtöbb internetböngésző használ.
- **URL-címek kezelése** – Segítségével letilthat, engedélyezhet és kizárhat az ellenőrzésből URL-címeket.
- **A ThreatSense paraméterei** – Itt további víruskeresési beállításokkal megadhatja az ellenőrizendő objektumok típusát (e-mailek, archívumok stb.), a webhozzáférés-védelmi észlelési módszereket stb.



A webhozzáférés-védelem haladó beállításai

A **További beállítások (F5) > Web és e-mail > Webhozzáférés-védelem > Általános** lehetőséget választva az alábbi beállítások érhetők el:

A webhozzáférés-védelem engedélyezése – Ha letiltja, a rendszer nem futtatja a [webhozzáférés-védelmet](#) és az

[adathalászat elleni védelmet.](#)

Böngészőparancsfájlok speciális ellenőrzésének engedélyezése – Ha engedélyezve van, a keresőmotor az internetböngészők által végrehajtott összes JavaScript programot ellenőrizni fogja.



Megjegyzés

Kifejezetten javasoljuk, hogy hagyja engedélyezve a Webhozzáférés-védelem funkciót.

Webprotokollok

Az ESET Endpoint Antivirus 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 Antivirus támogatja a HTTPS-protokollszűrést is. A HTTPS kommunikációtípus titkosított csatornán keresztül továbbítja az adatokat a szerver és a kliens között. Az ESET Endpoint Antivirus 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-címeteket.

Ha a HTTP-weboldalak mellett a HTTPS-címeteket 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.



Bizonyos fájlkiterjesztések letiltása vagy engedélyezése

Letilthatja vagy engedélyezhet adott fájltypusok megnyitását is az internetböngészés során az URL-címek kezelése segítségével. Ha például a végrehajtható fájlok megnyitását szeretné megakadályozni, a legördülő listában válassza azt a listát, amelyben blokkolni kívánja az ilyen fájlokat, és adja meg az "***.exe" maszkot.



Megbízható tartományok

Nem kerül sor a címek szűrésére, ha aktív a **Web és e-mail > SSL/TLS > Megbízható tartományokkal való kommunikáció kizárása** beállítás, és a tartomány megbízható.

Címlista

Lista neve	Címtípusok	Lista leírása
Engedélyezett címek listája	Engedélyezett	
Letiltott címek listája	Letiltva	
Ellenőrzésből kizárt címek listája	A megtalált kártevő mell...	

Hozzáadás Szerkesztés Törlés

Ha helyettesítő karaktert (*) ad a letiltott címek listájához, az engedélyezett címek listájában szereplők kivételével az összes URL-címet letilthatja.

OK Mégse

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.

Címlista

Lista neve	Címtípusok	Lista leírása
Engedélyezett címek listája	Engedélyezett	
Letiltott címek listája	Letiltva	
Ellenőrzésből kizárt címek listája	A megtalált kártevő mell...	

HozzáadásSzerkesztésTörlés

Ha helyettesítő karaktert (*) ad a letiltott címek listájához, az engedélyezett címek listájában szereplők kivételével az összes URL-címet letilthatja.

OKMégse



Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

- [Biztonságos webhely feloldása önálló munkaállomáson az ESET Endpoint Antivirus programban](#)
- [Biztonságos webhely feloldása végponton az ESET Security Management Center segítségével](#)

További információt az [URL-címek kezelése](#) című témakörben talál.

Új URL-címlista létrehozása

Ebben a csoportban megadhatja a letiltott vagy engedélyezett, illetve az ellenőrzésből kizárt URL-címeket és -maszkokat definiáló listákat.

Új lista létrehozásakor az alábbi beállításokat adhatja meg:

Címlista típusa – Három előre definiált listatípus áll rendelkezésre:

- **Ellenőrzésből kizárva** – A program a listában szereplő egyetlen cím esetén sem keres kártevő kódokat.
- **Letiltott** – Az ebben a listában szereplő címeket nem érheti el a felhasználó.
- **Engedélyezett** – Ha a házirend úgy van beállítva, hogy használja ezt a funkciót, és a helyettesítő karakter (*) értéke hozzá van adva ehhez a listához, akkor a listán szereplő címeket akkor is elérheti, ha ezek a címek a tiltott listában is szerepelnek.

Lista neve – Ebben a mezőben adható meg a lista neve. A mező nem érhető el, ha éppen szerkeszti a három előre definiált lista egyikét.

Lista leírása – A mezőben rövid ismertetőt írhat a listához (ez nem kötelező). A mező nem érhető el, ha éppen szerkeszti a három előre definiált lista egyikét.

Lista aktiválása – a lista aktiválásához válassza a csúszkát.

Értesítés alkalmazáskor – Ha értesülni szeretne arról, hogy egy adott listát felhasználnak egy Ön által már felkeresett HTTP-webhely értékeléséhez, válassza a csúszkát. Ebben az esetben értesítést kap például arról, ha egy webhelyet letiltanak vagy engedélyeznek, mivel az szerepel a letiltott vagy az engedélyezett címek listáján. Az értesítésben szerepelni fog a szóban forgó webhelyet megadó lista neve.

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

Vezérlőelemek

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

Szerkesztés – A meglévő cím módosítása a listában. Csak a **Hozzáadás** gombbal létrehozott címek esetén használható.

Eltávolítás – Meglévő címek eltávolítása a listából. Csak a **Hozzáadás** gombbal létrehozott címek esetén használható.

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

URL-maszk hozzáadása

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

Az ESET Endpoint Antivirus 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 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 *.tartomány.hu maszk például nem fog megfelelni a <http://barmelytartomány.hu/barmelyeleresiut#.tartomány.hu> címnek (ilyen utótag bármelyik URL-címhez hozzáfűzhető anélkül, hogy az hatással lenne a letöltésre). A „*” továbbá egy üres sztringnek is megfelel ebben a speciális esetben. Ennek célja, hogy egyetlen maszk használatával lehessen engedélyezni egy teljes tartományt a hozzá tartozó esetleges altartományokkal együtt. A *.tartomány.hu maszk például a <http://tartomány.hu> címnek is megfelel. A *.tartomány.hu használata helytelen lenne, mivel az a <http://masiktartomány.hu> címnek is megfelelné.

Adathalászat elleni védelem

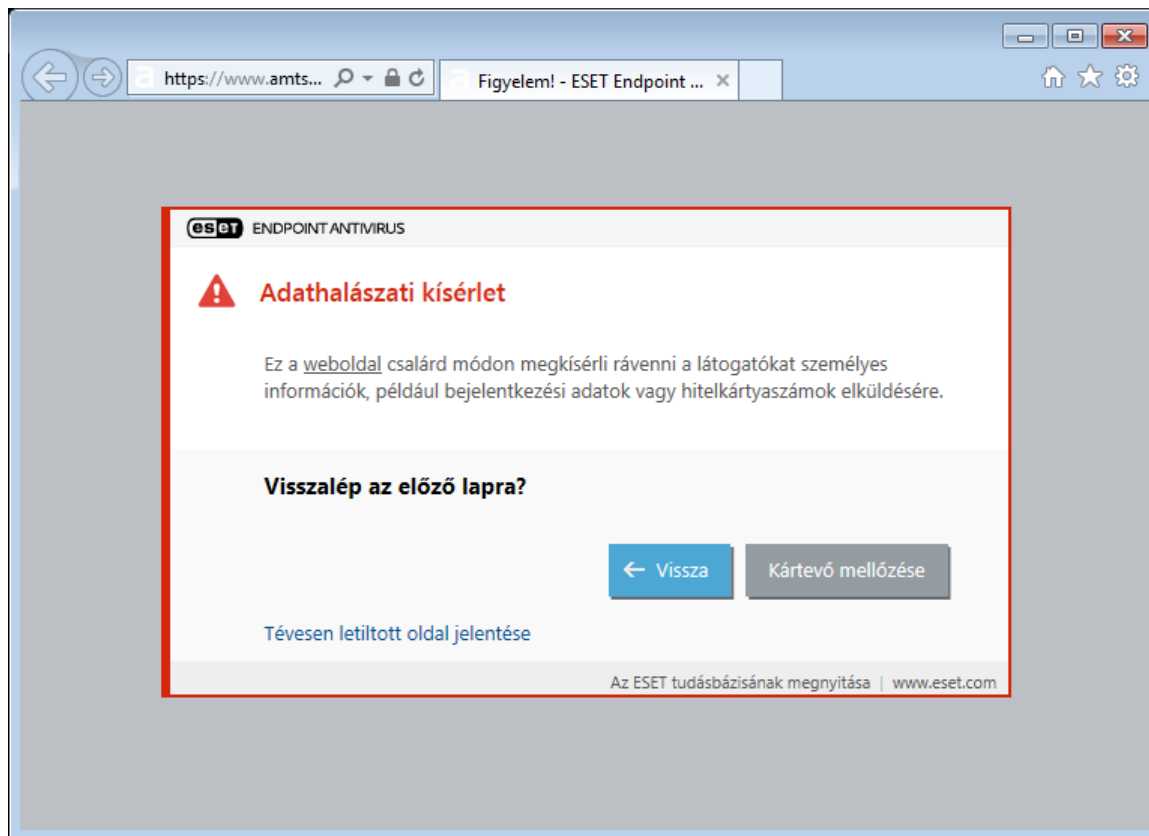
Az adathalászat kifejezés olyan bűnözői tevékenységet határoz meg, amely pszichológiai manipulációt alkalmaz (vagyis a felhasználót bizalmas információk kiszolgáltatására veszi rá). Az adathalászat gyakran bizalmas adatok, többek között bankszámlaszámok, PIN kódok vagy más adatok megszerzésére irányul. Erről a tevékenységről a [szószedetben](#) olvashat bővebben. Az ESET Endpoint Antivirus az ilyen tartalommal rendelkező ismert weboldalak letiltásának lehetővé tételével támogatja az adathalászat elleni védelmet.

Javasoljuk, hogy engedélyezze az adathalászat elleni védelmet az ESET Endpoint Antivirus alkalmazásban. Ehhez nyissa meg a **További beállítások** párbeszédpanelt (az F5 billentyű lenyomásával), és keresse meg a **Web és e-mail > Adathalászat elleni védelem** lehetőséget.

A [tudásbáziscikkünk](#) további információkat tartalmaz az ESET Endpoint Antivirus adathalászat elleni védelméről.

Adathalász webhely elérése

Az ismert adathalász webhelyek megnyitásakor az alábbi párbeszédpanel jelenik meg a böngészőben. Ha továbbra is meg szeretné nyitni a webhelyet, kattintson a **Tovább a webhelyre** (nem javasolt) gombra.



Megjegyzés

Az engedélyezőlistán szereplő lehetséges adathalász webhelyek alapértelmezés szerint néhány óra múlva lejárnak. Webhelyek végleges engedélyezéséhez használhatja az [URL-címkék kezelése](#) eszközt. Az (F5 billentyű lenyomásával) megnyitható **További beállítások** párbeszédpanelen kattintson a **Web és e-mail > Webhozzáférés-védelem > URL-címkék 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.



Megjegyzés

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.).

A program frissítése

Az ESET Endpoint Antivirus 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 kártevők elleni maradéktalan védelem fontos összetevője a víruskereső motor és a programösszetevők frissítése, ezért érdemes figyelmet fordítani 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 Antivirus 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.



Megjegyzés

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

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

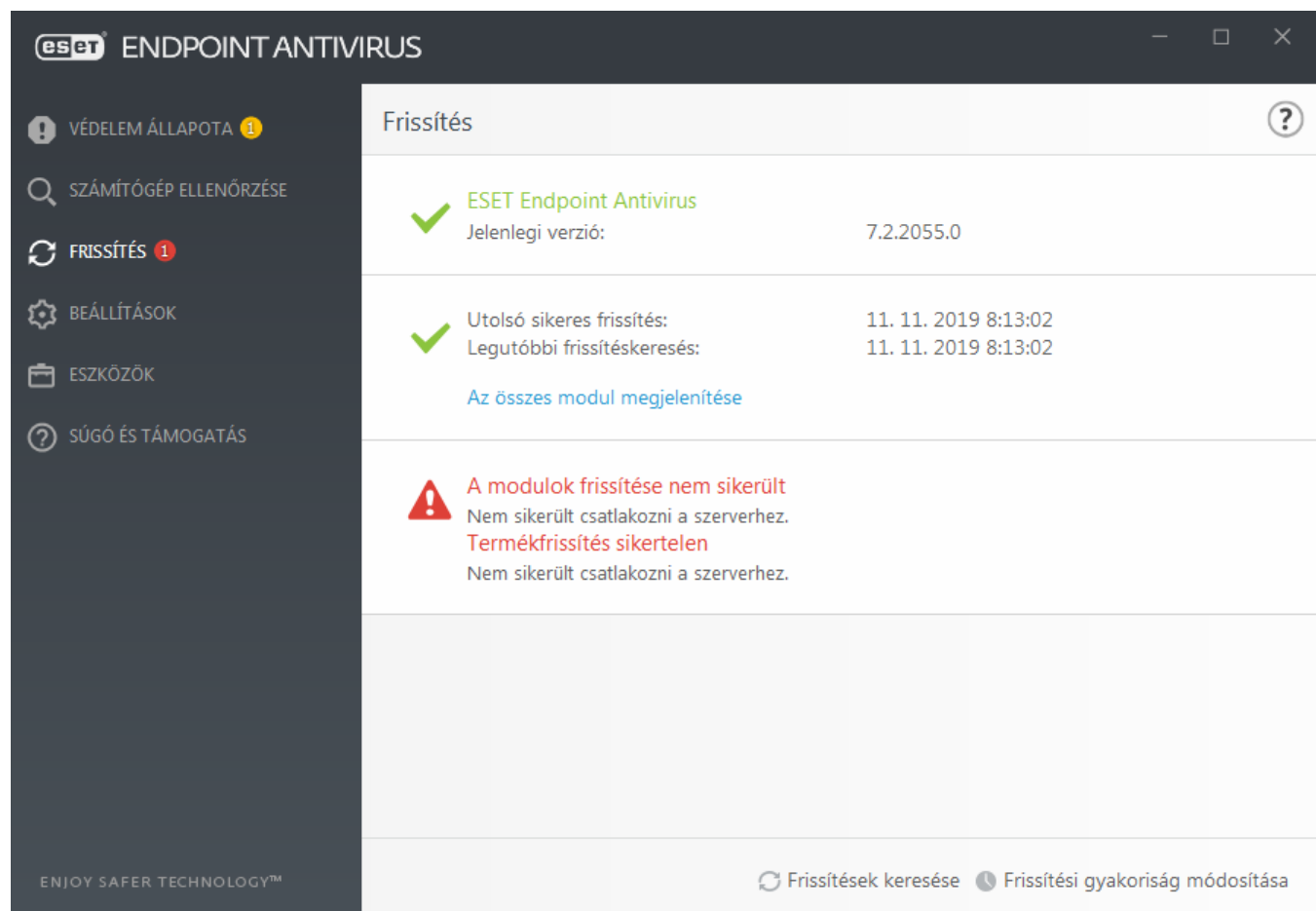
Utolsó sikeres frissítés – Itt látható a legutóbbi sikeres frissítés dátuma és időpontja. Ennek közelmúltbeli dátumnak kell lennie, ugyanis ez jelzi, hogy a keresőmotor naprakész.

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.



Fontos

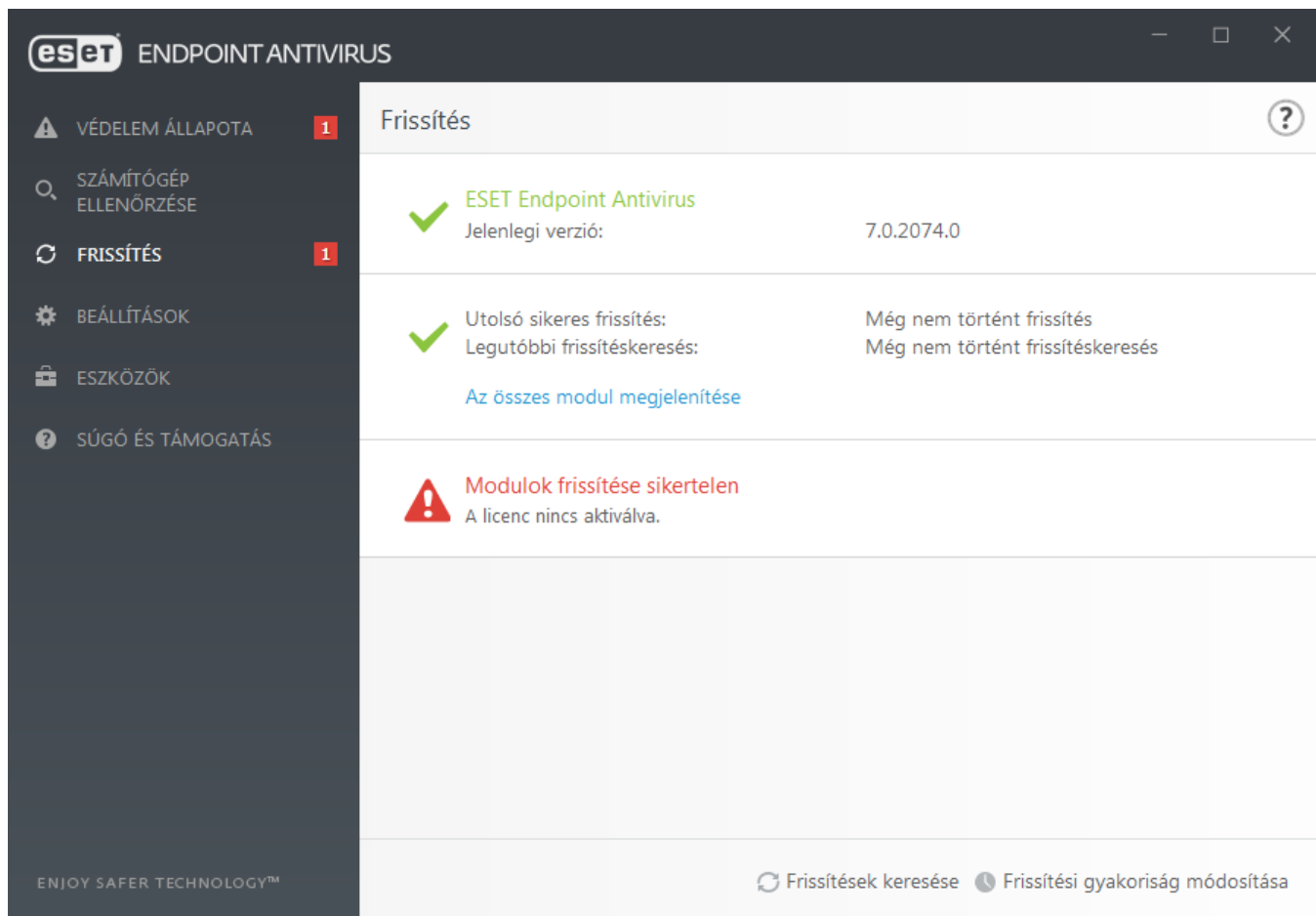
Szokásos körülmények között a modulok frissítése naponta többször is megtörténik. Ellenkező esetben ugyanis a program elavult, és sokkal sérülékenyebb a fertőzésekkel szemben. Ilyenkor a lehető leghamarabb frissítse a modulokat.

A keresőmotor elavult – Ez a hibaüzenet a modulok frissítésére tett több sikertelen kísérletet követően jelenik meg. Azt 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.

ENDPOINT ANTIVIRUS

VÉDELEM ÁLLAPOTA

SZÁMÍTÓGÉP ELLENŐRZÉSE

FRISSÍTÉS 1

BEÁLLÍTÁSOK

ESZKÖZÖK

SÚGÓ ÉS TÁMOGATÁS

Frissítés

ESET Endpoint Antivirus
 Jelenlegi verzió: 6.6.2046.1

Legutóbbi frissítés: Még nem történt frissítés
 Legutóbbi frissítéskeresés: Még nem történt frissítéskeresés
[Az összes modul megjelenítése](#)

Modulok frissítése sikertelen
 Nem sikerült csatlakozni a szerverhez.

Frissítések keresése
 Frissítési gyakoriság módosítása



Megjegyzés

További információt az [ESET 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 frissítési beállítások megfelelő megadása

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 [Frissítési profilok](#) című részt.

Frissítési értesítések konfigurálása (korábban: **A kapott frissítési értesítések kiválasztása** – A **Szerkesztés** elemre kattintva kiválaszthatja a megjeleníteni kívánt [alkalmazásértesítéseket](#). Ezenkívül választhat a **Megjelenítés az**

asztalon és a **Küldés e-mailben** beállítás közül.

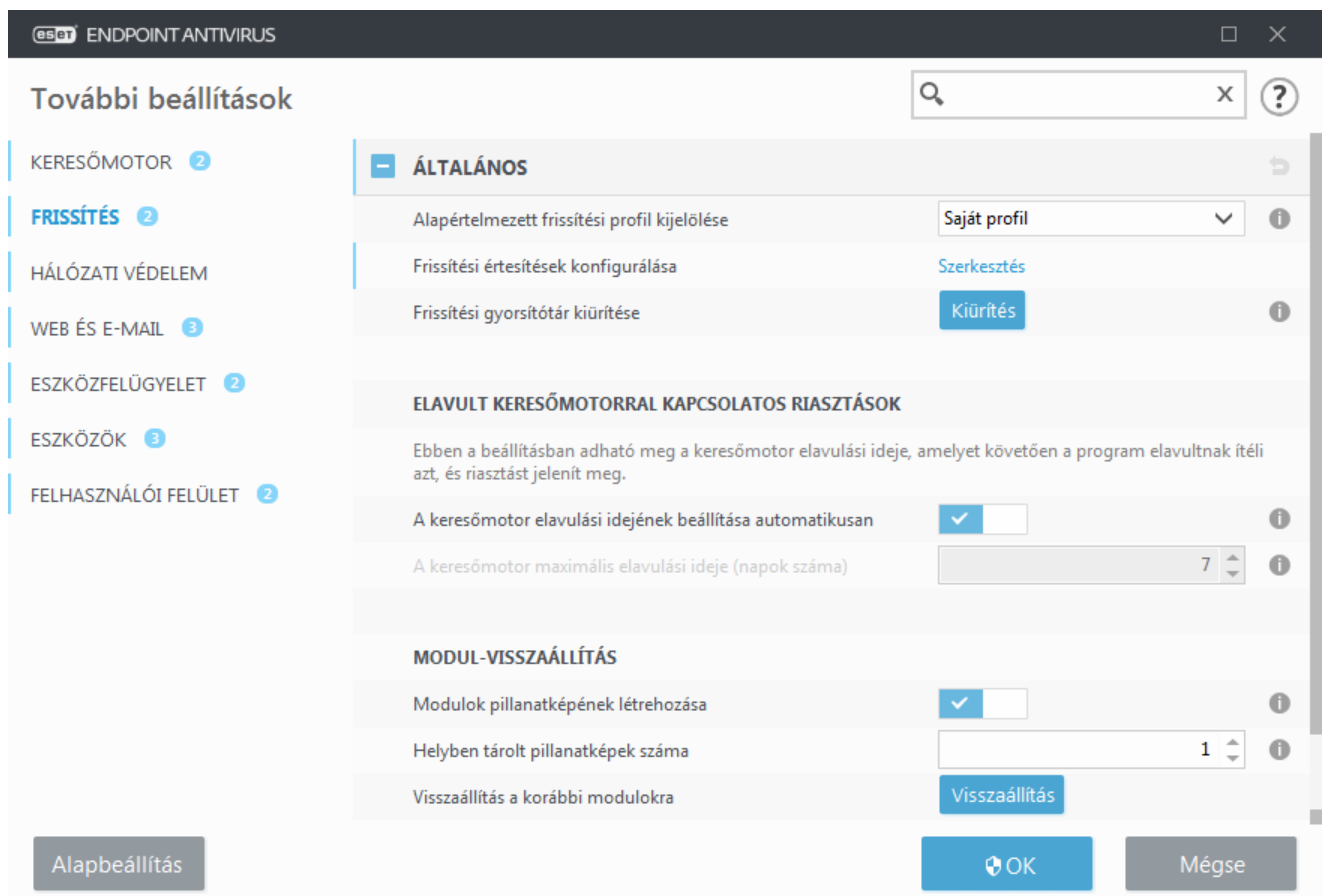
Ha a modulfrissítések letöltése során problémát tapasztal, a **Frissítési gyorsítótár kiürítése** felirat melletti **Kiürítés** gombra kattintva törölje az ideiglenes frissítési fájlokat/ürítse ki a gyorsítótárat.

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 jelteni. **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

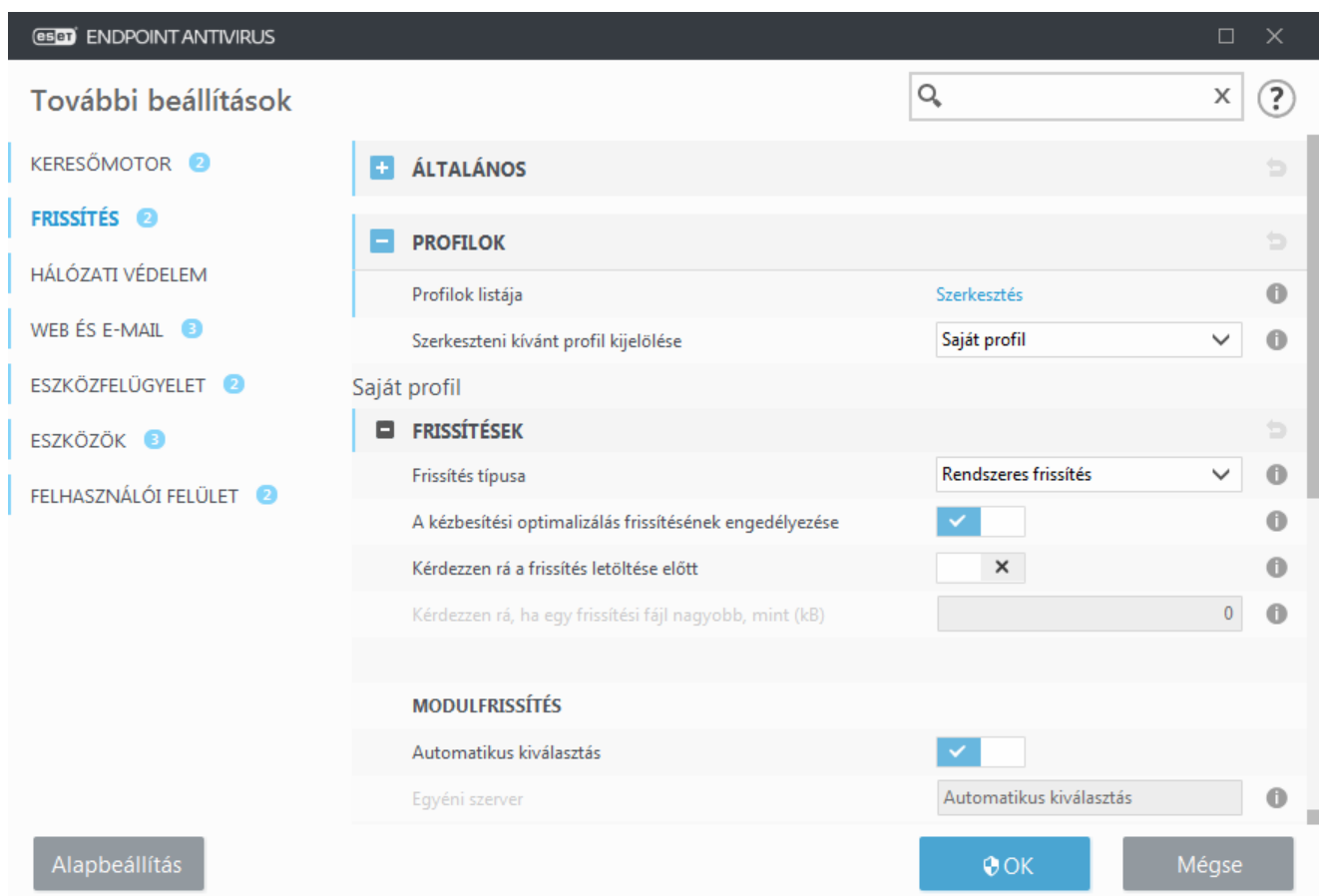
a **Profil neve** mezőbe, és kattintson a **Hozzáadás** elemre.

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. Az előzetes frissítések (a **Tesztelési mód** opció) választásakor olyan frissítéseket használ, amelyek belső tesztelésen estek át, és hamarosan nyilvánosan is elérhetőek lesznek. Az előzetes frissítések engedélyezése esetén hozzáférhet a legfrissebb felismerési módszerekhez és javításokhoz. Az előzetes frissítések veszélyeztethetik 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 órák 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 tölthetnek 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 tükört tartalmaz. Az **Automatikus** beállítás választásakor a frissítés a háttérben fut. Ha meg szeretné jeleníteni a frissítési párbeszédpanelet, 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



HTTP szerverportszám

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

Programösszetevők frissítése

Lásd: [Programösszetevők frissítése](#).

Frissítési tábla

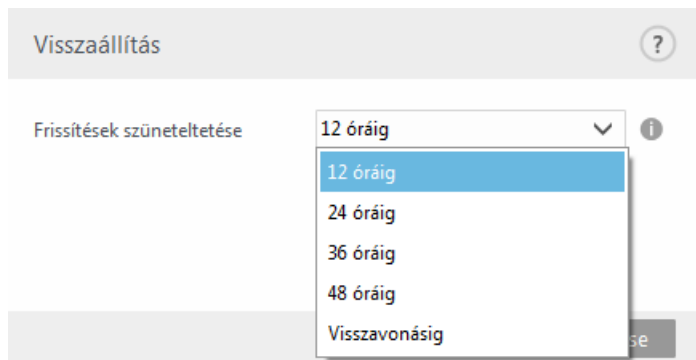
Lásd: [Frissítési tábla](#).

Frissítési fájlok visszaállítása

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. Másik lehetőségként engedélyezheti a korábban letiltott frissítéseket, ha bizonytalan időre elhalasztotta azokat.

Az ESET Endpoint Antivirus pillanatfelvételeket készít a keresőmotorról és a programmodulokról a visszaállítás funkcióhoz való használatra. A vírusdefiníciós adatbázis pillanatfelvételeinek létrehozásához hagyja engedélyezve a **Modulok pillanatképeinek létrehozása** kapcsolót. A **Helyben tárolt pillanatképek száma** mező meghatározza a keresőmotor korábbi pillanatképeinek helyileg tárolt számát.

Ha a **Visszaállítás (További beállítások (F5) > Frissítés > Alapbeállítások > Modul-visszaállítás)** beállítást választja, a legördülő listában jelöljön ki egy időtartamot, amely során a keresőmotor és a programmodulok frissítései szünetelnek.



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

A program a keresőmotor verzióját az elérhető legkorábbira minősíti vissza, és pillanatfelvételnként tárolja a helyi számítógép fájlrendszerében.



Megjegyzés

Tételezzük fel, hogy a keresőmotor legújabb verziójának száma 19959. A 19958-es és a 19956-as verziót a keresőmotor pillanatképeként tárolja a rendszer. Ügyeljen arra, hogy a 19957-es nem érhető el, mert például leállították a számítógépet, és egy újabb frissítés jelent meg a 19957-es letöltése előtt. Ha a **Helyben tárolt pillanatképek száma** mezőben a 2 (kettő) számot adta meg, és a **Visszaállítás** gombra kattintott, a keresőmotor (a programmodulokat is beleértve) a 19956-as számú verzióra áll vissza. Ez a folyamat kis időt igénybe vehet. Az ESET Endpoint Antivirus fő programablakának [Frissítés](#) csoportjában ellenőrizze, hogy a program visszaminősítette-e a keresőmotor verzióját.

Programösszetevők frissítése

A **Programösszetevők frissítése** szakaszban található a programösszetevők frissítéséhez kapcsolódó beállítások. Megadható, hogy miként viselkedjen a program abban az esetben, ha valamelyik programösszetevőhöz frissítés érhető el.

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

A **Frissítési mód** legördülő listában a következő három lehetőség áll rendelkezésre:

- **Kérdezzen rá a frissítés előtt** – Az alapértelmezett beállítás. A programösszetevők frissítésekor megjelenik egy párbeszédpanel, ahol megerősítheti vagy elutasíthatja a frissítést.
- **Automatikusan frissítsen** – A programösszetevő frissítésének letöltése és telepítése automatikusan megtörténik. Ne felejtse el, hogy a számítógép újraindítására lehet szükség.
- **Ne frissítsen** – Egyáltalán nem történik programösszetevő-frissítés. Ezt a beállítást szervertelepítések esetén érdemes használni, hiszen a szerverek általában csak karbantartás esetén indíthatók újra.

Alapértelmezés szerint a programösszetevők frissítései az ESET-adattárszerverekről töltődnek le. Nagy méretű vagy offline környezetben elosztható a forgalom a programösszetevő-fájlok belső gyorsítótárazása érdekében.

[Egyéni szerver megadása a programösszetevők frissítéséhez](#)

1. Az **Egyéni szerver** mezőben megadhatja az elérési utat a programösszetevők frissítéséhez. 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 Antivirus szokásos frissítésével tesztelje, hogy rendelkezésre áll-e programösszetevő-frissítés.



Megjegyzés

A beállításokat az adott munkaállomástól függően kell kiválasztani. Érdemes figyelembe venni a munkaállomások és szerverek közötti különbségeket (súlyos károkat okozhat például, ha egy programfrissítést 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 Antivirus frissítéséhez nem használ proxyszervert, a **Proxyszerver használatának mellőzése** választógombot jelölje be.

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

- Az ESET Endpoint Antivirus 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 Antivirus azonban a frissítések beszerzése érdekében proxyszerverhez kapcsolódik.
- A számítógépe proxyszerveren keresztül csatlakozik az internetre. A beállításokat a program telepítés közben az Internet Explorer böngészőből veszi át, ám célszerű ellenőrizni, hogy azóta nem módosultak-e (például nem változott-e meg az internetszolgáltató), mert a program csak helyes beállításokkal tud

csatlakozni a frissítési szerverekhez.

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

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.



Figyelmeztetés

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

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

Frissítési tükör

Az ESET Endpoint Antivirus 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 terheléelosztást, és internetes sávszélességet szabadít fel.

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 Antivirus\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.

Programösszetevők frissítése

Fájlok – A tükrözés beállításakor meghatározhatja azt is, hogy mely nyelvi verziókhoz szeretne frissítéseket letölteni. A kijelölt nyelveket a felhasználó által beállított tükröszervernek támogatnia kell.

Összetevők automatikus frissítése – Segítségével telepítheti az új funkciókat, illetve a meglévő funkciók frissítéseit. A frissítések automatikusan, felhasználói beavatkozás nélkül is végrehajthatók, de értesítés is kérhető. A programösszetevő-frissítések telepítése után a rendszer újraindítására lehet szükség.

Összetevők frissítése – A programösszetevők frissítése a legújabb verzióra.



HTTP-szerver

Szerverport – A szerverport alapértelmezett 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 módszert nyújt, a hitelesítéshez pedig a tükröszerveren létrehozott felhasználót használja. Az alapértelmezett beállítás a **Nincs**, amellyel a frissítési fájlok hitelesítés nélkül is elérhetők.

Fűzze hozzá a **tanúsítványlánc fájlját** (vagy hozzon létre egy ön aláírt 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 adatátvitel 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.



Megjegyzés

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

Frissítés tükröből

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 > Tükrözés** 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**. A **Hitelesítés** beállítás adja meg 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 módszert nyújt, a hitelesítéshez pedig a tükröszerverten létrehozott felhasználót használja. Az alapértelmezett beállítás a **Nincs**, amellyel a frissítési fájlok hitelesítés nélkül is elérhetők.



Figyelmeztetés

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

SSL HTTP-szerverhez

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



Megjegyzés

Érvénytelen a felhasználónév és/vagy a jelszó hiba jelenik meg a főmenü Frissítés ablaktáblájában a keresőmotor tükröből való frissítésének 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 tükröszervert konfigurálása után hozzá kell adnia az új frissítési szervert a munkaállomásokon. Ehhez tegye az alábbiakat:

- **Nyissa meg a További beállítások (F5) párbeszédpanelét**, és kattintson a **Frissítés > Profilok > Alapbeállítások** fülre.
- Kapcsolja 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 Antivirus programot.

Ezután a **További beállítások > Frissítés > Profilok > Tükrözés** lapon a **Frissítési fájlok biztosítása belső HTTP-szerveren keresztül** opció 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 Antivirus **További beállítások** párbeszédpaneljét, és kattintson a **Frissítés > Profilok > 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 Antivirus **További beállítások** párbeszédpaneljét, és kattintson a **Frissítés > Profilok > Frissítések** elemre.
2. Kapcsolja ki a **Modulfrissítések** felirat melletti **Automatikus kiválasztás** opciót, és a **Frissítési szerver mezőben** az `\\UNC\PATH` formátumot használva vegyen fel egy új szervert.



Megjegyzés

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 termékcsoporthoz frissítési fájlok találhatók. Meg kell adnia a teljes elérési utat a megfelelő mappához a tükröt használó termék frissítési beállításaiban.

Például az ESMC 7 tükörből való frissítéséhez adja meg a következőt a [Frissítési szerver](#) beállításnál (a HTTP-szerver gyökerhelye 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 **Programösszetevők frissítése** opció, nem kell a **Frissítés** elemre kattintani, mert amikor elérhetővé válnak, a program automatikusan a helyi tükörről másolja a fájlokat. A programösszetevők frissítéséről a [Frissítési mód](#) című fejezetben olvashat bővebben.

A tükrözésből történő frissítéssel kapcsolatos hibaelhárítás

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

Az ESET Endpoint Antivirus hibát jelez, miközben a tükröszerverhez próbál csatlakozni – A hiba oka valószínűleg a munkaállomás által használandó frissítési szerver adatainak helytelensége (nem megfelelő hálózati elérési út vagy tükrömappa). 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 Antivirus 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 tükröszerverhez, 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 tükröszerver 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 Antivirus hibát jelez, miközben a tükröszerverhez próbál csatlakozni – A tükrő HTTP-verziójának eléréséhez megadott porton valami gátolja a kommunikációt.

Az ESET Endpoint Antivirus hibát jelez frissítési fájlok letöltésekor – A hiba oka valószínűleg az, hogy helytelenül van beállítva (hálózati elérési út a Tükrő 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 Antivirus programban alapértelmezés szerint az alábbi feladatok aktívak:

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

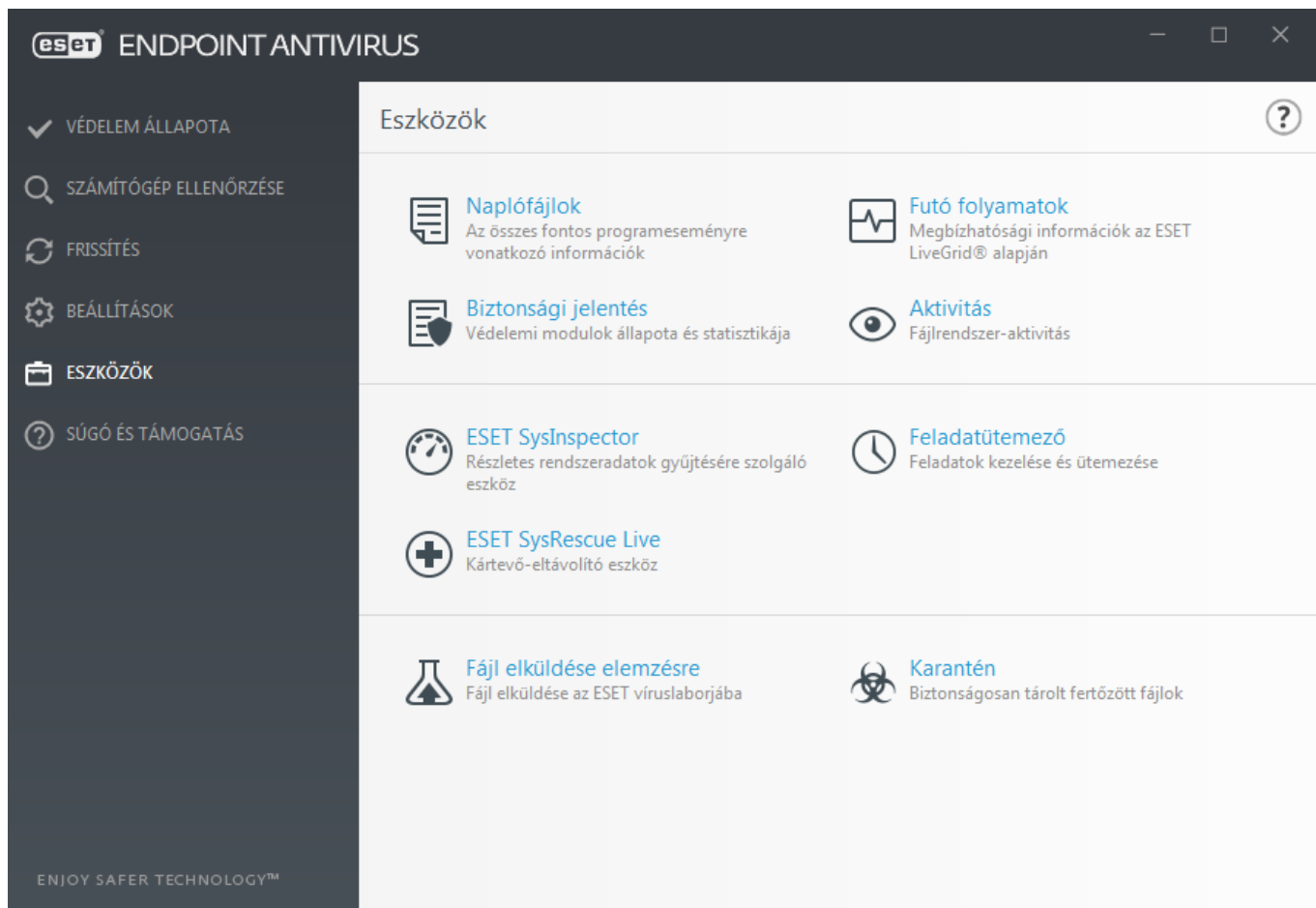
Minden frissítési feladat módosítható az igényeinek megfelelően. Az alapértelmezett frissítési feladatok mellett a felhasználó által definiált konfigurációjú új feladatok is létrehozhatók. A frissítési feladatok létrehozásáról és beállításáról a [Feladatütemező](#) című fejezet nyújt részletes tájékoztatást.

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](#)
- [Biztonsági jelentés](#)
- [Futó folyamatok](#) (ha az ESET LiveGrid® engedélyezve van az ESET Endpoint Antivirus alkalmazásban)
- [Aktivitás](#)
- [Feladatütemező](#)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#) – Átírányítja az ESET SysRescue Live webhelyre, ahol letöltheti az ESET SysRescue Live .iso CD-/DVD-képet.
- [Karantén](#)
- [Minta elküldése elemzésre](#) – A gyanús fájlok elküldése elemzésre az ESET víruslaborjába. A hivatkozásra kattintva egy párbeszédpanel jelenik meg, amelynek leírását ebben a szakaszban találja.



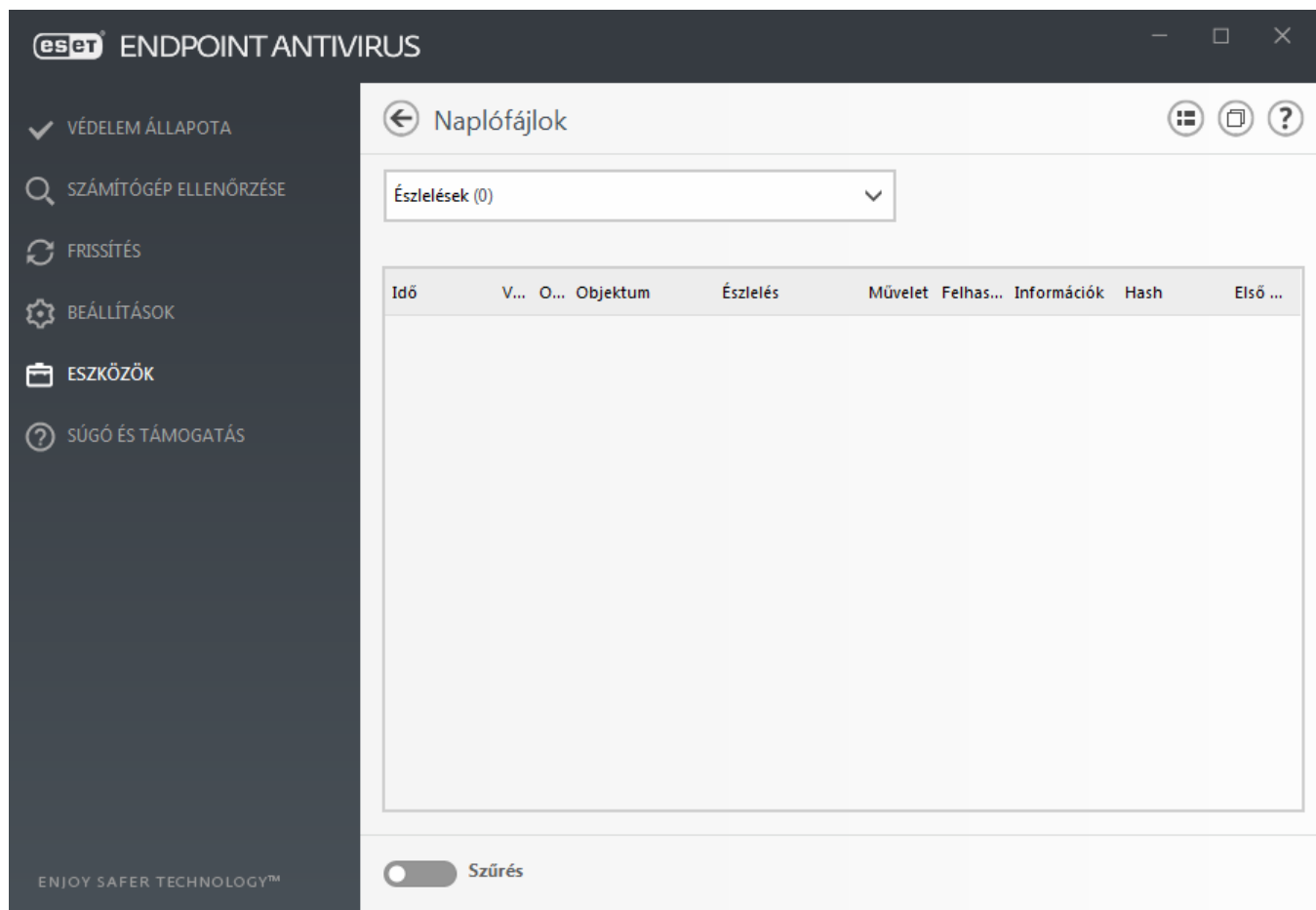
Naplófájlok

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 Antivirus környezetéből tekintheti meg. A naplófájlok archiválására is van lehetőség.


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

- **Észlelések** – Ez a napló részletes információkat szolgáltat az ESET Endpoint Antivirus 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** – A program az ESET Endpoint Antivirus által elvégzett összes műveletet rögzíti az eseménynaplókban. Az eseménynapló a programban történt eseményekre és hibákra vonatkozó információkat tartalmazza. Ezt a lehetőséget választva a rendszergazdák és a felhasználók megoldhatják az esetleges problémákat. Ezek az információk gyakran hozzájárulnak a programban fellépő hibák megoldásához.
- **Számítógép ellenőrzése** – Ebben az ablakban minden ellenőrzési eredmény megjelenik. Minden sor egy-egy számítógép-ellenőrzésnek felel meg. Az egyes bejegyzésekre duplán kattintva megjelennek az adott ellenőrzés részletes adatai.
- **Letiltott fájlok** – A letiltott és nem elérhető fájlokról tartalmaz adatokat. A protokoll megjeleníti az okot és a forrásmodult, amely letiltotta a fájlt, valamint a fájlt végrehajtott alkalmazást és felhasználót.
- **Elküldött fájlok** – Az ESET LiveGrid®, illetve az [ESET Dynamic Threat Defense](#) 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](#) által észlelt összes távoli támadást. A tűzfalnapló megjeleníti a tűzfal által észlelt összes távolról indított támadást, valamint a számítógép ellen indított támadások adatait. Az Esemény oszlopban láthatók az észlelt támadások, a Forrás oszlop további információkat szolgáltat a támadóról. a Protokoll oszlop pedig a támadáshoz használt protokollt ismerteti. A tűzfal naplójának elemzésével időben felderítheti a rendszer ellen végrehajtott behatolási kísérleteket, és megakadályozhatja a számítógéphez való jogosulatlan hozzáférést. Adott hálózati támadásokról az [IDS és további beállítások](#) című fejezetben olvashat bővebben.
- **Szűrt webhelyek** – Ebben a listában láthatók a [webhozzáférés-védelem](#) által letiltott webhelyek. Ezekben a naplókban látható az idő, az URL-cím, a felhasználó és az adott webhely felé kapcsolatot megnyitó alkalmazás.

- **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, és 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 a kijelölt naplóról egy új ablakban.
- **Azonos rekordok szűrése** – Ha aktiválja ezt a szűrőt, csak az azonos típusú bejegyzések jelennek meg (diagnosztika, figyelmeztetések stb.).
- **Szűrés.../Keresés...** – 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(ek)e)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 megfelelőek) 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**, amiktől 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.

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 Antivirus 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** – 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, és egyébekkel kapcsolatos) hibákat naplózza.



Megjegyzés

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 végett 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.



ESET Log Collector

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 Antivirus 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

ESET ENDPOINT ANTIVIRUS

✓ VÉDELEM ÁLLAPOTA

🔍 SZÁMÍTÓGÉP ELLENŐRZÉSE

🔄 FRISSÍTÉS

⚙️ BEÁLLÍTÁSOK

📁 ESZKÖZÖK

❓ SÚGÓ ÉS TÁMOGATÁS

ENJOY SAFER TECHNOLOGY™

Naplófájlok

Auditálási naplók (219)

Idő	Típus	Leírás	Forrás	Felhasználó
8.11.2019...	Funkció módos...	A(z) Botnet állapota megváltozott – Inaktív ->...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Frissítés állapota megváltozott – Inaktív ->...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Hálózati támadások elleni védelem (IDS) á...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Eszközfelügyelet állapota megváltozott – ...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Adathalászat elleni védelem állapota meg...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Eszközfelügyelet állapota megváltozott – ...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Frissítés állapota megváltozott – Inaktív ->...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Valós idejű fájlrendszervédelem állapota ...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Dokumentumvédelem állapota megváltoz...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Zsarolóprogram-ellenőrzés állapota megv...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Exploit blokkoló állapota megváltozott – I...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Speciális memóriaellenőrzés állapota meg...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Behatolásmegelőző rendszer (HIPS) állap...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Eszközfelügyelet állapota megváltozott – ...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Frissítés állapota megváltozott – Inaktív ->...	SYSTEM	NT AUTHORITY\SYSTEM
8.11.2019...	Funkció módos...	A(z) Botnet állapota megváltozott – Inaktív ->...	SYSTEM	NT AUTHORITY\SYSTEM

☐ Szűrés

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 ESMC 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.

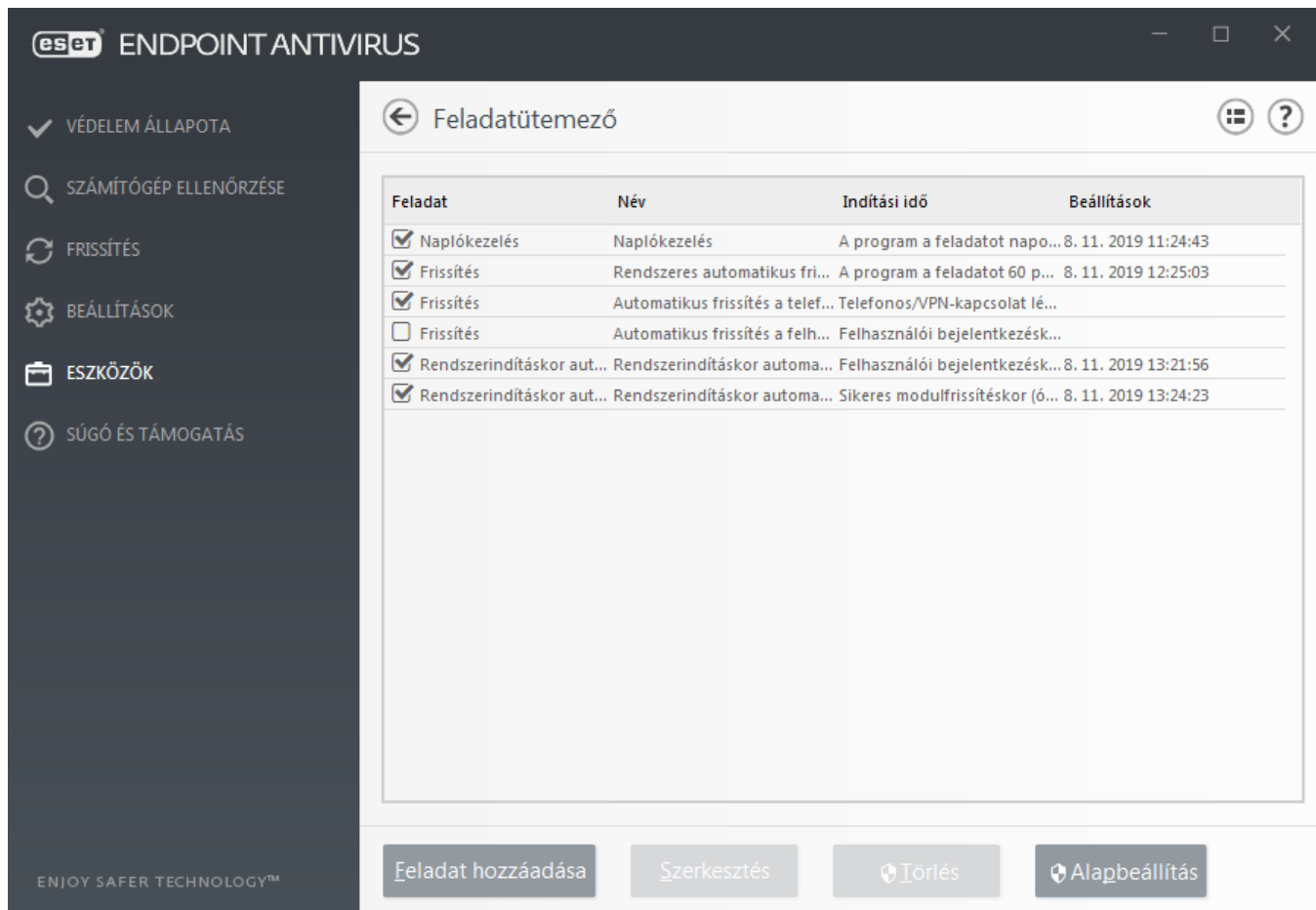
A Feladatütemező az ESET Endpoint Antivirus fő programablakából érhető el az **Eszközök > Feladatütemező** lehetőségre kattintással. A **Feladatütemező** valamennyi ütemezett feladat és beállított tulajdonságainak (például előre definiált dátum, időpont és ellenőrzési profil) összesített listáját tartalmazza.

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. Írja be 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.
- **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 időzírtési 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** mezőben 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.

Ütemezett feladat áttekintése

Feladat neve

Automatikus frissítés a felhasználó bejelentkezése után

Feladat típusa

Frissítés

A feladat futtatása

Felhasználói bejelentkezéskor (óránként legfeljebb egyszer)

Elvégzendő művelet, amennyiben a feladat nem fut a megadott időpontban

A következő ütemezett időpontban

OK

Védelem statisztikája

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

Az ESET Endpoint Antivirus 7.1-es verziója egy új típusú jelentésre ad lehetőséget – ez a [Biztonsági jelentés](#). A Védelem statisztikája szakasz nem lesz elérhető a továbbiakban.

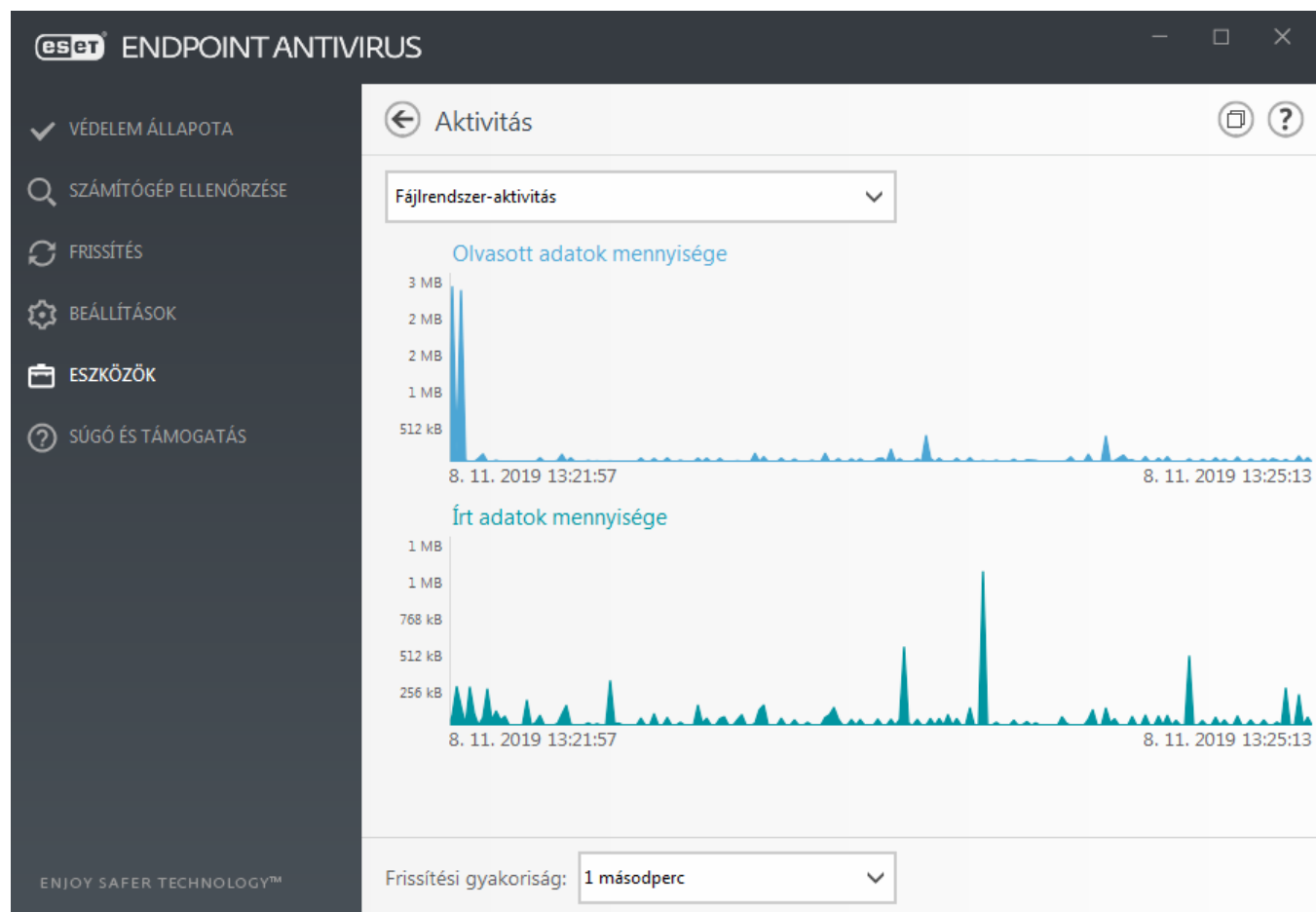
A megtekinthető statisztikai grafikonok az alábbiak:

- **Vírus- és kémprogramvédelem** – A fertőzött és a megtisztított objektumok számát jeleníti meg.
- **Fájlrendszervédelem** – Csak az olvasott és a fájlrendszerhez írt objektumokat jeleníti meg.
- **E-mail védelem** – Csak a levelezőprogramok által küldött vagy fogadott objektumokat jeleníti meg.
- **Webhozzáférés- és adathalászat elleni védelem** – Csak a böngészők által letöltött objektumokat jeleníti meg.

A statisztikai grafikon mellett látható az összes ellenőrzött objektum, a fertőzött objektumok, a megtisztított objektumok és a tiszta objektumok száma. A **Alaphelyzet** gombra kattintva törölheti a statisztikai adatokat, **Az összes visszaállítása** gombra kattintva pedig törölheti és eltávolíthatja az összes meglévő adatot.

Aktivitás

Az aktuális **fájlrendszer-aktivitás** grafikonos formában való megjelenítéséhez az **Eszközök** lapon válassza az **Aktivitás** lehetőséget. A grafikon alján egy idősor található, amely valós időben, a kiválasztott időköz alapján rögzíti a fájlrendszer-aktivitást. Ha módosítani szeretné az időközt, jelölje ki az új értéket a **Frissítési gyakoriság** legördülő listában.



A választható lehetőségek az alábbiak:

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

A **Fájlrendszer-aktivitás grafikon** függőleges tengelye az olvasott (kék színű) és az írt adatokat (türkiz színű) jeleníti meg. Mindkét érték kB (kilobájt)/MB/GB mértékegységben van megadva. Ha az egér mutatóját a grafikon alatti Olvasott adatok mennyisége vagy Írt adatok mennyisége felirat fölé viszi, a grafikon csak az adott aktivitástípushoz tartozó adatokat fogja megjeleníteni.

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.
- **Összevetés** – Két meglévő napló összehasonlítása.
- **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 (ugyanazt az eredményt érheti el a naplóra duplán kattintva).
- **Összehasonlítás** – Két meglévő napló összehasonlítása.

- **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 Antivirus alapértelmezés szerint elküldi a gyanús fájlokat elemzésre az ESET víruslaborjába. A küldött fájlok között néhány fájltypus – 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 Antivirus a keresőmotor frissítésénél gyorsabban reagál az új kártevőkre.



Kapcsolódó információk

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 Antivirus 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.

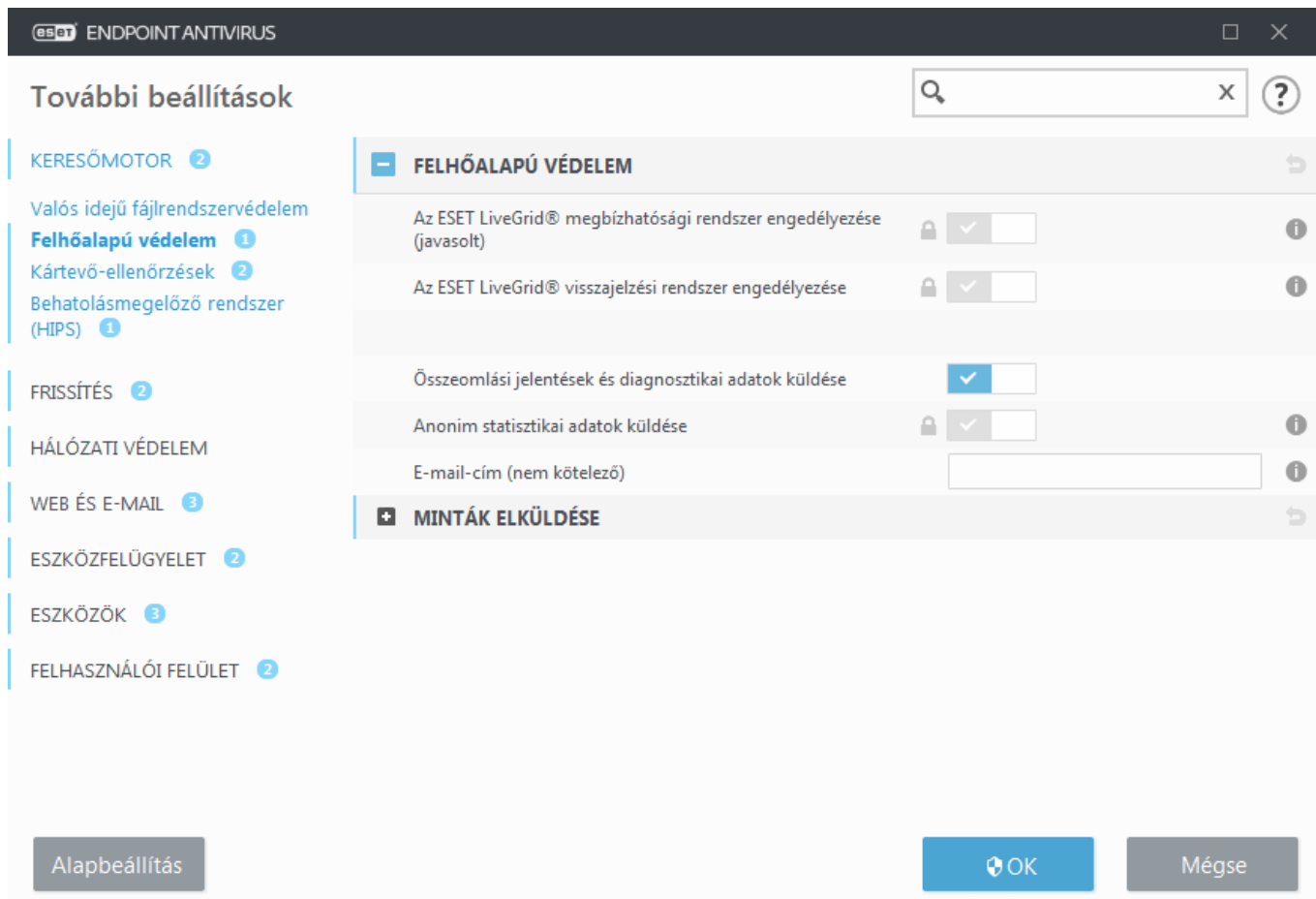
Az ESET LiveGrid® visszajelzési rendszer engedélyezése – Elküldi a megfelelő felismerési adatokat (lásd az alábbi **Minták elküldése** szakaszban), valamint a hibajelentéseket és statisztikákat az ESET víruslaborjába további elemzés céljából.

Az ESET Dynamic Threat Defense engedélyezése (nem látható az ESET Endpoint Antivirus termékben) – Az ESET Dynamic Threat Defense 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 csak akkor keresik, ha a gyanús fájlokkal kapcsolatban további információra van szükség.



Minták elküldése

Az észlelt vírusminták automatikus elküldése

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

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

Gyanús minták automatikus elküldése

Ezeket a mintákat akkor is megkapja az ESET, ha a keresőmotor nem észlelte őket. Például olyan mintákat, amelyeknek az észlelése majdnem megghiúsult, illetve ha az ESET Endpoint Antivirus [védelmi moduljainak](#) egyike gyanúsnak vagy zavaros viselkedésűnek találja a mintákat.

- **Végrehajtható fájlok** – Például a következő fájlok: .exe, .dll, .sys
- **Tömörített fájlok** – Például a következő fájltypusok: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Tömörített fájlok** – Például a következő fájltypusok: .bat, .cmd, .hta, .js, .vbs, .ps1.

- **Egyéb** – Például a következő fájltypusok: .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 dokumentumfájltypus 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 fájltypusok alapértelmezés szerint ki vannak zárva (.doc stb.). A kizárt fájlok listája szükség szerint bővíthető.

ESET Dynamic Threat Defense

Ha az ESET Dynamic Threat Defense szolgáltatást kliensgépen szeretné engedélyezni az ESMC Webkonzol segítségével, tekintse meg az [ESET Endpoint Antivirus EDTD-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 fájltypusok (többek között a .doc stb.) alapértelmezés szerint ki vannak zárva.

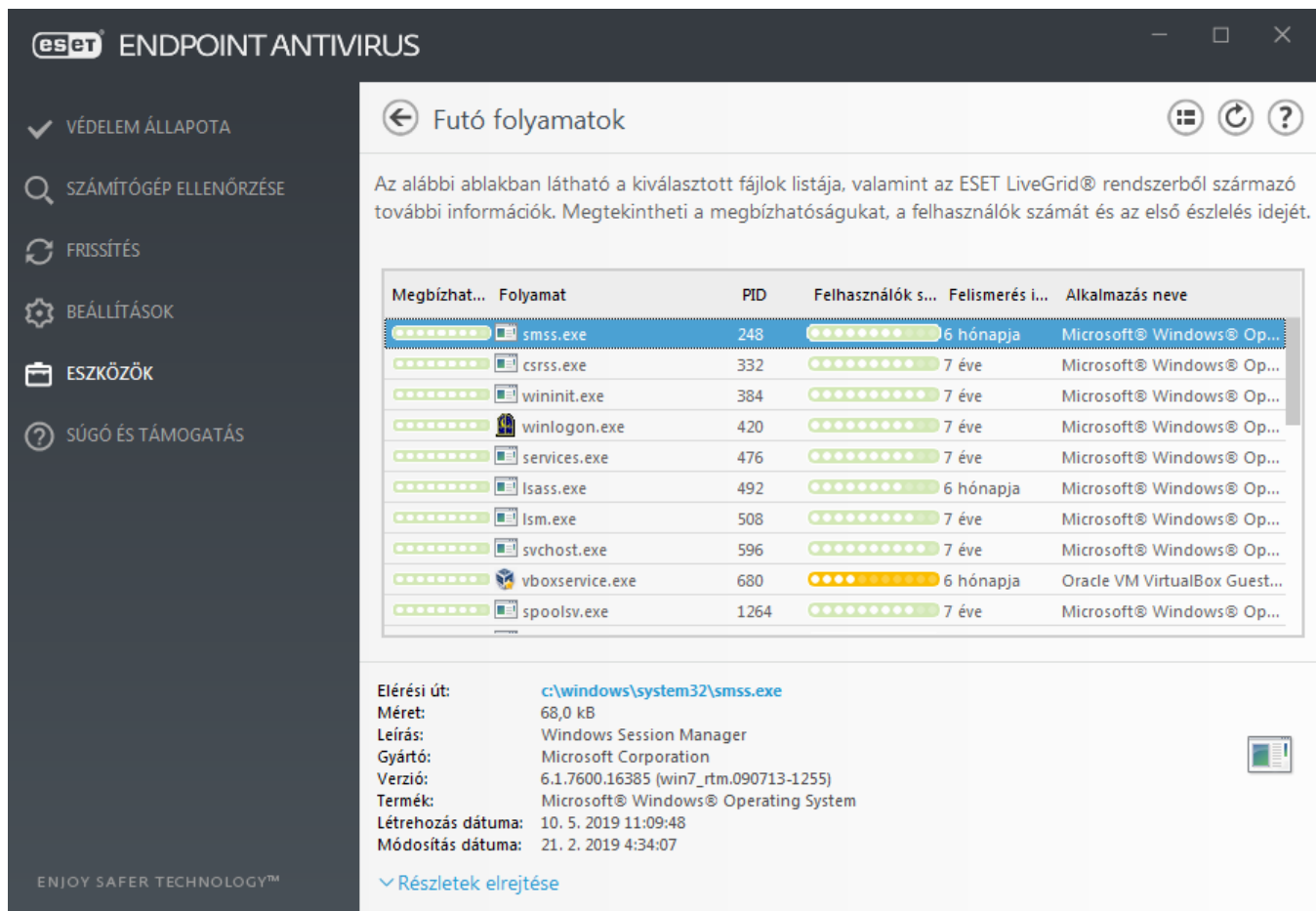


Megjegyzés

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

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 Antivirus részletes adatokat szolgáltat a futó folyamatokról, amelyek segítségével az engedélyezett [ESET LiveGrid®](#) technológia biztosítja a felhasználók védelmét.



Megbízhat...	Folyamat	PID	Felhasználók s...	Felismerés i...	Alkalmazás neve
●●●●●●	smss.exe	248	●●●●●●	6 hónapja	Microsoft® Windows® Op...
●●●●●●	csrss.exe	332	●●●●●●	7 éve	Microsoft® Windows® Op...
●●●●●●	wininit.exe	384	●●●●●●	7 éve	Microsoft® Windows® Op...
●●●●●●	winlogon.exe	420	●●●●●●	7 éve	Microsoft® Windows® Op...
●●●●●●	services.exe	476	●●●●●●	7 éve	Microsoft® Windows® Op...
●●●●●●	lsass.exe	492	●●●●●●	6 hónapja	Microsoft® Windows® Op...
●●●●●●	lsmd.exe	508	●●●●●●	7 éve	Microsoft® Windows® Op...
●●●●●●	svchost.exe	596	●●●●●●	7 éve	Microsoft® Windows® Op...
●●●●●●	vboxservice.exe	680	●●●●●●	6 hónapja	Oracle VM VirtualBox Guest...
●●●●●●	spoolsv.exe	1264	●●●●●●	7 éve	Microsoft® Windows® Op...

Elérési út: [c:\windows\system32\smss.exe](#)
Méret: 68,0 kB
Leírás: Windows Session Manager
Gyártó: Microsoft Corporation
Verzió: 6.1.7600.16385 (win7_rtm.090713-1255)
Termék: Microsoft® Windows® Operating System
Létrehozás dátuma: 10. 5. 2019 11:09:48
Módosítás dátuma: 21. 2. 2019 4:34:07

▼ Részletek elrejtése

Megbízhatóság – A legtöbb esetben az ESET Endpoint Antivirus 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.



Megjegyzés

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 az időtartam, amióta az ESET LiveGrid® technológia észlelte az alkalmazást.



Megjegyzés

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.

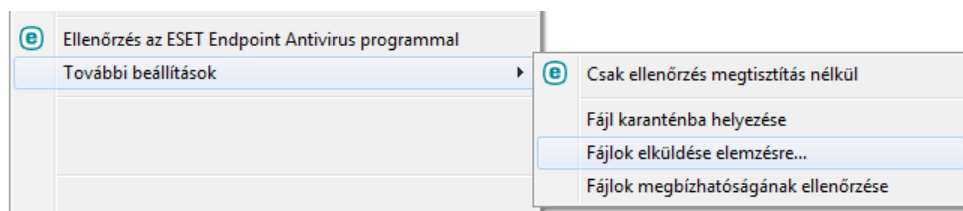
Ha az ablak alján egy alkalmazásra kattint, az alábbi információk jelennek meg róla:

- **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.



Megjegyzés

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.

Észlelt kórtelen alkalmazások – A [kórtelen alkalmazások](#) 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.

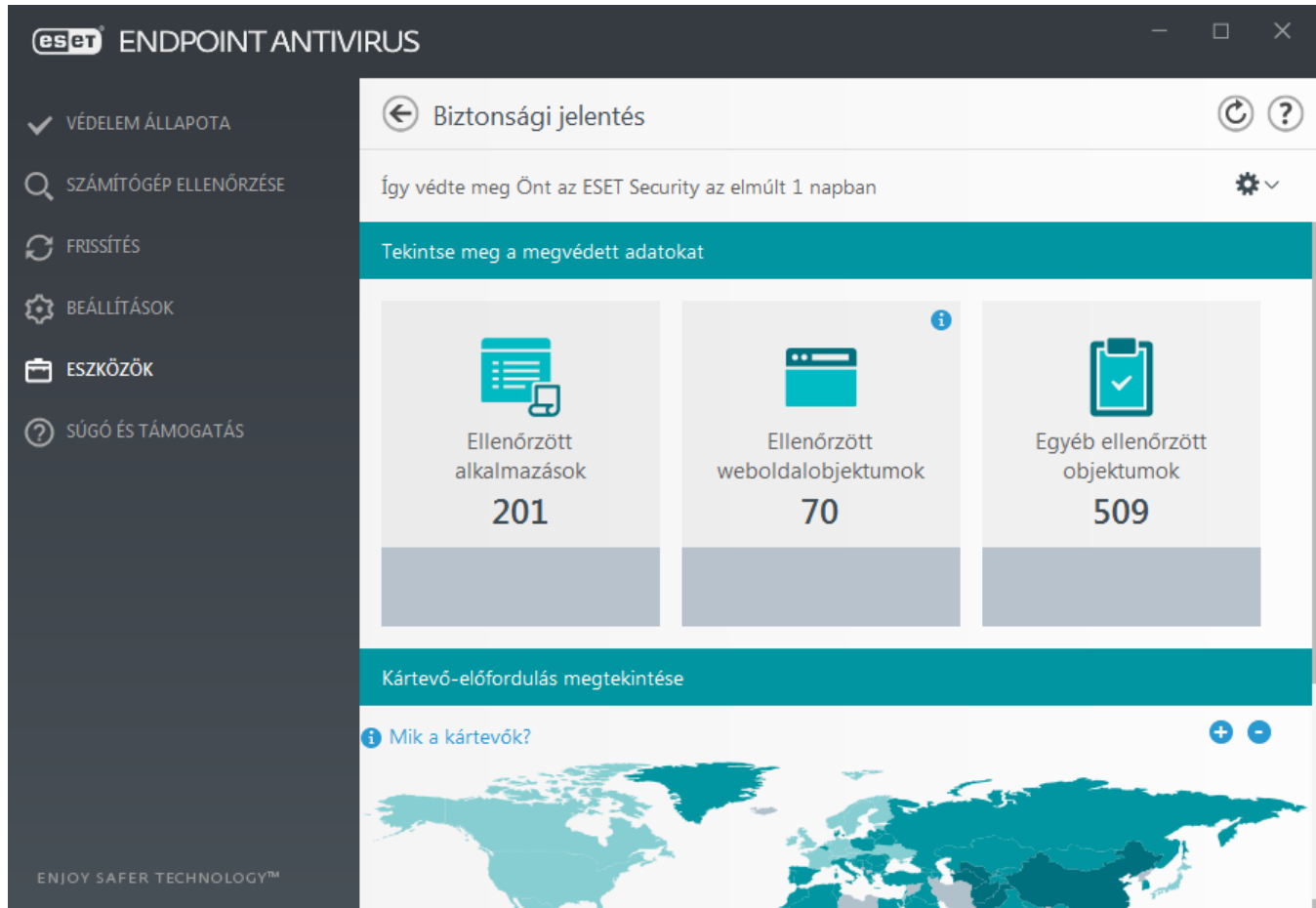
Ellenőrzött weboldalobjektumok – Az ellenőrzött weboldalobjektumok számát jeleníti meg.

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 kategóriák alatt látható a vírusokkal kapcsolatos aktuális helyzet világtérképpel kiegészítve. Különböző színek jelzik a vírusok mennyiségét az egyes országokban (minél sötétebb a szín, annál több található). Szürke színűek azok az országok, amelyek esetén nem áll rendelkezésre adat. Vigye az egeret az országok fölé az adatok megjelenítéséhez. Ha kiválaszthat egy kontinenst, automatikusan megjelenik nagyobb méretben.

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 Antivirus 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.



A képernyő a "Biztonsági jelentés" címmel rendelkező ablakot mutatja. A bal oldali sötét sávban a következő elemek láthatók: VÉDELEM ÁLLAPOTA, SZÁMÍTÓGÉP ELLENŐRZÉSE, FRISSÍTÉS, BEÁLLÍTÁSOK, ESZKÖZÖK, SÚGÓ ÉS TÁMOGATÁS. A fő tartalomterületen a "Biztonsági jelentés" cím alatt a "Így védte meg Önt az ESET Security az elmúlt 1 napban" szöveg látható. Alatta a "Tekintse meg a megvédett adatokat" gomb van. A következő sorban három kártya látható: "Ellenőrzött alkalmazások" (201), "Ellenőrzött weboldalobjektumok" (70), és "Egyéb ellenőrzött objektumok" (509). Alatta a "Kártevő-előfordulás megtekintése" gomb van. A legalsó részben a "Mik a kártevők?" szöveg látható, mellette egy világtérkép, amely a kártevők elterjedését mutatja. A térkép alján az "ENJOY SAFER TECHNOLOGY™" szöveg látható.

Az **Adatok visszaállítása** lehetőség kiválasztásakor törlődnek a statisztikai adatok és a Biztonsági jelentésben található adatok. A műveletet meg kell erősíteni, kivéve akkor, ha inaktíválja a **Rákérdezés a statisztika alaphelyzetbe állítása előtt** funkciót a **További beállítások > Felhasználói felület > Riasztások és értesítési ablakok > Megerősítési üzenetek** lapon.

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.



Mielőtt leadna mintákat az ESET-nek

Ne küldjön be mintát, ha az nem felel meg legalább egy feltételnek a következők közül:

- Az ESET-termék egyáltalán nem észleli a mintát
- A program tévesen kártevőként észlelte a mintát
- Nem fogadjuk el a személyes fájlokat (amelyek esetén azt szeretné, hogy vizsgálja meg őket az ESET) mintaként (az ESET kutatólaborja nem hajt végre egyéni ellenőrzést a felhasználók számára)
- A levél tárgysorában jelezze röviden a problémát, a levélben pedig adjon meg minél több információt a fájlról (például mellékeljen képernyőfotót vagy annak a webhelynek a címét, ahonnan letöltötte).

A következő módszerekkel küldheti el a mintát (fájlt vagy webhelyet) az ESET-nek elemzésre:

1. A 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 vagy tévesen levélszemétnek észlelt elemek bejelentése [ez 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.



Előfordulhat, hogy az ESET nem ad választ

Az ESET csak akkor válaszol, ha további információkra van szüksége. Szervereink fájlok tízezreit fogadják nap mint nap, így nem tudunk válaszolni minden egyes üzenetre. Ha a minta valóban egy kártékony alkalmazás vagy webhely, bekerül a vírusdefiníciós adatbázis valamelyik későbbi ESET-frissítésébe.

Minta kiválasztása elemzésre – Gyanús fájl

Kártevőfertőzés észlelt jelei és tünetei – Adja meg a gyanús fájl számítógépen észlelt viselkedésének leírását.

Fájl eredete (URL-cím vagy gyártó) – Adja meg a fájl eredetét (forrását), és azt is, hogy miként talált rá.

Megjegyzések és további információk – Itt olyan kiegészítő információt, illetve leírást adhat meg, amely segítheti a gyanús fájl azonosításának feldolgozását.



Megjegyzés

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** – Különbféle 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.



Megjegyzés

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 fájl 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.

Értesítések

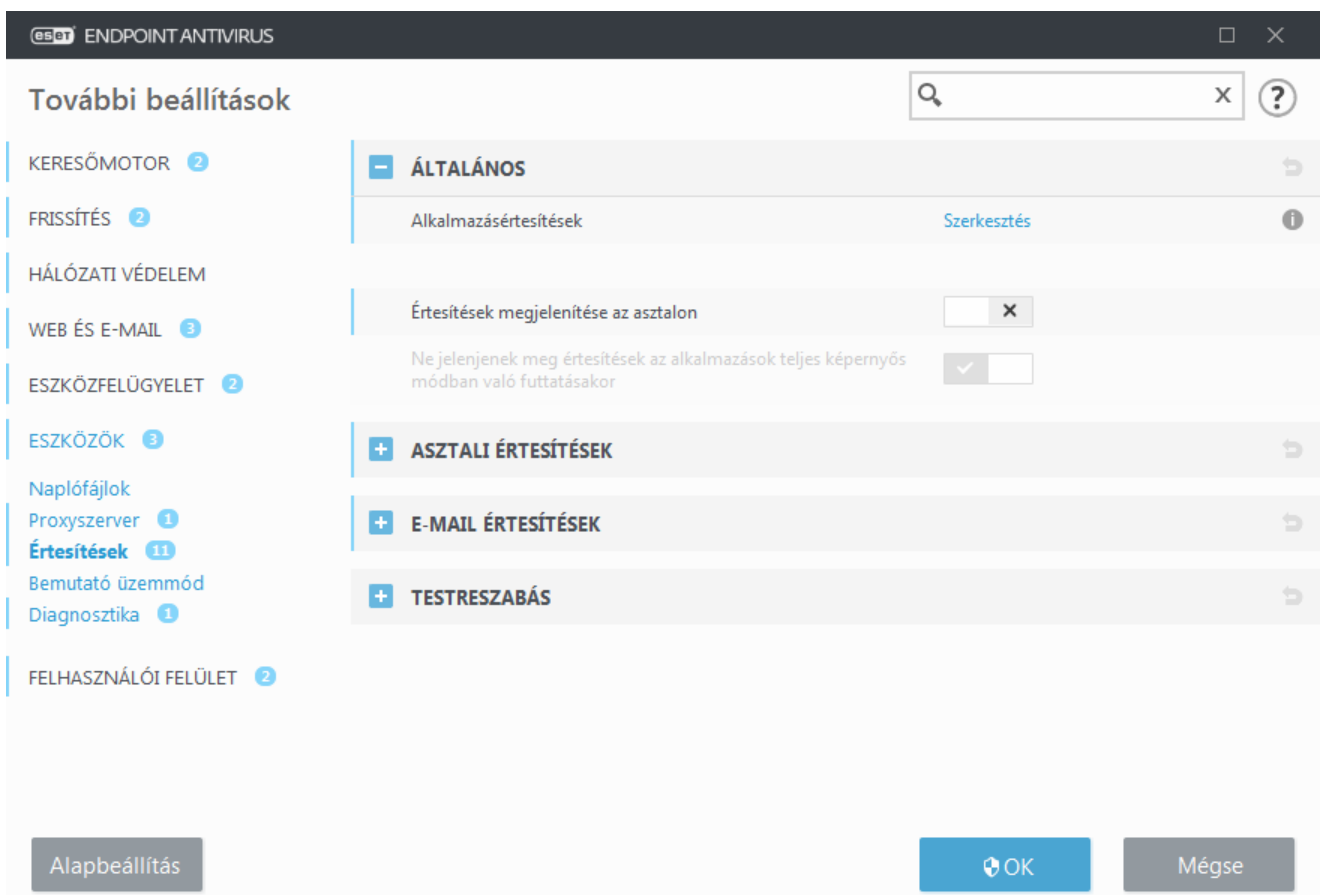
Ha meg szeretné adni, hogy az ESET Endpoint Antivirus milyen módon értesítse a felhasználót az eseményekről, lépjen a **További beállítások (F5) > Eszközök > Értesítések** ablakba. Itt a következő típusú értesítések állíthatók be:

- [Alkalmazásértesítések](#) – Közvetlenül a program főablakában jelennek meg.
- [Asztali értesítések](#) – Az asztali értesítések egy kis előugró ablakban jelennek meg a rendszertálcán.
- [E-mail értesítések](#) – Az e-mail-értesítések a megadott e-mail-címre érkeznek.
- [Az értesítések testreszabása](#) – Egyéni üzenet adható meg például egy asztali értesítés esetén.

Az **Általános** szakaszban a megfelelő kapcsolókkal a következők állíthatók be:

Kapcsoló	Alapbeállítás	Leírás
Értesítések megjelenítése az asztalon	<input checked="" type="checkbox"/>	Ha letiltja a funkciót, akkor nem fognak megjelenni előugró értesítések a rendszertálcán. Azt javasoljuk, hogy ne tiltsa le, mert így a termék értesíteni tudja új események esetén.
Ne jelenjenek meg értesítések...	<input checked="" type="checkbox"/>	Ne tiltsa le a Ne jelenjenek meg értesítések az alkalmazások teljes képernyős módban való futtatásakor funkciót, ha nem szeretne megjeleníteni felhasználói beavatkozást nem igénylő értesítéseket.
Biztonsági jelentésről szóló értesítések megjelenítése	<input type="checkbox"/>	Engedélyezze a funkciót, ha értesítést szeretne kapni, amikor a Biztonsági jelentés egy új verziója jön létre.
Sikeres frissítésről szóló értesítés megjelenítése	<input type="checkbox"/>	Engedélyezze a funkciót, ha értesítést szeretne kapni, amikor a termék frissíti az összetevőit és a keresőmotor-modulokat.
Értesítés küldése e-mailben	<input type="checkbox"/>	Engedélyezze a funkciót, ha aktiválni szeretné az e-mail értesítéseket .

Egy adott [alkalmazásértesítés](#) engedélyezéséhez vagy letiltásához kattintson a **Szerkesztés** elemre az **Alkalmazásértesítések** felirat mellett.



Alkalmazásértesítések

Ha módosítani szeretné az alkalmazásértesítések láthatóságát (amelyek a képernyő jobb alsó sarkában jelennek meg), lépjen az **Eszközök > Értesítések > Általános > Alkalmazásértesítések** szakaszhoz az ESET Endpoint Antivirus További beállítások fájában.

Az értesítések listája három oszlopra van felosztva. Az értesítések neve kategóriák szerint van rendezve az első oszlopban. Annak módosításához, hogy a termék milyen módon értesítse az új eseményekről, jelölje be az adott jelölőnégyzeteket a **Megjelenítésének az asztalon**, illetve a **Küldés e-mailben** oszlopban.

A kijelölt alkalmazásértesítések megjelennek

Név	Megjelenítés az asztalon	Küldés e-mailben
ÁLTALÁNOS		
A fájl elemzésre küldése megtörtént	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
A karanténba helyezés sikertelen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Adatok elküldve a terméktámogatásnak	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anonim statisztika elküldve	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Az illesztőprogram telepítése nem sikerült	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fájl elemzése	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fájl elemzés alatt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fájl nincs elemzve	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Módosult a Felülbíráls mód	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Nem sikerült adatokat küldeni a terméktámogatásnak	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Mégse

Ha az asztali értesítések általános beállításait szeretné megadni, például azt, hogy mennyi ideig jelenjenek meg az üzenetek, illetve a megjelenő események minimális részletességét, lépjen az [Asztali értesítések](#) szakaszhoz a **További beállítások > Eszközök > Értesítések** lapon.

Az e-mailek formátumának és az SMTP-szerverbeállítások konfigurálásához lépjen az [E-mail értesítések](#) szakaszhoz a **További beállítások > Eszközök > Értesítések** lapon.

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 Antivirus elsődleges eszköze a felhasználóval való kommunikációban: értesít a sikeres termékfrissítésről, új eszköz csatlakoztatásakor, a víruskeresések befejezéséről és új kártevők észlelésekor.

Az **Asztali értesítések** szakaszban testre szabható az előugró értesítések viselkedése. A következő jellemzők állíthatók be:

Időtartam – Beállítható, hogy mennyi ideig legyenek láthatók az értesítések. 3 és 30 másodperc közötti érték adható meg.

Átlátszóság – Beállítható az értesítések átlátszóságának százalékos aránya. 0 (nem átlátszó) és 80 (nagy átlátszóság) közötti érték adható meg.

A megjelenítendő események minimális részletessége – A legördülő listában beállítható, hogy milyen súlyossági szinttől kezdve jelenjenek meg az értesítések:

- **Diagnosztikai** – Az alábbiak 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 – Írja be azoknak a felhasználói fiókoknak a teljes nevét, amelyeknek engedélyezni szeretné az asztali értesítések fogadását. Ha például a számítógépen nem csak a rendszergazdai fiókot használja, és értesülni szeretne a termékkel kapcsolatos újdonságokról.

E-mail értesítések

Az ESET Endpoint Antivirus automatikusan értesítő e-maileket tud küldeni a kiválasztott részletességi szintű események előfordulása esetén. Az [Általános](#) szakaszban jelölje be az **Értesítések küldése e-mailen keresztül** jelölőnégyzetet az e-mail-értesítések aktiválásához.

SMTP szerver

SMTP-szerver – Az értesítések küldéséhez használt SMTP-szerver (például *smtp.provider.com:587*, az előre definiált port a 25-ös).



Megjegyzés

A TLS titkosítású SMTP-szervereket nem támogatja az ESET Endpoint Antivirus.

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** – Az alábbiak 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 változtatlanul 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.

Az értesítések testreszabása

Ebben az ablakban testre szabhatja az értesítésekben használt üzeneteket.

Alapértelmezett értesítési üzenet – Az értesítések láblécén megjelenítendő alapértelmezett üzenet.

Kártevők

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 **Kártevőkre vonatkozó értesítés** mezőbe az egyéni értesítési üzenet használatához.

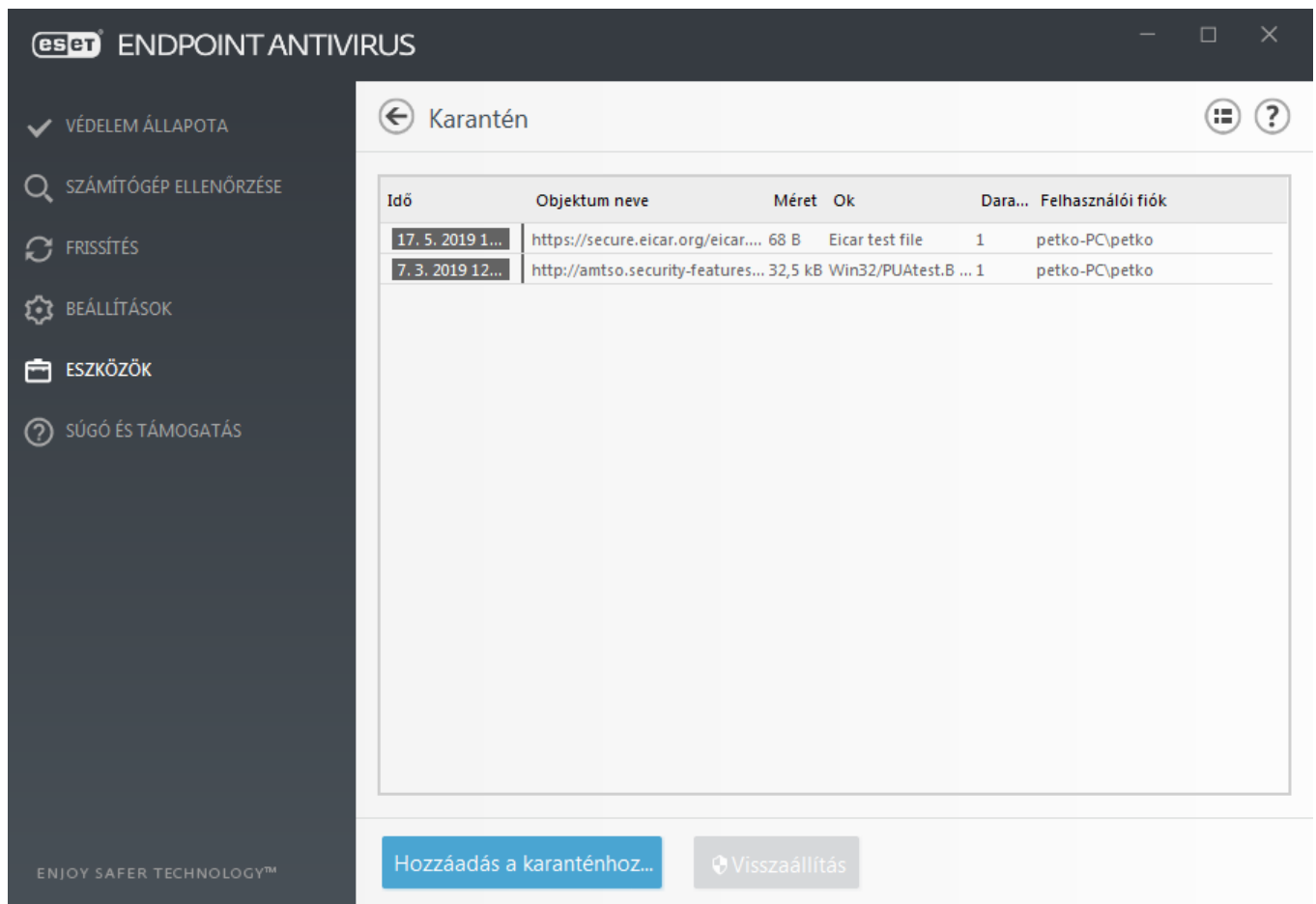
Karantén

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

A karantén az ESET Endpoint Antivirus fő programablakából érhető el az **Eszközök > Karantén** elemre kattintva.

Karanténba helyezheti bármelyik fájlt, illetve az áthúzási funkció segítségével manuálisan karanténba helyezheti a kívánt fájlt. Ehhez kattintson rá, tartsa lenyomva az egér gombját, és vigye az egérmutatót a megjelölt területre,

majd engedje fel. Ezután az alkalmazás az előtérbe kerül. Egy fájlt akkor érdemes karanténba helyezni, ha gyanús a viselkedése, viszont a víruskereső nem észleli. A karanténba helyezett fájlok elemzés céljából elküldhetők az ESET víruslaborjának.



A karanténmappában lévő fájlokat egy táblázat jeleníti meg, amelyben látható a karanténba helyezés dátuma és időpontja, a fertőzött fájl eredeti helyének elérési útja, a fájl bájttban megadott mérete, a karanténba helyezés oka (például a felhasználó vette fel az objektumot) és a fertőzések száma.

Fájlok karanténba helyezése

Az ESET Endpoint Antivirus automatikusan karanténba helyezi a törölt fájlokat (ha nem tiltotta le ezt a beállítást a riasztási ablakban). Szükség esetén a **Karanténba helyezés elemre kattintva bármely gyanús fájlt karanténba helyezhet manuálisan is**. Az eredeti fájlt a program eltávolítja az eredeti helyéről. A művelet a helyi menüből is végrehajtható: kattintson a jobb gombbal a **Karantén** ablakra, és válassza ki a **Karanténfájl** lehetőséget.

Visszaállítás a karanténból

A karanténba helyezett fájlok visszaállíthatók az eredeti helyükre. Ha vissza szeretne állítani egy karanténba helyezett fájlt, kattintson a jobb gombbal a Karantén ablakra, és a helyi menüből válassza a **Visszaállítás** parancsot. Ha [kéretlen alkalmazásként](#) van megjelölve egy fájl, a **Visszaállítás és kizárás az ellenőrzésből** opció is elérhető. A helyi menüben megtalálható a **Visszaállítás megadott helyre** parancs is, amellyel nem csak abba a mappába állíthatók vissza a fájlok, amelyből törölték őket.

Törlés a karanténból – Kattintson a jobb gombbal egy adott elemre, és válassza a **Törlés a karanténból** parancsot, vagy jelölje ki a törlendő elemet, és a billentyűzetten nyomja le a **Delete** billentyűt. Kijelölhet és egyszerre törölhet több elemet is.



Megjegyzés

Ha a program tévesen helyezett karanténba egy ártalmatlan fájlt, akkor a visszaállítása után [zárja ki azt az ellenőrzésből](#), és küldje el az ESET műszaki támogatási szolgálatához.

Fájl elküldése a karanténból

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

A proxyszerver beállításai

Nagyméretű helyi hálózatokon a számítógép és az internet közötti kommunikáció egy proxyszerveren keresztül folyhat. E konfiguráció használatakor meg kell adni az alábbi beállításokat, különben előfordulhat, hogy a program nem frissül automatikusan. Az ESET Endpoint Antivirus 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 Antivirus összes globális proxyszerver-beállítását meghatározza. Az itt található paramétereket fogja használni az internetkapcsolatot igénylő összes modul.

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

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



Megjegyzés

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

Közvetlen kapcsolat használata, ha nem érhető el proxy – Ha az ESET Endpoint Antivirus proxy használatára van konfigurálva, és a proxy nem érhető el, az ESET Endpoint Antivirus 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.

További beállítások

KERESŐMOTOR 1

FRISSÍTÉS 4

HÁLÓZATI VÉDELEM

WEB ÉS E-MAIL 3

ESZKÖZFELÜGYELET 1

ESZKÖZÖK 3

Naplófájlok

Proxyszerver 1

E-mail értesítések 3

Bemutató üzemmód

Diagnosztika

FELHASZNÁLÓI FELÜLET 1

PROXYSZERVER

Proxyszerver használata

Proxyszerver

Port

A proxyszerver hitelesítést igényel

Felhasználónév

Jelszó

Proxyszerver felismerése

Közvetlen kapcsolat használata, ha nem érhető el proxy

Alapbeállítás

OK

Mégse

Időközök

Létrehozásuk után az időközök az **Eszközfelügyelet**. Az **Időközök** beállítás a **További beállítások > Eszközök** lapon található. 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.

Időközök

Név

Leírás

Work time

Weekdays 8:00-17:00

Off-work

Evenings & weekends

Hozzáadás

Szerkesztés

Törlés

OK

Mégse

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 műveletet.

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](#).

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 Antivirus 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 Antivirus 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 Antivirus naponta csak egyszer, illetve a számítógép újraindulásakor ellenőrzi a licencszervert.



Fontos

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 Antivirus-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 Antivirus 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 Antivirus minimalista felhasználói felületének beállítása](#) (felügyelt környezetben hasznos).

Felhasználói felület elemei

Az ESET Endpoint Antivirus felhasználói felületének beállításai lehetővé teszik, hogy a felhasználó a saját igényei szerint alakítsa ki munkakörnyezetét. Ezek a beállítások az ESET Endpoint Antivirus 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.



Megjegyzés

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 Antivirus** pontjából. Az ESET Security Management Center segítségével, házi rendet használva is elvégezheti ezt.

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

Ha azt szeretné, hogy az ESET Endpoint Antivirus 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 Antivirus parancsainak beillesztése a helyi menükbe.

Állapotok

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

Licenc adatok

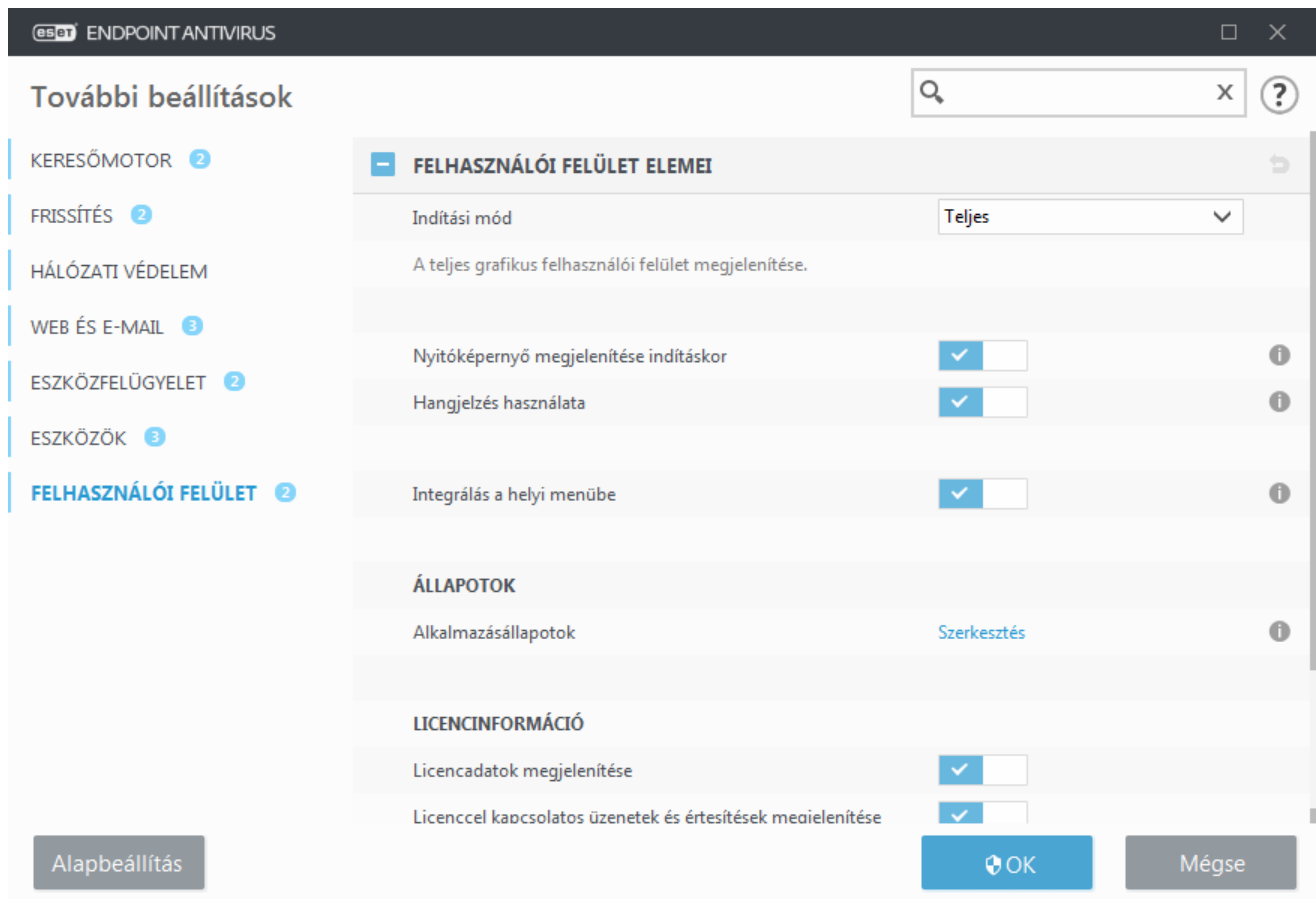
Licenc adatok megjelenítése – Ha le van tiltva, a licenc lejárat dátuma a **Védelem állapota** és a **súgó és támogatás** képernyőn nem jelenik meg.

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



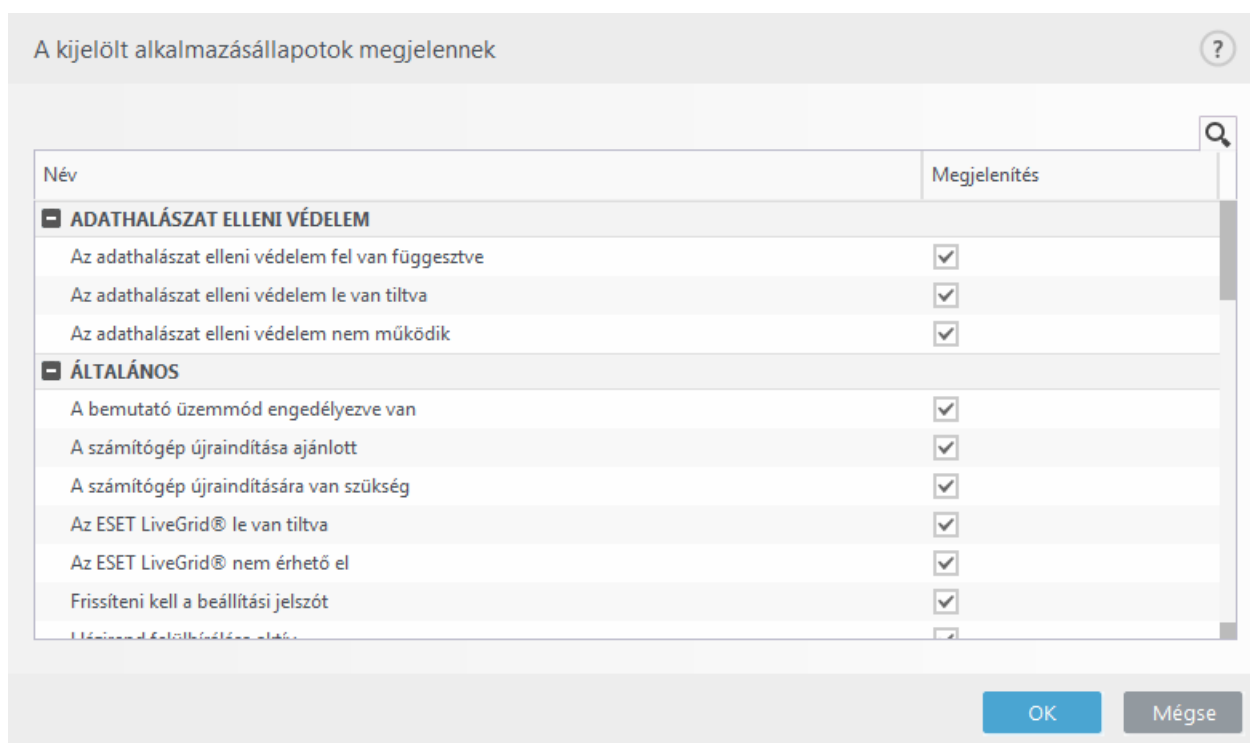
Megjegyzés

A licenc adatok beállításai érvényesek, de nem érhetők el MSP-licenccel aktivált ESET Endpoint Antivirus esetén.



Alkalmazásállapotok

Az ESET Endpoint Antivirus első ablaktábláján megjelenő termékállapotok beállításához lépjen a **Felhasználói felület > Felhasználói felület elemei > Alkalmazásállapotok** szakaszhoz az ESET Endpoint Antivirus További beállítások fájlban.



Itt engedélyezheti vagy letilthatja a különböző alkalmazásállapotok megjelenítését. Erre például a vírus- és kémprogramvédelem szüneteltetése vagy a bemutató üzemmód engedélyezése esetén lehet szükség. Akkor is megjelenik alkalmazásállapot, ha a termék nincs aktiválva, vagy ha lejárt a licenc. Ez a beállítás az [ESET Security Management Center házirendjein](#) keresztül módosítható.

Hozzáférési beállítások

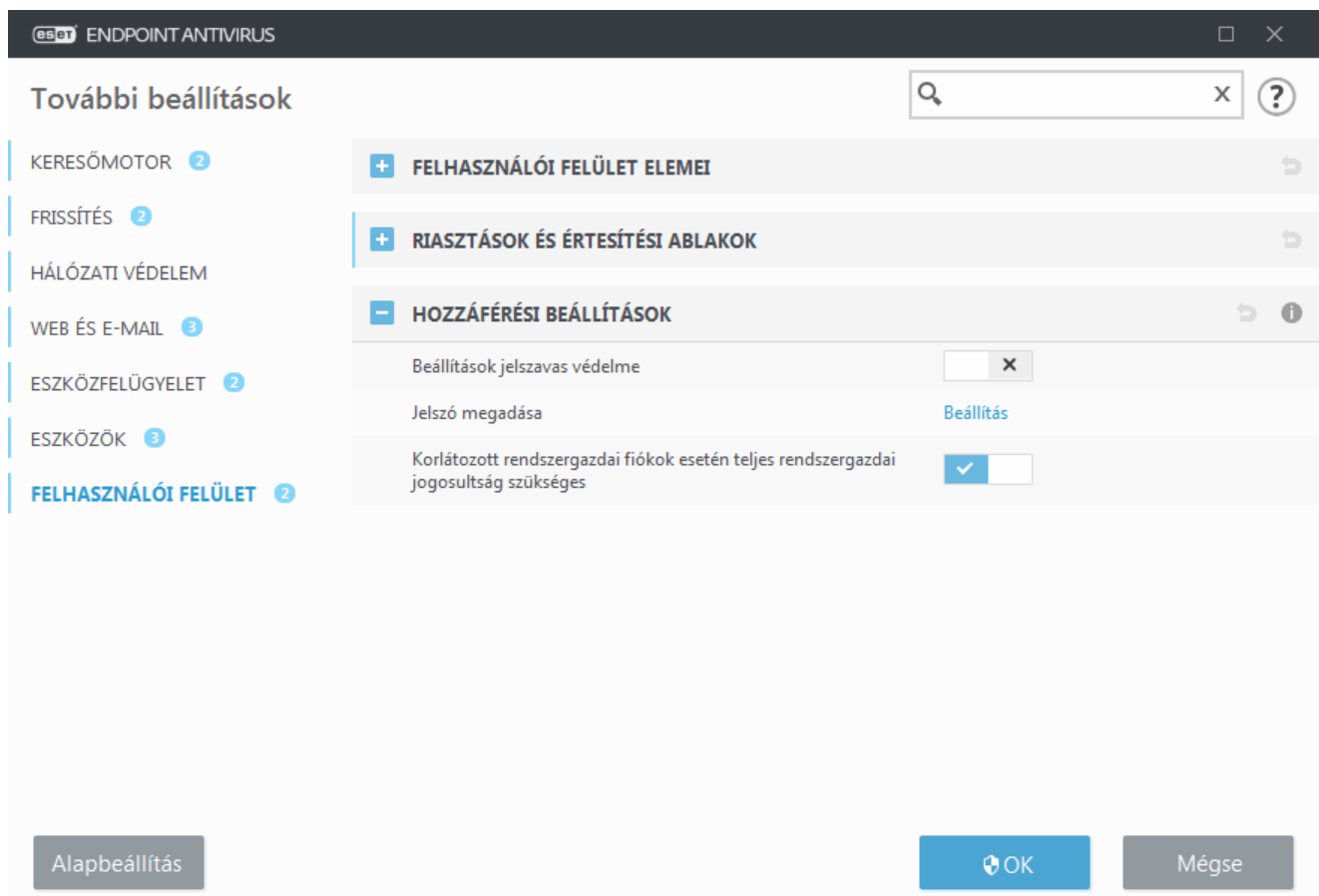
A rendszer maximális biztonsága érdekében fontos, hogy az ESET Endpoint Antivirus megfelelően legyen konfigurálva. A nem hozzáértő módosítások akár a lényeges adatok elvesztéséhez is vezethetnek. A jogosulatlan módosítások elkerülése érdekében az ESET Endpoint Antivirus beállításai jelszóval védhetők.

Felügyelt környezetek

A rendszergazda egy házirend létrehozásával megvédheti jelszóval az ESET Endpoint Antivirus 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.

Korlátozott rendszergazdai fiókok esetén teljes rendszergazdai jogosultság szükséges – Hagyja bekapcsolva ezt az opciót, ha az aktuális felhasználótól (ha nem rendelkezik rendszergazdai jogosultsággal) rendszergazdai felhasználónevet és jelszót szeretne kérni egyes rendszerparaméterek módosításakor (a Windows Vista rendszer UAC szolgáltatásához hasonlóan). A módosítások közé tartozik a védelmi modulok kikapcsolása.

Csak Windows XP esetén:

Rendszergazdai jogosultság bekérése (UAC-támogatás nélküli rendszer esetén) – Engedélyezze ezt az opciót, ha azt szeretné, hogy az ESET Endpoint Antivirus rendszergazdai hitelesítő adatokat kérjen.

Jelszó a További beállításokhoz

Ha az ESET Endpoint Antivirus 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 Antivirus 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 Antivirus 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 \(7.0-s és régebbi verziók\)](#)

[Kattintson ide, ha elfelejtette az ESET által biztosított licenckulcsot](#), a licenc lejáratát vagy az ESET Endpoint Antivirus egyéb licenclési adatait.

Riasztások és értesítési ablakok



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 **Felhasználói felület** részben található **Riasztások és értesítési ablakok** (korábban **Riasztások és értesítések**) szakasz segítségével beállítható, hogy az észlelt elemeket hogyan kezelje az ESET Endpoint Antivirus, 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

ESET Endpoint Antivirus 7.2-es és újabb verzió:

- Nem felügyelt felhasználók esetén azt javasoljuk, hogy maradjon meg az alapértelmezett beállítás (aktiválva).

- Felügyelt felhasználók esetén hagyja aktíválva 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).

ESET Endpoint Antivirus 7.1-es és korábbi verzió:

A beállítás neve **Riasztások megjelenítése**, és nem lehet testreszabni előre meghatározott műveleteket bizonyos interaktív riasztási ablakok esetén.

Asztali értesítések

Az [asztali](#) és buborékértesítések csupán a tájékoztatást szolgálják, nem igényelnek felhasználói beavatkozást. Az **Asztali értesítések** szakasz átkerült a További beállítások **Eszközök > Értesítések** lapjára (7.1-es és újabb verziók).

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

Ez a szakasz bemutat több olyan interaktív riasztási ablakot, amelyet az ESET Endpoint Antivirus megjelenít bármilyen művelet végrehajtása előtt.

A konfigurálható interaktív riasztások viselkedésének beállításához lépjen a **Felhasználói felület > Riasztások és értesítési ablakok > Interaktív riasztások listája** lapra az ESET Endpoint Antivirus További beállítások fájában, majd kattintson a **Szerkesztés** elemre.



Cél

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.

Válassza ki, mely interaktív riasztások jelenjenek meg ?

Név	Rákérdez	Művelet alkalmazva, amikor nincs meg...
Cserélhető adathordozók		
Új eszköz észlelve	<input checked="" type="checkbox"/>	Ellenőrzési beállítások megjelenítése
Hálózati védelem		
Hálózathoz való hozzáférés letiltva	<input checked="" type="checkbox"/>	Nincs
Hálózati kommunikáció blokkolva	<input checked="" type="checkbox"/>	Tiltás
Hálózati kártevő letiltva	<input checked="" type="checkbox"/>	Tiltás
Webbongészós riasztások		
A program nemkívánatos tartalmat talált	<input checked="" type="checkbox"/>	Tiltás
Webhely blokkolva adathalászat miatt	<input checked="" type="checkbox"/>	Tiltás

OK Mégse

Tekintsen meg a kívánt interaktív riasztási ablak súgóoldalát is:

Cserélhető adathordozók

- [Új eszköz észlelve](#)

Hálózati védelem

- A [Hálózathoz való hozzáférés letiltva](#) riasztás akkor jelenik meg, ha aktiválódik a munkaállomás **Számítógép elkülönítése a hálózattól** kliensfeladata az ESMC felől.
- [Hálózati kommunikáció blokkolva](#)
- [Hálózati kártevő letiltva](#)

Webbongészós 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 \(ajánlott\)](#)



Korlátozások

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 Antivirus További beállítások fájában, majd kattintson a **Szerkesztés** elemre.

A kijelölt üzenetek jelennek meg

- ☒ A Windows Live Mail levelezőprogram termékmegerősítési párbeszédpaneinek megjelenítése
- ☒ 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 párbeszédpaneinek megjelenítése
- ☒ Az Outlook levelezőprogram termékmegerősítési párbeszédpaneinek megjelenítése
- ☒ Rákérdezés a Feladatütemezőben ütemezett feladatok eltávolítása előtt
- ☒ Rákérdezés a Feladatütemezőben ütemezett feladatok futtatása előtt
- ☒ Rákérdezés a bejegyzések naplóból történő eltávolítása előtt
- ☐ Rákérdezés a beállítások elvetése előtt a További beállítások ablakban
- ☒ Rákérdezés a statisztika alaphelyzetbe állítása előtt
- ☒ Rákérdezés az ESET SysInspector-naplók törlése előtt

OK Mégse

Ezen a párbeszédpanelen az ESET Endpoint Antivirus által a műveletek végrehajtása előtt megjelenített megerősítési üzeneteket találja. Az egyes üzenetek melletti jelölőnégyzetek bejelölésével vagy jelölésük törlésével engedélyezheti vagy letilthatja az üzeneteket.

A további beállításokkal kapcsolatos ütközési hiba

Ez a hiba akkor fordulhat elő, ha valamely összetevő (pl. a behatolásmegelőző rendszerés a felhasználó egyidejűleg interaktív vagy tanuló módban hozzák létre a szabályokat.



Fontos

Saját szabályok létrehozásához javasoljuk, hogy változtassa a szűrési módot az alapértelmezett **Automatikus üzemmódra**. Bővebben lásd: [A behatolásmegelőző rendszer és a szűrési üzemmódok](#).

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.

Select which interactive alert will be displayed

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

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 Antivirus fő programablakában, az [Alkalmazásállapotok ablakban](#) törölje a jelet **A számítógép újraindítása szükséges** és **A számítógép újraindítása ajánlott** jelölőnégyzetből.

Selected application statuses will be displayed

Name	Show
- DEVICE CONTROL	
Device control is not fully functional	<input checked="" type="checkbox"/>
Device control is paused	<input checked="" type="checkbox"/>
- GENERAL	
Computer restart recommended	<input type="checkbox"/>
Computer restart required	<input type="checkbox"/>
ESET LiveGrid® is disabled	<input checked="" type="checkbox"/>
ESET LiveGrid® is not accessible	<input checked="" type="checkbox"/>
Policy override active	<input checked="" type="checkbox"/>
Presentation mode is enabled	<input checked="" type="checkbox"/>
Settings password has to be updated	<input checked="" type="checkbox"/>
Windows updates available	<input checked="" type="checkbox"/>

OK Cancel

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.

Select which interactive alert will be displayed ?

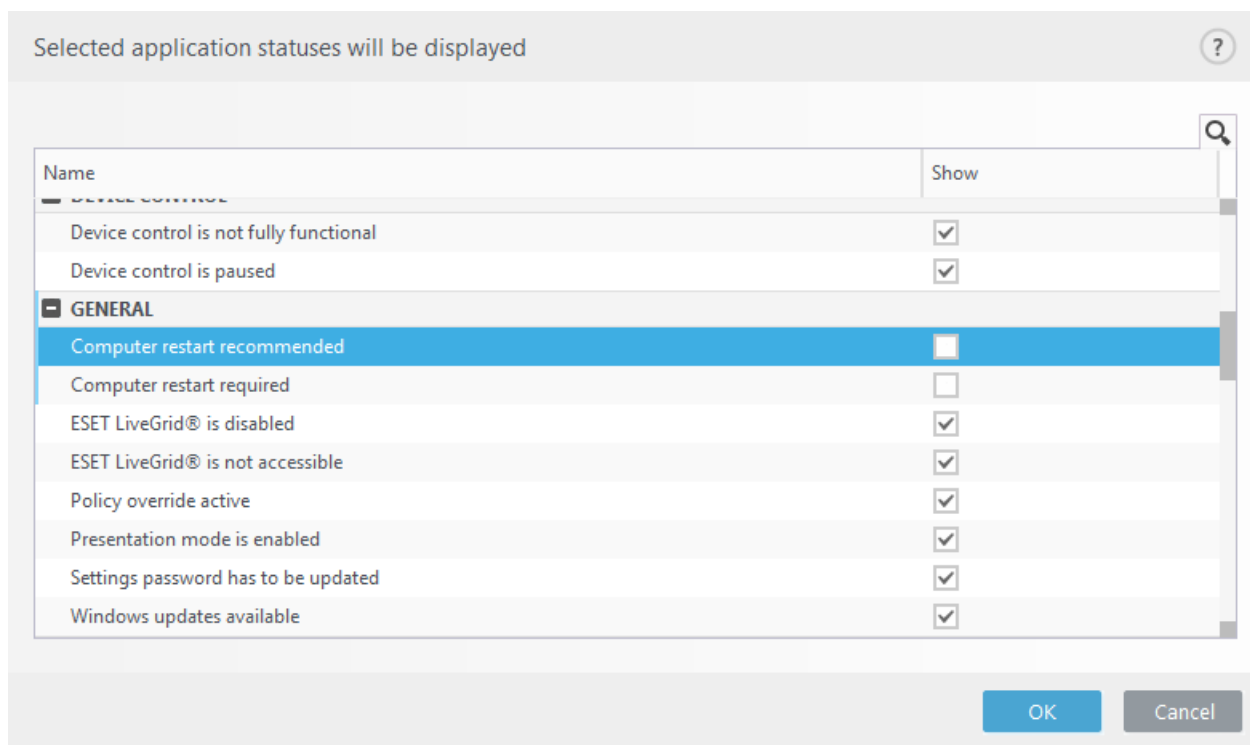
Name	Ask user	Action applied when not displayed
Removable media		
Network protection		
Web browser alerts		
Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

3.Az **OK** gombra kattintva mentse a módosításokat mindkét megnyitott ablakban.

4.A figyelmeztetések ezután nem fognak megjelenni a végpontgépen.

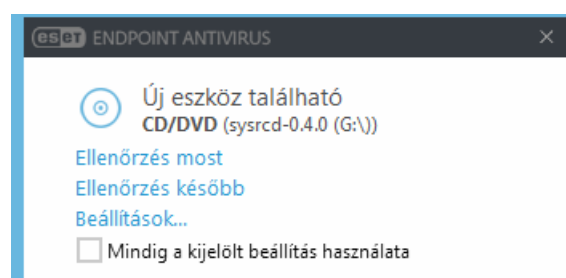
5.(opcionális) Ha le szeretné tiltani az alkalmazásállapotokat az ESET Endpoint Antivirus fő programablakában, az [Alkalmazásállapotok ablakban](#) törölje a jelet **A számítógép újraindítása szükséges** és **A számítógép újraindítása ajánlott** jelölőnégyzetből.



Cserélhető adathordozók

Az ESET Endpoint Antivirus lehetővé teszi a cserélhető adathordozók (CD, DVD, USB stb) automatikus ellenőrzését a számítógépbe való behelyezésük után. Ez különösen hasznos lehet akkor, ha a számítógép rendszergazdája meg kívánja akadályozni, hogy a felhasználók kéretlen tartalmú cserélhető adathordozót helyezzenek a számítógépbe.

Az alábbi párbeszédpanel jelenik meg, ha cserélhető adathordozót helyeznek be, és az **Ellenőrzési beállítások megjelenítése** funkció be van állítva az ESET Endpoint Antivirus szolgáltatásban:



A párbeszédpanel beállításai:

- **Ellenőrzés most** – Erre a hivatkozásra kattintva elindíthatja a cserélhető adathordozó ellenőrzését.
- **Ellenőrzés később** – Ezzel elhalaszthatja a cserélhető adathordozó ellenőrzését.
- **Beállítások** – Megnyílik a **További beállítások** szakasz.
- **Mindig a kijelölt beállítás használata** – A jelölőnégyzet bejelölése esetén ugyanazt a műveletet végzi el a program, amikor legközelebb cserélhető adathordozót helyez be.

Az ESET Endpoint Antivirus tartalmazza ezenkívül az Eszközfelügyelet funkciót, amely lehetővé teszi külső eszközök adott számítógépen való használatának szabályozását. Az eszközfelügyeletről további tudnivalókat olvashat az [Eszközfelügyelet](#) című szakaszban.

ESET Endpoint Antivirus 7.2 és újabb

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 **Rákérdez** lehetőség nincs kiválasztva, válassza ki a kívánt műveletet, miután behelyezett 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.
- **Ellenőrzési beállítások megjelenítése** – Megnyitja az **Interaktív riasztások** beállítási szakaszt.

ESET Endpoint Antivirus 7.1 és korábbi

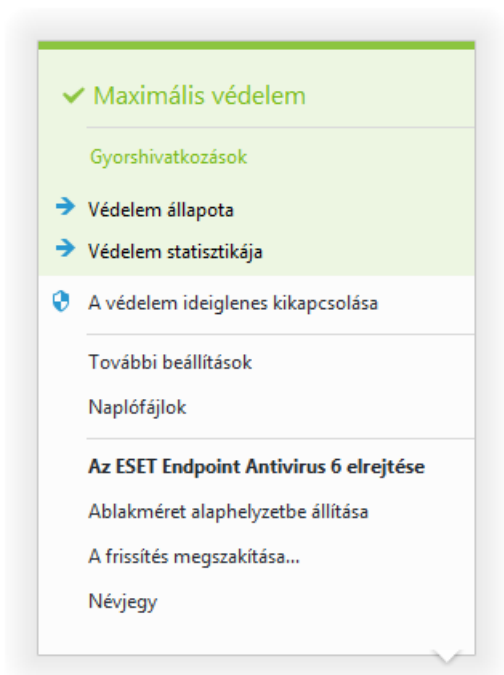
A cserélhető adathordozók ellenőrzésére vonatkozó beállítások kezeléséhez nyissa meg a További beállítások (F5) > Keresőmotor > Kártevő-ellenőrzések > Cserélhető adathordozók ablakot.

A cserélhető adathordozó behelyezése után szükséges művelet – Válassza ki a cserélhető adathordozó (CD/DVD/USB) számítógépbe történő behelyezését követően végrehajtandó alapértelmezett műveletet. Válassza ki, hogy milyen művelet menjen végbe, miután cserélhető adathordozót helyeztek a számítógépbe:

- **Nincs ellenőrzés** – Nincs művelet, és az **Új eszköz található** ablak nem nyílik meg.
- **Eszköz automatikus ellenőrzése** – A behelyezett cserélhető adathordozó eszköz ellenőrzése.
- **Ellenőrzési beállítások megjelenítése** – Megnyitja a **Cserélhető adathordozók** csoportot.

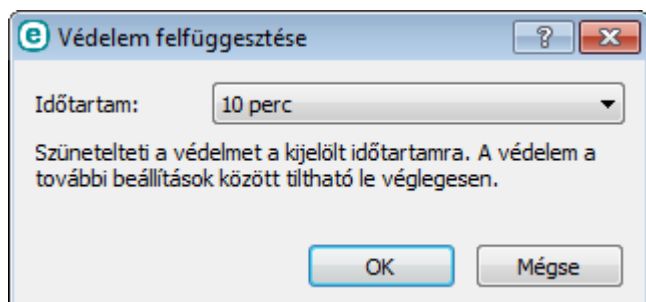
A rendszer tálcáikonja

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



A védelem ideiglenes kikapcsolása – Megjeleníti a fájlok, a webes tevékenységek és az elektronikus levelezés felügyeletén keresztül a rendszert a kártevőktől és támadásoktól védő [Keresőmotort](#) letiltó megerősítési párbeszédpanelt.

Az **Időpont** legördülő listában adhatja meg, hogy milyen időtartamra szeretné letiltani a védelmet.



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 Antivirus megnyitása – Megnyílik az ESET Endpoint Antivirus fő programablaka a tálcáikonról.

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

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

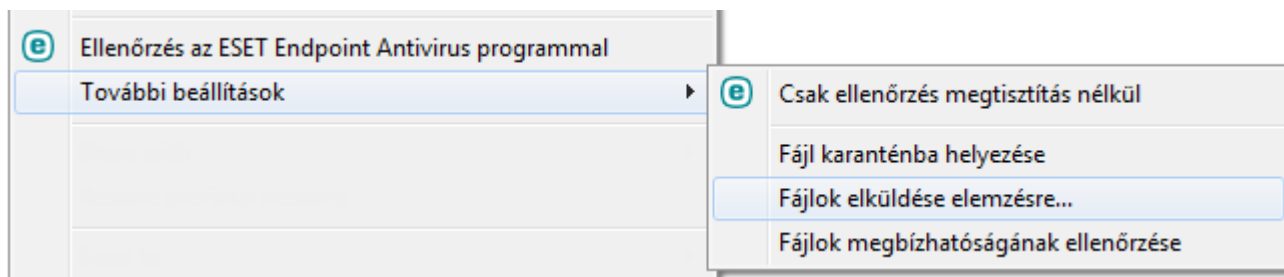
Névjegy – Megjeleníti a rendszer-információkat, köztük az ESET Endpoint Antivirus telepített verziójának számát és a telepített programmodulok adatait, valamint a licenc lejáratát. Az operációs rendszerrel és a rendszererőforrásokkal kapcsolatos információk az oldal alján találhatók.

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 Antivirus 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 Antivirus parancsainak beillesztése a helyi menükbe.



Súgó és támogatás

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

Súgó

Keresés az ESET tudásbázisban – 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.

A súgó megnyitása – Kattintson erre a hivatkozásra az ESET Endpoint Antivirus súgójának megnyitásához.

Gyakori kérdések megoldásai – Erre a hivatkozásra kattintva megoldásokat találhat a leggyakrabban előforduló problémákra. Mielőtt a műszaki támogatási szolgálathoz fordulna, érdemes elolvasni ezeket a rövid útmutatókat.

Műszaki terméktámogatás

Terméktámogatási kérelem küldése – Ha nem talál megoldást a problémájára, az ESET webhelyén megtalálható űrlapon keresztül gyorsan kapcsolatba léphet műszaki támogatási szolgálatunkkal.

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.

Támogatási eszközök

Kártevő-enciklopédia – Az ESET kártevő-enciklopédiájára mutató hivatkozásokkal az egyes fertőzések különféle típusainak veszélyeire és tüneteire vonatkozó információkat kereshet.

A keresőmotor előzményei – Az ESET Vírusradarra mutató hivatkozások, amelyek az ESET kereső-adatbázis (korábbi nevén „vírusdefiníciós adatbázis”) egyes verzióira vonatkozó információkra mutatnak.

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 naplót, hogy segítségükkel gyorsabban megoldhassa a problémákat. További információkért tekintse meg az [ESET Log Collector online felhasználói útmutatóját](#).

ESET Speciális eltávolító – Általános kártevőfertőzések eltávolító eszköze. További információkat az [ESET tudásbáziscikkében](#) talál.

Termék- és licencinformációk

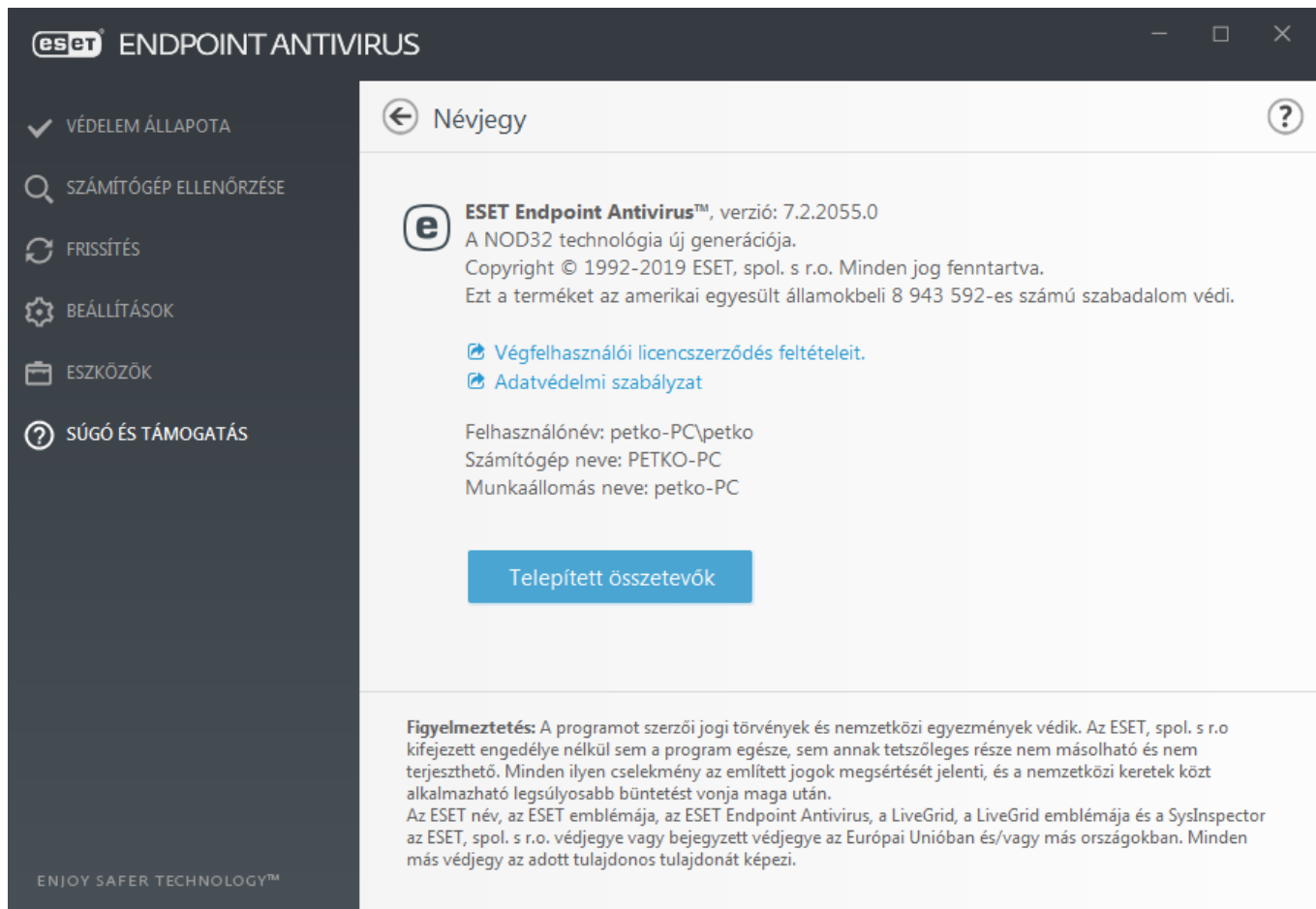
Az ESET Endpoint Antivirus névjegye– Információkat jelenít meg az [ESET Endpoint Antivirus](#) példányáról.

Licenc aktiválása/Licenc módosítása – Kattintson ide az aktiválási ablak elindításához és a licenc aktiválásához.

Az ESET Endpoint Antivirus névjegye

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

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



eset ENDPOINT ANTIVIRUS

✓ VÉDELEM ÁLLAPOTA

🔍 SZÁMÍTÓGÉP ELLENŐRZÉSE


🔄 FRISÍTÉS

⚙️ BEÁLLÍTÁSOK

📁 ESZKÖZÖK

❓ SÚGÓ ÉS TÁMOGATÁS

← Névjegy ⓘ

 **ESET Endpoint Antivirus™**, verzió: 7.2.2055.0
A NOD32 technológia új generációja.
Copyright © 1992-2019 ESET, spol. s r.o. Minden jog fenntartva.
Ezt a terméket az amerikai egyesült államokbeli 8 943 592-es számú szabadalom védi.

[Végfelhasználói licencszerződés feltételeit.](#)
[Adatvédelmi szabályzat](#)

Felhasználónév: petko-PC\petko
Számítógép neve: PETKO-PC
Munkaállomás neve: petko-PC

Telepített összetevők

Figyelmeztetés: A programot szerzői jogi törvények és nemzetközi egyezmények védik. Az ESET, spol. s r.o. kifejezett engedélye nélkül sem a program egésze, sem annak tetszőleges része nem másolható és nem terjeszthető. Minden ilyen cselekmény az említett jogok megsértését jelenti, és a nemzetközi keretek közt alkalmazható legsúlyosabb büntetést vonja maga után.
Az ESET név, az ESET emblémája, az ESET Endpoint Antivirus, a LiveGrid, a LiveGrid emblémája és a SysInspector az ESET, spol. s r.o. védjegye vagy bejegyzett védjegye az Európai Unióban és/vagy más országokban. Minden más védjegy az adott tulajdonos tulajdonát képezi.

ENJOY SAFER TECHNOLOGY™

Rendszer-konfigurációs adatok küldése

A lehető leggyorsabb és legpontosabb segítségnyújtáshoz az ESET számára meg kell adnia az ESET Endpoint Antivirus konfigurációját, a részletes rendszer-információkat, a futó folyamatokra vonatkozó adatokat (az [ESET SysInspector naplófájliját](#)), 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 a **Mindig küldje el ezeket az információit** opciót, ha szeretné menteni ezt 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.



Megjegyzés

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.

Profilkezelő

A profilkezelőt az ESET Endpoint Antivirus 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 céltérületekkel, 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, [A ThreatSense keresőmotor beállításai](#) című részben megtalálja az ellenőrzési beállítások egyes paramétereinek a leírását.



Megjegyzés

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 Antivirus 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)
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 Antivirus 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

Eszközfelügyelet speciális naplózásának engedélyezése – Az Eszközfelügyelet modulban előforduló összes esemény rögzítése. Ez segíteni tud a fejlesztőknek az Eszközfelügyelet modullal kapcsolatos problémák felismerésében és javításában.

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.

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.

Scanner részletes naplózásának engedélyezése – Rögzíthetők azok a problémák, amelyek akkor lépnek fel, amikor a Számítógép ellenőrzése, illetve a Valós idejű fájlrendszervédelem ellenőrzi a fájlokat és a mappákat (a 7.2-es és újabb verziókban).

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 Szülői felügyelet modulban előforduló összes esemény rögzítése. Ez segíti a fejlesztőket a Szülői felügyelet modullal kapcsolatos problémák felismerésében és javításában.

Naplófájl helye

Operációs rendszer	Naplófájl könyvtára
Windows Vista és újabb	C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics\
A következő korábbi verziói: Windows	C:\Documents and Settings\All Users\...

Parancssori víruskereső

Az ESET Endpoint Antivirus vírusvédelmi modulja a parancssor használatával is elindítható – akár manuálisan az „ecls” parancssal, akár egy .bat kiterjesztésű kötegfájllal. Az ESET parancssoros ellenőrzőjének szintaxisa:

```
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 megabájtjánál 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 másodperccig
/max-arch-size=MÉRET	csak a MÉRET bájtjánál kisebb fájlok ellenőrzése tömörített fájlok esetén (alapbeállítás: 0 = korlátlan)

/max-sfx-size=MÉRET	önkicsomagoló tömörített fájlokban csak a MÉRET megadójánál 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 megtisztítási MÓD használata a fertőzött objektumokhoz
/clean-mode=MÓD	A választható lehetőségek az alábbiak:
	• none (nincs) – Nem történik automatikus tisztítás.
	• standard (normál, alapbeállítás) – Az ecl.s.exe megkísérli automatikusan megtisztítani vagy törölni a fertőzött fájlokat.
	• strict (teljes) – Az ecl.s.exe megkísérli felhasználói beavatkozás nélkül, automatikusan megtisztítani vagy törölni a fertőzött fájlokat (nem kell jóváhagynia a fájlok törlését).
	• rigorous (alapos) – Az ecl.s.exe a tisztítás megkísérlése nélkül törli a fájlokat, függetlenül attól, hogy milyen fájlról van szó.
/quarantine	• delete (törlés) – Az ecl.s.exe a tisztítás megkísérlése nélkül törli a fájlokat, a fontos fájlokat, például a Windows rendszerfájljait azonban meghagyja.
	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



Megjegyzés

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 Antivirus-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 fájl 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, vagy a jelszó nem egyezik meg, illetve ha az .xml/konfigurációs fájl nincs aláírva, a rendszer nem importálja a konfigurációt.

Az ESET CMD engedélyezését követően parancssor használatával importálhat és exportálhat ESET Endpoint Antivirus-konfigurációkat. Ezt végezheti manuálisan, illetve automatizálási célból létrehozhat egy parancsfájlt.



Fontos

Speciális ecmd parancsok használatához rendszergazdai jogosultságokkal kell futtatnia őket, vagy a **Futtatás rendszergazdaként** parancssal 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.



Megjegyzés

A speciális ecmd parancsok csak helyileg futtathatók. Kliensfeladatot az ESMC **Run command** (Parancs futtatása) parancsával nem lehet végrehajtani.



Példa

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>`



Fontos

A `/version` paraméter értéke az ESET Endpoint Antivirus verziójától függ. A 7-es és az újabb verziókhoz a következőt használja: `/version 2`.

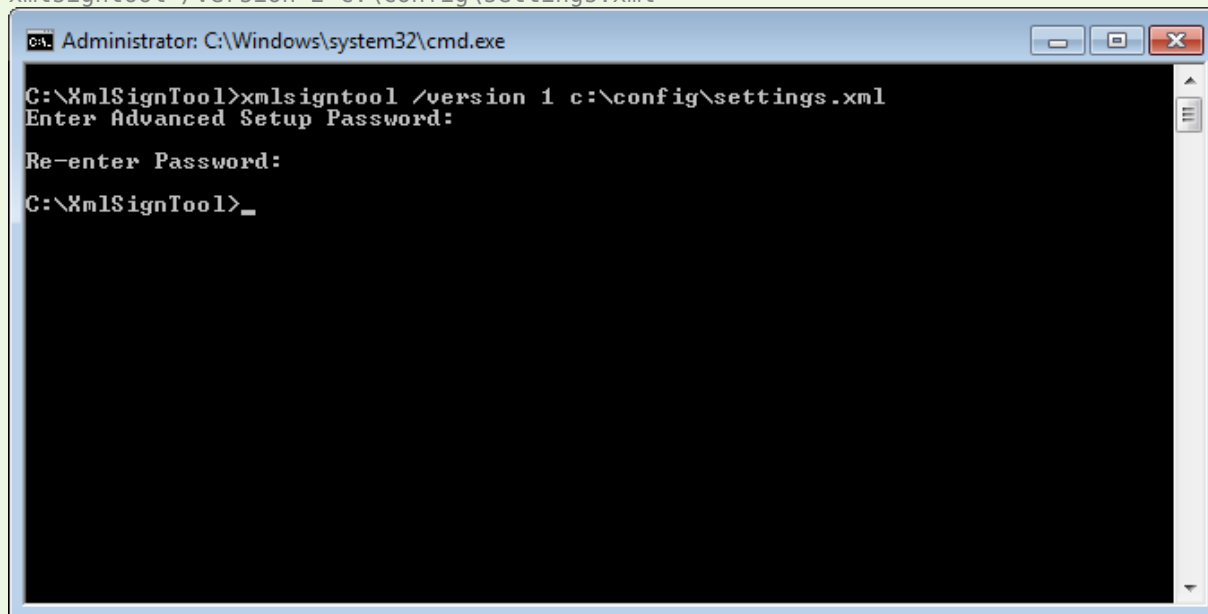
5. Az XmlSignTool kérésére adja meg, majd újból adja meg a [további beállítások jelszavát](#). Az .xml/konfigurációs fájl most már alá van írva, és használható importáláshoz a ESET Endpoint Antivirus másik példányán az ESET CMD funkció beállítások jelszava hitelesítési módjának használatával.



Példa

Exportált konfigurációs fájl aláírási parancs:

```
xmlsigntool /version 2 c:\config\settings.xml
```



Megjegyzés

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 Antivirus.



Figyelmeztetés

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 végezzenek.

Az ecmd-parancsok listája

A Futtatás ESMC-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
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 Antivirus testre szabott .xml konfigurációs fájlját a **Beállítások** menüből importálhatja, illetve exportálhatja.

Mindkét művelet hasznos abban az esetben, ha az ESET Endpoint Antivirus 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.

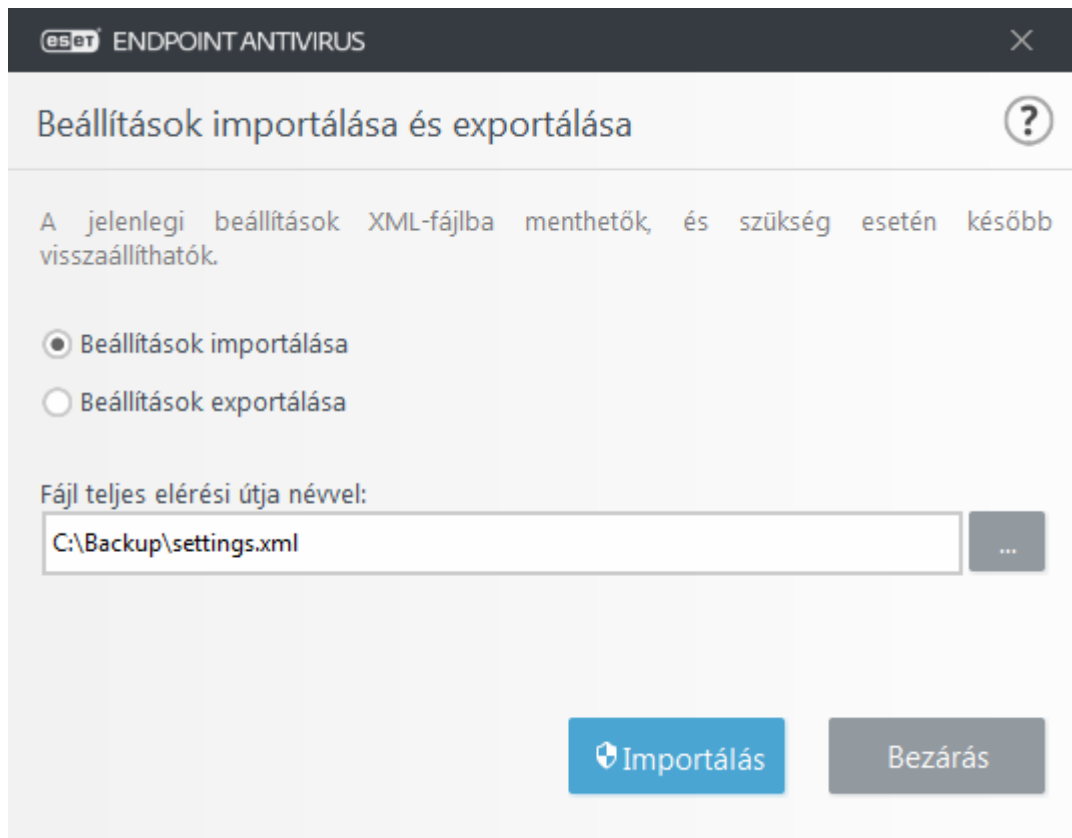
A konfigurációk importálása igen egyszerű: A program főablakában válassza a **Beállítások > Beállítások importálása és exportálása** lehetőséget, és jelölje be a **Beállítások importálása** választógombot. Írja be a konfigurációs fájl nevét, vagy a ... gombra kattintva keresse meg az importálandó fájlt.

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.



Megjegyzés

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 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 Antivirus alapértelmezett telepítése tartalmazza az `ermm.exe` nevű fájlt a végpontalkalmazásban, a könyvtárban 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-ügynökökkel 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 Antivirus](#)

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](#)

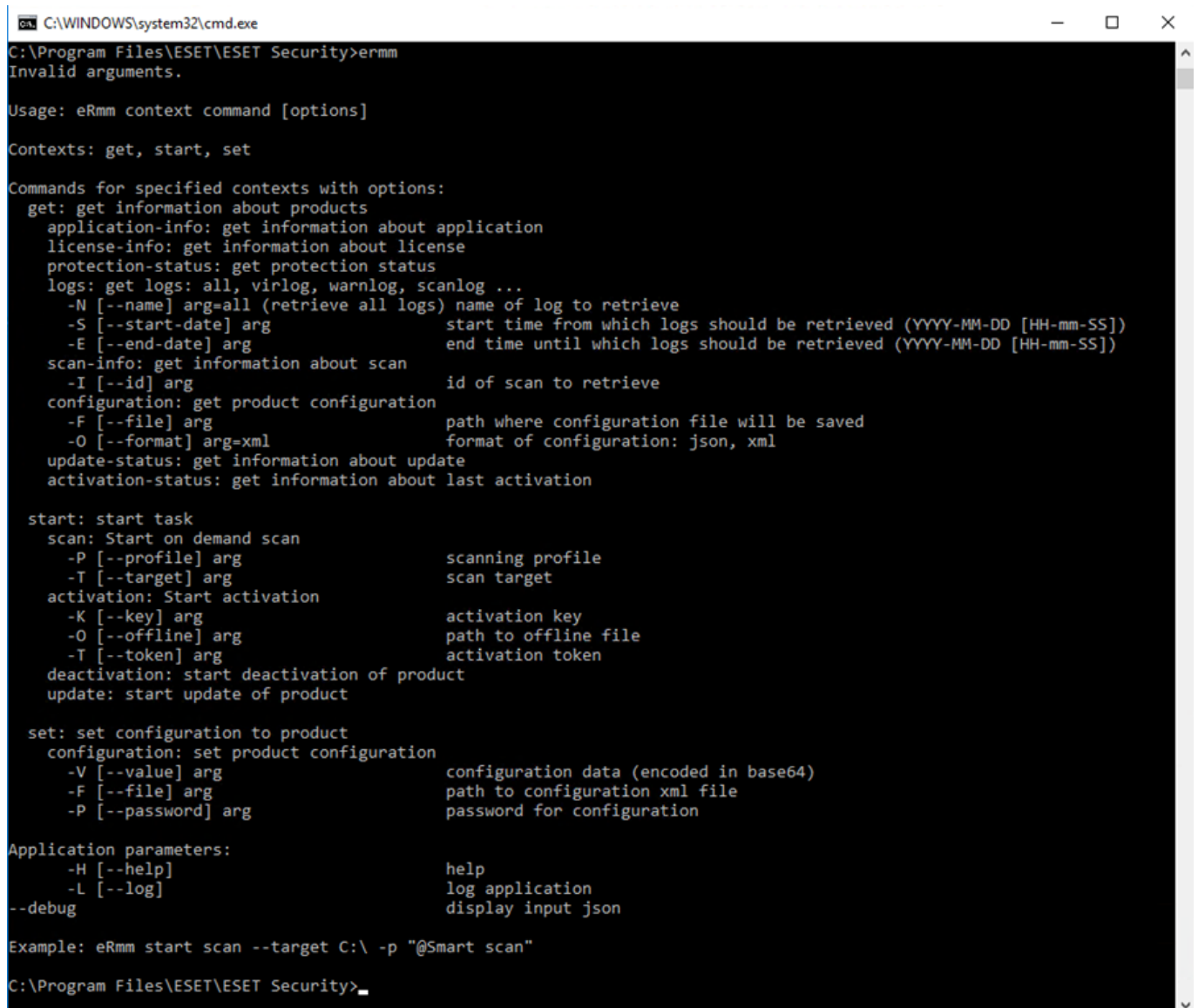
Az ERMM-parancssor

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus 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.



```

C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:
get: get information about products
  application-info: get information about application
  license-info: get information about license
  protection-status: get protection status
  logs: get logs: all, virlog, warnlog, scanlog ...
    -N [--name] arg=all (retrieve all logs) name of log to retrieve
    -S [--start-date] arg start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    -E [--end-date] arg end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
  scan-info: get information about scan
    -I [--id] arg id of scan to retrieve
  configuration: get product configuration
    -F [--file] arg path where configuration file will be saved
    -O [--format] arg=json, xml format of configuration: json, xml
  update-status: get information about update
  activation-status: get information about last activation

start: start task
  scan: Start on demand scan
    -P [--profile] arg scanning profile
    -T [--target] arg scan target
  activation: Start activation
    -K [--key] arg activation key
    -O [--offline] arg path to offline file
    -T [--token] arg activation token
  deactivation: start deactivation of product
  update: start update of product

set: set configuration to product
  configuration: set product configuration
    -V [--value] arg configuration data (encoded in base64)
    -F [--file] arg path to configuration xml file
    -P [--password] arg password for configuration

Application parameters:
  -H [--help] help
  -L [--log] log application
--debug display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"

C:\Program Files\ESET\ESET Security>

```

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
	naplók	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
	Ellenőrzés	Start on demand scan
	aktiválás	Start activation of product
	deactivation	Start deactivation of product
	frissítés	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": "EkrrnNotActivated",
      "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 antispayware 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, devctrlog } : 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, error }

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" | --token "activation token"
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

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 Antivirus frissítése](#)
- [Az ESET Endpoint Antivirus aktiválása](#)
- [Új termék aktiválása az aktuális hitelesítő adatokkal](#)
- [Vírus eltávolítása a számítógépről](#)
- [Új feladat létrehozása a feladatütemezőben](#)
- [Heti számítógép-ellenőrzés ütemezése](#)
- [A termék csatlakoztatása az ESET Security Management Center alkalmazáshoz](#)
- [A Felülbíráls mód használata](#)
- [Ajánlott házirend alkalmazása az ESET Endpoint Antivirus szolgáltatásra](#)
- [Tükrözés beállítása](#)
- [Frissítés Windows 10-re az ESET Endpoint Antivirus programmal](#)
- [Távoli figyelés és kezelés aktiválása](#)
- [Hogyan akadályozható meg bizonyos fájltypusok letöltése az internetről?](#)
- [Az ESET Endpoint Antivirus minimalista felhasználói felületének beállítása](#)

Ha a megoldandó problémát nem találja a fenti listában, próbálja megkeresni az ESET Endpoint Antivirus 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 7 – 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.

Az ESET Endpoint Antivirus frissítése


Az ESET Endpoint Antivirus 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 (a feladatütemezőre vonatkozó információkért [kattintson ide](#)).

Az ESET Endpoint Antivirus 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 Antivirus licencét közvetlenül a programból szeretné aktiválni, a rendszertálcán kattintson az  ikonra, és a menüből válassza **A termék licencének aktiválása** parancsot. A szoftver licencét a főmenüből is aktiválhatja a **Súgó és támogatás > A licenc aktiválása** vagy a **Védelem állapota > A licenc aktiválása** részen.


Az ESET Endpoint Antivirus aktiválásához az alábbi lehetőségek közül választhat:

- **Licenckulcs** – 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 Security Management Center 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 Antivirus terméket, [konvertálja régi hitelesítő adatait licenckulcsra](#).

[Nem sikerült a termékaktiválás?](#)

A terméklicenc bármikor módosítható. Ehhez kattintson a **Súgó és támogatás > Licenc módosítása** lehetőségre 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 megnyitáshoz kattintson a jobb gombbal a rendszertálcán  ikonjára.



Megjegyzés

Az ESET Security Management Center képes értesítés nélkül, a rendszergazda által elérhetővé tett licenceket használva aktiválni a kliensszámítógépeket. Ennek módját az [ESET Security Management Center online súgóban](#) találja meg.

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.

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.
- **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** mezőben 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 Antivirus csatlakoztatása az ESET Security Management Center alkalmazáshoz

Ha telepítette az ESET Endpoint Antivirus szolgáltatást a számítógépére, és az ESET Security Management Center segítségével szeretne kapcsolódni, akkor telepítse az ESET Management Agentet is a kliensszámítógépekre. Minden olyan kliensmegoldás szerves részét képezi, amely az ESMC-szerverrel kommunikál.

- [Az ESET Management Agent telepítése vagy központi telepítése kliensszámítógépekre](#)

Lásd még:

- [Távolról felügyelt végpontok dokumentációja](#)
- [A Felülbíráls mód használata](#)
- [Ajánlott házirend alkalmazása az ESET Endpoint Antivirus](#) szolgáltatásra

A Felülbíráls mód használata


A Windows rendszerhez készült ESET Endpoint termékek (6.5-ös és újabb verziók) felhasználói használhatják a Felülbíráls módot. A Felülbíráls mód lehetővé teszi a felhasználóknak, hogy kliensszámítógép-szinten akkor is módosítsák a beállításait a telepített ESET szoftverben, ha a beállításokra házirend vonatkozik. A Felülbíráls mód bizonyos AD-felhasználókhoz engedélyezhető, illetve jelszóval védhető. A funkció egyszerre legfeljebb négy órára engedélyezhető.



Figyelmeztetés

- Az aktiválása után a Felülbíráls mód nem állítható le az ESMC Webkonzolban. A Felülbíráls mód automatikusan leáll, ha letelik a felülbíráls időszak. A kliensgépen is kikapcsolható.
- A Felülbíráls módot használó felhasználónak is Windows rendszergazdai jogosultságokkal kell rendelkeznie. Ellenkező esetben a felhasználó nem tudja menteni a módosításokat az ESET Endpoint Antivirus beállításaiiban.
- Active Directory-csoporthitelesítésre az ESET Endpoint Antivirus 7.0.2100.4-es és újabb verziói esetén van lehetőség.

A **Felülbíráls 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** (Felülbíráls mód) lehetőségre, és adja meg a felülbíráls mód szabályait.
5. Az **Assign** (Hozzárendelés) csoportban válassza ki a számítógépet vagy a számítógépcsoportot, amelyre a

házipolitikát alkalmazni szeretné.

6. Tekintse át a beállításokat a **Summary** (Összegzés) csoportban, és a házipolitikát alkalmazásához kattintson a **Finish** (Befejezés) elemre.

The screenshot shows the ESET Security Management Center interface. The top navigation bar includes the ESET logo, 'SECURITY MANAGEMENT CENTER', a search bar, and user information. The left sidebar contains navigation icons and a list of tabs: Basic, Settings (selected), Assign, and Summary. The main content area is titled 'New Policy' and shows the 'Summary' tab. It displays a list of policy categories on the left, including 'ESET Endpoint for Windows', 'DETECTION ENGINE', 'UPDATE', 'NETWORK PROTECTION', 'WEB AND EMAIL', 'DEVICE CONTROL', 'TOOLS', 'USER INTERFACE', and 'OVERRIDE MODE'. The 'OVERRIDE MODE' section is expanded, showing 'TEMPORARY CONFIGURATION OVERRIDE' and 'OVERRIDE CREDENTIALS' settings. The 'TEMPORARY CONFIGURATION OVERRIDE' section includes options for 'Allow override by local admin', 'Maximum override time' (set to 4 hours), and 'Scan computer after override'. The 'OVERRIDE CREDENTIALS' section includes 'Authentication type' (set to Active directory user) and 'Active directory user' (set to Edit). At the bottom, there are three buttons: 'CONTINUE', 'FINISH', and 'CANCEL'.



Példa

Ha *Jánosnak* problémája van az Endpoint beállításával, 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 ESMC 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** (Felülbírlás mód) lehetőségre, engedélyezze a Felülbírlás 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 **Felülbírlás módot** az ESET Endpoint szoftverében, és kézzel kell módosítania a beállításokat ezen a gépen.
6. Az ESMC 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 felülbírlási házirendet.

Ajánlott házirend alkalmazása az ESET Endpoint Antivirus szolgáltatásra

Miután megtörtént az ESET Endpoint Antivirus és az ESET Security Management Center csatlakoztatása, a legcélszerűbb megoldás egy ajánlott vagy egyéni [házirend](#) alkalmazása.

Több beépített házirend is rendelkezésre áll az ESET Endpoint Antivirus 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, kóros 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 ESMC- és az EEI-csatlakozások kivételével	Minden forgalom tiltása, kivéve az ESET Security Management Centerhez és az ESET Enterprise Inspector 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 Antivirus szolgáltatáshoz:

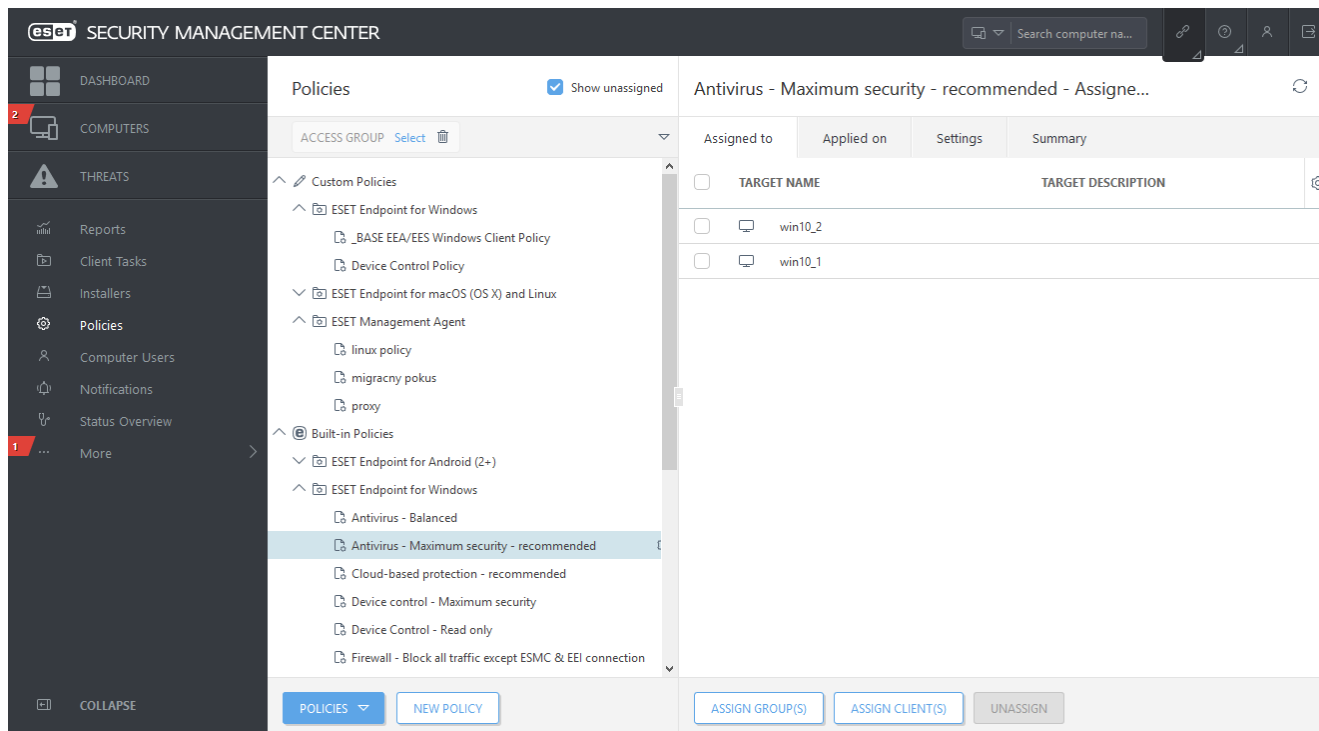


Ábrákkal ellátott útmutató

Előfordulhat, hogy a következő ESET-tudásbáziscikkek csak angolul állnak rendelkezésre:

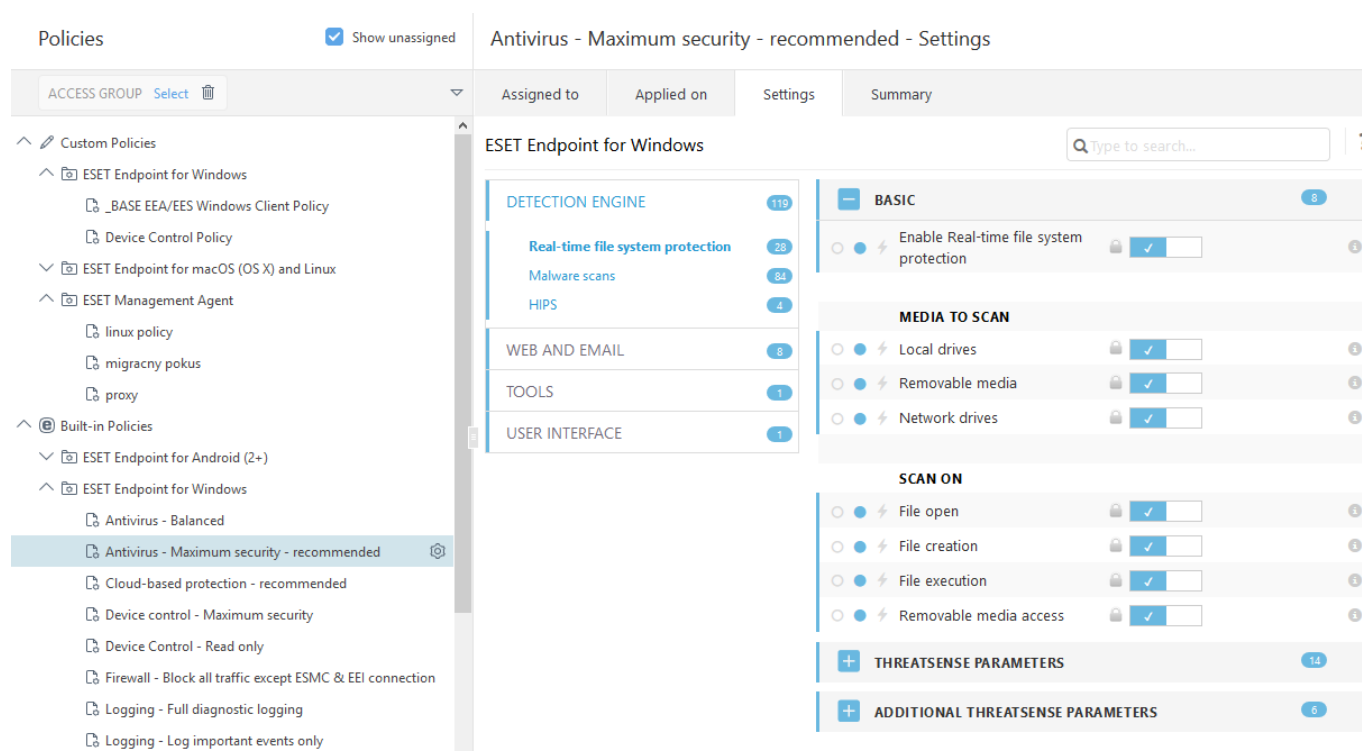
- [Ajánlott vagy előre megadott házirend alkalmazása az ESET Endpoint Antivirus szolgáltatáshoz az ESMC segítségével](#)

1. Nyissa meg az ESMC 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 ESMC-házirendekről](#)



Tükrözés beállítása

Az ESET Endpoint Antivirus 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 Antivirus beállítása tükröszerverként 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 [Frissítési tükör](#) című részt.

Tükröszerver 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.



Megjegyzés

Ha nem szeretne a belső HTTP-szerveren keresztül modulokat frissíteni, kapcsolja ki a **Frissítési tükör létrehozása** funkciót.

Frissítés Windows 10-re az ESET Endpoint Antivirus programmal



Figyelmeztetés

Azt javasoljuk, hogy mielőtt frissítene a Windows 10 rendszerre, frissítse ESET-szoftverét a legújabb verzióra, majd töltsse 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 töltsse 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:



Fontos

Az 5-ös verziójú ESET Endpoint termékek jelenlegi állapota az [Alapszintű támogatás](#). Ez azt jelenti, hogy a builddek már nem érhetők el nyilvánosan letöltésre. Azt javasoljuk, mindenképpen frissítsen [az ESET Endpoint termékek legújabb verziójára](#). Ha hozzáférést szeretne kérni az MSI-telepítőkhöz, kérjen segítséget az [ESET műszaki támogatási szolgálatától](#).

Más nyelvű verziók:

Ha az ESET Endpoint szoftver más nyelven kiadott verzióját keresi, [látogasson el a letöltési lapunkra](#).

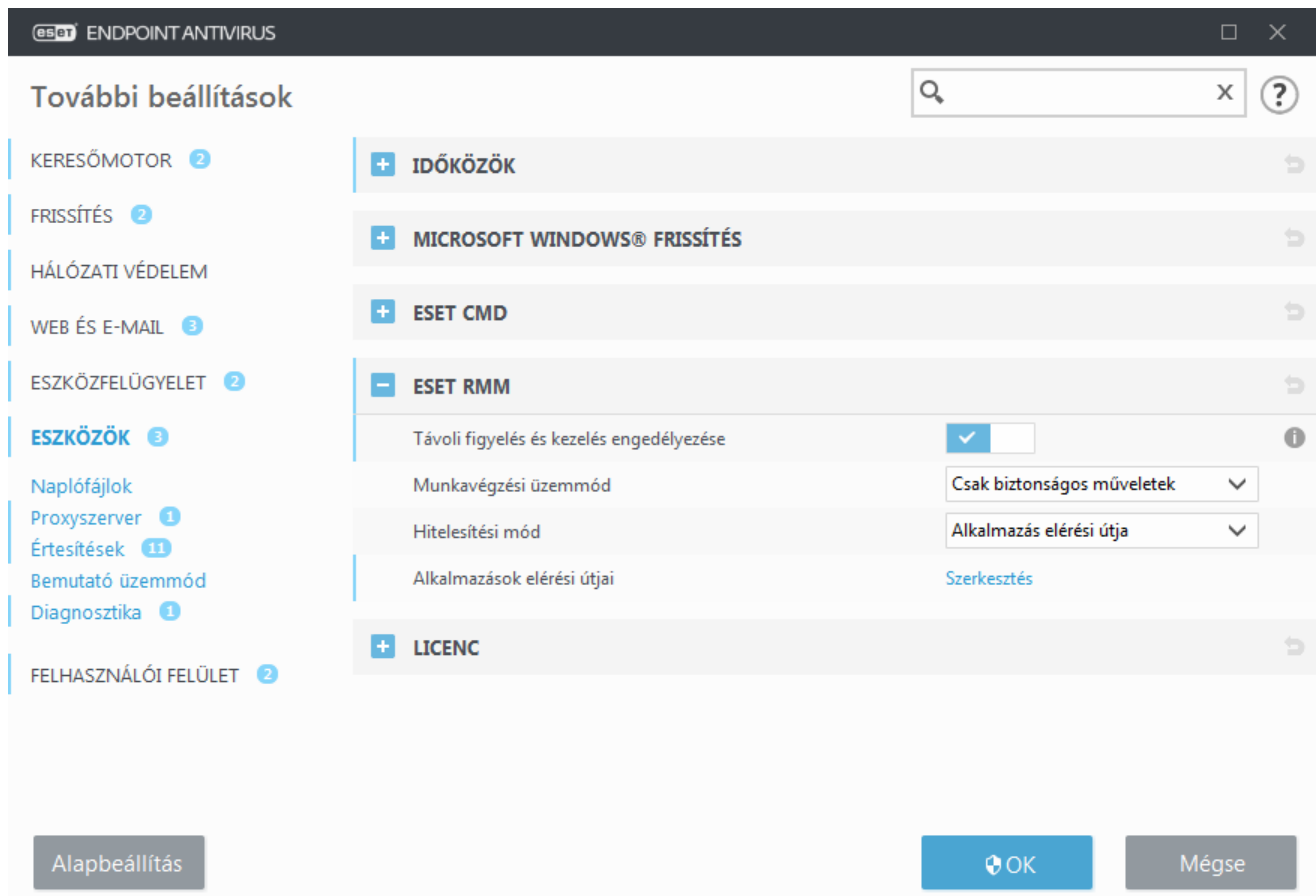


Megjegyzés

[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 Antivirus 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.



Figyelmeztetés

A Távoli figyelés és kezelés funkciónak engedélyezést használva meg kell akadályoznia, hogy a kártevő szoftverek letiltsák vagy megkerüljék az ESET Endpoint-védelmet.

Alkalmazások elérési újtjai – 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 újtjai** beállításlap 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 Antivirus 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 fájltypusok letöltése az internetről?

Ha nem szeretné engedélyezni bizonyos fájltypusok (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 fájltypus elérésekor, aktiválja az Értesítés az alkalmazásakor csúszkát. Válassza ki a naplózás részletességét a legördülő menüből. A Remote Administrator Figyelmeztetés részletességű rekordokat tud gyűjteni.

Lista szerkesztése

Címlista típusa

Letiltva

Lista neve

Letiltott címek listája

Lista leírása

Lista aktiválása

☒

Értesítés az alkalmazásakor

☐

Naplózás részletessége

Információk

Címlista

*?.exe

..zip

..exe

Hozzáadás

Szerkesztés

Törlés

Importálás

OK

Mégse

A Hozzáadás gombra kattintva adjon meg egy olyan maszkot, amely a letöltésből kizárni kívánt fájltypusokat 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 Antivirus 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](#).

Végfelhasználói licencszerződés

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 [ADATKEZELÉSI SZABÁLYZATOT](#).**

Végfelhasználói licencszerződést

Jelen végfelhasználói licencszerződés (a továbbiakban „a Szerződés”) alapján, amely egyfelől az ESET, spol. s r. o. (székhelye: Einsteinova 24, 851 01 Bratislava, Slovak Republic; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B; cégjegyzékszám: 31333532; a továbbiakban „ESET” vagy „Gyártó”), másfelől Ön mint természetes vagy jogi személy (a továbbiakban „Ön” vagy „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. Ha nem ért egyet a Szerződés 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 mellékelte 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 (a továbbiakban „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, tenyészámítógépeket, 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, és megfelel az itt előírt összes feltételnek, a Gyártó az alábbi jogokat (a továbbiakban „Licenc”) biztosítja az Ön számára:

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 licenckulcs 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) (a továbbiakban „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 levelezésszerver-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) **Business Edition.** A Szoftver Business Edition verzióját kell beszerezni 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 szoftver használata arra a számítógépre korlátozott, 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 lejárat.** 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 saját költségén vissza kell küldenie az ESET címére vagy abba az üzletbe, ahol a Szoftvert beszerezte. A Licenc lejárat 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 időről időre kiadni a Szoftver frissítéseit („Frissítések”). 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.

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-keretéről (a továbbiakban „Kártevők”), majd a mintákat elküldi a Gyártónak, beleértve, de nem kizárólag a telepítési folyamatra, arra a számítógépre és/vagy platformra vonatkozó adatokkal, amelyen a Szoftver telepítve van, illetve a szoftver működésével és funkcióival, valamint a helyi hálózaton található eszközökkel kapcsolatos adatokkal (ideértve a típust, a gyártót, a modellt és/vagy az eszköz nevét) (a továbbiakban „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. Ön ezennel hozzájárul értesítések és üzenetek fogadásához, ideértve többek között a marketinginformációkat is.

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 súgóiban 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 Licenckulcsok továbbadása, illetve a Szoftver használata olyan Licenckulccsal, 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 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 MÉRTEKBE 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 NYERESÉGGIESÉSEÉRT, 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 SZERZŐDÉSÉBŐL, SZÁNDÉKOS KÁROKOZÁSÉBŐL, GONDATLANSÁGBÓL, VAGY MÁS, FELELŐSÉGET MEGALAPOZÓ TÉNYBŐL ERED, HA EZEK A SZOFTVER 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 jóállás vagy jognyilatkozatok nélkül, saját döntésüknek megfelelően terméktámogatást nyújtanak. 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, felfüggeszse 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 számítógéprendszerrel 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 (a továbbiakban „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 licenelési 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 (a továbbiakban „Exportálási felügyeleti törvények”), 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 továbbiakban „Szankcionálási 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 cselekedet végrehajtására vagy bizonyos cselekedet mellőzésére (illetve arra, hogy beleegyezzenek ilyen cselekedet végrehajtásába vagy bizonyos cselekedet mellőzésébe).

20. Értesítések. Minden értesítést, a visszaküldendő Szoftvert és Dokumentációt a következő címre kell küldeni: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

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. Amennyiben bármilyen ellentmondás van a jelen Szerződés különböző nyelvi változatai között, az angol változat az irányadó. Jelen Szerződés csak írásban módosítható, amely módosításokat a Gyártó meghatalmazott képviselőjének vagy egy olyan személynek kell aláírnia, aki ügyvédi meghatalmazással kifejezetten eljárhat ebben a hatáskörben.

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.

EULA ID: BUS-STANDARD-20-01

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.

- Licenclési információkra, például licencaazonosítóra 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 licenclési 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