ESET Endpoint Antivirus for macOS

Felhasználói útmutató

Ide kattintva megjelenítheti a dokumentum verzióját

Digital Security
Progress. Protected.

Az ESET Endpoint Antivirus for macOS terméket az ESET, spol. s r.o. fejlesztette ki

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

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

REV. 2024.04.12.

ESET Endpoint Antivirus for macOS

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

Az ESET Endpoint Antivirus for macOS 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.

A szoftver elsősorban kisvállalati/vállalati környezetben működő munkaállomásokhoz készült. Az ESET PROTECT On-Prem szoftverrel, együtt lehetővé teszi tetszőleges számú munkaállomás egyszerű kezelését, házirendek és szabályok alkalmazását, észlelések figyelését és bármely hálózati számítógép távoli felügyeletét.

A 7-es verzió újdonságai

Az ESET Endpoint Antivirus for macOS 7-es verziója a termékünk egy új generációját képviseli, amely nem egyetlen szolgáltatáson, hanem mikroszolgáltatásokon alapul.

- Az Apple ARM chip natív támogatása (a 7.1.1700.0-s verziótól)
- Natív 64 bites architektúra
- Jobb teljesítmény és stabilitás. Ha az ESET Endpoint Antivirus for macOS összeomlik, akkor automatikusan újra tud indulni anélkül, hogy ezt a felhasználó észrevenné.
- Nagyobb fokú biztonság azáltal, hogy a folyamatok függetlenebbek egymástól.
- Új fő programablak, amely tartalmazza a következőket:
  - A Sötét mód támogatása
  - Natív asztali értesítések
  - A grafikus felhasználói felület letiltása a végfelhasználó számára
- Hatékonyabb valós idejű fájlrendszervédelem
  - A legújabb natív 64 bites ellenőrző motor
  - Többmagos teljesítményre optimalizálva
  - Valós idejű ellenőrzés a helyi felhasználónál
- Vadonatúj natív grafikus felhasználói felület
- Kiterjesztett ESET LiveGrid-konfiguráció az ESET PROTECT On-Prem és az ESET PROTECT CLOUD révén

- Parancssori parancsok egyesítése a Linux platformmal.
- A védelmi állapotok konfigurálása
- Támogatás a teljesítményhez és az összes észlelési kivételhez (útvonal, útvonal és észlelt elem, kivonat alapján)

A 6-os és 7-es verzió összehasonlítása

Funkció	6-os verzió	7.3-as és 7.4-es verzió
Architektúra		
Architektúra	Monolitikus	Mikroszolgáltatások
Architekturális biztonsági profil	A fő folyamat a gyökér alatt fut (az összes fontos műveletet a fő folyamat végzi)	Minden szolgáltatás a lehető legalacsonyabb jogosultságokkal fut Alacsonyabb potenciális támadási vektor Az egyik szolgáltatás biztonsági rése nem teszi sebezhetővé az egész alkalmazást. Egy termékfolyamat összeomlása vagy eltérítése esetén nincs letiltva az összes védelem
Architekturális stabilitási profil	A monolitikus kereső összeomlása időbeli űrt okoz a védelemben Automatikus folyamat-újraindítás összeomlás esetén	A nem kritikus szolgáltatás-összeomlás nem okoz szünetet a védelemben Meghatározott feladatokhoz optimalizált egyszerűbb szolgáltatások Automatikus szolgáltatás-újraindítás összeomlás esetén
macOS-támogatás	10.12 (Sierra) 10.13 (High Sierra) 10.14 (Mojave) 10.15 (Catalina) 11 (Big Sur) 12 (Monterey) 13 (Ventura)	10.15 Catalina (csak 7.3-as verzió) 11 (Big Sur) 12 (Monterey) 13 (Ventura) 14 (Sonoma)
Natív 64 bites ellenőrző motor	x	x
Natív 64 bites alkalmazás	x	x
Többnyelvű támogatás	nyelvspecifikus telepítési csomag	minden nyelv egy csomagban (a GUI nyelve ugyanaz, mint a rendszeré)
Natív ARM-támogatás		a 7.1.1700.0-s verziótól
Rosetta ARM támogatása	x	x
Fájlrendszervédelem		

Funkció	6-os verzió	7.3-as és 7.4-es verzió
Kéretlen, veszélyes és gyanús alkalmazások észlelése	x	x
Teljesítménybeli kivételek	x	x
Észlelési kizárások útvonal és észlelt elem alapján	Az észlelési kizárás ESET PROTECT On-Prem szolgáltatásban való létrehozása után (a fájlok ellenőrizve, de a problémák figyelmen kívül hagyva), teljesítménybeli kivételek jönnek létre (a fájlok nem lesznek ellenőrizve).	x
Észlelés szerinti észlelési kivételek		x
Észlelési kivételek pontos fájl (hash) alapján		x
Valós idejű fájlrendszervédelem	x	x
Hálózati kötetek kompatibilitásának növelése	x	nem szükséges
Ellenőrzés a bejelentkezett felhasználónál		x
Helyi meghajtók ellenőrzése	x	x
Cserélhető adathordozók ellenőrzése	x	x
Hálózati meghajtók ellenőrzése	x	x
Ellenőrzés megnyitáskor, létrehozáskor	x	x
Ellenőrzés indításkor	x	Igen, a megnyitás része
Folyamatkivételek		x
Felhőalapú védelem	x	x
ESET LiveGrid© megbízhatósági rendszer	x	x (kibővítve)
ESET LiveGrid© Visszajelzési rendszer	x	x
Az elküldhető elemek részletes konfigurációja		x
Kártevő-ellenőrzések (kézi indítású)	x	x
Szimbolikus hivatkozások ellenőrzése	x	x
E-mail-fájlok ellenőrzése	x	x
Postaládák ellenőrzése	x	x
Tömörített fájlok ellenőrzése	x	x
Önkicsomagoló tömörített fájlok ellenőrzése	x	x
Futtatás közbeni tömörítők ellenőrzése	x	x
Változó adatfolyamok ellenőrzése (ADS)	x	x
Optimalizálás engedélyezése	x	x
A rendszermappák kizárása az ellenőrzésből	x	Nem szükséges
Háttérben futó ellenőrzések indítása alacsony prioritással		x
Utolsó hozzáférés időbélyegének megőrzése	x	x
Rendszerindításkor futtatott ellenőrzés	x	

Funkció	6-os verzió	7.3-as és 7.4-es verzió
Webhozzáférés- és e-mail védelem		
Alkalmazáskivételek	x	x
IP-címek kizárása	x	x
Webhozzáférés-védelem (HTTP-ellenőrzés)	x	x
E-mail védelem	x	x
Adathalászat elleni védelem	x	x
Modulokfrissítés		
Egyéni proxyszerver az elsődleges/másodlagos frissítési kiszolgálóhoz	x	x
Modulok-visszaállítás	x	x
Tesztelési mód	x	x
Késleltetett frissítések	x	x
Egyéb főbb funkciók		
Eszközfelügyelet	x	
Tűzfal		
Webfelügyelet		
ERMM-támogatás (parancssori interfész a Távoli figyelés és kezelés integrációjához)	x	
Az ESET Enterprise Inspector támogatása	x	x
Egyéb kisebb funkciók		
Parancssori felület	x	x (egyesítve az ESET Endpoint for Linux szolgáltatással)
Észlelési napló	x	x
Eseménynapló	x	x
Számítógép-ellenőrzés naplója	x	x
Beállítások importálása és exportálása	x	x
Karantén	x	x
Helyi feladatütemező	x	x
Proxyszerver-konfiguráció	x	x
Bemutató üzemmód	x	x (natív rendszerbeli Ne zavarjanak)
Felhasználói felület		
Naplófájlok	x	x
Észlelt kártevők	x	x
Események	x	x
Számítógép ellenőrzése	x	x
Eszközfelügyelet	x	
Tűzfal	(Az Endpoint Security szolgáltatásban)	
Szűrt webhelyek	x	x

Funkció	6-os verzió	7.3-as és 7.4-es verzió
Webfelügyelet	(Az Endpoint Security szolgáltatásban)	
Napló szűrése	x	x
Védelem statisztikája	x	x
Feladatütemező	x	x
Futó folyamatok	x	
Karantén	x	x
Fájlok elküldése elemzésre	x	x (7.4)
Védelem állapota	x	x
Manuális modulfrissítés	x	x
Helyi beállítások/konfiguráció a felhasználó által	x	x
Beállítások importálása és exportálása a GUI-ból	x	
Súgó	x	x
Vadonatúj natív grafikus felhasználói felület		x
A Sötét mód támogatása		x
Nagy felbontású kijelzők támogatása	x	x
Le lehet tiltani a grafikus felhasználói felületet a felhasználó számára		x
Natív értesítések		x
Menüsáv	x	x
Elrejthető a menüsor ikonja	x	x
Integrálás a helyi menübe	x	
A GUI-ban/ESET PROTECT On-Prem vagy ESET PROTECT CLOUD szolgáltatásban feltüntetett védettségi állapot részletes szabályozása	x	x
Rendszerfrissítési értesítések	x	x
Telepítés		
Helyi GUI-alapú telepítés	x	x
Komponensalapú telepítés	x	
Távoli komponensalapú telepítés (komponens telepítéséhez további lépések szükségesek)	x	
Csendes telepítés támogatása (MDM-előjóváhagyásokkal)	x	x
Termékfrissítés újratelepítéssel	x	x
Termékfrissítés az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD révén	x	x
Licenc aktiválása		
Aktiválás licenckulccsal	x	x
Előfizetéses licenc támogatása	x	x
Aktiválás az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD segítségével	x	x

Funkció	6-os verzió	7.3-as és 7.4-es verzió
Aktiválás offline licencfájllal	x	x
Kompatibilitás az ESET felügyeleti konzolokkal		
Kompatibilitás az ESET PROTECT CLOUD szolgáltatással	x	x
Kompatibilitás az ESET PROTECT On-Prem szolgáltatással	x	x

Beállítások átköltöztetése

Az átköltöztetési folyamat

A 7.2-es és újabb verzióktól az ESET Endpoint Antivirus for macOS 6-os verziójából származó beállítások automatikusan átköltöznek az új verzióba a frissítési folyamat során.

Miután az átköltöztetési folyamat befejeződött, az ESET Endpoint Antivirus for macOS megjeleníti a következő értesítést a beállítások sikeres átköltöztetésének kezdőlapján: **A beállítások átkerültek az új verzióba**.

Az ESET PROTECT On-Prem és az ESET PROTECT CLOUD házirendek nem települnek át automatikusan, mivel az ESET Endpoint Antivirus for macOS 6-os verziójának nem minden funkciója található meg a 7-es verzióban. A 7-es verzióra való frissítés után felül kell vizsgálnia a meglévő házirendeket, és új házirendeket kell létrehoznia a 7-es verzióban található funkciók alapján. A Házirendek című témakörben további információt találhat arról, hogyan hozhat létre vagy törölhet házirendeket:

- Házirendek: ESET PROTECT On-Prem
- Házirendek: ESET PROTECT CLOUD

Az ESET PROTECT On-Prem és az ESET PROTECT CLOUD for ESET Endpoint Antivirus for macOS 6-os és 7-es verziójára vonatkozó irányelvek egyszerre lehetnek aktívak.

Ha már frissített az ESET Endpoint Antivirus for macOS 6-os verziójáról a 7-es vagy 7.1-es verzióra, akkor is átköltöztetheti a beállításokat, amikor egy későbbi verzióra frissít. Útmutatásért tekintse meg az ESET-tudásbázis átköltöztetésről szóló cikkét.

A 7.X verzióban elérhető összes beállítás átköltözik a 6-os verzióról, a következő kivételekkel:

- Jogosultsági beállítások (a 7-es verzióban nem támogatottak)
- Egyéni proxykiszolgáló a frissítésekhez (az egyéni proxy nem támogatott a 7-es verzióban)
- A karantén tartalma
- Megtisztítási szintek az ellenőrzésekhez
- Célprofilok a kézi indítású ellenőrzéshez

A következő szolgáltatások beállításait az átköltöztetési .xml fájl tárolja, és akkor tölthetők majd be, ha a funkciók megtalálhatók lesznek az ESET Endpoint Antivirus for macOS következő verziójában:

- Eszközfelügyelet
- Naplók

- Webhozzáférés-védelem
- Bemutató üzemmód

Egyéb átköltöztetési problémák

- Az egyéni ellenőrzési profilok áttelepülnek, és az ESET PROTECT On-Prem, az ESET PROTECT CLOUD vagy az alkalmazásbeállítások segítségével kezelhetők.

Változásnapló

Rendszerkövetelmények

Az ESET Endpoint Antivirus for macOS optimális működéséhez a rendszernek meg kell felelnie az alábbi hardver- és szoftverkövetelményeknek:

	Rendszerkövetelmények:
Processzor	Intel 64-bit, Apple ARM 64 bites
Operációs rendszer	macOS Big Sur (11)–macOS Sonoma (14)
Memória	300 MB
Szabad tárhely	600 MB

Az ESET Endpoint Antivirus for macOS funkcionális internetkapcsolatot igényel a telepítés során.

Az ESET Endpoint Antivirus for macOS 7.1.1700.0-s és újabb verziója natív támogatást nyújt az Apple ARM chiphez.

Az ESET Endpoint Antivirus for macOS 6-os verziójának frissítése a 7-es verzióra

Az ESET Endpoint Antivirus for macOS 6-os verziójáról a 7-es verzióra való frissítés után az ESET Endpoint Antivirus for macOS visszatér az alapértelmezett beállításokhoz. Ez magában foglalja az ESET felügyeleti konzol házirendjeit is.
Az ESET Endpoint Antivirus for macOS 7-es verziója sok eltérést tartalmaz a 6-os verzióhoz képest, és néhány funkció eltűnt belőle. Mielőtt úgy dönt, hogy végrehajtja az ESET Endpoint Antivirus for macOS frissítését, azt javasoljuk, hogy olvassa el a következő témakört: A 6-os és 7-es verzió összehasonlítása.

- Helyi frissítés
- Frissítés parancssoron keresztül
- Frissítés az ESET felügyeleti konzolon keresztül
- Beállítások átköltöztetése

Helyi frissítés

1. Töltse le a legújabb ESET Endpoint Antivirus for macOS-telepítőfájlt ((.dmg)).

2. Nyissa meg a (.dmg) telepítőfájlt.

3. Kattintson duplán az ESET Endpoint Antivirus for macOS telepítése ikonra  .

4. Kattintson a Folytatás gombra, ha nincs más biztonsági alkalmazás telepítve a gépre. Ha van egy másik vírusirtó alkalmazás telepítve rá, akkor a telepítés sikertelen lehet.

5. Kattintson a Folytatás gombra a rendszerkövetelmények megerősítéséhez.

6. Kattintson az Elfogadom gombra a végfelhasználói licencszerződés és az adatvédelmi szabályzat elfogadásához.

7. Ha módosítani szeretné a célmappát, vagy módosítani szeretné azt, hogy minden felhasználó hozzá tudjon-e férni az ESET Endpoint Antivirus for macOS szolgáltatáshoz, akkor kattintson a Telepítés helyének módosítása gombra. A telepítés elindításához kattintson a Telepítés gombra.

Telepítés helyének módosítása

Válassza ki a telepítési célpontot. Válassza ki, hogy az ESET Endpoint Antivirus for macOS szolgáltatást a számítógép összes felhasználója számára vagy csak az aktuális felhasználó számára telepíti. Az ESET Endpoint Antivirus for macOS telepítéséhez kiválaszthat egy adott mappát is. Válassza ki a kívánt lehetőséget, majd kattintson a Folytatás gombra a Telepítés típusa lépéshez való visszatéréshez.

8. Felszólítást kaphat a rendszergazdai jelszó megadására a telepítés kezdetén.

9. Kattintson a Bezárás gombra a telepítés befejezéséhez.

10. A telepítés után megjelenik a használatbavételi varázsló, kövesse az itt leírt lépéseket a számítógép védelmének biztosítása érdekében.

Frissítés parancssoron keresztül

Az ESET Endpoint Antivirus for macOS 7-es verzióra való frissítése parancssoron keresztül:

1. Töltse le az ESET Endpoint Antivirus for macOS 7-es verzióját.

2. Továbbítsa a .dmg fájlokat a célszámítógépekre.

3. Futtassa a telepítést a Parancssori telepítés című témakörben leírtak szerint.

Az ESET Endpoint Antivirus for macOS frissítése az ESET PROTECT On-Prem

vagy az ESET PROTECT CLOUD segítségével

A frissítés előtt a következő módosításokat kell végrehajtani az MDM konfigurációs profiljaiban:

- A Teljes lemezhozzáférés konfigurációs profilban

6-os verzió		7-os verzió	
Azonosító	com.eset.eea.6	Azonosító	com.eset.eea.g2

- Ha macOS 12 vagy újabb verzióra telepíti az ESET Endpoint Antivirus for macOS szolgáltatást, akkor engedélyeznie kell a Teljes lemezhozzáférést az Uninstaller.app számára. Erre azért van szükség, hogy eltávolítsa a 6-os verziót a rendszerből, és lehetővé tegye a 7-es verzió távolról történő eltávolítását a későbbiekben. A Teljes lemezelérés konfigurációs profilhoz adja hozzá a következőt:

ESET Endpoint Antivirus és ESET Endpoint Security a macOS 12 Monterey rendszerben	
Azonosító	com.eset.app.Uninstaller
Azonosító típusa	bundleID
Kódkövetelmény	identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Alkalmazás vagy szolgáltatás	SystemPolicyAllFiles
Hozzáférés	Allow

- A Web- és e-mail-védelem konfigurációs profiljában

6-os verzió		7-os verzió	
Az egyéni SSL VPN azonosítója	com.eset.sysext.manager	Az egyéni SSL VPN azonosítója	com.eset.network.manager

Ha eltávolítja a 6-os verzió beállításait a 7-es verzióra való frissítés előtt, akkor a felhasználók értesítést kapnak, mintha az adott beállítások nem lettek volna alkalmazva. Azt javasoljuk, hogy hozzon létre egy új konfigurációs profilt az ESET Endpoint Antivirus for macOS 7-es verziójához, telepítse a konfigurációs profilt a célszámítógépekre, frissítse az ESET Endpoint Antivirus for macOS szolgáltatást, és távolítsa el a 6-os verzióhoz tartozó konfigurációs profilokat. Azt is javasoljuk, hogy győződjön meg arról, hogy csak egy telepítési házirend van az ESET Endpoint Antivirus for macOS szolgáltatáshoz egy eszközön. Az ESET PROTECT On-Prem és a Jamf együttes használatakor győződjön meg arról, hogy mindegyiknek csak egy telepítési házirendje van.

Az ESET Endpoint Antivirus for macOS 7-es verziójához tartozó új konfigurációs profilokat a Telepítés előtti beállítások című témakörben találhatja meg.

Az új konfigurációs profilok telepítése után a Telepítés az ESET felügyeleti konzolon keresztül című témakörben leírtak szerint folytassa a telepítést.

Telepítés

Telepítési módszerek

Telepítési módszerek	A telepítés típusa	Megjegyzések
Telepítés a felhasználói felület segítségével	Helyi	Az ESET Endpoint Antivirus for macOS helyileg a telepítő .dmg fájlból telepíthető. A telepítés megkezdése előtt zárja be az összes megnyitott számítógépes programot. Az ESET Endpoint Antivirus for macOS olyan összetevőket tartalmaz, amelyek ütközhetnek a számítógépre telepített más vírusirtó programokkal. Ezért azt javasoljuk, hogy távolítsa el az összes többi vírusirtó programot az esetleges problémák megelőzése érdekében. A telepítés után megjelenik a használatbavételi varázsló, kövesse az itt leírt lépéseket a számítógép védelmének biztosítása érdekében.
Parancssori telepítés	Helyi/Távoli	Az ESET Endpoint Antivirus for macOS anélkül is telepíthető, hogy a telepítő felhasználói felületét használnia kellene. Ezzel a módszerrel az ESET Endpoint Antivirus for macOS távoli telepítése is elvégezhető. Ha az ESET Endpoint Antivirus for macOS távoli telepítését szeretné elvégezni, akkor azt javasoljuk, hogy a telepítés előtt MDM-en keresztül alkalmazzon felhasználói beleegyezési beállításokat.
ESET PROTECT On-Prem	Távoli	Ha a számítógép regisztrálva van az ESET PROTECT On-Prem szolgáltatásban, akkor létrehozhat egy telepítési feladatot az ESET Endpoint Antivirus for macOS célszámítógépekre való telepítéséhez.
ESET PROTECT CLOUD	Távoli	Ha a számítógép regisztrálva van az ESET PROTECT CLOUD szolgáltatásban, akkor létrehozhat egy telepítési feladatot az ESET Endpoint Antivirus for macOS célszámítógépekre való telepítéséhez.

Az ESET Endpoint Antivirus for macOS működéséhez felhasználói beleegyezési beállítások szükségesek. Ezeket a beállításokat manuálisan kell alkalmazni a telepítés után. Az eszközt regisztrálni kell az MDM-ben, hogy ne kelljen minden egyes számítógéphez hozzáadni a felhasználói beleegyezési beállításokat. Az MDM segítségével ezután továbbíthatók a konfigurációs profilok a célszámítógépekre. Ha a telepítés előtt nem alkalmazza ezeket a beállításokat, a felhasználók több előugró párbeszédablakot fognak látni, amelyek arra kérik őket, hogy manuálisan alkalmazzák a felhasználói beleegyezési beállításokat. A konfigurációs profilok továbbítását az ESET Endpoint Antivirus for macOS telepítése előtt javasoljuk.

Használatbavétel

Az ESET Endpoint Antivirus for macOS telepítése után megjelenik a **Használatbavételi varázsló** – a képernyők végigvezetik az ajánlott és kötelező lépéseken, amelyek az ESET Endpoint Antivirus for macOS hiánytalan működéséhez szükségesek.

1. Engedélyezze az **ajánlott védelmi beállításokat**, válassza ki a kívánt beállításokat, majd kattintson a **Folytatás** gombra. Az **ESET LiveGrid©** rendszerről és a **kéretlen alkalmazásokról**, a szójegyzékünkben olvashat bővebben.

2. Kötelező lépés: **ESET-rendszerbővítmények** engedélyezése. A telepítés folytatásához kövesse a képernyőn megjelenő utasításokat.

3. Kötelező lépés: **Proxykonfiguráció** hozzáadása A megjelenő riasztási ablakban válassza ki az **Engedélyezés** lehetőséget.

4. Kötelező lépés: Adjon az ESET Endpoint Antivirus for macOS számára **Teljes lemezhozzáférést**. Kövesse a képernyőn megjelenő utasításokat, és engedélyezze a teljes lemezhozzáférést.

5. Ezután a varázsló kéri az **ESET Endpoint Antivirus for macOS** aktiválását. Több aktiválási lehetőséget is ismertet az Aktiválás című fejezet.

6. **Az értesítések engedélyezése** Azt javasoljuk, hogy engedélyezze az értesítéseket, hogy folyamatosan tájékozódjon a rendszert érintő esetleges fenyegetésekről.

A ESET Endpoint Antivirus for macOS használatbavételi varázsló kihagyása
A **Beállítás később** gombra kattintva kihagyhatja a kötelező beállítást, de vegye figyelembe, hogy a védelem csak részben fog működni.

A használatbavételi varázsló újraindítása
Nyissa meg a **Finder** > **Alkalmazások** lapot > a Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) az **ESET Endpoint Antivirus for macOS** ikonra > válassza ki a **Csomag tartalmának a megjelenítése** menüpontot a helyi menüben > nyissa meg a **Contents** elemet > nyissa meg a **Helpers** > **Használatbavétel** elemet. A kötelező biztonsági beállításokat is beállíthatja manuálisan a Kézi használatbavétel című fejezet követésével.

Az ESET Endpoint Antivirus for macOS telepítése után célszerű ellenőrizni, hogy a számítógép nem tartalmaz-e kártékony kódokat. A program főablakában kattintson a **Ellenőrzés** > **Ellenőrzés most** elemre. A Kézi indítású számítógép-ellenőrzés című fejezetben bővebben olvashat a kézi indítású számítógép-ellenőrzésről.

Rendszerbővítmények engedélyezése

Az ESET Endpoint Antivirus for macOS első alkalommal történő telepítéskor engedélyeznie kell az ESET Endpoint Antivirus for macOS számára a **rendszerbővítmények** és a **teljes lemezhozzáférés** védelmét.

macOS Ventura (13) és újabb

1. Nyissa meg a **Rendszerbeállításokat**.
2. Válassza ki az **Adatvédelem és biztonság** menüpontot a bal oldali menüből.
3. Görgessen le a **Biztonság** szakaszhoz, majd kattintson a **Részletek** gombra a „Néhány rendszerszoftver figyelmet igényel a használat előtt” szöveg alatt.

Ha a **Néhány rendszerszoftver figyelmet igényel a használat előtt** és a **Részletek** gomb nem látható, akkor már engedélyezte a rendszerbővítményeket, így nincs további teendője.

4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata gombra**, és írja be a **felhasználónevét** és **jelszavát**, majd kattintson a **Feloldás** gombra.
5. Engedélyezze az **ESET Valós idejű fájlrendszervédelem** és az **ESET Web- és e-mail-védelem** funkciót a kapcsolókra kattintva.
6. Kattintson az **OK** gombra.
7. Megjelenik az **ESET Web- és e-mail-védelem** figyelmeztetés, amely felszólítja a **proxykonfiguráció hozzáadására**. Válassza ki az **Engedélyezés** lehetőséget. Ha a figyelmeztetés megjelenésekor nem engedélyezi a proxykonfigurálást, akkor újra kell indítania a számítógépet a figyelmeztetés megjelenítéséshez, és újra engedélyeznie kell a proxykonfigurálást.

macOS Monterey (12) és régebbi

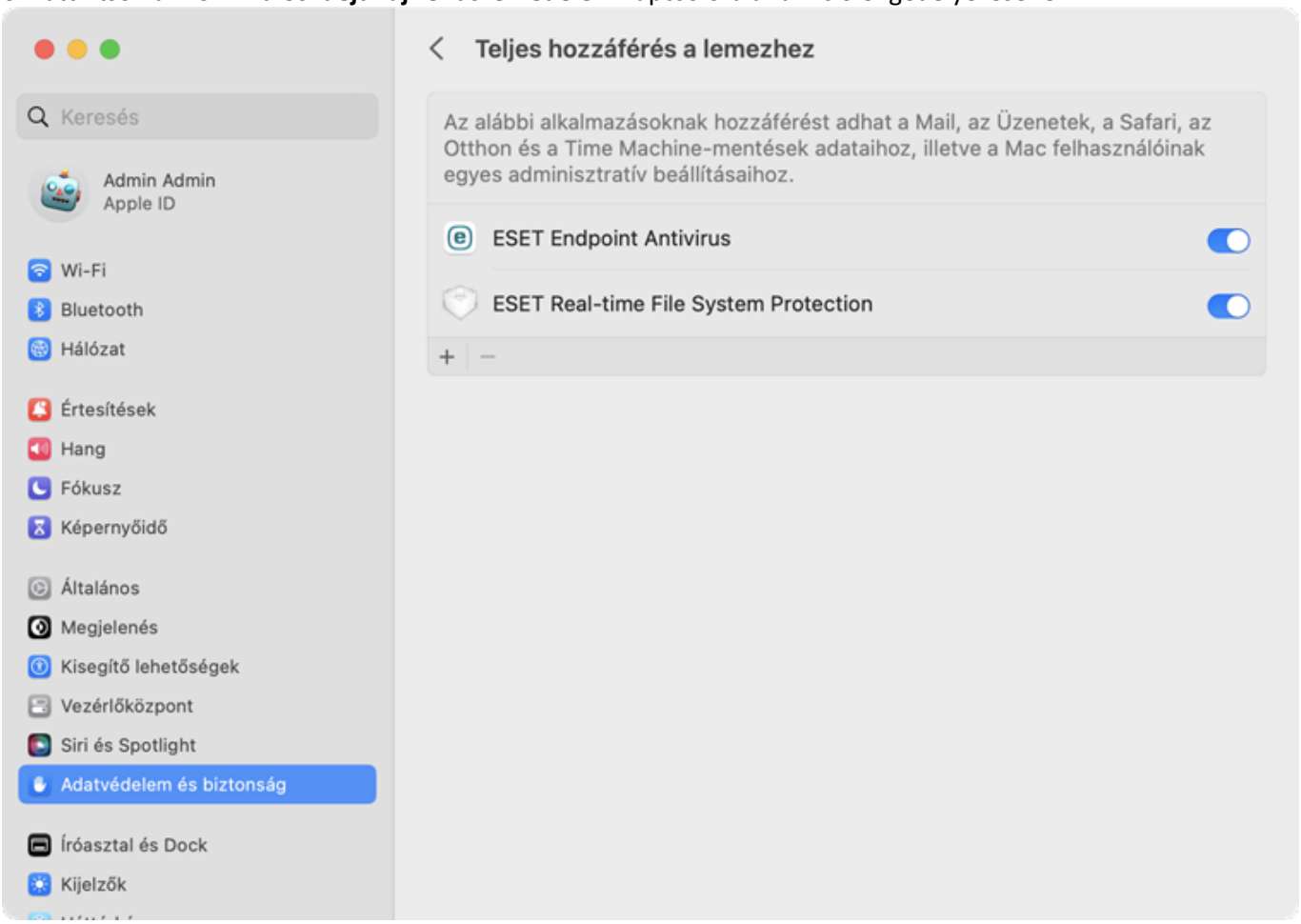
1. Nyissa meg a **Rendszerbeállításokat**.
2. Válassza ki a **Biztonság és adatvédelem** lehetőséget.
3. A bal alsó sarokban található lakatra kattintva engedélyezze a módosításokat a beállítási ablakban.
4. Használja a **Touch ID**-t, vagy kattintson a **Jelszó használata** gombra, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.
5. Kattintson a **Részletek** elemre.
6. Válassza ki mindegyik **ESET Endpoint Antivirus for macOS** opciót.
7. Kattintson az **OK** gombra.

A Teljes lemezhozzáférés engedélyezése

Az ESET Endpoint Antivirus for macOS első alkalommal történő telepítéskor engedélyeznie kell az ESET Endpoint Antivirus for macOS számára a rendszerbővítmények és a **teljes lemezhozzáférés** védelmét.

macOS Ventura (13) és újabb

1. Nyissa meg a **Rendszerbeállításokat**.
2. Válassza ki az **Adatvédelem és biztonság** menüpontot a bal oldali menüből.
3. Kattintson a **Teljes lemezhozzáférés** elemre, majd az ESET Endpoint Antivirus for macOS kapcsolóra a funkció engedélyezéséhez.
4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata gombra**, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.
5. Ha megjelenik egy felszólítás az ESET Endpoint Antivirus for macOS újraindítására, kattintson a **Később** gombra.
6. Kattintson az **ESET Valós idejű fájlrendszervédelem** kapcsolóra a funkció engedélyezéséhez.



macOS Monterey (12) és régebbi

1. Nyissa meg a **Rendszerbeállításokat**.
2. Lépjen az **Adatvédelem** lapra, és válassza ki a **Teljes lemezhozzáférés** menüpontot a bal oldali menüből.
3. A bal alsó sarokban található lakatra kattintva engedélyezze a módosításokat a beállítási ablakban.
4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata** gombra, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.
5. Válassza ki az **ESET Endpoint Antivirus for macOS** szolgáltatást a listából.
6. Ekkor megjelenik az ESET Endpoint Antivirus for macOS újraindítását lehetővé tevő értesítés. Kattintson a **Később** gombra.
7. Válassza ki az **ESET Valós idejű fájlrendszervédelem** elemet a listában.

> Ha a **Valós idejű fájlrendszervédelem** opció nem érhető el, először engedélyeznie kell a rendszerbővítményeket a ezeket a lépéseket követve.

8. Kattintson az **Újrakezdés** gombra a riasztási ablakban az ESET Endpoint Antivirus for macOS újraindításához és a módosítások érvényesítéséhez, vagy indítsa újra a számítógépet. További információkért tekintse meg tudásbáziscikkünket.

Parancssori telepítés

Kihagyhatja a grafikus felhasználói felület segítségével történő telepítést az ESET Endpoint Antivirus for macOS parancssori telepítésével. Ha a számítógép nincs regisztrálva az MDM-ben, a Rendszerbeállításokban akkor is manuálisan engedélyeznie kell a felhasználói hozzáférést az ESET Endpoint Antivirus for macOS számára.

> Ha a parancssori telepítést alkalmazza az ESET Endpoint Antivirus for macOS távolról történő telepítéséhez, akkor azt javasoljuk, hogy az ESET Endpoint Antivirus for macOS telepítése előtt ossza szét a konfigurációs profilokat a felhasználói beleegyezési beállításokkal együtt az MDM-en keresztül. A konfigurációs profilok beállításait a Telepítés előtti beállítások című témakörben találhatja meg.

1. ESET Endpoint Antivirus for macOS Letöltés.

2. A letöltött .dmg fájl felcsatolásához kattintson duplán a fájlra, vagy használja a következő parancssori folyamatot:

   a.A Terminalban lépjen a fájlhoz. Írja be a következőt: `cd ~/Letöltések`
   A `Letöltések` szó helyére a letöltött fájl helyét írja.

   b.Írja be a következőt: `hdiutil attach eea_osx_mlp_0.dmg`.
   Az `eea_osx_mlp_0` helyére a fájlnevet írja.

3. Írja be a következőt a Terminalban: `sudo installer -pkg /Volumes/ESET\ Endpoint\ Antivirus/.resources/Installer.pkg -target /`
Előfordulhat, hogy le kell cserélnie az Installer.pkg elérési útját az Installer.pkg helyére.

4. A telepítés után engedélyeznie kell a felhasználói hozzájárulási beállításokat az ESET Endpoint Antivirus for macOS számára Kézi használatbavétel szakaszban a teljes védelem biztosításához.

Távoli telepítés

A telepítés előtt

Az ESET Endpoint Antivirus for macOS használatához olyan jogosultsági beállítások szükségesek, amelyek megakadályozzák a teljes távoli telepítését, ha az eszköz nincs regisztrálva egy MDM-ben. Ha az eszköz

regisztrálva van egy MDM-ben, akkor az MDM segítségével konfigurációs profilokon keresztül továbbíthatja ezeket a beállításokat. Ha az eszköz nincs regisztrálva van egy MDM-ben, akkor a jogosultsági beállításokat manuálisan kell engedélyezni mindegyik számítógépen.

Ha a Jamfet használja, megtekintheti a Jamfra vonatkozó útmutatónkat is.

Konfigurációs profilok beállítása az ESET Endpoint Antivirus for macOS szolgáltatáshoz

Mielőtt telepítené az ESET Endpoint Antivirus for macOS szolgáltatást, engedélyeznie kell a következő beállításokat a célszámítógépeken:

- **ESET-rendszerbővítmények**
  Ha az ESET rendszerbővítményei nincsenek engedélyezve a telepítés előtt, a felhasználók a Rendszerkiterjesztések letiltva értesítést kapják addig, amíg az ESET rendszerkiterjesztéseit nem engedélyezik.

- **Teljes lemezhozzáférés**
  Ha a teljes lemezhozzáférés nincs engedélyezve a telepítés előtt, a felhasználók A számítógép részben védett értesítést kapják addig, amíg a teljes lemezhozzáférést nem engedélyezik.

- **Webhozzáférés- és e-mail védelem**
  A Web- és e-mail védelem konfigurációját hozzá kell adnia a rendszerbeállításokhoz ahhoz, hogy a Web- és e-mail védelem működjön.
  Ha az ESET Endpoint Antivirus for macOS telepítése után hiányzik a Web- és e-mail-védelem konfigurációja, a felhasználók Az „ESET Endpoint Antivirus for macOS” hálózati tartalmat szeretne szűrni értesítést kapják. Amikor megkapják ezt az értesítést, kattintsanak az Engedélyezés gombra. Ha a Tiltás gombra kattintanak, a Web- és e-mail-védelem nem fog működni.

A fenti ESET-beállítások távoli engedélyezéséhez regisztrálnia kell számítógépét egy MDM- (mobileszköz-felügyeleti) szerveren, amilyen például a Jamf.

ESET-rendszerbővítmények engedélyezése

A rendszerbővítmények távoli engedélyezéséhez hajtsa végre az alábbi műveletek egyikét a telepítés előtt:

- Töltse le a .plist adatcsomagfájlt. Hozzon létre konfigurációs profilt az MDM-ben a `.plist` adatcsomag segítségével.

- Hozzon létre konfigurációs profilt az MDM-ben a következő beállításokkal:

Csapatazonosító (TeamID)	`P8DQRXPVLP`
Csomagazonosító (BundleID)	`com.eset.endpoint` `com.eset.network`

A teljes lemezhozzáférés engedélyezése

A teljes lemezhozzáférés távoli engedélyezéséhez hajtsa végre az alábbi műveletek egyikét a telepítés előtt:

- Töltse le a.plist adatcsomagfájlt az ESET Endpoint Antivirus for macOS alkalmazáshoz.Hozzon létre konfigurációs profilt az MDM-ben a `.plist` adatcsomag segítségével.
  Ha az eszközt az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD kezeli, engedélyeznie kell a teljes

lemezhozzáférést az ESET Management Agent számára is. Töltse le a .plist adatcsomagfájlt az ESET Management Agent szolgáltatáshoz.

oHozzon létre konfigurációs profilt a következő beállításokkal:

ESET Endpoint Antivirus	
Azonosító	`com.eset.eea.g2`
Azonosító típusa	`bundleID`
Kódkövetelmény	`identifier "com.eset.eea.g2" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Alkalmazás vagy szolgáltatás	`SystemPolicyAllFiles`
Hozzáférés	`Allow`

Azonosító	`com.eset.endpoint`
Azonosító típusa	`bundleID`
Kódkövetelmény	`identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Alkalmazás vagy szolgáltatás	`SystemPolicyAllFiles`
Hozzáférés	`Allow`

A macOS 12 Monterey és újabb rendszerben	
Azonosító	`com.eset.app.Uninstaller`
Azonosító típusa	`bundleID`
Kódkövetelmény	`identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Alkalmazás vagy szolgáltatás	`SystemPolicyAllFiles`
Hozzáférés	`Allow`

ESET Management Agent	
Azonosító	`com.eset.remoteadministrator.agent`
Azonosító típusa	`bundleID`
Kódkövetelmény	`identifier "com.eset.remoteadministrator.agent" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Alkalmazás vagy szolgáltatás	`SystemPolicyAllFiles`
Hozzáférés	`Allow`

Miután távolról engedélyezte a teljes lemezhozzáférést és a rendszerbővítményeket, a Rendszerbeállítások > Adatvédelem és biztonság lapon ezek a beállítások letiltottnak tűnhetnek. Ha az ESET Endpoint Antivirus for macOS nem jelenít meg figyelmeztetéseket, a teljes lemezhozzáférés és a rendszerbővítmények engedélyezve vannak, függetlenül a Rendszerbeállítások > Adatvédelem és biztonság lapon látható állapotuktól.

Webhozzáférés- és e-mail védelem

Ha a Web- és e-mail-védelem konfigurációját távolról szeretné hozzáadni a rendszerbeállításokhoz, hajtsa végre az alábbi műveletek egyikét a telepítés előtt:

- Töltse le a .plist adatcsomagfájlt. Hozzon létre konfigurációs profilt az MDM-ben a `.plist` adatcsomag segítségével. Regisztrálnia kell számítógépét az MDM-szerveren ahhoz, hogy telepíteni tudja a konfigurációs profilokat a számítógépekre.

- Saját konfigurációs profil létrehozásához hozzon létre egy VPN típusú konfigurációs profilt a következő beállításokkal:

VPN-típus	VPN
Kapcsolat típusa	Custom SSL
Az egyéni SSL VPN azonosítója	com.eset.network.manager
szerverét	localhost
Szolgáltatói csomagazonosító	com.eset.network
Felhasználói hitelesítés	Tanúsítvány
Szolgáltató típusa	App-proxy
Szolgáltató által kijelölt követelmény	identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Az Igény szerinti VPN engedélyezése	✓
Igény szerinti szabálykonfigurálási XML	<array> <dict> <key>Action</key> <string>Connect</string> </dict> </array>
Üresjárati időzítő	Ne csatlakozzon le
Proxybeállítás	Nincs

A Web- és e-mail-védelem konfigurációja törlődni fog az ESET Endpoint Antivirus for macOS eltávolítása után. Ha törölni, majd telepíteni szeretné az ESET Endpoint Antivirus for macOS szolgáltatást, ismét telepítenie kell a Web- és e-mail-védelem konfigurációját a célszámítógépre az eltávolítás után.

Jamf előtelepítési beállítások

A Jamf főablakában kattintson a **Számítógépek** > **Konfigurációs profilok** elemre.

Webhozzáférés- és e-mail védelem

A Web- és e-mail védelem konfigurációját hozzá kell adnia a rendszerbeállításokhoz ahhoz, hogy a Web- és e-mail védelem működjön. Ha az ESET Endpoint Antivirus for macOS telepítése után hiányzik a Web- és e-mail-védelem konfigurációja, a felhasználók Az „ESET Endpoint Antivirus for macOS” hálózati tartalmat szeretne szűrni értesítést kapják.

A Webhozzáférés-védelem konfiguráció törlődik az ESET Endpoint Antivirus for macOS eltávolítása után. Ha törölni, majd újratelepíteni szeretné az ESET Endpoint Antivirus for macOS szolgáltatást, ismét telepítenie kell a Web- és e-mail-védelem konfigurációját a célszámítógépre.

Az **Általános** részben töltse ki a következőket:

Név	éldául ESET Web&Email Protection
Szint	Számítógépes szint
Szétosztási módszer	általában: Telepítse automatikusan

A **VPN** részben töltse ki a következőket:

VPN-típus	VPN
Kapcsolat típusa	Egyéni SSL
Azonosító	com.eset.network.manager
szerver	localhost
Szolgáltatói csomagazonosító	com.eset.network
Felhasználói hitelesítés	Tanúsítvány
Szolgáltató típusa	App-proxy
Szolgáltató által kijelölt követelmény	identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Azonosságtanúsítvány	Nincs
Az Igény szerinti VPN engedélyezése	✓
Igény szerinti szabálykonfigurálási XML	<array> <dict> <key>Action</key> <string>Connect</string> </dict> </array>
Üresjárati időzítő	Ne csatlakozzon le
Proxybeállítás	Nincs

ESET-rendszerbővítmények engedélyezése

Az **Általános** részben töltse ki a következőket:

Név	például ESET SEXT
Szint	Számítógépes szint
Szétosztási módszer	általában Telepítse automatikusan

A **Rendszerbővítmények** részben töltse ki a következőket:

Megjelenítendő név	például ESET SEXT
Rendszerbővítmény-típusok	Engedélyezett rendszerbővítmények
Csapatazonosító	P8DQRXPVLP
Engedélyezett rendszerbővítmények	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

---

A teljes lemezhozzáférés engedélyezése

Az **Általános** részben töltse ki a következőket:

Név	például ESET teljes lemezhozzáférés
Szint	Számítógépes szint
Szétosztási módszer	általában Telepítse automatikusan

Az **Adatvédelmi beállítások irányelvének vezérlője** részben töltse ki a következőket:

Azonosító	com.eset.endpoint
Azonosító típusa	Csomagazonosító
Kódkövetelmény	identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Alkalmazás vagy szolgáltatás	SystemPolicyAllFiles
Hozzáférés	Engedélyezés

Azonosító	com.eset.devices
Azonosító típusa	Csomagazonosító
Kódkövetelmény	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Alkalmazás vagy szolgáltatás	SystemPolicyAllFiles
Hozzáférés	Engedélyezés

Azonosító	com.eset.eea.g2
Azonosító típusa	Csomagazonosító

Kódkövetelmény	identifier "com.eset.eea.g2" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Alkalmazás vagy szolgáltatás	SystemPolicyAllFiles
Hozzáférés	Engedélyezés

Azonosító	com.eset.app.Uninstaller
Azonosító típusa	Csomagazonosító
Kódkövetelmény	identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Alkalmazás vagy szolgáltatás	SystemPolicyAllFiles
Hozzáférés	Engedélyezés

Miután távolról engedélyezte a teljes lemezhozzáférést és a rendszerbővítményeket, a Rendszerbeállítások > Adatvédelem és biztonság lapon ezek a beállítások letiltottnak tűnhetnek. Ha az ESET Endpoint Antivirus for macOS nem jelenít meg figyelmeztetéseket, a teljes lemezhozzáférés és a rendszerbővítmények engedélyezve vannak, függetlenül a Rendszerbeállítások > Adatvédelem és biztonság lapon látható állapotuktól.

Telepítés az ESET felügyeleti konzolon keresztül

Az ESET Endpoint Antivirus for macOS használatához olyan jogosultsági beállítások szükségesek, amelyek megakadályozzák a teljes távoli telepítését, ha az eszköz nincs regisztrálva egy MDM-ben. Ha az eszköz regisztrálva van egy MDM-ben, akkor az MDM segítségével konfigurációs profilokon keresztül továbbíthatja ezeket a beállításokat. Ha az eszköz nincs regisztrálva van egy MDM-ben, akkor a jogosultsági beállításokat manuálisan kell engedélyezni mindegyik számítógépen.

ESET PROTECT On-Prem

Mielőtt telepítené az ESET Endpoint Antivirus for macOS szolgáltatást az ESET PROTECT On-Prem segítségével, továbbítania kell az ESET Management Agent programot a célszámítógépre.

1. Az ESET Management Agent telepítéséhez hozza létre az Agent Live Installert.

2. Töltse le a macOS Agent Live Installert.

3. Bontsa ki az .sh szkriptet a letöltött .tar.gz archívumból.

4. Telepítse és futtassa az .sh szkriptet a célszámítógépen az Agent telepítéséhez. Ha a Jamfot használja MDM-ként, a Jamf segítségével telepítheti és futtathatja a szkriptet.

5. Az Agent célszámítógépre való telepítése után a számítógép láthatóvá válik az ESET PROTECT On-Prem szolgáltatásban.

Az ESET Endpoint Antivirus for macOS telepítéséhez hozza létre és futtassa a Szoftvertelepítés feladatot az ESET PROTECT On-Prem szolgáltatásban.

ESET PROTECT CLOUD

Az ESET Endpoint Antivirus for macOS az ESET PROTECT CLOUD segítségével és az ESET Management Agent egyszerre telepíthető egy Live Installer létrehozásával.

Ha van licence, és az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD szolgáltatáshoz csatlakozik, akkor a licenc automatikusan bekerül a telepítőcsomagba, és az ESET Endpoint Antivirus for macOS automatikusan aktiválódik.

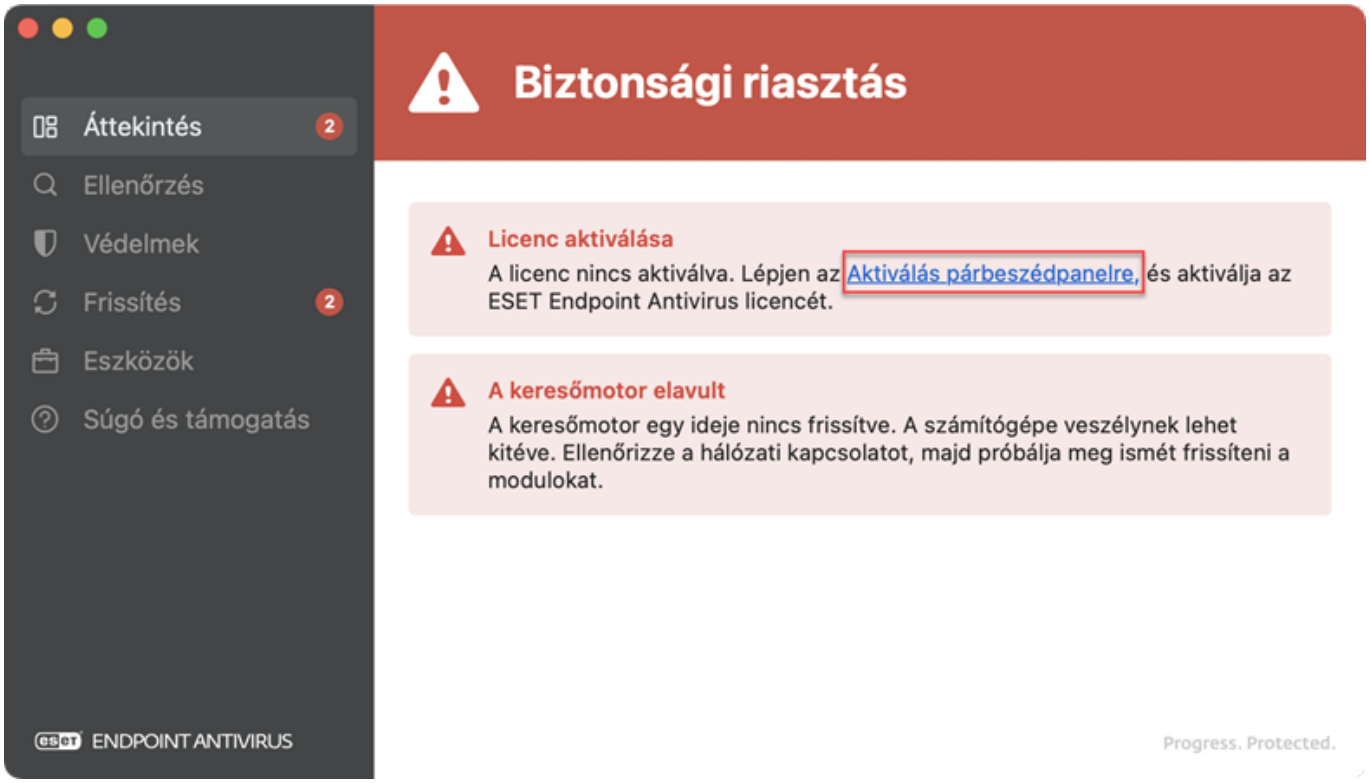
Hol találom a licencemet?

Ha vásárolt licencet, két e-mailt kellett kapnia az ESET-től. Az első e-mail az ESET Business Account portálról tartalmaz információkat. A második e-mail a licenckulcsról (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) vagy a nyilvános licencazonosítóról (xxx-xxx-xxx), a termék nevéről (vagy a termékek listájáról) és a mennyiségről tartalmaz részleteket.

Helyi aktiválás

1. Nyissa meg az ESET Endpoint Antivirus for macOS szolgáltatást.

2. A Termékaktiválás biztonsági riasztásban kattintson az Aktiválás párbeszédpanel szövegre.



3. Miután megjelent az aktiválási párbeszédpanel, írja be a licenckulcsot, majd kattintson a Folytatás gombra.

4. Kattintson a Befejezés elemre.

Aktiválás a Terminalon keresztül

Használja az `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic` segédprogramot jogosult felhasználóként az ESET Endpoint Antivirus for macOS Terminal-ablakból történő aktiválásához.

Szintaxis: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic [OPTIONS]`

Példa

Az alábbi parancsokat jogosult felhasználóként kell futtatni.

Aktiválás licenckulcs segítségével

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic -k XXXX-XXXX-XXXX-XXXX-XXXX
```

vagy

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
```

az `XXXX-XXXX-XXXX-XXXX-XXXX` az ESET Endpoint Antivirus for macOS-licenckulcs.

Távoli aktiválás

Ha az ESET Endpoint Antivirus for macOS szolgáltatást az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD segítségével telepíti, és van licence az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD szolgáltatáshoz csatlakoztatva, akkor a licenc automatikusan bekerül a telepítőcsomagba, és az ESET Endpoint Antivirus for macOS automatikusan aktiválódik.

Az ESET Endpoint Antivirus for macOS aktiválása távolról az ESET PROTECT On-Prem segítségével

Az ESET Endpoint Antivirus for macOS szolgáltatás ESET PROTECT On-Prem vagy ESET PROTECT CLOUD való későbbi aktiválásához jelentkezzen be az ESET PROTECT On-Prem webkonzolba, és használja a Termékaktiválás kliensfeladatot.

Távolról felügyelt végpontok dokumentációja

Az ESET Endpoint Antivirus for macOS 7-es verziója távolról kezelhető az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD segítségével. Az ESET távoli felügyeleti eszközeivel egyetlen helyről telepíthet ESET-megoldásokat, kezelhet feladatokat, érvényesíthet biztonsági irányelveket, felügyelheti a rendszerállapotot, és reagálhat gyorsan a távoli számítógépeken fellépő problémákra és fertőzésekre.

ESET távoli felügyeleti eszközök

Az ESET Endpoint Antivirus for macOS az ESET felügyeleti konzollal távolról is kezelhető.

- Az ESET PROTECT On-Prem ismertetése
- Az ESET PROTECT CLOUD ismertetése

Mobileszközök menedzselése (MDM)

Az ESET Endpoint Antivirus for macOS távoli telepítéséhez az eszközöket regisztrálni kell az MDM-ben. Ha eszközei nincsenek regisztrálva az MDM-ben, fizikailag hozzá kell férnie minden eszközhöz az ESET Endpoint Antivirus for

macOS telepítéséhez.

A mobileszköz-felügyeleti (MDM) megoldások lehetővé teszik a rendszergazdák számára szervezeti és konfigurációs házirendek telepítését, eszközök felügyeletét, alkalmazások telepítését vagy eltávolítását és még sok minden mást. Nem minden MDM-megoldás támogatja az Apple-eszközöket. Az MDM-megoldás kiválasztásához segítséget nyújt az Apple által összeállított Válasszon MDM-megoldást című útmutató.

Az MDM-ekkel kapcsolatban további információkat az Apple dokumentációjában és az adott MDM-gyártó dokumentációjában talál.

Az ESET Endpoint Antivirus for macOS MDM-en keresztül elvégzendő konfigurációja univerzális letölthető adatcsomagokat tartalmaz, amelyek segítségével konfigurációs profilokat hozhat létre bármely MDM-en. Ha a Jamfet használja MDM-ként, használhatja a Jamf specifikus útmutatót is.

Termékkonfiguráció az ESET PROTECT On-Prem szolgáltatásban

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

Keresőmotor

A keresőmotor a fájlok 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.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A keresőmotorban a következő beállításokat adhatja meg:

Általános

Víruskereső beállításai

Kéretlen alkalmazások keresésének engedélyezése – Lásd a kéretlen alkalmazások kifejezést a szószedetünkben.

Veszélyes alkalmazások keresésének engedélyezése – Lásd a veszélyes alkalmazások kifejezést a szószedetünkben.

Gyanús alkalmazások keresésének engedélyezése – A gyanús alkalmazások olyan tömörítőprogramokkal vagy védelmi modulokkal tömörített szoftverek, amelyeket gyakran a visszafejtés megakadályozása vagy a végrehajtható fájlok tartalmának elrejtése (például a kártevők jelenlétének elrejtése) céljából használnak saját tömörítő vagy titkosító módszerek alkalmazásával.

Ez a kategória magában foglal minden ismeretlen, a kártevők tömörítéséhez gyakran használt csomagolókkal vagy védelmi modulokkal tömörített alkalmazást.

Kivételek

Teljesítménybeli kivételek – Ha kizár útvonalakat (mappákat) az ellenőrzésből, sokkal kevesebb idő alatt kiszűrhetők a kártevők a fájlrendszerből.

Kivétel létrehozása:

1. Kattintson a Szerkesztés gombra a Teljesítménybeli kivételek szöveg mellett.

2. Kattintson a Hozzáadás gombra, és határozza meg, hogy a kereső melyik útvonalat hagyja ki. Opcionálisan megjegyzést is megadhat tájékoztatási célból.

3. Kattintson az OK > Mentés elemre a kizárás létrehozásához és a párbeszédpanel bezárásához.

Valós idejű fájlrendszervédelem

A Valós idejű fájlrendszervédelem a rendszer összes, a vírusvédelemhez köthető eseményét ellenőrzi. A program a fájlok számítógépen történő megnyitásakor, létrehozásakor vagy futtatásakor ellenőrzi, hogy nem tartalmaznak-e kártevő kódot. Alapértelmezés szerint a Valós idejű fájlrendszervédelem a rendszer indításakor indul el, és megszakítás nélküli ellenőrzést biztosít.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Keresőmotor Valós idejű fájlrendszervédelem lapon a következő beállításokat adhatja meg:

Általános

Alapértelmezés szerint a Valós idejű fájlrendszervédelem a rendszerindításkor indul el, és folyamatos ellenőrzést biztosít. Egyes esetekben (például egy másik valós idejű víruskereső okozta ütközéskor) a Valós idejű fájlrendszervédelem letiltható A valós idejű fájlrendszervédelem engedélyezése szöveg melletti csúszkára koppintva.

Ellenőrizendő adathordozók

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

- Helyi meghajtók – Az összes helyi meghajtó ellenőrzése
- Cserélhető adathordozók – CD-k, DVD-k, USB-tárolóeszközök stb. ellenőrzése
- Hálózati meghajtók – Az összes hálózati meghajtó ellenőrzése.

Az ESET azt tanácsolja, hogy az alapértelmezett beállításokat használja, és csak bizonyos esetekben módosítsa őket – például amikor egyes adathordozók ellenőrzése jelentősen lelassítja 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 – Ezzel a jelölőnégyzettel engedélyezheti vagy letilthatja az ellenőrzést a fájlok megnyitásakor.
- Fájlok létrehozásakor – Ezzel a jelölőnégyzettel engedélyezheti vagy letilthatja az ellenőrzést a fájlok

létrehozásakor.

• Cserélhető adathordozó elérésekor – Engedélyezheti vagy letilthatja a cserélhető adathordozók automatikus ellenőrzését, amikor a számítógéphez csatlakoztatja őket.

Folyamatkivételek

Ellenőrzésből kizárandó folyamatok – Ha kizár folyamatokat az ellenőrzésből, sokkal kevesebb idő alatt kiszűrhetők a kártevők a rendszerből.

Kivétel létrehozása:

1. Kattintson a Szerkesztés gombra az Ellenőrzésből kizárandó folyamatok szöveg mellett.

2. Kattintson a Hozzáadás gombra, majd határozza meg a végrehajtható fájl elérési útját.

3. Kattintson a Mentés > Mentés elemre a kizárás létrehozásához és a párbeszédpanel bezárásához.

ThreatSense paraméterek

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-paraméterek 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.

Felhőalapú védelem

A ESET LiveGrid® egy korszerű, több felhőalapú technológiából álló riasztási rendszer. Lehetővé teszi az új rosszindulatú programok korai felismerését a megbízhatósági felmérések alapján, és javítja az engedélyezőlistára helyezés hatékonyságát.

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

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Keresőmotor > Felhőalapú védelem területen a következő beállításokat konfigurálhatja:

Felhőalapú védelem

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

Az ESET víruslaborja megkapja a mintákat további elemzésre.

Összeomlási jelentések és diagnosztikai adatok küldése

Elküldhet például olyan adatokat, mint az összeomlási jelentések vagy a modul-memóriaképek.

Segítse a termék tökéletesítését anonim használati statisztikai adatok beküldésével

Engedélyezheti az ESET-nek, hogy begyűjtse az újonnan észlelt kártevőkre vonatkozó anonim információkat (név, az észlelés dátuma és időpontja, az észlelési mód és a kapcsolódó metaadatok), az ellenőrzött fájlokat (kivonat, fájlnév, a fájl eredete, telemetria), a letiltott és gyanús URL-címeket, a termékverziót és -konfigurációt, beleértve az Ön rendszerének adatait.

E-mail-cím (nem kötelező)

E-mail-címét a program a gyanús fájlokkal együtt elküldi az ESET víruslaborjába. Az ESET munkatársai azonban csak akkor keresik fel, ha a gyanús fájlokkal kapcsolatban további információra van szükségük.

Minták elküldése

Az észlelt vírusminták automatikus elküldése

A kiválasztott beállítás alapján fertőzött mintákat küldheti be az ESET víruslaborjának elemzésre és a kártevőészlelés fejlesztése céljából.

- Az összes fertőzött minta
- Az összes minta a dokumentumok kivételével
- Ne küldje be

Gyanús minták automatikus elküldése

A kártevőkre hasonlító és szokatlan tulajdonságokat vagy viselkedést mutató gyanús mintákat a rendszer elküldi elemzésre az ESET víruslaborjába.

Végrehajtható fájlok – Például a következő végrehajtható fájlok: *.exe*, *.dll*,*.sys*.

Tömörített fájlok – Például a következő tömörített fájltípusok: *.zip*, *.rar*, *.7z*, *.arch*, *.arj*, *.bzip2*, *.gzip*, *.ace*, *.arc*, *.cab*

Szkriptek – Például a következő szkriptfájltípusok: *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, , *.ps1*

Egyéb – Például a következő fájltípusok: *.jar*, *.reg*, *.msi*, *.swf*, *.lnk*

Dokumentumok – A Microsoft Office, a Libre Office vagy más irodai eszközben létrehozott dokumentumok vagy aktív tartalommal rendelkező PDF-fájlok.

Kivételek

Kattintson a Szerkesztés gombra a Kivételek szó mellett bizonyos fájlok vagy mappák kizárásához. A kizárt fájlokat akkor sem kapja meg az ESET víruslaborja, ha gyanús kódot tartalmaznak.

Minták maximális mérete (MB)

Meghatározhatja a minták maximális méretét.

Kártevő-ellenőrzések

A kézi indítású víruskereső a vírus- és kémprogramvédelem fontos része, és a 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.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Keresőmotor > Kártevőellenőrzések lapon megadhatja a Kézi indítású ellenőrzési profilok beállításait:

Kiválasztott profil – Válassza ki a szerkeszteni kívánt profilt.

Profilok listája – Új létrehozásához vagy meglévő eltávolításához kattintson a Szerkesztés gombra. Írja be a profil nevét, majd kattintson a Hozzáadás gombra. Az új profil megjelenik a Kiválasztott profil legördülő menüben, amely felsorolja a meglévő ellenőrzési profilokat.

ThreatSense-paraméterek – Az ellenőrzési profil konfigurációs beállításai, például a vezérelni kívánt fájlkiterjesztések, ellenőrizendő objektumok, alkalmazott észlelési módszerek stb. Részletes információkért lásd a

ThreatSense paraméterek című részt.

ThreatSense paraméterek

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

A ThreatSense motor beállításaival több ellenőrzési paraméter megadható:

- Az ellenőrizendő fájltípusok és kiterjesztések
- Különböző észlelési módszerek kombinációja
- A megtisztítás mértéke stb.

A különböző biztonsági körülmények eltérő konfigurációkat igényelhetnek. Ennek érdekében a ThreatSense külön beállítható az alábbi védelmi modulokhoz:

- Valós idejű fájlrendszervédelem
- Kártevő-ellenőrzések
- Webhozzáférés-védelem
- E-mail védelem

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).

Ellenőrizendő objektumok

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

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 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 (pl. UPX, yoda, ASPack, FSG) 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 még nem létező, illetve a korábbi vírusdefiníciós adatbázisban még nem szereplő kártevő szoftvereket is képes felismerni. Hátránya, hogy (nagyon ritkán) téves riasztásokat is küldhet.

Kiterjesztett heurisztika/DNA-vírusdefiníciók – A kiterjesztett heurisztika az ESET saját, a számítógépes férgek és trójai programok felismerésére optimalizált, magas szintű programozási nyelveken fejlesztett heurisztikus algoritmusa. A kiterjesztett heurisztika használata jelentősen javítja az ESET-termékek kártevő-észlelési hatékonyságát. A vírusdefiníciók alapján a program megbízhatóan felismeri és azonosítja a vírusokat. Az automatizált frissítési rendszeren keresztül a definíciós frissítések a kártevők felfedezése után mindössze néhány órával elérhetővé válnak. A vírusdefiníciók hátránya, hogy csak az ismert vírusok (vagy azok alig módosított változatai) ismerhetők fel velük.

Megtisztítás

A ThreatSense-paraméterek a következő tisztítási szinteket teszik lehetővé:

Automatikus megtisztítás szintje	**Leírás**
Nincs megtisztítás	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 fertőzés esetén.
Szokásos módon megtisztít	Az észlelt kártevő megtisztítása 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 tisztítható meg, akkor az objektum az eredeti helyén marad.
Automatikusan megtisztít	Az észlelt kártevő megtisztítása 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.
Alapos megtisztítás	Az észlelt kártevő megtisztítása az objektumok tisztítása közben. Egyes esetekben, ha nem hajtható végre művelet, a végfelhasználó interaktív figyelmeztetést kap, és ki kell választania egy megtisztítási műveletet (például törlés vagy figyelmen kívül hagyás). Legtöbb esetben ez a beállítás ajánlott.
Törlés	Az összes fertőzött fájl törlésének megkísérlése végfelhasználói beavatkozás nélkül.

Kivételek

A kiterjesztés a fájlnév ponttal elválasztott része. A kiterjesztés határozza meg a fájl típusát és tartalmát. A ThreatSense keresőmotor beállításait tartalmazó lap jelen részén határozhatók meg az ellenőrzésből kizárandó fájlok típusai.

Más

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

Változó adatfolyamok ellenőrzése – 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.

Optimalizálás engedélyezése – A jelölőnégyzet bejelölése esetén a program a legoptimálisabb beállításokat használja a leghatékonyabb ellenőrzési szint, ugyanakkor a leggyorsabb ellenőrzési sebesség biztosításához. A különböző védelmi modulok intelligensen végzik az ellenőrzést, kihasználják és az adott fájltípusokhoz alkalmazzák a különböző ellenőrzési módszereket. Az optimalizálás letiltása esetén a program csak a felhasználók által az egyes modulok ThreatSense-alapbeállításaiban megadott beállításokat alkalmazza az ellenőrzések végrehajtásakor.

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

Korlátok

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

Objektumok ellenőrzésének beállításai

Tiltsa le az Alapbeállítások használata az objektumok ellenőrzéséhez szöveg melletti csúszkát a következő beállítások megadásához:

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

Tiltsa le az Alapbeállítások használata a tömörített fájlok ellenőrzéséhez szöveg melletti csúszkát a következő beállítások megadásához:

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.

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

További ThreatSense-paraméterek

Ezek a beállítások csak a Valós idejű fájlrendszervédelemhez érhetők el.

A fertőzés valószínűsége az újonnan létrehozott vagy módosított fájlok esetén magasabb, mint a meglévő fájloknál, ezért a program további ellenőrzési paraméterekkel ellenőrzi a fájlt. Az ESET Endpoint Antivirus for macOS kiterjesztett heurisztikát használ, amely még a keresőmotor frissítésének megjelenése előtt a vírusdefiníció-alapú ellenőrzési módszerekkel együtt észleli az új kártevőket.

Az újonnan létrehozott fájlok mellett az ellenőrzés az önkicsomagoló (.sfx) fájlokra és a futtatás közbeni tömörítőkre (belsőleg tömörített végrehajtható fájlokra) is kiterjed. A tömörített fájlokat a program alapértelmezés szerint a 10. mélységi szintig ellenőrzi, az ellenőrzés a fájlok méretétől függetlenül megtörténik. A tömörített fájlok ellenőrzési beállításainak a módosításához törölje az Alapbeállítások használata a tömörített fájlok ellenőrzéséhez jelölőnégyzet jelölését.

Megtisztítási szintek

Automatikus megtisztítás szintje	**Leírás**
Nincs megtisztítás	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 fertőzés esetén.
Szokásos módon megtisztít	Az észlelt kártevő megtisztítása 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 tisztítható meg, akkor az objektum az eredeti helyén marad.
Automatikusan megtisztít	Az észlelt kártevő megtisztítása 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.
Alapos megtisztítás	Az észlelt kártevő megtisztítása az objektumok tisztítása közben. Egyes esetekben, ha nem hajtható végre művelet, a végfelhasználó interaktív figyelmeztetést kap, és ki kell választania egy megtisztítási műveletet (például törlés vagy figyelmen kívül hagyás). Legtöbb esetben ez a beállítás ajánlott.
Törlés	Az összes fertőzött fájl törlésének megkísérlése végfelhasználói beavatkozás nélkül.

Frissítés

Ebben a szakaszban adhatja meg a frissítési források beállításait, például a használatban lévő frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Frissítés részben a következő beállításokat konfigurálhatja:

Általános

Alapértelmezés szerint a Frissítés típusa Rendszeres frissítés. Ez biztosítja, hogy a kereső-adatbázis és a termékmodulok automatikusan frissüljenek az ESET frissítési szerverekről.

A tesztelési mód tartalmazza a legutóbbi hibajavításokat és észlelési módszereket, amelyek hamarosan elérhetők lesznek a nagyközönség számára is. Előfordulhat azonban, hogy nem mindig stabilak, ezért nem ajánlott termelési környezetben használni őket.

A késleltetett frissítések lehetővé teszik a speciális frissítési szerverekről való frissítést, amelyek a vírusadatbázisok új verzióit biztosítják legalább X órás késéssel (vagyis valós környezetben tesztelt és stabilnak tartott adatbázisok).

Modul-visszaállítás

Ha a keresőmotor egyik frissítése vagy a programmodulok feltehetően nem stabilak, illetve sérültek, az ESET PROTECT On-Prem Modulfrissítés visszaállítása feladatával visszaállhat az előző verzióra, és átmenetileg letilthatja a frissítéseket. Másik lehetőségként engedélyezheti a korábban letiltott frissítéseket, ha visszavonásig elhalasztotta őket.

Az ESET Endpoint Antivirus for macOS pillanatfelvételeket készít a keresőmotorról és a programmodulokról a visszaállítás funkcióhoz való használatra. A moduladatbázis pillanatfelvételeinek létrehozásához hagyja engedélyezve a Modulok pillanatképének létrehozása funkciót. Ha a Modulok pillanatképének létrehozása funkció engedélyezve van, az első pillanatkép az első frissítés alkalmával jön létre. A következő 48 óra múlva jön létre. A Helyben tárolt pillanatképek száma mező meghatározza a keresőmotor pillanatképeinek tárolt számát.

Amikor elérte a pillanatképek maximális mennyiségét (például három), a legrégebbi pillanatképet 48 óránként új pillanatfelvétel váltja fel. Az ESET Endpoint Antivirus for macOS visszaállítja a keresőmotor és a programmodulok frissítési verzióját a legrégebbi pillanatfelvételre.

Frissítési tükör (egyéni frissítési szerverek)

A tükör – amely a frissítési fájlok helyi hálózati környezetben létrehozott másolata – azért hasznos, mert így a frissítési fájlokat nem kell minden egyes munkaállomásnak újra és újra letöltenie a gyártó frissítési szerveréről. A frissítések letöltődnek a helyi tükörszerverre, majd a rendszer szétosztja őket az egyes munkaállomásokra, így nyújtva védelmet a hálózati túlterhelés ellen. A munkaállomások tükörből történő frissítése javítja a hálózati terheléselosztást, és internetes sávszélességet szabadít fel.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Frissítés > Elsődleges szerver vagy Másodlagos szerver lapon beállíthatja, hogy az ESET Endpoint Antivirus for macOS frissítési tükröt (egyéni frissítési szervereket) használjon:

1. Az Általános szakaszban tiltsa le a csúszkát az Automatikus kiválasztás szöveg mellett.

2. A Frissítési szerver mezőbe írja be a tükörszerver URL-címét az alábbi formátumok egyike szerint:

```
http://<IP>:<port>
```

```
http://<hostname>:<port>
```

> A frissítések telepítéséhez a következő szervert kell használni:
> `http://update.eset.com/eset_upd/businessmac/`

3. Írja be a megfelelő felhasználónevet és jelszót.

Ha több tükörszerver is van a hálózatban, ismételje meg a fenti lépéseket a másodlagos szerverkonfigurálásához.

Adathalászat elleni védelem

Az Adathalászat elleni védelem további védelmet biztosít azokkal a nem szabályszerű webhelyekkel szemben, amelyek jelszavakat és más bizalmas információkat kísérelnek meg megszerezni.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

Az Adathalászat elleni védelem alapértelmezés szerint engedélyezve van. Ha le szeretné tiltani az Adathalászat elleni védelmet, lépjen a Webes és e-mail > Adathalászat elleni védelem lapra, majd kattintson az Adathalászat elleni védelem engedélyezése szöveg melletti csúszkára.

Webhozzáférés-védelem

A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP protokollon alapuló szabályokat.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Web és e-mail > Webhozzáférés-védelem lapon a következő beállításokat konfigurálhatja:

Általános

Webvédelem engedélyezése – A böngészők és a távoli szerverek közötti kommunikáció figyelése.

Webprotokollok

HTTP-protokollszűrés engedélyezése – Bármely alkalmazás által használt HTTP-kommunikáció ellenőrzése.

A program csak a HTTP protokoll által használt portok beállításban meghatározott portok forgalmát ellenőrzi. Szükség esetén más kommunikációs portok is hozzáadhatók. A portszámokat vesszővel kell elválasztani.

URL-címek kezelése

Az URL-címek kezelése segítségével megadhatók a letiltandó, engedélyezendő, illetve az ellenőrzésből kizárandó HTTP-címek. A Letiltva címek listájában szereplő webhelyeket nem fogja tudni elérni. A megtalált kártevő mellőzve listán szereplő webhelyek elérése közben a program nem keres kártékony kódokat.

Ha csak az Engedélyezett címlistán szereplő címekhez szeretne hozzáférést biztosítani, engedélyezze az URL-címek korlátozása szöveg melletti jelölőnégyzetet.

Lista aktiválásához engedélyezze a Lista aktiválása szöveg melletti csúszkát az adott listanévnél. Ha értesítést szeretne kapni, amikor beírnak egy címet az adott listából, engedélyezze az Értesítés az alkalmazásakor szöveg melletti csúszkát.

A címlisták összeállításakor használható a * (csillag) és a ? (kérdőjel) speciális szimbólum. 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.

ThreatSense paraméterek

A ThreatSense-paraméterek lehetővé teszik a webhozzáférés-védelem konfigurációs beállításainak megadását, például az ellenőrizendő objektumokat, az alkalmazott észlelési módszereket stb. Részletes információkért lásd a ThreatSense-paraméterek című részt.

E-mail védelem

E-mail védelem – A POP3 és az IMAP protokollon keresztül érkező e-mailes kommunikáció szabályozását biztosítja.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Web és e-mail > E-mail-védelem szakaszban a következő beállításokat konfigurálhatja:

Általános

Az ESET Endpoint Antivirus for macOS és az e-mail-kliens integrálása növeli az e-mailekben található rosszindulatú kódok elleni aktív védelem szintjét. Az ESET azt javasolja, hogy soha ne kapcsolja ki Az e-mail védelem engedélyezése funkciót.

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 a POP3 protokollnál fejlettebb funkciókkal rendelkezik. Például több ügyfél egyszerre csatlakozhat ugyanahhoz a postaládához, és fenn tudják tartani az üzenetek állapotát, például azt, hogy az adott üzenetet elolvasták, megválaszolták, vagy törölték-e. A szabályozást biztosító védelmi modul automatikusan elindul a rendszer indításakor, majd ezután aktív marad a memóriában.

Az ESET Endpoint Antivirus for macOS védelmet nyújt ezeknek a protokolloknak, függetlenül a használt e-mail-klienstől, és nincs szükség az e-mail-kliens újrakonfigurálására. A program csak az IMAP/POP3 protokoll által használt portok beállításban meghatározott portok forgalmát ellenőrzi. Szükség esetén más kommunikációs portok is hozzáadhatók. A portszámokat vesszővel kell elválasztani.

ThreatSense paraméterek

A ThreatSense-paraméterek lehetővé teszik az e-mail-védelem konfigurációs beállításainak megadását, például az ellenőrizendő objektumokat, az alkalmazott észlelési módszereket stb. Részletes információkért lásd a ThreatSense-paraméterek című részt.

Riasztások és értesítések

Miután a program ellenőriz egy-egy levelet, az ellenőrzés eredményét ismertető értesítést is hozzáfűzhet. Bejelölheti az Értesítés hozzáfűzése a fogadott és elolvasott e-mailekhez jelölőnégyzetet. Ügyeljen arra, hogy a problémás HTML-üzenetekben az értesítések néha eltűnhetnek, illetve egyes kártevők képesek meghamisítani őket. Az értesítések a beérkezett és az elolvasott üzenetekhez 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 %VIRUSNAME%] Hello”. Az %VIRUSNAME% változó az észlelt kártevőt jelöli.

Eszközök

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

Az Eszközök lapon a következő beállításokat konfigurálhatja:

Feladatütemező

A Feladatütemező kézi indítású beütemezett feladatok előre definiált beállításokkal és jellemzőkkel történő kezelését és indítását végzi.

Kattintson a Szerkesztés gombra a Feladatok szó mellett az összes ütemezett feladat és konfigurációs jellemző megtekintéséhez.

Egy már meglévő ütemezett feladat beállításainak módosításához válassza ki a feladatot, majd kattintson a Szerkesztés elemre. A feladat törléséhez válassza ki a feladatot, majd kattintson az Eltávolítás gombra.

Új feladat hozzáadása:

1. Kattintson a Hozzáadás gombra a lista alján.

2. Adja meg a feladat nevét, majd állítsa be a feladat végrehajtásának időpontját.

3. Válassza ki azokat a napokat, amelyeken a feladatot ismételten futtatni szeretné. Kattintson a Továbbgombra.

4. Válassza az ütemezett ellenőrzés során használni kívánt Ellenőrzési profilt. Az ellenőrzési profilok megtekintéséről és szerkesztéséről a Kártevő-ellenőrzések című részben olvashat.

5. Adja meg az ellenőrizendő célterületeket, válassza ki, hogy az észlelt elemeket megtisztítja-e, és hogy az ütemezett ellenőrzés az ellenőrzési profil konfigurációjában beállított kivételeket is megvizsgálja-e.

6. Kattintson a Befejezés > Mentés elemre.

Proxyszerver

Nagyméretű helyi hálózatokon a kommunikációt egy proxyszerver tudja közvetíteni a számítógép és az internet között. E készülék használata meg kell adni az alábbi beállításokat. Különben előfordulhat, hogy a program nem frissül majd.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

> Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

> Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

Az Eszközök > Proxyszerverek lapon megadhatja a proxyszerver beállításait. Az itt definiált paramétereket minden olyan modul felhasználja, amely kapcsolódik az internethez.

A proxyszerver konfigurálása:

1. Engedélyezze a Proxyszerver használata opciót, majd írja be a proxyszerver címét a Proxyszerver mezőbe, a proxyszerver portszámát pedig a Port mezőbe.

2. Ha a proxyszerverrel folytatott kommunikációhoz hitelesítés szükséges, akkor engedélyezze A proxyszerver hitelesítést igényel funkciót, majd adjon meg egy érvényes felhasználónevet és jelszót a megfelelő mezőkben.

3. Engedélyezze a Közvetlen kapcsolat használata, ha nem érhető el proxy funkciót, ha azt szeretné, hogy meg legyen kerülve a proxy, és közvetlenül az ESET-szerverekkel folyjon a kommunikáció, ha a proxy nem érhető el.

Naplófájlok

Módosíthatja az ESET Endpoint Antivirus for macOS naplózási konfigurációját. A naplófájlokat az ESET PROTECT On-Prem segítségével tekintheti meg.

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

Az Eszközök > Naplófájlok lapon a következő beállításokat konfigurálhatja:

Naplók minimális részletessége

A naplózási részletesség azt határozza meg, hogy milyen részletesek legyenek a naplófájlok.

- Kritikus figyelmeztetések – Csak a kritikus hibákat tartalmazza (például nem sikerült elindítani a vírusirtót).
- Hibák – A „Hiba a fájl letöltésekor és más kritikus hibák bejegyzése a naplóba.
- Figyelmeztetések – Kritikus hibák és figyelmeztető üzenetek bejegyzése a naplóba.
- Tájékoztató bejegyzések – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett bejegyzéseket).
- Diagnosztikai bejegyzések – A fentiek mellett a program pontos beállításához szükséges információk megjelenítése.

Az ennél régebbi naplóbejegyzések törlése (nap) – A megadott napszámnál régebbi naplóbejegyzések automatikusan törlődnek.

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. A teljesítmény és a naplók feldolgozási sebességének javítása érdekében a program eltávolítja az összes üres naplóbejegyzést. A teljesítményjavulás különösen a nagyszámú bejegyzést tartalmazó naplófájloknál látványos.

Syslog-összetevő

A Syslog-összetevő egy olyan Syslog naplózási paraméter, amely hasonló naplóüzenetek csoportosítására használható. Például a démonnaplók (amelyek a démon Syslog-összetevőn keresztül gyűjtenek naplókat) a *~/log/daemon.log* helyre léphetnek, ha konfigurálva vannak. A systemd-re és annak naplójára való legutóbbi váltással a Syslog-összetevő kevésbé fontos, de továbbra is használható naplók szűrésére.

Felhasználói felület

Az ESET Endpoint Antivirus for macOS távoli konfigurálásához:

1. Az ESET PROTECT On-Prem szolgáltatásban kattintson a Házirendek > Új házirend elemre, majd írja be a házirend nevét.

Az ESET Endpoint for macOS (V7+) egyik meglévő házirendjének módosításához a házirendek listájában kattintson a módosítani kívánt házirendre, majd a Szerkesztés > Beállítások elemre.

2. Kattintson a Beállítások elemre, majd válassza ki az ESET Endpoint for macOS (V7+) menüpontot a legördülő menüből.

3. Adja meg a kívánt beállításokat.

4. Kattintson a Folytatás > Hozzárendelés elemre, majd válassza ki a megfelelő számítógépcsoportot.

5. Kattintson az OK > Befejezés elemre.

Az ESET Endpoint Antivirus for macOS helyi konfigurálásához lásd az alkalmazásbeállításokat.

A Felhasználói felület lapon a következő beállításokat konfigurálhatja:

Felhasználói felület elemei

Grafikus felhasználói felület megnyitásának engedélyezése a felhasználó számára – A beállítás letiltásával megakadályozhatja, hogy a felhasználók elérhessék a grafikus felhasználói felületet. Ez felügyelt környezetben, illetve olyan esetekben lehet hasznos, amikor meg kell őriznie a rendszererőforrásokat.

Ikon megjelenítése a menüsáv extrái között – A beállítás letiltásával eltávolíthatja az ESET Endpoint Antivirus for macOS ikonját a macOS menüsáv extrái közül (a képernyő tetején).

Értesítések

Értesítések megjelenítése az asztalon – Az asztali értesítések (például sikeres frissítési üzenetek, víruskeresési feladatok befejezése vagy új kártevők) a macOS menüsor melletti kis előugró ablakban jelennek meg. Ha engedélyezve van, az ESET Endpoint Antivirus for macOS tájékoztatja, ha új esemény következik be.

Állapotok

Alkalmazásállapotok – A Szerkesztés gombra koppintva konfigurálhatja, hogy mely alkalmazásállapotok jelenítsenek meg értesítést a Védelem állapota ablakban, és hogy mely alkalmazásállapotokat jelentse a rendszer az ESET PROTECT On-Prem webkonzolnak.

Az ESET PROTECT CLOUD ismertetése

Az ESET PROTECT CLOUD lehetővé teszi, hogy egyetlen központi helyről felügyeljen ESET-termékeket munkaállomásokon és szervereken hálózati környezetben anélkül, hogy szükség lenne fizikai vagy virtuális szerverre, mint az ESET PROTECT On-Prem vagy ESET Security Management Center 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.

Az ESET PROTECT On-Prem ismertetése

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

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

Az ESET PROTECT On-Prem a következő összetevőkből áll:

- ESET PROTECT On-Prem Szerver – Az ESET PROTECT On-Prem Szerver Windows- és Linux-szerverekre is telepíthető, és virtuális eszközként is rendelkezésre áll. Kezeli az ügynökökkel folytatott kommunikációt, és összegyűjti és tárolja az alkalmazásadatokat az adatbázisban.

- ESET PROTECT On-Prem Webkonzol – Az ESET PROTECT On-Prem Webkonzol az elsődleges interfész, amely lehetővé teszi a kliensszámítógépek felügyeletét az adott környezetben. Megjeleníti a hálózaton lévő kliensek állapotát, és a segítségével ESET-megoldások telepíthetők távolról nem felügyelt számítógépekre. Az ESET PROTECT On-Prem Szerver telepítése után a webböngészőben érhető el a Webkonzol. Ha elérhetővé teszi a webszervert az interneten keresztül, akkor az ESET PROTECT On-Prem bárhonnan, illetve bármilyen készülékről használhatóvá válik, ha rendelkezésre áll internetkapcsolat.

- ESET Management Ügynök – Az ESET Management Ügynök megkönnyíti a kommunikációt az ESET PROTECT On-Prem Szerver és kliensszámítógépek között. Az Ügynököt telepíteni kell a kliensszámítógépre annak érdekében, hogy létrejöjjön a kommunikáció a számítógép és az ESET PROTECT On-Prem Szerver között. Mivel a kliensszámítógépen található, és több biztonsági forgatókönyvet tud tárolni, az ESET Management Ügynök használatakor sokkal gyorsabban lehet reagálni az új kártevőkre. Az ESET PROTECT On-Prem Webkonzol segítségével telepíthető az ESET Management Ügynök az Active Directory vagy az ESET RD-érzékelő által beazonosított felügyelet nélküli számítógépekre. Manuálisan is telepíthető az ESET Management Ügynök kliensszámítógépekre szükség esetén.

- Rogue Detection Sensor – A ESET PROTECT On-Prem Rogue Detection (RD) Sensor észleli a hálózaton lévő felügyelet nélküli számítógépeket, és elküldi az adataikat az ESET PROTECT On-Prem Szervernek. Ezáltal egyszerűen hozzáadhat új kliensszámítógépeket a biztonságos hálózatához. Az RD-érzékelő megjegyzi a beazonosított számítógépeket, így még egyszer nem küldi el ugyanazokat az információkat.

- ESET Bridge – Ez a szolgáltatás az ESET PROTECT On-Prem rendszerrel együtt használható a következőkhöz:

  - Frissítések küldése a kliensszámítógépekre és telepítőcsomagok továbbítása az ESET Management Ügynöknek.

  - Kommunikáció továbbítása az ESET Management Ügynököktől az ESET PROTECT On-Prem Szerverhez.

- Mobile Device Connector – Ez az összetevő lehetővé teszi az ESET PROTECT On-Prem rendszerrel együtt végzett mobileszköz-felügyeletet, így mobileszközöket (Android és iOS) felügyelhet, és kezelheti az ESET Endpoint Security for Android szolgáltatást.

- ESET PROTECT On-Prem Virtuális eszköz – Az ESET PROTECT On-Prem VE olyan felhasználóknak készült, akik az ESET PROTECT On-Prem rendszert virtualizált környezetben szeretnék futtatni.

- Tükrözési eszköz – A tükrözési eszközre az offline modulfrissítésekhez van szükség. Ha a kliensszámítógépek nem rendelkeznek internetkapcsolattal, a tükrözési eszköz segítségével tölthet le frissítési fájlokat az ESET frissítési szervereiről, és helyben tárolhatja őket.

- ESET Remote Deployment Tool – Ez az eszköz lehetővé teszi az ESET PROTECT On-Prem Webkonzolban létrehozott univerzális csomagok telepítését. Segítségével kényelmesen továbbítható az ESET Management Ügynök egy ESET-termékkel a hálózaton lévő számítógépekre.

- ESET Business Account – Az ESET üzleti termékek új licencelési portálja lehetővé teszi a licencek kezelését. Az ESET Business Account felhasználói útmutatójában kapcsolatos további információkat talál az ESET Business Account használatáról.

- ESET Enterprise Inspector – Ez egy átfogó észlelési és válaszadási rendszer, amely például a következő funkciókat tartalmazza: események észlelése, események felügyelete és reagálás, adatgyűjtés, fertőzésészlelési mutatók, anomáliák észlelése, viselkedésészlelés és házirendek megszegése.

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

További információkat az ESET PROTECT On-Prem online felhasználói útmutatójában talál.

Értesítések letiltása MDM-en keresztül

Az ESET Endpoint Antivirus for macOS-értesítések az ESET felügyeleti konzolon jelennek meg. Nem szükséges ESET Endpoint Antivirus for macOS-értesítéseket fogadnia, ha az ESET termékeit az ESET felügyeleti konzolon kezeli.

Az értesítéseket az MDM-en keresztül tilthatja le.

Konfigurációs profil létrehozásához töltse le a .plist adatcsomagfájlt.

A legtöbb MDM lehetővé teszi a .plist adatcsomag csatolását, vagy másolja át a fájl tartalmát a konfigurációs profilba.

Jamf-felhasználók

1. A Jamf főablakában kattintson a **Számítógépek** > **Konfigurációs profilok** elemre.

2. Az **Általános** részben töltse ki a következőket:

Beállítás	Érték
Név	Például ESET-értesítés
Szint	Számítógépes szint
Szétosztási módszer	Általában Telepítse automatikusan

3. Az **Értesítés** szakaszban kattintson a **Hozzáadás+** gombra, és töltse ki a következőket:

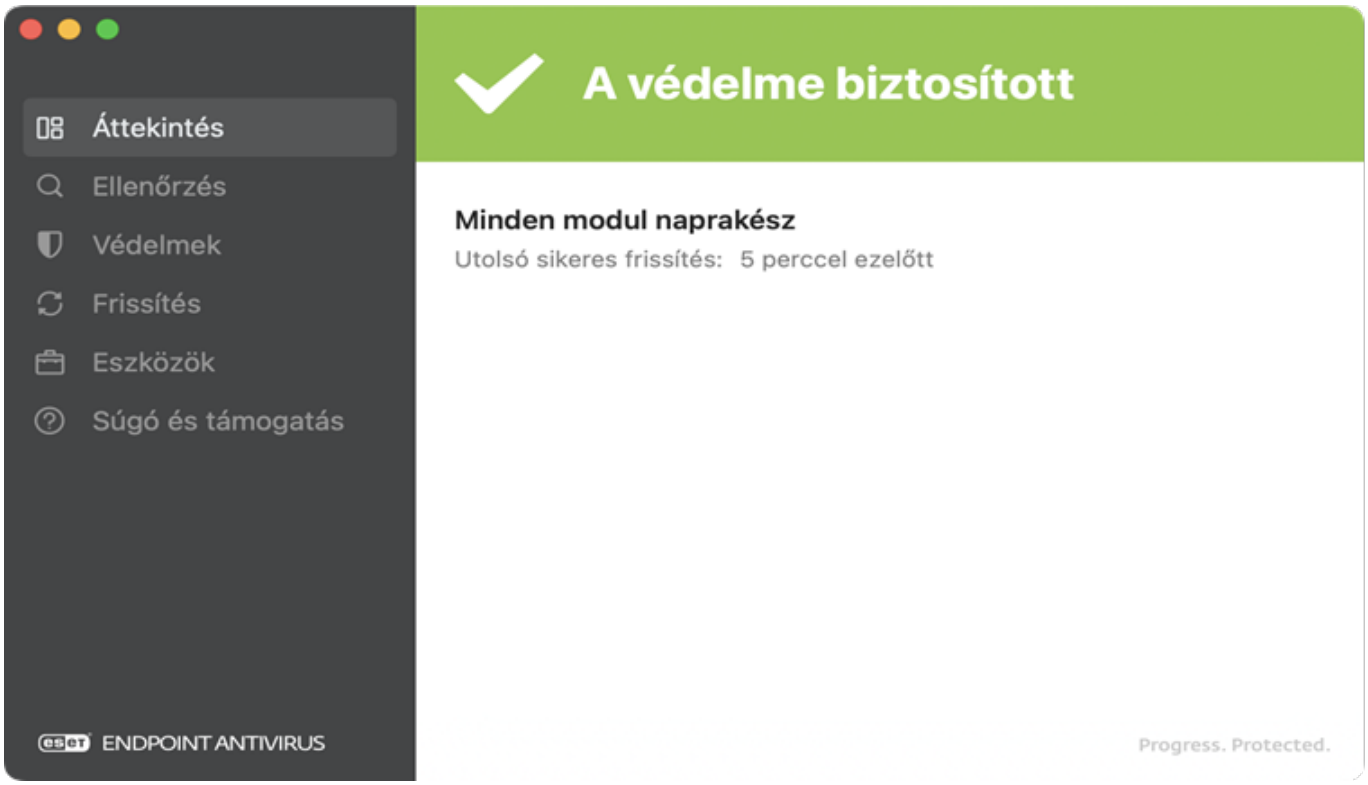
Beállítás	Érték
Alkalmazás neve	ESET Endpoint Antivirus for macOS

Beállítás	Érték
Csomagazonosító	com.eset.eea.agent
Kritikus riasztások	Letiltás
Értesítések	Letiltás

Az ESET Endpoint Antivirus for macOS használata

A program főablakának megnyitásához kattintson a macOS menüsávján látható ESET Endpoint Antivirus for macOS ikonra (a képernyő tetején), majd Az ESET Endpoint Antivirus for macOS megjelenítése gombra.

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



A főmenüben a következő lehetőségek állnak rendelkezésre:

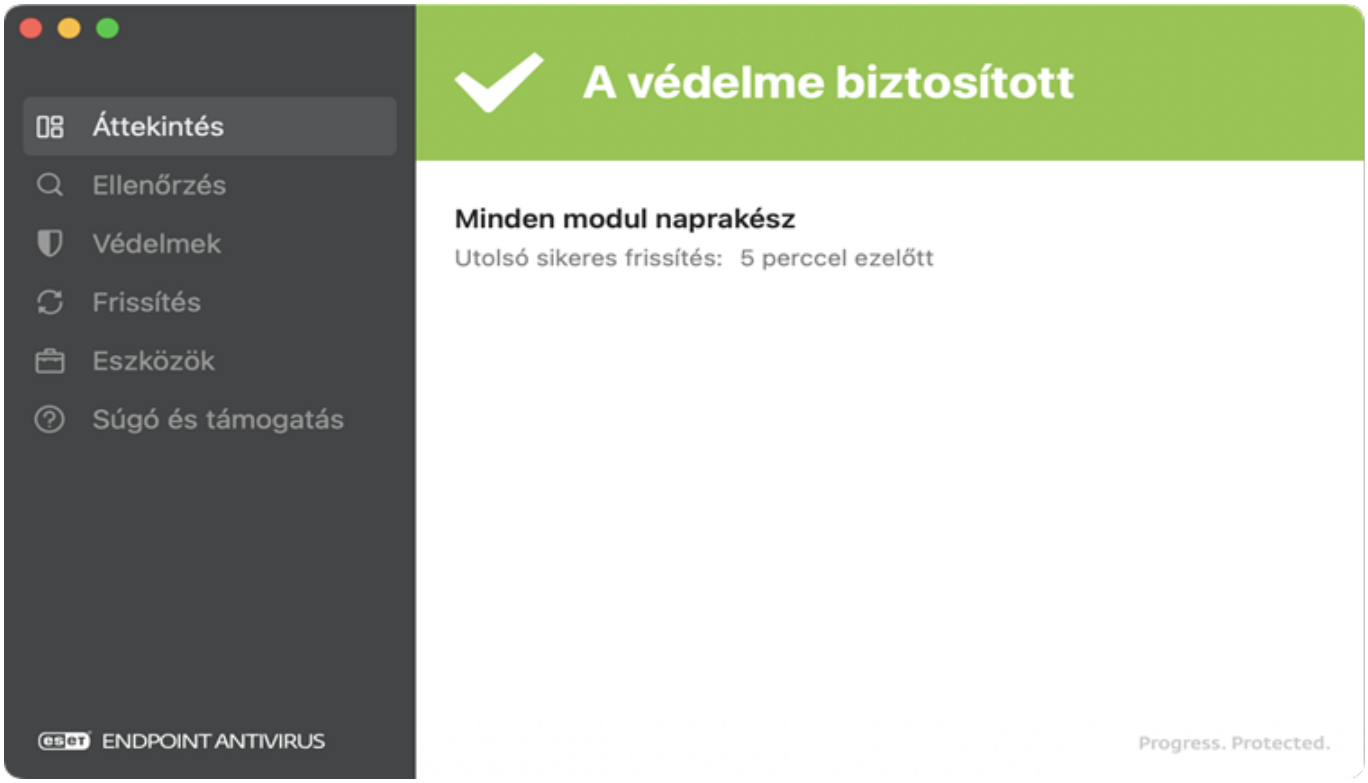
- Áttekintés
- Ellenőrzés
- Védelmek
- Frissítés
- Eszközök
- Súgó és támogatás

Az ESET Endpoint Antivirus for macOS speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint

Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget. Ha az ESET Endpoint Antivirus for macOS felügyelve van, az ESET Endpoint Antivirus for macOS beállításait az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD segítségével konfigurálhatja.

Áttekintés

A program főablakában kattintson az Áttekintés elemre a számítógép aktuális védelmi szintjére vonatkozó információk megtekintéséhez.



Az Áttekintés ablak az aktuális frissítési állapotot is megjeleníti, beleértve az utolsó sikeres frissítés dátumát és időpontját is.

Az ESET Endpoint Antivirus for macOS az alábbi védelmi állapotok egyikét jeleníti meg:

- A védelme biztosított zöld fejléccel – a lehető legmagasabb szintű védelem van biztosítva.
- Beavatkozás szükséges narancssárga fejléccel – az ESET Endpoint Antivirus for macOS beavatkozást igényel egy nem kritikus probléma miatt.
- Biztonsági riasztás piros fejléccel– kritikus probléma van jelen, és a maximális védelem nem biztosított

Ha a védelem állapota a Beavatkozás szükséges vagy a Biztonsági riasztás, akkor a védelmi állapot ablaka további információkat és javasolt megoldásokat tartalmazó értesítéseket jelenít meg.

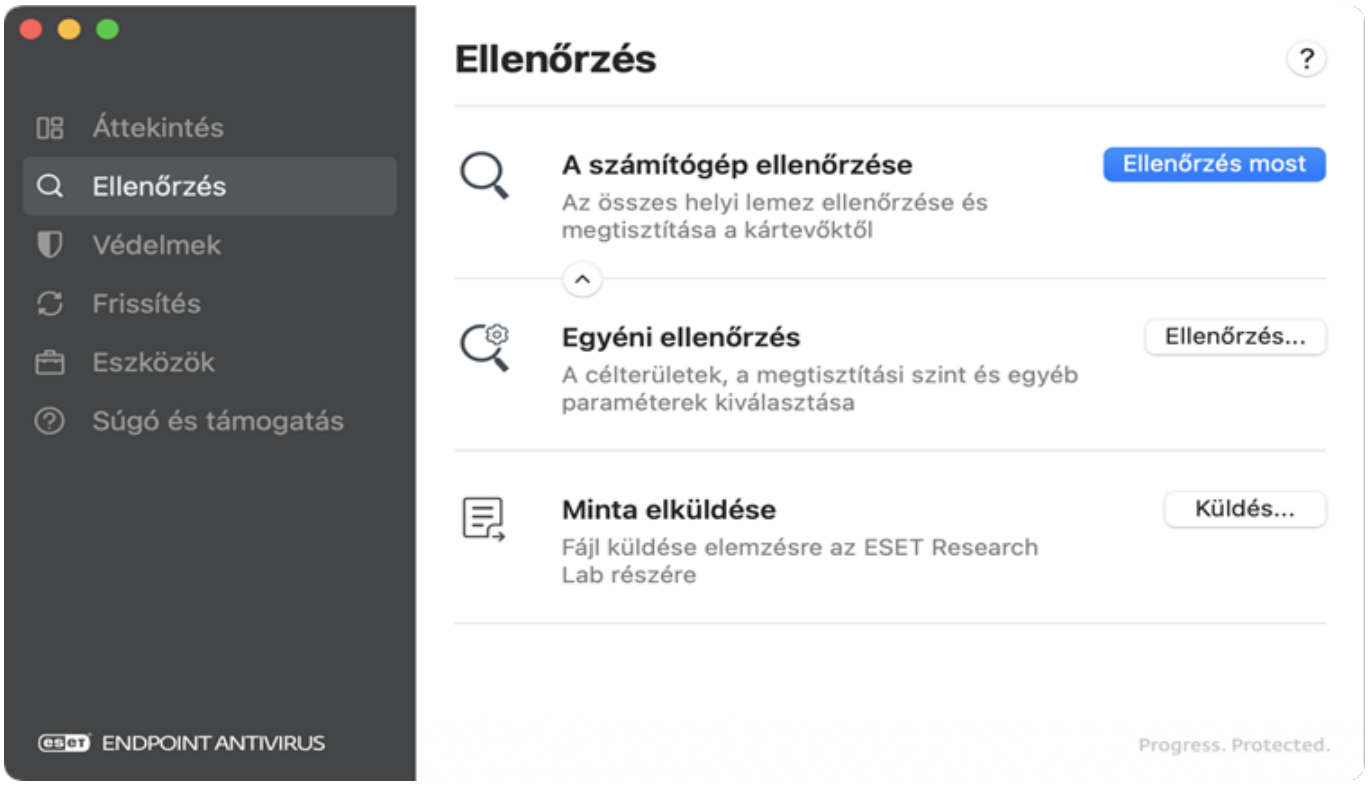
Ha a javasolt megoldásokkal nem szüntethető meg a probléma, az ESET tudásbázisában is megoldást kereshet rá. Ha további segítségre van szüksége, elküldhet egy támogatási kérelmet az ESET részére.

Ellenőrzés

Kattintson az **Ellenőrzés** gombra a program főablakában a számítógépes fájlok és mappák ellenőrzéséhez.

A kézi indítású víruskereső a vírus- és kémprogramvédelem fontos része, és a 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.

A rendszer alapos és rendszeres ellenőrzését javasoljuk a Valós idejű fájlrendszervédelem által nem észlelt vírusok kiszűrése céljából. Ilyen akkor történhet, ha a Valós idejű fájlrendszervédelem ki van kapcsolva az adott időben, a keresőmotor elavult, illetve a lemezre íráskor a program nem ismeri fel vírusként a fájlt.



A számítógép ellenőrzése

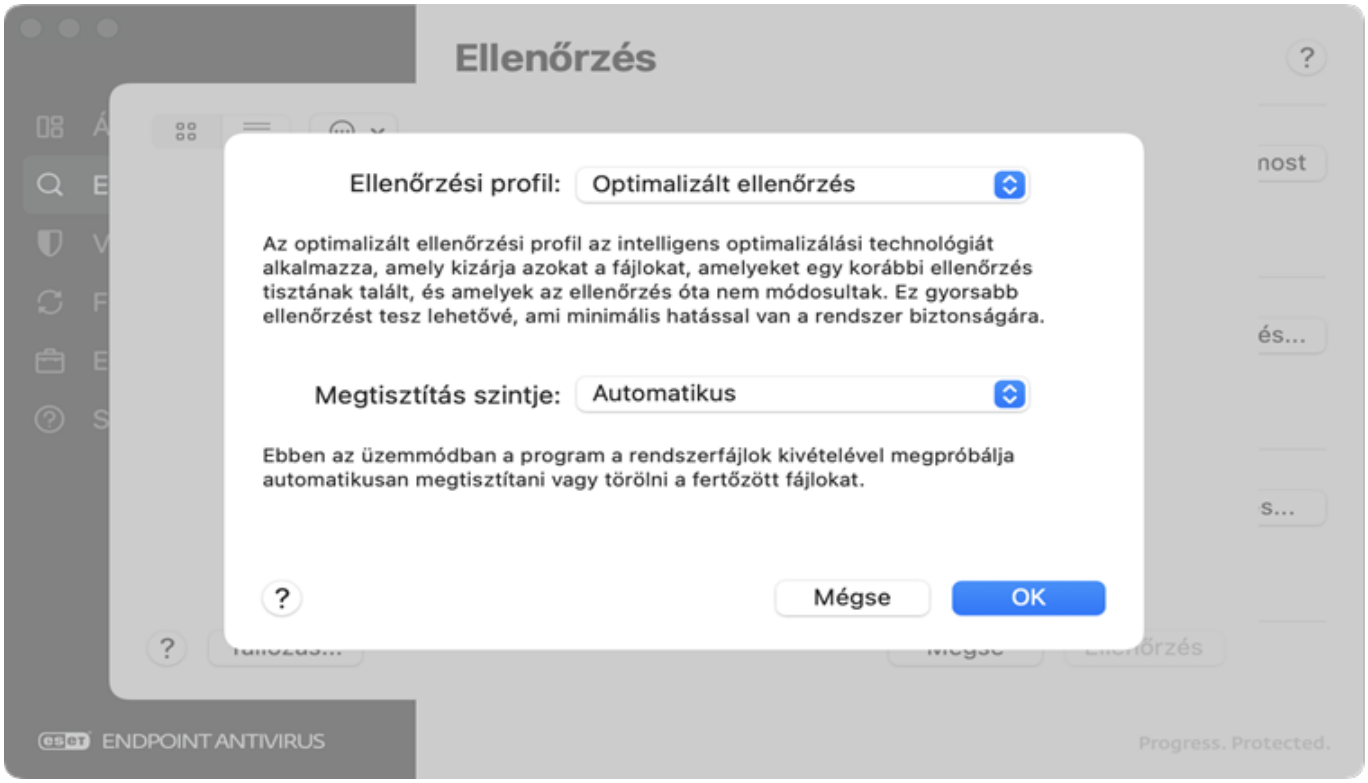
Az Ellenőrzés most gombra koppintva gyorsan elindíthatja a számítógép ellenőrzését, és felhasználói beavatkozás nélkül megtisztíthatja a fertőzött fájlokat. A számítógép ellenőrzése egyszerűen végrehajtható, és nincs szükség az ellenőrzési beállítások részletes megadására. Ez az ellenőrzés a helyi meghajtókon lévő összes fájlt ellenőrzi, és automatikusan megtisztítja vagy törli az észlelt fertőzéseket.

Kattintson a nyílikonra az **Egyéni ellenőrzés** és a **Minta elküldése** opció megjelenítéséhez.

Egyéni ellenőrzés

Kattintson az Ellenőrzés gombra az egyéni ellenőrzés ablakának megnyitásához.

Az Egyéni ellenőrzés lehetővé teszi az ellenőrzési paraméterek megadását, például az ellenőrzési célokat, az ellenőrzési profilt, a tisztítási szintet és a kivételeket.



Egyéni ellenőrzési célok hozzáadása:

- Húzza át manuálisan a fájlt vagy a mappát úgy, hogy a fájlra vagy mappára kattint, az egérmutatót a megjelölt területre viszi, miközben az egér gombját lenyomva tartja, majd felengedi az egér gombját.
- Kattintson a Tallózás gombra, majd válassza ki az ellenőrizni kívánt fájlokat vagy mappákat.

Kattintson a menüikonra ⋯ a speciális ellenőrzési lehetőségek megjelenítéséhez:

Ellenőrzési profil kiválasztása – válasszon Ellenőrzési profilt és Megtisztítási szintet az egyéni ellenőrzéshez.

> Szerkesztheti az ellenőrzési profilokat az ESET PROTECT On-Prem, az ESET PROTECT CLOUD vagy az alkalmazásbeállítások segítségével.

Kizárások beállítása – az ellenőrzésből kizárni kívánt fájlok vagy mappák hozzáadása.

A Terminalon keresztül az **odscan** segédprogram segítségével történő kézi indítású ellenőrzés futtatásáról a Kézi indítású ellenőrzés a Terminálon keresztül című témakörben olvashat.

Minta elküldése

Ez az opció lehetővé teszi, hogy kiválasszon egy gyanúsan viselkedő fájlt a számítógépén vagy egy gyanús internetes webhelyet, és elküldheti elemzésre az ESET kutatólaborjába.

Kattintson a **Küldés** gombra az elemzésre elküldeni kívánt fájl megadásához. Először válassza ki a beküldés okát, majd válassza ki a fájlt. Manuálisan áthúzhatja a fájlt vagy a mappát úgy, hogy a fájlra vagy mappára kattint, az egérmutatót a megjelölt területre viszi, miközben az egér gombját lenyomva tartja, majd felengedi az egér gombját. Lehetősége van az e-mail-címe megadására is, amely lehetővé teszi számunkra, hogy kapcsolatba lépjünk Önnel, ha további információra van szükségünk. Nem kell megadnia az e-mail-címét, ha engedélyezi az **Elküldés névtelenülkapcsolót.**

A beküldött mintának meg kell felelnie legalább egynek az alábbi feltételek közül:

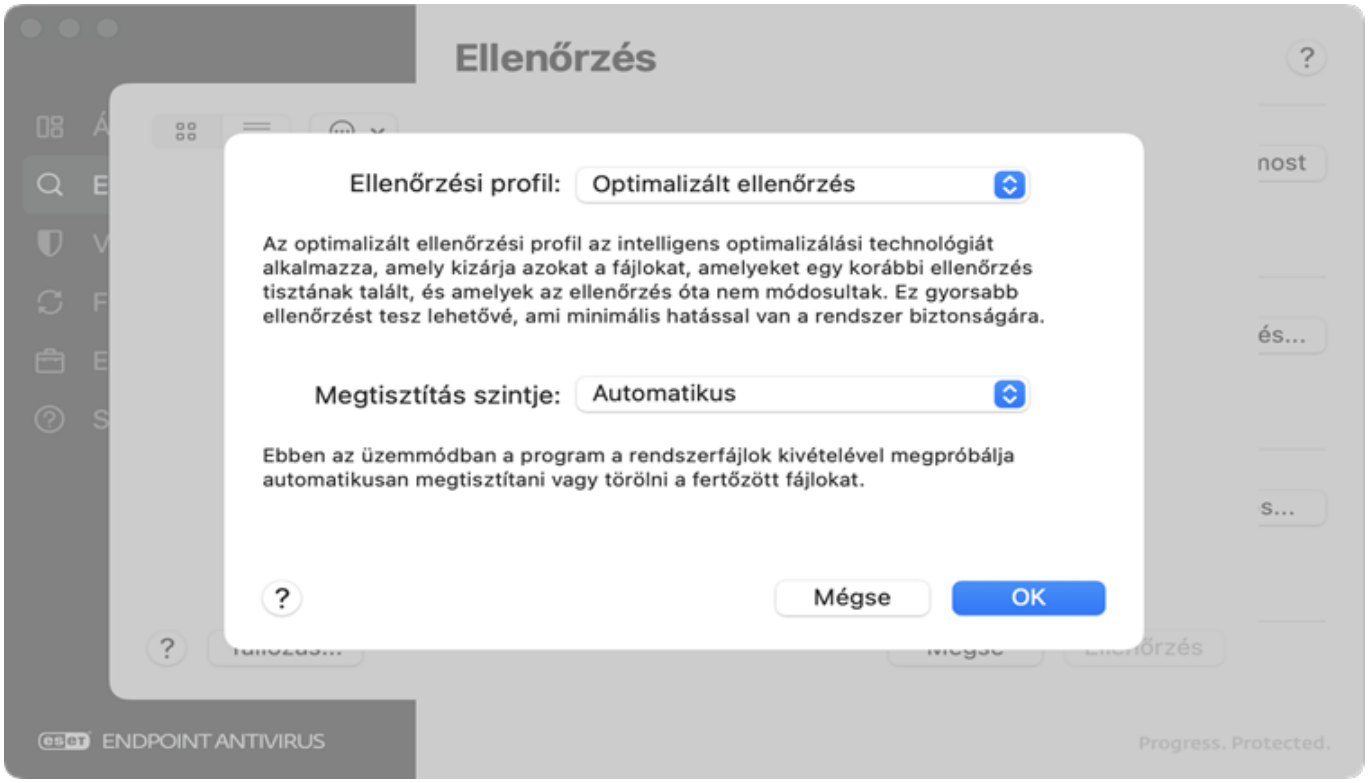
- Az Ön által használt ESET-termék nem észleli a mintát
- A program tévesen kártevőként észlelte a mintát

A **Tovább** gombra kattintva eljuthat az utolsó lépéshez, ahol további információkat adhat meg a mintafájlról, például a kártevő általi fertőzésre utaló jeleket vagy hibajelenségeket és a fájl eredetét. További információk megadásával elősegíti, hogy laboratóriumaink azonosítsák és feldolgozzák a mintákat.

> Az ESET nem fogad el személyes fájlokat (ha azt szeretné, hogy az ellenőrizze a kártevők jelenlétét bennük) mintaként. Az ESET kutatólaborja nem végez kézi indítású ellenőrzéseket a felhasználók számára.

Egyéni ellenőrzés

Az Egyéni ellenőrzés lehetővé teszi az ellenőrzési paraméterek megadását, például az ellenőrzési célokat, az ellenőrzési profilt, a tisztítási szintet és a kivételeket.



Egyéni ellenőrzési célok hozzáadása:

- Húzza át manuálisan a fájlt vagy a mappát úgy, hogy a fájlra vagy mappára kattint, az egérmutatót a megjelölt területre viszi, miközben az egér gombját lenyomva tartja, majd felengedi az egér gombját.
- Kattintson a Tallózás gombra, majd válassza ki az ellenőrizni kívánt fájlokat vagy mappákat.

Kattintson a menüikonra a speciális ellenőrzési lehetőségek megjelenítéséhez:

Ellenőrzési profil kiválasztása – válasszon Ellenőrzési profilt és Megtisztítási szintet az egyéni ellenőrzéshez.

> Szerkesztheti az ellenőrzési profilokat az ESET PROTECT On-Prem, az ESET PROTECT CLOUD vagy az alkalmazásbeállítások segítségével.

Kizárások beállítása – az ellenőrzésből kizárni kívánt fájlok vagy mappák hozzáadása.

Minta elküldése

Az alkalmazás főablakának bal oldali menüjében válassza ki az **Ellenőrzés** elemet, kattintson a nyíl ikonra a **Minta elküldése** opció megjelenítéséhez.

Ez az opció lehetővé teszi, hogy kiválasszon egy gyanúsan viselkedő fájlt a számítógépén vagy egy gyanús internetes webhelyet, és elküldheti elemzésre az ESET kutatólaborjába.

Kattintson a **Küldés** gombra az elemzésre elküldeni kívánt fájl megadásához. Először válassza ki a beküldés okát, majd válassza ki a fájlt. Manuálisan áthúzhatja a fájlt vagy a mappát úgy, hogy a fájlra vagy mappára kattint, az egérmutatót a megjelölt területre viszi, miközben az egér gombját lenyomva tartja, majd felengedi az egér gombját. Lehetősége van az e-mail-címe megadására is, amely lehetővé teszi számunkra, hogy kapcsolatba lépjünk Önnel, ha további információra van szükségünk. Nem kell megadnia az e-mail-címét, ha engedélyezi az **Elküldés névtelenül** kapcsolót.

A beküldött mintának meg kell felelnie legalább egynek az alábbi feltételek közül:

- Az Ön által használt ESET-termék nem észleli a mintát
- A program tévesen kártevőként észlelte a mintát

A **Tovább** gombra kattintva eljuthat az utolsó lépéshez, ahol további információkat adhat meg a mintafájlról, például a kártevő általi fertőzésre utaló jeleket vagy hibajelenségeket és a fájl eredetét. További információk megadásával elősegíti, hogy laboratóriumaink azonosítsák és feldolgozzák a mintákat.

> Az ESET nem fogad el személyes fájlokat (ha azt szeretné, hogy az ellenőrizze a kártevők jelenlétét bennük) mintaként. Az ESET kutatólaborja nem végez kézi indítású ellenőrzéseket a felhasználók számára.

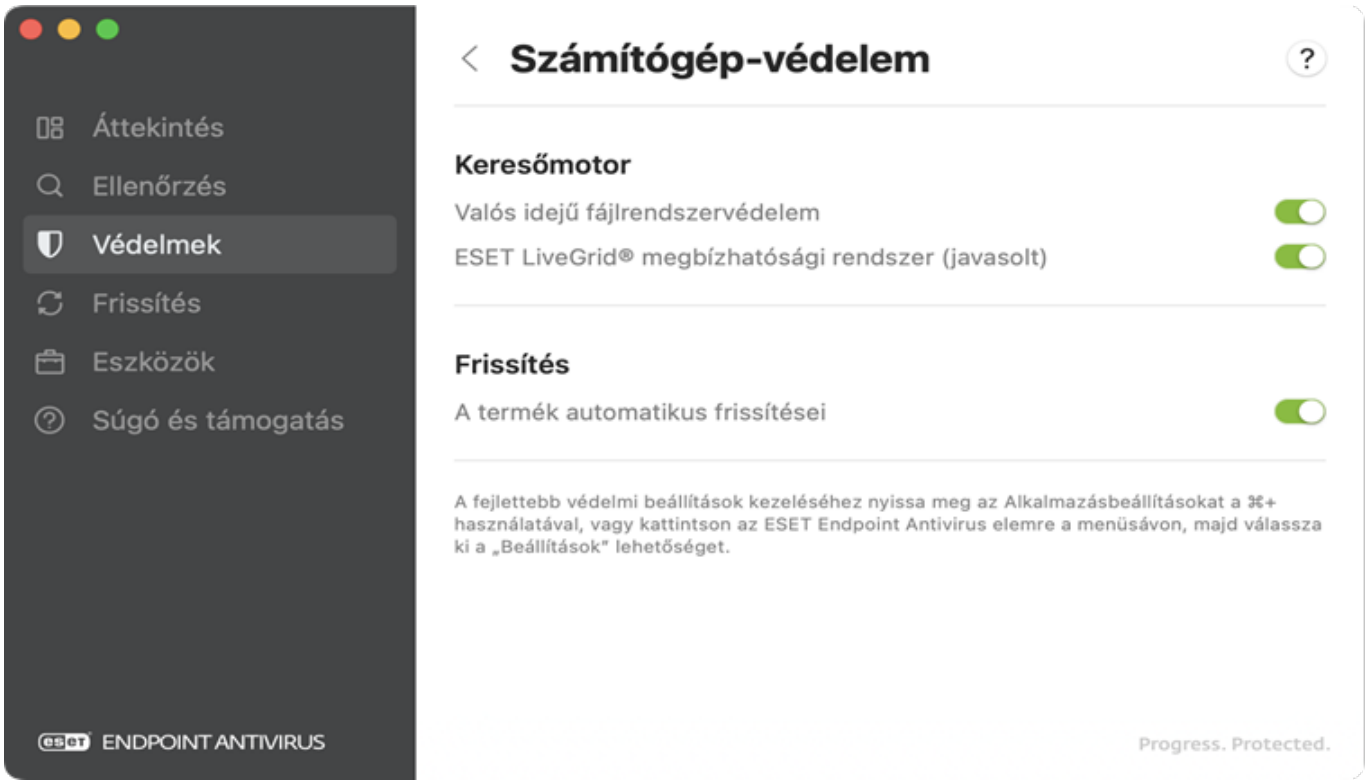
Védelmek

Módosíthatja a számítógép, valamint az internet és az e-mailek védelmi szintjét az alkalmazás főablakában található **Védelmek** opció segítségével. Mind a Számítógép-védelem, mind a Web- és e-mail-védelem szakasz védelmi modulokat tartalmaz, amelyek engedélyezhetők vagy letilthatók. Azt javasoljuk, hogy az összes modult engedélyezze, hogy teljes mértékben kiaknázhassa az ESET Endpoint Antivirus for macOS funkcióit és

biztonságban legyen a számítógépe.

Számítógép

A számítógép védelmi konfigurációja a **Védelmek** > **Számítógép** szakaszban található. Ez az ablak a **Valós idejű fájlrendszervédelem** és az **ESET LiveGrid© megbízhatósági rendszer** modul állapotát jelzi. Azt javasoljuk, hogy mindkét modult engedélyezze, mivel bármelyik kikapcsolása csökkentheti a számítógép védelmi szintjét.



A kapcsolóra kattintva engedélyezheti vagy letilthatja az **Automatikus frissítés** funkciót a **Frissítés** szakaszban. Ha az Automatikus frissítés engedélyezve van, az ESET Endpoint Antivirus for macOS megkeresi a legújabb termékfrissítéseket, és automatikusan letölti őket.

Web és e-mail

A webhozzáférés- és e-mail védelem eléréséhez a főmenüben kattintson a **Védelmek** > **Web és e-mail** elemre. Az egyes modulok fejlettebb beállításainak kezeléséhez nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombinációval vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget. A Web- és e-mail-védelemben a következő védelmi modulok érhetők el:

- **Web** – A böngészők és a távoli szerverek közötti kommunikáció figyelése.
- **Adathalászat elleni védelem** – A webhelyekről és tartományokból származó minden potenciális adathalászati támadást letilt.
- **E-mail** – A POP3 és az IMAP protokollon keresztül érkező e-mailes kommunikáció szabályozását biztosítja.

Frissítés

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

Az ESET Endpoint Antivirus for macOS rendszeres frissítésével biztosítható a leghatékonyabban a számítógép maximális védelmi szintje. Az automatikus frissítések biztosítják, hogy a programmodulok és a rendszerösszetevők mindig naprakészek legyenek. Az automatikus frissítések mellett a Frissítések keresése hivatkozásra koppintva kézzel is elindíthat egy frissítést. Ha rendelkezésre áll egy termékfrissítés, megjelennek az aktuális és az elérhető verzió adatai, valamint a frissítés mérete és kiadási dátuma. A termékfrissítés folytatásához el kell fogadnia a **végfelhasználói licencszerződést**, és jóvá kell hagynia az **adatvédelmi irányelveket** – választhat az **Elfogadás és frissítés most** és az **Elfogadás és frissítés újraindításkor** műveletek közül. Az egyes termékverziókkal kapcsolatos további részletek megtekintéséhez kattintson a **Változásnapló megtekintése** hivatkozásra.

Utolsó sikeres frissítés – Itt látható a legutóbbi sikeres frissítés dátuma. Ha nem látható friss dátum, lehetséges, hogy a termékmodulok elavultak.

Frissítések legutóbbi keresése – Itt látható a legutóbbi sikeres frissítéskeresés dátuma.

Az ESET Endpoint Antivirus for macOS speciális **frissítési** beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget. Ha az ESET Endpoint Antivirus for macOS felügyelve van, konfigurálhatja a speciális frissítési beállításokat távolról is az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD segítségével.

A következő témakörből megtudhatja, hogyan frissíthetők a keresőmodulok a Terminalon keresztül az **upd** segédprogram segítségével: Az észlelő modulok frissítése a Terminalon keresztül.

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**
- **Karantén**

Naplófájlok

A Naplófájlok lap a fontos programeseményekről tájékoztatást, az észlelt kártevőkről áttekintést nyújt. A naplózás elengedhetetlen a rendszerelemzéshez, a kártevők észleléséhez és a hibaelhárításhoz. A naplózás a háttérben folyik aktívan, felhasználói beavatkozás nélkül. Az információkat az aktuális naplórészletességi beállításoknak megfelelően rögzíti. A szöveges üzenetek és a naplófájlok közvetlenül az ESET Endpoint Antivirus for macOS-programkörnyezetből is megtekinthetők, és a naplófájlok is archiválhatók.

A naplófájlok az ESET Endpoint Antivirus for macOS főmenüjéből érhetők el az **Eszközök** > **Naplófájlok** lehetőséget választva. Jelölje ki a kívánt naplótípust az ablak jobb felső részén található legördülő listában. A választható naplók az alábbiak:

- **Észlelések** – A fertőzések észlelésével kapcsolatos eseményekre vonatkozó információk.

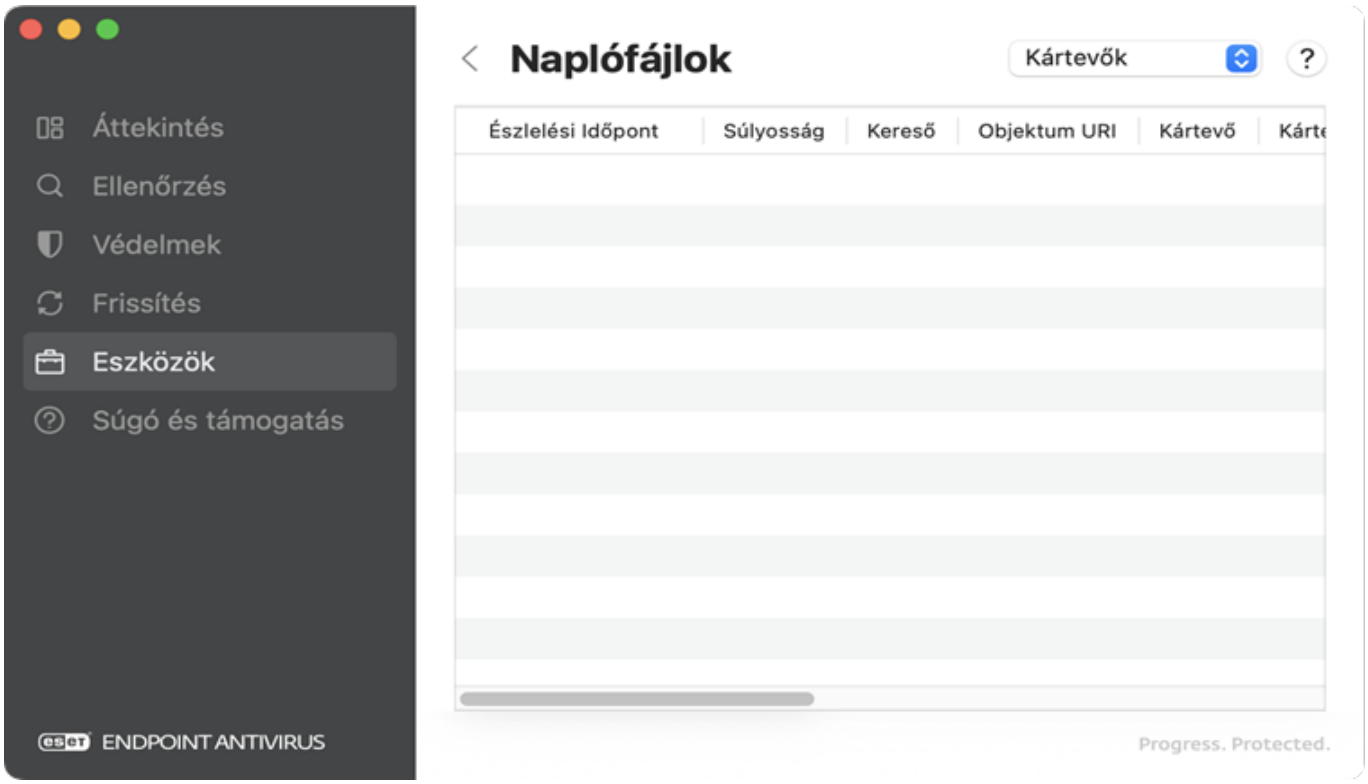
- **Számítógép ellenőrzése** – Az összes befejezett ellenőrzés eredményének megjelenítése. Az egyes bejegyzésekre duplán kattintva megjelennek az adott kézi indítású számítógép-ellenőrzés részletes adatai.

- **Események** – A rendszergazdáknak és a felhasználóknak nyújt segítséget az esetleges problémák megoldásához. A program az ESET Endpoint Antivirus for macOS által végrehajtott összes fontos műveletet rögzíti az eseménynaplókban.

- **Letiltott fájlok** – Az ellenőrzés során blokkolt fájlok rekordjait tartalmazza az ESET Inspect által konfigurált letiltott fájlok (letiltott kivonatok) listája alapján.

- **Szűrt webhelyek** – A Webhozzáférés-védelem által letiltott webhelyek listája. . Ezekben a naplókban látható az idő, az URL-cím, az állapot, az IP-cím, a felhasználó és az adott webhely felé kapcsolatot megnyitó alkalmazás.

- **Elküldött fájlok** – Az elemzésre elküldött minták rekordjait tartalmazza.

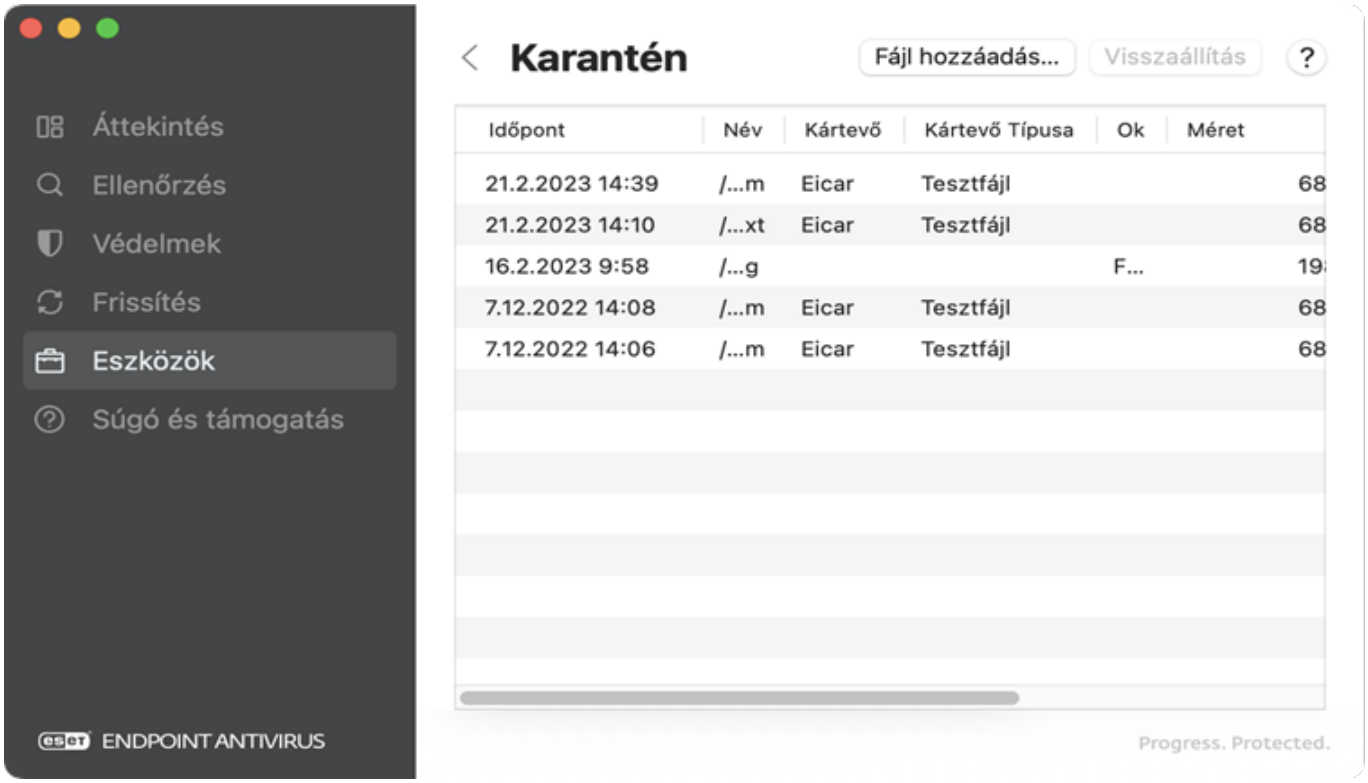


Karantén

A karantén biztonságosan tárolja a fertőzött fájlokat. A fájlokat akkor kell a karanténba helyezni, ha nem tisztíthatók meg, ha a törlésük kockázattal jár vagy nem ajánlott, illetve ha az ESET Endpoint Antivirus for macOS tévesen észlelte őket.

A karanténmappában lévő fájlokat egy táblázatban láthatja, amely jelzi a karanténba helyezés dátumát és időpontját, a fertőzött fájl eredeti helyének elérési útját, a fájl bájtban megadott méretet, a karanténba helyezés okát (például a felhasználó vette fel) és a fertőzések számát (például azt, hogy egy több fertőzést is hordozó tömörített fájlról van-e szó). A karanténba helyezett fájlokat tartalmazó karanténmappa (*/Library/Application Support/Eset/Security/Cache/Quarantine*) az ESET Endpoint Antivirus for macOS eltávolítása után is a rendszerben marad. A karanténba helyezett fájlok tárolása biztonságos titkosított formában történik, és az ESET

Endpoint Antivirus for macOS telepítése után ismét visszaállíthatók.



Karantén fájlok

Az ESET Endpoint Antivirus for macOS automatikusan karanténba helyezi a törölt fájlokat (ha nem tiltotta le ezt a beállítást a riasztási ablakban). Kattintson a **Fájl hozzáadása** gombra a gyanús fájlok manuális karanténba helyezéséhez. Át is húzhatja a fájlt vagy a mappát úgy, hogy a fájlra vagy mappára kattint, az egérmutatót a megjelölt területre viszi, miközben az egér gombját lenyomva tartja, majd felengedi az egér gombját.

Visszaállítja a karanténból

Jelölje ki a karanténba helyezett fájlt, majd kattintson a **Visszaállítás** gombra az eredeti helyére történő visszaállításához. Ez a funkció úgy is elérhető, hogy a Control billentyűt lenyomva tartva kattint (vagy a jobb gombbal kattint) egy adott fájlra a **Karantén** ablakban, majd a **Visszaállítás** elemre kattint. A helyi menüben megtalálható a **Visszaállítás megadott helyre** menüpont is, amellyel a törlés helyétől eltérő mappába is visszaállíthatók a fájlok.

Fájl elküldése a karanténból

Ha karanténba helyezett egy, a program által nem észlelt gyanús fájlt, vagy ha a szoftver tévesen jelölt meg fertőzöttként (például a kód heurisztikus elemzésével), majd helyezett a karanténba egy fájlt, kérjük, küldje el azt az ESET víruslaborjába. A karanténban lévő fájl elküldéséhez a Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) a fájlra, majd válassza ki a **Minta elküldése** menüpontra a helyi menüben. A mintafájl beküldésével kapcsolatos további részletekért tekintse meg a Minta elküldése című részt.

Súgó és támogatás

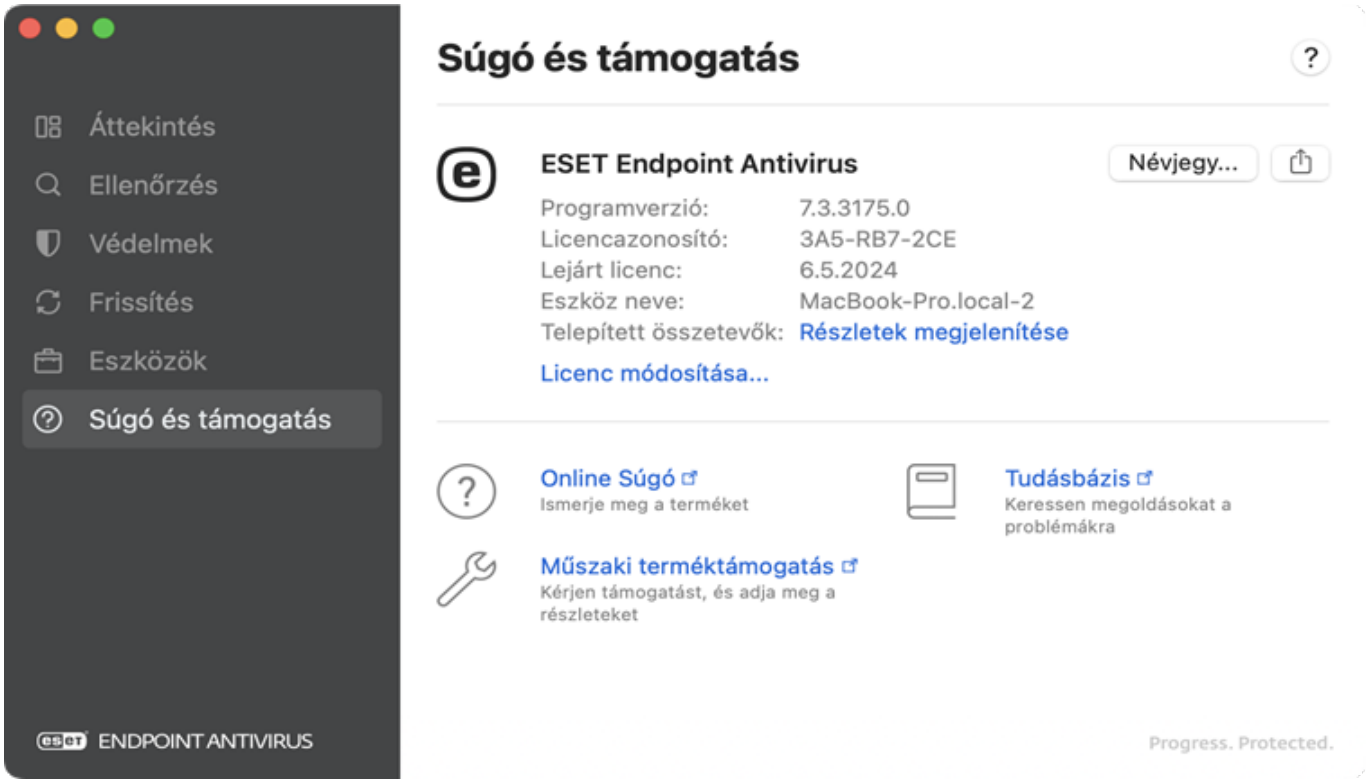
Az ESET Endpoint Antivirus for macOS súgója hibaelhárítási eszközöket és támogatási információkat tartalmaz, amelyek segítséget nyújtanak a felmerülő problémák megoldásában. A Súgó és támogatás szakasz az alkalmazás fő ablakában található. A telepített összetevők listájának megjelenítéséhez kattintson a **Részletek megjelenítése** elemre a **Telepített összetevők** szöveg mellett. **Az összes másolása** elemre koppintva a vágólapra másolhatja a listát. Ez a hibakereséshez, illetve a terméktámogatási szolgálattal folytatott kommunikáció során lehet hasznos.

Az **ESET Endpoint Antivirus for macOS** termékverziója és a terméklicenc azonosítója látható. Lehetőség van a licenc módosítására is: kattintson erre az opcióra az aktiválási ablak elindításához és a termék aktiválásához. A Névjegy gombra kattintva további részleteket tekinthet meg az ESET Endpoint Antivirus for macOS szolgáltatásról.

Súgóoldal – Kattintson erre a hivatkozásra az ESET Endpoint Antivirus for macOS súgójának megnyitásához.

Műszaki terméktámogatás – Vegye fel a kapcsolatot az ESET műszaki terméktámogatással, ha nem tudja megoldani az adott problémát a súgóoldalaink segítségével.

Tudásbázis – Látogasson el az ESET tudásbázisába, ahol válaszokat találhat a gyakran feltett kérdésekre és számos problémára megoldást kaphat. Az ESET műszaki szakemberei által rendszeresen frissített tudásbázis a különböző problémák megoldásának leghatékonyabb eszköze.



Terminal-segédprogramok és démonok

Parancssori segédprogramok

- ./Islog – Naplólistázási segédprogram, amely az ESET Endpoint Antivirus for macOS által gyűjtött naplók megjelenítésére használható

• ./odscan – Kézi indítású víruskereső, amellyel kézi indítású víruskeresést futtathat a Terminal-ablakon keresztül.

• ./cfg – Az ESET Endpoint Antivirus for macOS beállításainak importálására/exportálására használható konfigurációs segédprogram.

• ./mdm-info – mdm információs segédprogram, amely megjeleníti azokat az információkat, amelyekkel létrehozhatja azokat a konfigurációs profilokat, amelyek szükségesek a telepítés előtti beállítás MDM-en keresztüli elvégzéséhez.

• ./lic – Licencelési segédprogram, amellyel az ESET Endpoint Antivirus for macOS aktiválható a megvásárolt licenckulccsal, illetve amellyel az aktiválási állapot és a licenc érvényessége ellenőrizhető.

• ./upd – Modulfrissítési segédprogram, amely a modulfrissítések kezelésére vagy a frissítési beállítások módosítására használható.

• ./quar – Karanténkezelő segédprogram, amely a karanténba helyezett elemek kezelésére használható.

Karantén

A karantén biztonságosan tárolja a fertőzött fájlokat. A fájlokat akkor kell a karanténba helyezni, ha nem tisztíthatók meg, ha törlésük kockázattal jár vagy nem ajánlott, illetve ha az ESET Endpoint Antivirus for macOS tévesen észlelte őket. Bármilyen fájlt karanténba helyezhet, ami akkor javasolt, ha egy fájl viselkedése gyanús, a víruskereső azonban nem észleli. A karanténba helyezett fájlokat elküldheti az ESET víruslaborjába elemzés céljából.

A karanténba helyezett elemek kezelése a Terminalon keresztül

Szintaxis: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar [OPTIONS]`

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
-i	--import	Fájl importálása a karanténba
-l	--list	A karanténban lévő fájlok listájának megjelenítése
-r	--restore=id	Az id által azonosított, karanténba helyezett elem visszaállítása a --restore-path által meghatározott útvonalra
-e	--restore-exclude=id	Az id által azonosított és a kizárható oszlopban „x” jelöléssel ellátott, karanténba helyezett elem visszaállítása
-d	--delete=id	Az id által azonosított, karanténba helyezett elem törlése
	--restore-path=path	Új elérési út, amelybe visszaállítható a karanténba helyezett elem
-h	--help	Súgó megjelenítése
-v	--version	Verzióadatok megjelenítése és kilépés

Visszaállítás
A visszaállítás nem érhető el, ha a parancs nem jogosult felhasználóként hajtják végre.

Példa

A „0123456789" azonosítójú, karanténba helyezett elem törlése:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -d 0123456789
```

vagy

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --delete=0123456789
```

A „9876543210" azonosítójú, karanténba helyezett elem visszaállítása a bejelentkezett felhasználó *Download* mappájába és átnevezése *restoredFile.test* névre:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -r 9876543210 --
restore-path=/Users/$USER/Desktop/restoredFile.test
```

vagy

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --
restore=9876543210 --restore-path=/Users/$USER/Desktop/restoredFile.test
```

A „9876543210" azonosítójú, a **kizárható** oszlopban „**x**” jelzésű karanténba helyezett elem visszaállítása a *Download* mappába:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -e 9876543210 --
restore-path=/Users/$USER/Downloads/restoredFile.test
```

vagy

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --restore-
exclude=9876543210 --restore-path=/Users/$USER/Downloads/restoredFile.test
```

Fájl visszaállítása a karanténból a Terminalon keresztül

1. A karanténba helyezett elemek felsorolása.
```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -l
```

2. Keresse meg a visszaállítani kívánt, karanténba helyezett objektum azonosítóját és nevét, majd futtassa a következő parancsot:
```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --
restore=ID_OF_OBJECT_TO_RESTORE --restore-
```

Konfiguráció

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/cfg --export-xml=/tmp/export.xml
```

Konfiguráció importálása

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/cfg --import-xml=/tmp/export.xml
```

Rendelkezésre álló beállítások

Rövid formátum	Hosszú formátum	Leírás
	--import-xml	beállítások importálása
	--export-xml	beállítások exportálása
-h	--help	súgó megjelenítése
-v	--version	verzióadatok megjelenítése

Események

Az ESET Endpoint Antivirus for macOS webes felületén végrehajtott fontos műveletek, sikertelen bejelentkezési kísérletek a webes felületre, a Terminálon keresztül végrehajtott ESET Endpoint Antivirus for macOS-parancsok és néhány további információ kerül naplózásra az **Események** képernyőn.

Minden rögzített művelet a következő információkat tartalmazza: az esemény bekövetkezésének időpontja, összetevő (ha rendelkezésre áll), esemény, felhasználó

Események megjelenítése a Terminalon keresztül

Az **Események** képernyő tartalmának Terminal-ablakon keresztüli megjelenítéséhez használja az `lslog` parancssori eszközt.

Szintaxis: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog [OPTIONS]`

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
-f	--follow	Várakozás új naplókra és hozzáfűzésük az eredményhez
-o	--optimize	Naplók optimalizálása.
-c	--csv	Naplók megjelenítése CSV formátumban
-e	--events	Eseménynaplók listázása
-u	--urls	URL-naplórekordok listázása
-n	--sent-files	Az elemzésre beküldött fájlok listájának megjelenítése
-s	--scans	Kézi indítású ellenőrzéseket tartalmazó naplók listázása.
	--with-log-name	A Naplónév oszlop megjelenítése kiegészítésképpen

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
	--ods-details=log-name	Kézi indítású ellenőrzés részleteinek megjelenítése naplónév szerint
	--ods-events=log-name	Az adott kézi indítású ellenőrzés során nem ellenőrzött kártevők és fájlok nyomtatása naplónév szerint.
	--ods-detections=log-name	Kézi indítású ellenőrzés során észlelt elemek megjelenítése naplónév szerint
	--ods-notscanned=log-name	Kézi indítású ellenőrzés nem ellenőrzött elemeinek megjelenítése naplónév szerint
-d	--detections	Észlelési naplóbejegyzések listázása
-b	--blocked files	Blokkolt fájlok naplójának listázása

Példák

Az összes eseménynapló megjelenítése:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog -e
```

Az összes eseménynapló mentése CSV formátumú fájlba az aktuális felhasználó *Dokumentumok* könyvtárába:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog -
ec > /Users/$USER/Desktop/eventlogs.csv
```

Az észlelő modulok frissítése a Terminalon keresztül

Modulok frissítése a Terminalon keresztül

Az összes termékmodul Terminal-ablakból történő frissítéséhez hajtsa végre a következő parancsot:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd -u
```

Frissítés és visszaállítás a Terminal segítségével

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
-u	--update	Modulok frissítése
-c	--cancel	Modulok letöltésének megszakítása
-e	--resume	Frissítések feloldása
-r	--rollback=VALUE	A víruskereső modul visszaállítása a legkorábbi pillanatképre, és az összes frissítés letiltása ÉRTÉK órára.
-l	--list-modules	A termékmodulok listájának megjelenítése
	--check-app-update	Az új termékverzió elérhetőségének ellenőrzése az adattárban

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
	--download-app-update	Új termékverzió letöltése, ha elérhető
	--perform-app-update	Új termékverzió letöltése és telepítése, ha elérhető
	--accept-license	Licencmódosítások elfogadása

upd korlátozás
Az upd segédprogram nem használható a termékkonfiguráció módosítására.

A frissítések 48 órára történő leállításához és a víruskereső modul legrégebbi pillanatképének visszaállításához hajtsa végre a következő parancsot jogosult felhasználóként:
```
sudo /opt/eset/efs/bin/upd --rollback=48
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```
A víruskereső modul automatikus frissítésének folytatásához hajtsa végre a következő parancsot jogosult felhasználóként:
```
sudo /opt/eset/efs/bin/upd --resume
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```
A „192.168.1.2” IP-címen és a „2221-es” porton elérhető tükörszerverről történő frissítéshez hajtsa végre a következő parancsot jogosult felhasználóként:
```
sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```

Kézi indítású ellenőrzés a Terminálon keresztül

Szintaxis: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan [OPTIONS..]`

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
-l	--list	A jelenleg futó ellenőrzések megjelenítése
	--list-profiles	Az összes rendelkezésre álló ellenőrzési profil megjelenítése
	--all	A más felhasználók által végrehajtott ellenőrzések megjelenítése is (gyökérjogosultság szükséges hozzá)
-r	--resume=session_id	A korábban szüneteltetett ellenőrzés folytatása session_id szerint
-p	--pause=session_id	Ellenőrzés szüneteltetése session_id szerint
-t	--stop=session_id	Az ellenőrzése leállítása session_id szerint
-s	--scan	Start scan
	--show-scan-info	Alapvető információk megjelenítése (log_name is) az elindított ellenőrzésről
	--profile=PROFILE	Ellenőrzés a kijelölt PROFIL-lal
	--profile-priority=PRIORITÁS	A feladat a megadott prioritással fog futni. A prioritás lehet: normál, alacsonyabb, legalacsonyabb, tétlen
	--readonly	Csak ellenőrzés megtisztítás nélkül
	--local	Helyi meghajtók ellenőrzése
	--network	Hálózati meghajtók ellenőrzése
	--removable	Cserélhető adathordozók ellenőrzése

Beállítások – rövid formátum	Beállítások – hosszú formátum	Leírás
	--exclude=FILE	Kijelölt fájl vagy könyvtár kihagyása
	--ignore-exclusions	A kizárt útvonalak és bővítmények ellenőrzése is

Az `odscan` segédprogram a befejezett ellenőrzés után kilépési kóddal végződik. Futtassa az `echo $?` parancsot a Terminal-ablakban a befejezett ellenőrzés után a kilépési kód megjelenítéséhez.

Kilépési kódok

Kilépés kód	Jelentés
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

Példa

A */root/* könyvtár kézi indítású ellenőrzésének ismétlődő futtatása a „@Smart scan” ellenőrzési profillal háttérfolyamatként:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@Smart scan" / &
```

Kézi indítású ellenőrzés ismétlődő futtatása a „@Smart scan” ellenőrzési profillal több célállomásra vonatkozólag:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@Smart scan" /Application/ /tmp/ /home/
```

Az összes futó ellenőrzés listázása

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -l
```

Az ellenőrzés szüneteltetése a „15-ös” munkamenet-azonosítóval. Minden ellenőrzésnek megvan a maga egyedi munkamenet-azonosítója, amely az indításkor jön létre.

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -p 15
```

Az ellenőrzés leállítása a „15-ös” munkamenet-azonosítóval. Minden ellenőrzésnek megvan a maga egyedi munkamenet-azonosítója, amely az indításkor jön létre.

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -t 15
```

Kézi indítású ellenőrzés futtatása kizárt könyvtárral (*/exc_dir*) és kizárt fájllal (*/eicar.com*):

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@In-depth scan" --exclude=/exc_dir/ --exclude=/eicar.com /
```

Cserélhető eszközök rendszerindító szektorainak ellenőrzése. Futtassa az alábbi parancsot jogosult felhasználóként.

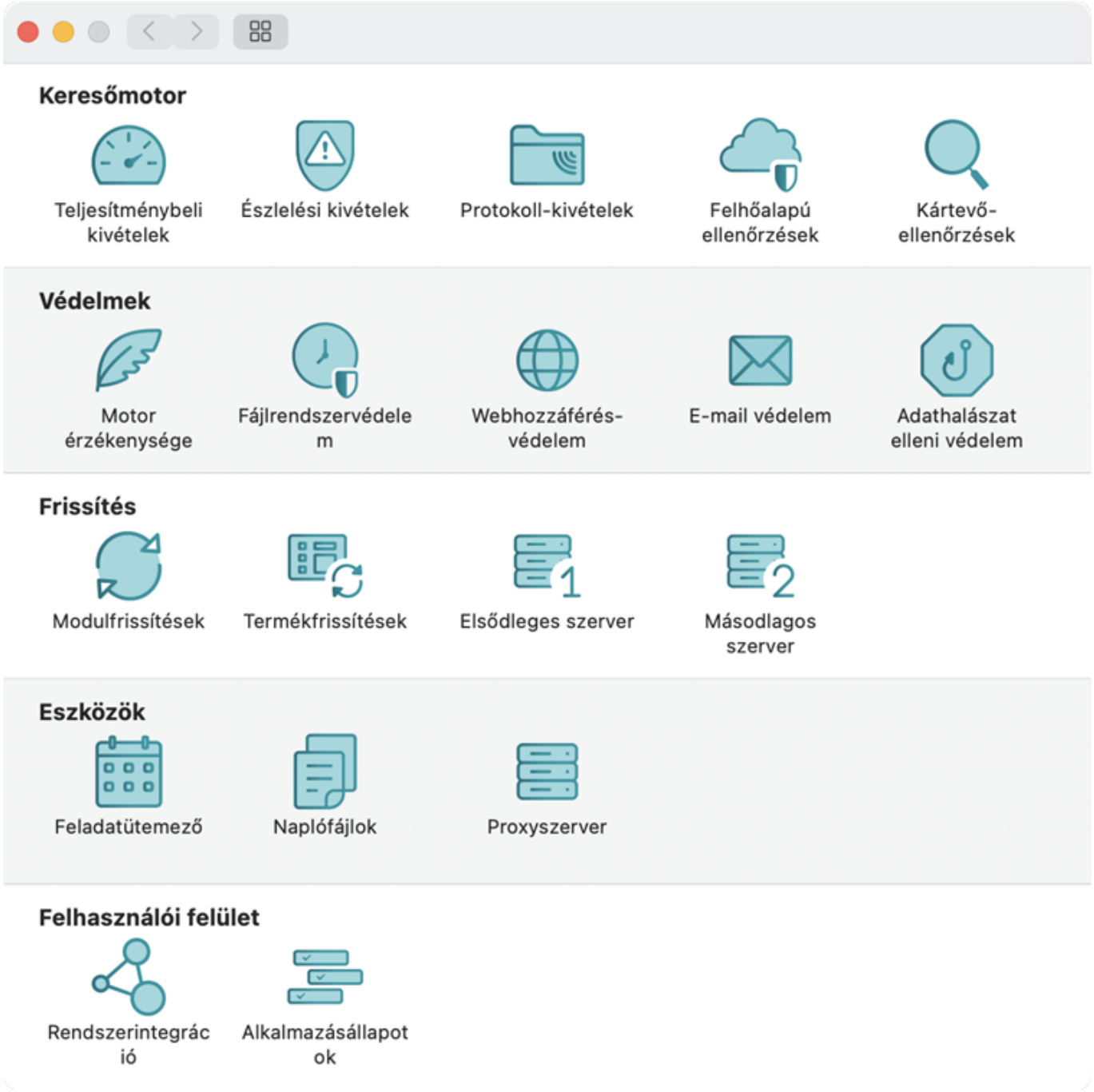
```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@In-depth scan" --boot-removable
```

Alkalmazásbeállítások

Az ESET Endpoint Antivirus for macOS speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

A következő kategóriákban konfigurálhatja a modulbeállításokat:

- Keresőmotor
- Védelmek
- Frissítés
- Eszközök
- Felhasználói felület



Keresőmotor

A keresőmotor a fájlok ellenőrzésével megakadályozza a kártékony kódok bejutását a rendszerbe. Ha például a program felismer egy kártevőnek minősülő objektumot, megkezdődik a kezelése. A keresőmotor meg tudja semmisíteni azáltal, hogy letiltja, majd megtisztítja, törli vagy karanténba helyezi.

Az ESET Endpoint Antivirus for macOS **Keresőmotor** speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Teljesítménybeli kivételek

A **Teljesítménybeli kivételek** csoportban megadhatja egyes fájlok, mappák, alkalmazások vagy IP/IPv6-címek kizárását az ellenőrzésből. Ha kizár útvonalakat (mappákat) az ellenőrzésből, sokkal kevesebb idő alatt kiszűrhetők a kártevők a fájlrendszerből.

-  – Új kivétel létrehozása; adja meg az objektum elérési útját
-  – A kijelölt bejegyzések eltávolítása.

Csak akkor szabad kizárni a fájlokat az ellenőrzésből, ha komoly problémákat tapasztal a valós idejű védelemmel kapcsolatban, mivel a fájlok ellenőrzésből való kizárása csökkenti az általános védelmet.

Észlelési kivételek

Az Észlelési kivételek csoportban objektumokat zárhat ki a tisztításból az észlelt elem neve, az objektum elérési útvonala vagy kivonata segítségével.

Észlelési kivételek beállításakor meg kell adni konkrét kizárási feltételeket. Meg kell adni egy érvényes észlelési nevet vagy SHA-1 kivonatot. Az érvényes fertőzésneveket vagy az SHA-1 kivonatokat 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 for macOS alkalmazásban. A valós fertőzések kizárása nagyon veszélyes – lehetőleg csak az érintett fájlokat vagy könyvtárakat zárja ki átmeneti időre. A kizárások a nemkívánatos, a nem biztonságos és a gyanús alkalmazásokra is vonatkoznak.

A következő típusú kizárási feltételek vannak:

- **Pontosan a fájl** – Fájl kizárása a megadott SHA-1 kivonat alapján, függetlenül a fájl típusától, tárolási helyétől, nevétől és kiterjesztésétől.
- **Észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve alapján.
- **Elérési út és észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve és elérési útja alapján (pl. `file:///Users/documentation/Downloads/eicar_com.zip`).

Csak akkor használjon észlelési kizárásokat, ha komoly problémákat tapasztal például egy kártevő észlelésével, mert a kártevők ellenőrzésből való kizárása csökkenti az általános védelmi szintet.

Protokoll-kivételek

A kivételek listájában szereplő címeken nem végez protokollszűrést a rendszer. A listára csak megbízható alkalmazásokat és címeket ajánlott felvenni.

Felhőalapú ellenőrzések

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

Az ESET víruslaborja megkapja a mintákat további elemzésre.

Minták elküldése

Az észlelt minták automatikus elküldése: A kiválasztott beállítás alapján fertőzött mintákat küldheti be az ESET víruslaborjának elemzésre és a kártevőészlelés fejlesztése céljából.

- Az összes észlelt minta
- Az összes minta a dokumentumok kivételével
- Ne küldje be

Gyanús minták automatikus elküldése: A kártevőkre hasonlító és szokatlan tulajdonságokat vagy viselkedést mutató gyanús mintákat a rendszer elküldi elemzésre az ESET víruslaborjába.

- Végrehajtható fájlok – fájltípusok: .exe, .dll, .sys
- Tömörített fájlok – fájltípusok: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- Szkriptek – fájltípusok: .bat, .cmd, .hta, .js, .vbs, .ps1
- Dokumentumok – A Microsoft Office, a Libre Office vagy más irodai eszközben létrehozott dokumentumok vagy aktív tartalommal rendelkező PDF-fájlok.
- Egyéb – fájltípusok: .jar, .reg, .msi, .swf, .lnk

Automatikus beküldési kivételek: A kizárt fájlokat akkor sem kapja meg az ESET víruslaborja, ha gyanús kódot tartalmaznak.

Összeomlási jelentések és diagnosztikai adatok küldése

Elküldhet például olyan adatokat, mint az összeomlási jelentések vagy a modul-memóriaképek.

Segítse a termék tökéletesítését anonim használati statisztikai adatok beküldésével

Engedélyezheti az ESET-nek, hogy begyűjtse az újonnan észlelt kártevőkre vonatkozó anonim információkat (név, az észlelés dátuma és időpontja, az észlelési mód és a kapcsolódó metaadatok), az ellenőrzött fájlokat (kivonat, fájlnév, a fájl eredete, telemetria), a letiltott és gyanús URL-címeket, a termékverziót és -konfigurációt, beleértve a rendszeradatokat.

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.

Kártevő-ellenőrzések

A kézi indítású víruskereső a vírus- és kémprogramvédelem fontos része, mert a 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. A **Kártevőellenőrzések** szakaszban konfigurálhatja a kézi indítású ellenőrzési profilok beállításait:

Profilok listája – Új létrehozásához vagy meglévő eltávolításához válassza ki a + vagy a − lehetőséget. Új profillista hozzáadásakor írja be a profil nevét, majd kattintson az **OK** gombra. Az új profil megjelenik a Kiválasztott profil legördülő menüben, amely felsorolja a meglévő ellenőrzési profilokat.

ThreatSense-paraméterek – Az ellenőrzési profil konfigurációs beállításai, például a vezérelni kívánt fájlkiterjesztések, ellenőrizendő objektumok, alkalmazott észlelési módszerek stb.

Védelmek

Az ESET Endpoint Antivirus for macOS speciális **védelmi** beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Motor érzékenysége

A motorérzékenység lehetővé teszi a következő kategóriák jelentési és védelmi szintjeinek konfigurálását az összes védelmi modulnál.

- **Kártevők** – Ezek rosszindulatú kódok, amelyek a számítógépen meglévő fájlok részét képezik.

- **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. További információ ezekről az alkalmazásokról a Szószedetben található.

- **Gyanús alkalmazások** – Ezek olyan programok, amelyeket tömörítőprogramokkal vagy védelmi modulokkal tömörítettek. Az ilyen védelmi modulokat gyakran használják a kártevőprogramok fejlesztői arra, hogy segítségükkel elkerüljék az észlelést. A tömörítő egy olyan futtatás közbeni, önkicsomagoló végrehajtható fájl, amely többféle kártevőt egyetlen csomagban egyesít. A leggyakoribb tömörítők az UPX, a PE_Compact, a PKLite és az ASPack. Ugyanazt a kártevőt különbözőképpen észlelheti a program attól függően, hogy a tömörítést melyik tömörítővel végezték. A tömörítőkre továbbá az is jellemző, hogy „aláírásuk” idővel mutáción megy keresztül, még jobban megnehezítve ezzel a kártevő észlelését és eltávolítását.

- **Veszélyes alkalmazások** – A kereskedelemben kapható olyan törvényes szoftverek, amelyekkel a támadók visszaélhetnek, ha a felhasználó beleegyezése nélkül telepítik azokat. Ez a besorolás olyan programokat tartalmaz, mint a távoli hozzáférési eszközök. Ez a beállítás alapértelmezés szerint le van tiltva.

Fájlrendszervédelem

Az ESET LiveGrid© technológia (a ThreatSense keresőmotor beállításai című témakörben ismertetjük) használatakor a valós idejű fájlrendszervédelem eltérő lehet az újonnan létrehozott fájlok és a meglévő fájlok esetében. Nagyobb fokú felügyelet érhető el az újonnan létrehozott fájlok esetén.

A következő adathordozókat zárhatja ki a Real-time ellenőrzésből:

- **Helyi meghajtók** – rendszermeghajtók
- **Cserélhető adathordozók** – USB-tárolóeszközök, Bluetooth-eszközök stb.
- **Hálózati adathordozók** – minden csatlakoztatott meghajtó

Alapértelmezés szerint a szolgáltatás az összes fájlt ellenőrzi **fájlok megnyitásakor** és **fájlok létrehozásakor**. Ajánlott az alapértelmezett beállítások megtartása, amelyek maximális szintű valós idejű védelmet biztosítanak a számítógép számára.

Bizonyos folyamatokat is kizárhat az ellenőrzésből.

Ajánlott az alapértelmezett beállításokat használni és csak bizonyos esetekben módosítani az ellenőrzésből kizárandó adathordozókat, például amikor egyes adathordozók ellenőrzése jelentősen lassítja az adatátvitelt.

Webhozzáférés-védelem

A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP protokollon alapuló szabályokat.

A webes szűrést úgy érheti el, hogy meghatározza a portszámokat a HTTP-kommunikációhoz és az URL-címekhez.

Webprotokollok

A webprotokollok szakaszban engedélyezheti vagy letilthatja a HTTP-protokollellenőrzést, és meghatározhatja a HTTP-kommunikációhoz használni kívánt portszámokat. Alapértelmezés szerint a 80-as, a 8080-as és a 3128-as portszám van beállítva.

URL-címek kezelése

Ebben a szakaszban megadhatók a letiltandó, engedélyezendő, illetve az ellenőrzésből kizárandó HTTP-címek. A Letiltva címek listájában szereplő webhelyeket nem fogja tudni elérni. A kizárt címek listáján szereplő webhelyek elérése közben a program nem keres kártékony kódokat.

Az engedélyezett, letiltott vagy kizárt címek listájának aktiválásához válasszon egy listát, és engedélyezze az **Lista aktiválása** opciót. Ha értesítést szeretne megjeleníteni az aktuális listán szereplő címek beírásakor, engedélyezze az **Értesítés az alkalmazásakor** opciót.

A *(csillag) és a ?(kérdőjel) speciális szimbólum bármely listában használható. 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.

E-mail védelem

E-mail védelem – A POP3 és az IMAP protokollon keresztül érkező e-mailes kommunikáció szabályozását biztosítja. A bejövő üzenetek vizsgálatakor az ESET Endpoint Antivirus for macOS a ThreatSense keresőmotor speciális ellenőrzési módszereit alkalmazza. A POP3 és az IMAP protokollon keresztül folytatott kommunikáció ellenőrzése nem függ attól, hogy milyen levelezőprogramot használ. A választható beállítások az alábbiak:

Levelezési protokollok

Itt engedélyezheti vagy letilthatja a POP3 és az IMAP protokollon keresztül érkező e-mailek ellenőrzését.

POP3-protokollszűrés

A POP3 a levelezőprogramok által a legszélesebb körben használt levélfogadási protokoll. Az ESET Endpoint Antivirus for macOS a levelezőprogramtól függetlenül képes védeni a POP3 protokollon keresztüli kommunikációt.

Az ellenőrzést biztosító védelmi modul automatikusan elindul az operációs rendszer indításakor, és aktív marad a memóriában. A modul megfelelő működéséhez ellenőrizze, hogy az IMAP-protokollszűrés engedélyezve van-e. Az automatikus IMAP-ellenőrzéshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 110-as porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. A portszámokat vesszővel elválasztva kell megadni.

Ha engedélyezi a **POP3 protokollellenőrzés** opciót, a rendszer ellenőrzi az összes POP3 forgalmat a rosszindulatú szoftverek szempontjából.

IMAP-protokollszűrés

Az IMAP (Internet Message Access Protocol) egy másik internetes protokoll, amely az e-mailek beolvasására szolgál, és van néhány előnyös tulajdonsága a POP3-mal szemben. Például több levelezőprogram is csatlakozhat ugyanahhoz a postaládához egy időben, miközben az üzenetek állapota (például hogy elolvasták, megválaszolták vagy törölték-e) megőrződik. Az ESET Endpoint Antivirus for macOS a használt levelezőprogramtól függetlenül képes az IMAP protokoll védelmére.

Az ellenőrzést biztosító védelmi modul automatikusan elindul az operációs rendszer indításakor, és aktív marad a memóriában. A modul megfelelő működéséhez ellenőrizze, hogy az IMAP-protokollszűrés engedélyezve van-e. Az automatikus IMAP-ellenőrzéshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 143-as porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. Vesszővel kell elválasztani a portszámokat.

Ha engedélyezi az **IMAP-protokollszűrést**, akkor a program az IMAP protokollon átmenő teljes forgalmat ellenőrzi kártevő szoftvereket keresve.

E-mail-címkék

Az e-mail-címkék használata lehetővé teszi címkeüzenet hozzáfűzését az e-mail-lábjegyzethez. Az e-mailek ellenőrzése után előfordulhat, hogy a program az ellenőrzés eredményét ismertető értesítést is hozzáfűz. A

címkeüzenetek hasznos eszközök, de nem érdemes az üzenet biztonságának meghatározásához használni őket, mivel a hibásan formázott HTML-üzenetekben eltűnhetnek, illetve egyes kártevők képesek azokat meghamisítani. A választható lehetőségek az alábbiak:

- **A kimenő e-mailekhez észlelés esetén** – Csak a kártevőket tartalmazó e-mailek lesznek megjelölve ellenőrzöttként.
- **Minden e-mailhez ellenőrzéskor** – Az összes ellenőrzött e-mail címkeüzenettel lesz ellátva.
- **Soha** – Semmilyen e-mail nem lesz ellátva címkeüzenettel.

Kapott e-mail tárgyának frissítése – Jelölje be ezt a jelölőnégyzetet, ha azt szeretné, hogy az e-mail-védelem kártevőre utaló figyelmeztetést szúrjon be a fertőzött e-mailekbe. Ez a funkció lehetővé teszi a fertőzött e-mailek egyszerű szűrését. Így a címzett számára megnő az üzenetek hitelességi szintje, és fertőzés észlelése esetén értékes információk nyerhetők az adott üzenet vagy feladója veszélyességi szintjéről.

Hozzáadás az észlelt e-mail tárgyához – A sablon szerkesztésével módosíthatja a fertőzött e-mail tárgyában szereplő előtag formátumát.

ThreatSense paraméterek

A speciális víruskeresési beállítások lehetővé teszik a megtisztítási szintek, az ellenőrzési beállítások és az ellenőrzésből kizárt fájlkiterjesztések konfigurálását.

Adathalászat elleni védelem

Az Adathalászat elleni védelem további védelmet biztosít azokkal a nem szabályszerű webhelyekkel szemben, amelyek jelszavakat és más bizalmas információkat kísérelnek meg megszerezni. Az adathalászat elleni védelem alapértelmezés szerint engedélyezve van, és azt javasoljuk, hogy ne is tiltsa le.

Frissítés

Ebben a szakaszban adhatja meg a frissítési források beállításait, például a használatban lévő frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat. Az ESET Endpoint Antivirus for macOS speciális **frissítési** beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Modul- és termékfrissítések

Modulfrissítések

Frissítés típusa

- **Rendszeres frissítés**. Ez az alapértelmezett frissítési típus, amely biztosítja, hogy a kereső-adatbázis és a termékmodulok automatikusan frissüljenek az ESET frissítési szerverekről.
- A **tesztelési mód** tartalmazza a legutóbbi hibajavításokat és észlelési módszereket, amelyek hamarosan elérhetők lesznek a nagyközönség számára is. Előfordulhat azonban, hogy nem mindig stabilak, ezért nem

ajánlott termelési környezetben használni őket.

- A **késleltetett frissítések** lehetővé teszik a speciális frissítési szerverekről való frissítést, amelyek a vírusadatbázisok új verzióit biztosítják legalább X órás késéssel (vagyis valós környezetben tesztelt és stabilnak tartott adatbázisok).

Modul-visszaállítás

Ha a keresőmotor egyik frissítése vagy a programmodulok feltehetően nem stabilak, illetve sérültek, visszaállhat az előző verzióra, és átmenetileg letilthatja a frissítéseket.

Modulok pillanatképének létrehozása

Az ESET Endpoint Antivirus for macOS rögzíti a keresőmotor és a programmodulok pillanatképét a visszaállítás funkcióhoz. A moduladatbázis pillanatfelvételeinek létrehozásához hagyja engedélyezve a **Modulok pillanatképének létrehozása** funkciót. Ha a **Modulok pillanatképének létrehozása** funkció engedélyezve van, az első pillanatkép az első frissítés alkalmával jön létre. A következő 48 óra múlva jön létre. A **Helyben tárolt pillanatképek száma** mező meghatározza a keresőmotor pillanatképeinek tárolt számát.

> Amikor elérte a pillanatképek maximális mennyiségét (például három), a legrégebbi pillanatképet 48 óránként új pillanatfelvétel váltja fel. Az ESET Endpoint Antivirus for macOS for macOS visszaállítja a keresőmotor és a programmodulok frissítési verzióját a legrégebbi pillanatfelvételre.

Termékfrissítések

A termékfrissítések biztosítják, hogy mindig a legújabb termékverziót használja. Engedélyezze az **Automatikus frissítések** kapcsolót, hogy a termékfrissítések automatikusan települjenek a következő újraindításkor, és folyamatosan hozzáférjen a legújabb funkciókhoz és védelemhez.

Elsődleges szerver és másodlagos szerver

Alapértelmezés szerint engedélyezve van az elsődleges és másodlagos frissítési szerverek közötti automatikus választás lehetősége. Mindkét szerver megadható, ha az automatikus kiválasztás kapcsolója le van tiltva.

Eszközök

Az ESET Endpoint Antivirus for macOS **Eszközök** speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Feladatütemező

A **Feladatütemező** segítségével beállíthat igény szerinti ellenőrzési feladatokat automatikusan végbemennek egy meghatározott időpontban. Új ütemezett feladat létrehozásához vagy egy meglévő eltávolításához válassza ki a + vagy a − elemet. Megadhatja azt a napot vagy napokat is, amikor a feladatot ismételni szeretné.

Naplófájlok

Naplózás részletessége

A naplózási részletesség meghatározza a naplófájlok részletességi szintjét.

- **Kritikus figyelmeztetések** – Csak kritikus hibákat tartalmaz (például: **Nem sikerült elindítani a vírusvédelmet**)
- **Hibák** – A kritikus figyelmeztetéseken kívül olyan hibák rögzítése, mint a **Hiba történt a fájl letöltésekor**
- **Figyelmeztetések** – Kritikus figyelmeztetések és figyelmeztető üzenetek rögzítése.
- **Tájékoztató bejegyzések** – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett bejegyzéseket).
- **Diagnosztikai bejegyzések** – A fentiek mellett a program pontos beállításához szükséges információk megjelenítése.

Naplófájlok megtisztítása

Az ennél régebbi naplóbejegyzések törlése (nap) – A megadott napnál régebbi naplóbejegyzések automatikusan törlődni fognak.

Naplófájlok optimalizálása

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. A teljesítmény és a naplók feldolgozási sebességének javítása érdekében a program eltávolítja az összes üres naplóbejegyzést. Ezt a javulást akkor láthatja, ha a naplók nagyszámú bejegyzést tartalmaznak.

A proxyszerver beállításai

Itt adhatja meg a proxyszerver beállításait. A megadott paramétereket minden olyan modul használni fogja, amelyhez internetkapcsolat szükséges.

A proxyszerver konfigurálása:

1. Engedélyezze a **Proxyszerver használata** funkciót, majd írja be a proxyszerver címét a **Proxyszerver** mezőbe és a proxyszerver **portszámát**.

2. Engedélyezze a **Közvetlen kapcsolat használata, ha nem érhető el proxy** funkciót, ha azt szeretné, hogy meg legyen kerülve a proxy, és közvetlenül az ESET-szerverekkel folyjon a kommunikáció.

3. Ha a proxyszerverrel folytatott kommunikációhoz hitelesítés szükséges, akkor engedélyezze **A proxyszerver hitelesítést igényel** funkciót, majd adjon meg egy érvényes **felhasználónevet** és **jelszót** a megfelelő mezőkben.

Felhasználói felület

Az ESET Endpoint Antivirus for macOS **felhasználói felület** speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Endpoint Antivirus for macOS elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Rendszerintegráció

Felhasználói felület elemei

Grafikus felhasználói felület megnyitásának engedélyezése a felhasználó számára – A beállítás letiltásával megakadályozhatja, hogy a felhasználók elérhessék a grafikus felhasználói felületet. Ez felügyelt környezetben, illetve akkor lehet hasznos, amikor meg kell őriznie a rendszererőforrásokat.

Ikon megjelenítése a menüsáv extrái között – A beállítás letiltásával eltávolíthatja az ESET Endpoint Antivirus for macOS ikonját a macOS menüsáv extrái közül (a képernyő tetején).

Értesítések

Értesítések megjelenítése az asztalon – Az asztali értesítések (például sikeres frissítésről, víruskeresési feladatok befejezéséről vagy új kártevőkről szóló üzenetek) a macOS menüsor melletti előugró ablakban jelennek meg. Ha engedélyezve van, az ESET Endpoint Antivirus for macOS tájékoztatja, ha új esemény következik be.

Alkalmazásállapotok

Itt kiválaszthatja az ESET Endpoint Antivirus for macOS termékben és a webkonzolban megjelenített alkalmazásállapotokat. Ha az **Állapot megjelenítése** kapcsoló le van tiltva egy probléma jelentésekor, az ESET Endpoint Antivirus for macOS alkalmazás megőrzi a zöld **A védelme biztosított** állapotot.

Eltávolítás

Helyi eltávolítás

Az ESET Endpoint Antivirus for macOS nem távolítható el teljesen úgy, hogy az ESET Endpoint Antivirus for macOS ikonját az Alkalmazások mappából a Kukába húzza. A rendszerbővítmény telepítve marad a számítógépen, és az Uninstaller.app később nem tudja majd eltávolítani.
Hogy a felhasználók ne távolíthassák el az ESET Endpoint Antivirus for macOS szolgáltatást, azt javasoljuk, hogy adjon hozzá egy Tilos módosítani jelölőt az ESET Endpoint Antivirus for macOS szolgáltatáshoz. A Tilos módosítani jelölő hozzáadásához futtassa a következő parancsot a célszámítógépen:

```
sudo chflags -Rf schg /Applications/ESET\ Endpoint\ Antivirus\.app
```

Az ESET Endpoint Antivirus for macOS eltávolítása előtt el kell távolítania a Tilos módosítani jelölőt. A Tilos módosítani jelölő eltávolításához futtassa a következő parancsot a célszámítógépen:

```
sudo chflags -Rf noschg /Applications/ESET\ Endpoint\ Antivirus\.app
```

Az ESET Endpoint Antivirus for macOS eltávolításához:

Ha az ESET Endpoint Antivirus for macOS szolgáltatást az ESET PROTECT On-Prem vagy az ESET PROTECT CLOUD segítségével kezeli, akkor létrehozhat és futtathat egy kliensfeladatot az ESET Endpoint Antivirus for macOS távolról történő eltávolításhoz:
- Hozza létre és futtassa a Szoftver eltávolítása feladatot az ESET PROTECT On-Prem szolgáltatásban.
- Hozza létre és futtassa a Szoftver eltávolítása feladatot az ESET PROTECT CLOUD szolgáltatásban.

1. Indítsa el az ESET Endpoint Antivirus for macOS eltávolítóprogramját. Az ESET Endpoint Antivirus for macOS eltávolítóprogramja többféleképpen indítható el:

- Nyissa meg az ESET Endpoint Antivirus for macOS telepítőfájlját (*.dmg*), és kattintson duplán az Eltávolítás elemre.

- Indítsa el a Findert, nyissa meg az Alkalmazások mappát a merevlemezen, a Control billentyűt lenyomva tartva kattintson (vagy kattintson a jobb gombbal) az **ESET Endpoint Antivirus for macOS** ikonra > válassza ki a **Csomag tartalmának a megjelenítése** lehetőséget a helyi menüből. Nyissa meg a **Contents** > **Helpers** mappát, és kattintson duplán az Uninstaller ikonra.

2. Kattintson az **Eltávolítás** gombra az eltávolítási folyamat elindításához. Felszólítást fog kapni a rendszergazdai jelszó beírására.

Ha probléma merül fel a rendszerbővítmények eltávolításával, felszólítást kaphat arra, hogy írja be a rendszergazdai jelszót az eltávolítási folyamat során.

3. Ha az ESET Endpoint Antivirus for macOS eltávolítását a macOS 12 Monterey rendszeren végzi, akkor felszólítást kap arra, hogy engedélyezze az Uninstaller.app számára az ESET Endpoint Antivirus for macOS által létrehozott felhasználók kezelését. A következő párbeszédablak fog megjelenni:
Az „Uninstaller.app” adminisztrálni szeretné az Ön számítógépét. A adminisztrációba beletartozik a jelszavak, a hálózat és a rendszerbeállítások módosítása.
Kattintson az OK gombra. Ha a Tiltás gombra kattint, akkor az ESET Endpoint Antivirus for macOS nem lesz teljesen eltávolítva.

4. A Bezárás gombra koppintva lépjen ki az eltávolítóprogramból.

5. Indítsa újra a számítógépet.

Eltávolítás a parancssoron keresztül

Az ESET Endpoint Antivirus for macOS úgy is eltávolítható, hogy a **Terminálban** futtatja az eltávolító szkriptet. Ha az ESET Endpoint Antivirus for macOS az alapértelmezett helyre van telepítve, akkor futtassa a következő parancsot:

```
sudo /Applications/ESET\ Endpoint\
Antivirus.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```

Műszaki terméktámogatás

Kapcsolatfelvétel a műszaki terméktámogatással

Ha nem talál megoldást a problémájára, az ESET webhelyén megtalálható űrlapon keresztül gyorsan kapcsolatba

léphet az ESET műszaki támogatási szolgálatával.

Információk összegyűjtése a terméktámogatás számára

A probléma gyors és sikeres megoldásának biztosításához a következőket javasoljuk a támogatási jegy létrehozásakor:

- Adjon meg olyan információkat, mint a licencadatok, a terméknév, a termékverzió és az operációs rendszer.
- Írja le részletesen a problémát.
- Csatoljon képernyőképeket vagy videót a problémáról.
- Csatolja az ESET LogCollector naplóit.

ESET LogCollector

Az ESET LogColletor naplókat hoz létre fontos információkkal, amelyek segítségével az ügyfélszolgálat és a fejlesztők azonosítani tudják az ESET Endpoint Antivirus for macOS használatakor fellépő problémákat.

Az ESET LogCollector szolgáltatásról részletesebb információkat az ESET-tudásbáziscikkében talál. Előfordulhat, hogy a cikk nem minden nyelven érhető el.

Naplók létrehozása az ESET LogCollector segítségével:

1. ESET LogCollector Letöltés.
2. Nyissa meg az **eset_logcollector.dmg** nevű fájlt, majd futtassa a LogCollector alkalmazást.
3. Kövesse a képernyőn megjelenő utasításokat a naplók létrehozásához.

> **Tippek az ESET LogCollector használatához**
> - Ha részletesebb naplókat szeretne létrehozni az ESET ügyfélszolgálatának, a **Replikáció** részben kattintson a fogaskereket ábrázoló ikonra a további beállítások megnyitásához.
> - Ne kezdje el a replikálást addig, amíg készen nem áll a probléma és a hozzá vezető lépések újbóli reprodukálására.

A naplófájlok létrehozása után az asztalon találja őket a **customer_info.zip** fájlban. Csatolja ezt a fájlt a támogatási kérelemhez.

Végfelhasználói licencszerződés

Hatályos 2021. október 19-től.

FONTOS: Kérjük, hogy a letöltés, telepítés, másolás vagy használat előtt olvassa el figyelmesen a termék használatára vonatkozó alábbi feltételeket. **A SZOFTVER LETÖLTÉSÉVEL, TELEPÍTÉSÉVEL, MÁSOLÁSÁVAL VAGY HASZNÁLATÁVAL ÖN ELFOGADJA EZEKET A FELTÉTELEKET, ÉS TUDOMÁSUL VESZI AZ ADATVÉDELMI SZABÁLYZATOT.**

Végfelhasználói licencszerződés

Jelen végfelhasználói licencszerződés („a Szerződés”) alapján, amely egyfelől az ESET, spol. s r. o. (székhelye: Einsteinova 24, 85101 Bratislava, Slovak Republic; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B; cégjegyzékszám: 31333532; („ESET” vagy „a Gyártó”), másfelől Ön mint természetes vagy jogi személy („Ön” vagy „a Végfelhasználó”) között jött létre, Ön jogosult a jelen Szerződés 1. pontjában meghatározott szoftver használatára. A jelen Szerződés 1. pontjában meghatározott Szoftver az alábbiakban megadott feltételeknek megfelelően adathordozón tárolható, e-mailben küldhető, az internetről vagy a Gyártó szervereiről letölthető, illetve más forrásokból beszerezhető.

JELEN SZERZŐDÉS VÉGFELHASZNÁLÓI JOGOSULTSÁGOKRA VONATKOZIK, ÉS NEM ÉRTÉKESÍTÉSI SZERZŐDÉS. Az értékesítési csomagban található szoftvermásolat és a fizikai adathordozó, valamint a jelen Szerződés alapján a Végfelhasználó által készíthető bármely másolat továbbra is a Gyártó tulajdonát képezi.

Ha az „Elfogadom” vagy egyéb, jóváhagyásra szolgáló gombra kattint a Szoftver telepítése, letöltése, másolása vagy használata közben, illetve bármilyen alkalmazásáruházból való telepítésekor, azzal elfogadja a jelen Szerződés feltételeit és jóváhagyja az Adatvédelmi szabályzatot. Ha nem ért egyet a Szerződés és vagy az Adatvédelmi szabályzatot bármely rendelkezésével, azonnal kattintson a megszakításra szolgáló gombra, szakítsa meg a letöltést vagy a telepítést, illetve semmisítse meg vagy küldje vissza a Szoftvert, a telepítési adathordozót, valamint a kapcsolódó dokumentációt és a vásárlási számlát a Gyártónak vagy abba az üzletbe, ahol a Szoftvert beszerezte.

ÖN ELFOGADJA, HOGY A SZOFTVER HASZNÁLATÁVAL KIFEJEZI, HOGY A JELEN SZERZŐDÉST ELOLVASTA, MEGÉRTETTE, ÉS RENDELKEZÉSEIT ÖNMAGÁRA NÉZVE KÖTELEZŐ ÉRVÉNYŰNEK ISMERTE EL.

1. **Szoftver**. A jelen Szerződésben a „Szoftver” kifejezés a következőt jelenti: (i) a jelen Szerződéshez mellékelt számítógépes program és annak összes komponense; (ii) a lemezek, CD-ROM-ok, DVD-k, e-mailek és mellékleteik vagy más adathordozók tartalma, amelyhez a jelen Szerződés tartozik, beleértve az adathordozón nyújtott vagy e-mailben küldött, illetve interneten letölthető Szoftver tárgykódját; (iii) minden kapcsolódó írásbeli használati utasítás vagy a Szoftverhez tartozó egyéb dokumentáció, beleértve többek között a szoftver bármilyen leírását, specifikációját, tulajdonságainak vagy működésének ismertetését, a működési környezet leírását, amelyben a Szoftvert használják, a Szoftver telepítési vagy használati útmutatóit, a Szoftver megfelelő használatára vonatkozó bármilyen leírást („Dokumentáció”); (iv) a Szoftver másolatai, lehetséges hibáinak javításai, kiegészítései, bővítményei, módosított verziói, összetevőinek frissítései (ha vannak), amelyekhez a Gyártó a jelen Szerződés 3. pontja szerint Önnek használati engedélyt adott. A Szoftver kizárólag végrehajtható tárgykód formájában szerezhető be.

2. **Telepítés, Számítógép és Licenckulcs**. Az adathordozón biztosított, e-mailben küldött vagy az internetről, illetve a Gyártó szervereiről letöltött vagy más forrásból megszerzett Szoftvert telepíteni kell. A Szoftvert megfelelően konfigurált számítógépre kell telepíteni, amely legalább a Dokumentációban közölt követelményeknek megfelel. A telepítési módszer leírása a Dokumentációban található. A Szoftvert futtató Számítógépre nem telepíthető olyan számítógépes program vagy hardver, amely kedvezőtlen hatással lehet a Szoftverre. A Számítógép olyan hardver – korlátozás nélkül ideértve a személyi számítógépeket, laptopokat, munkaállomásokat, tenyérszámítógépeket, okostelefonokat, kézi elektronikus készülékeket, illetve egyéb elektronikus eszközöket –, amelyre a Szoftver készült, és amelyre telepíteni fogják, illetve amelyen használni fogják a Szoftvert. A Licenckulcs szimbólumok, betűk, számok, illetve speciális jelek egyedi sorozata, amelyet a Végfelhasználó kap annak érdekében, hogy legálisan használhassa a Szoftvert vagy annak egy adott verzióját, illetve kiterjeszthesse a Licencet a jelen Szerződéssel összhangban.

3. **Licenc**. Amennyiben Ön elfogadja a jelen Szerződés rendelkezéseit, az érvényességi időn belül megfizeti a licencdíjat, és megfelel az itt előírt összes feltételnek, a Gyártó az alábbi jogokat (a továbbiakban „a Licenc”) biztosítja az Ön számára: a) Telepítés és használat:

a) **Telepítés és használat.** Nem kizárólagos és nem átruházható jogot szerez a Gyártótól arra, hogy a Szoftvert egy számítógép merevlemezére vagy más tartós adattárolásra alkalmas adathordozóra telepítse, a Szoftvert

számítógépes rendszerek memóriájába telepítse, és ott tárolja, valamint megjelenítse azt.

b) **A licencek számának kikötése.** A Szoftver használatára vonatkozó jogosultságot a Végfelhasználók száma határozza meg. Egy Végfelhasználónak kell tekinteni a következőt: (i) a Szoftver telepítése egyetlen számítógépre, vagy (ii) ha a licenc terjedelme az e-mail postafiókok számához kötött, a Végfelhasználó egy olyan számítógép-használót jelent, aki levelezőprogramon (Mail User Agent, levelezési felhasználói ügynök, „Levelezőprogram") keresztül fogad e-mailt. Ha egy Levelezőprogram e-mailt fogad, majd azt automatikusan továbbítja több felhasználónak, akkor a Végfelhasználók számának meghatározása az alapján történik, hogy ténylegesen hány felhasználó kapja meg a továbbítással az e-mailt. Ha a levelezési szerver levelezési kapuként működik, a Végfelhasználók száma megegyezik azon levelezésiszerver-használók számával, akiknek a kapu szolgáltatást nyújt. Csak egy számítógépre szükséges licencet szerezni, ha meghatározatlan számú e-mail-cím (alias) van átirányítva egy felhasználónak, és csak egyetlen felhasználó fogadja őket, továbbá a kliens nem továbbítja automatikusan az üzeneteket nagyszámú felhasználóhoz. A Licenc egyidejűleg csak egy számítógépen használható. A Végfelhasználó csak abban a mértékben jogosult megadni a Licenckulcsot a Szoftvernek, amennyi joga van használni a Szoftvert a Gyártó által adott Licencek száma alapján. A Licenckulcs bizalmas jellegű, Ön nem oszthatja meg harmadik féllel, illetve nem engedélyezheti a Licenckulcs használatát harmadik félnek, kivéve akkor, ha a jelen Szerződés vagy a Gyártó ezt megengedi. Ha a Licenckulcs illetéktelenekhez kerül, haladéktalanul értesítse a Gyártót.

c) **Otthoni/üzleti változat.** A Szoftver Otthoni verziója kizárólag privát, illetve nem kereskedelmi környezetben használható otthoni és családi használatra. A Szoftver Üzleti verzióját kereskedelmi környezetben való használatra lehet beszerezni, valamint a Szoftver levelezési szervereken, levelezési átjárókon vagy internetes átjárókon való használatához.

d) **A licenc érvényességi időszaka.** A Szoftver használatára vonatkozó jogosultság korlátozott időtartamra szól.

e) **Számítógép-gyártói (OEM-) szoftver.** A számítógép-gyártói (OEM) besorolású szoftver használata arra a számítógépre van korlátozva, amelyen beszerezte. amellyel megvásárolta azt, és másik számítógépre nem vihető át.

f) **Kereskedelmi forgalomba nem hozható termék és próbaverzió.** A „kereskedelmi forgalomba nem hozhatóként" minősített Szoftver és a próbaverzió nem lehet díjköteles, és kizárólag a Szoftver funkcióinak ellenőrzésére és tesztelésére, valamint szemléltetési célra használható.

g) **A licenc lejárata.** A Licenc az érvényességi időszak végén automatikusan lejár. Ha Ön nem teljesíti a jelen Szerződés bármely rendelkezését, a Gyártónak jogában áll felmondani a Szerződést bármely jogosultság vagy az ilyen esetekben a Gyártó számára elérhető jogorvoslati lehetőség megsértése nélkül. A Licenc felmondása esetén a Szoftvert, illetve az összes biztonsági másolatot haladéktalanul törölnie kell, meg kell semmisítenie, vagy a saját költségén vissza kell küldenie az ESET címére vagy abba az üzletbe, ahol a Szoftvert beszerezte. A Licenc lejárata esetén a Gyártónak szintjén jogában áll felmondania a Végfelhasználó jogosultságát a Szoftver olyan funkcióinak használatára, amelyek a Gyártó vagy harmadik felek szervereihez való kapcsolódást igényelnek.

4. **Adatgyűjtésre és internetkapcsolatra vonatkozó követelmények.** A Szoftver megfelelő működtetéséhez, valamint az Adatvédelmi szabályzatnak megfelelő adatgyűjtés céljából internetkapcsolat szükséges, és rendszeres időközönként csatlakoznia kell a Gyártó vagy a harmadik fél szervereihez. Az internetkapcsolatra és az adatgyűjtésre a Szoftver alábbi funkcióihoz van szükség:

a) **A Szoftver frissítései.** A Gyártó jogosult, de nem köteles időnként kiadni frissítéseket („Frissítések") a Szoftverhez. Ez a funkció a Szoftver általános beállításai között engedélyezve van, és a Frissítések ezért automatikusan települnek, kivéve ha a Végfelhasználó letiltotta a Frissítések automatikus telepítését. A frissítések biztosításához szükség van a Licenc eredetiségének ellenőrzésére, ideértve a Számítógépre vonatkozó információkat és/vagy annak ellenőrzését, hogy megfelel-e az Adatvédelmi szabályzatnak az a platform, amelyre a Szoftver telepítve van.

A Frissítések biztosítására az Életciklus végéről szóló szabályzat („EOL szabályzat”) vonatkozik, amely a https://go.eset.com/eol_business weboldalon érhető el. Nem biztosítunk Frissítéseket, miután a Szoftver vagy bármely funkciója elérte az EOL szabályzatban meghatározott Életciklus végét.

b) **Kártevők és információk továbbítása a Gyártónak.** A Szoftver olyan funkciókat tartalmaz, amelyek mintákat gyűjtenek a vírusokról és egyéb kártékony számítógépes programokról, a gyanús, problémás, kéretlen vagy veszélyes objektumokról, többek között fájlokról, URL-címekről, IP-csomagokról vagy Ethernet-keretekről („Kártevők”), majd a mintákat elküldik a Gyártónak, beleértve, de nem kizárólag a telepítési folyamatra, arra a számítógépre és/vagy platformra vonatkozó adatokkal, amelyen a Szoftver telepítve van, valamint a szoftver működésével és funkcióival („Adatok”) együtt. Ezek az Adatok és Kártevők magukban foglalhatják a Végfelhasználóval vagy a Szoftvert futtató számítógép más felhasználóival kapcsolatos adatokat (beleértve a véletlenszerűen vagy nem szándékosan megszerzett személyes adatokat is), valamint a kártevők által érintett fájlokat a kapcsolódó metaadatokkal együtt.

Az információkat és a kártevőket a szoftver következő funkciói gyűjthetik:

i. A LiveGrid megbízhatósági rendszer végzi a kártevőkkel kapcsolatos egyirányú kivonatok gyűjtését és elküldését a Gyártónak. Ez a funkció a Szoftver általános beállításai között engedélyezhető.

ii. A LiveGrid visszajelzési rendszer hajtja végre a kártevők gyűjtését és elküldését a Gyártónak a kapcsolódó metaadatokkal és információkkal együtt. Ezt a funkciót a Végfelhasználó aktiválja a Szoftver telepítése során.

A Gyártó a kapott Adatokat és Kártevőket kizárólag a Kártevők elemzésére és tanulmányozására, a Szoftver fejlesztésére, valamint a Licenc eredetiségének ellenőrzésére használja, és megfelelő intézkedésekkel biztosítja a kapott Adatok és Kártevők bizalmas kezelését. A Szoftver fent említett funkciójának aktiválásával Ön hozzájárul ahhoz, hogy a Gyártó összegyűjtsön és feldolgozzon Kártevőket és Adatokat az Adatvédelmi szabályzatot és a vonatkozó jogszabályokat betartva. Ez a funkció bármikor kikapcsolható.

A jelen Szerződés értelmében szükség van az olyan adatok gyűjtésére, feldolgozására és tárolására, amelyek lehetővé teszik a Gyártónak az Ön beazonosítását az Adatvédelmi szabályzatnak megfelelő módon. Ön elfogadja, hogy a Gyártó saját eszközeinek segítségével ellenőrizheti, hogy Ön a jelen Szerződés előírásainak megfelelően használja-e a Szoftvert. Ön elfogadja azt is, hogy a jelen Szerződés értelmében szükség van az Ön adatainak átvitelére a Szoftver és a Gyártó számítógépes rendszerei, illetve a Gyártó forgalmazói és támogatási hálózatának részét képező üzleti partnerei által működtetett számítógépes rendszerek között folyó kommunikáció során a Szoftver működésének biztosításához, a Szoftver használatához szükséges engedélyezés, valamint a Gyártó jogainak védelme érdekében.

A Szerződés megkötését követően a Gyártó, illetve a Gyártó forgalmazói és támogatási hálózatának részét képező üzleti partnerei jogosult az Önt azonosító alapvető adatok átadására, feldolgozására és tárolására számlázási célból, a jelen Szerződés végrehajtása érdekében, valamint azért, hogy az értesítések továbbíthatók legyenek az Ön Számítógépére.

Az adatvédelemről, a személyes adatok védelméről és az Önt mint adatalanyt megillető jogokról az Adatvédelmi szabályzat tartalmaz részletes információkat, amely a Gyártó webhelyén található, és közvetlenül a telepítési eljárás során érhető el. A szoftver súgójában is talál erről információkat.

5. **A Végfelhasználó jogainak gyakorlása**. Ön a Végfelhasználó jogait kizárólag személyesen vagy alkalmazottjai útján gyakorolhatja. Végfelhasználóként a Szoftvert csak a saját tevékenységének biztosítására és csak azon Számítógépek vagy számítógépes rendszerek védelmére használhatja fel, amelyekre vonatkozóan a Licencet megszerezte.

6. **A jogok korlátozása.** A Szoftvert nem másolhatja, nem terjesztheti, nem nyerheti ki az összetevőit, és nem készíthet belőle semmilyen származtatott tartalmat. A Szoftver használatakor az alábbi korlátozásokat kell

betartania:

a) Biztonsági másolatként készíthet a Szoftverről egy másolatot tartós adattárolásra alkalmas adathordozón, feltéve, hogy a biztonsági másolatot később más számítógépen nem telepíti vagy nem használja. A Szoftver bármilyen, ettől eltérő módon történő másolása a jelen Szerződés megszegését jelenti.

b) Ön a jelen Szerződésben kifejezetten megengedett eseteken kívül nem jogosult a szoftvert és annak másolatait használni, módosítani, lefordítani, többszörözni és a használati jogát átruházni.

c) Ön a Szoftvert nem értékesítheti, használatát nem adhatja tovább, nem adhatja sem bérbe, sem kölcsön más személynek, illetve nem veheti bérbe más személytől, és nem használhatja kereskedelmi szolgáltatások nyújtásához.

d) Ön a Szoftvert nem jogosult visszafordítani, visszafejteni, vagy egyéb módon megkísérelni a Szoftver forráskódjának megszerzését, azon eseteket kivéve, melyek körében az e rendelkezés által előírt korlátozást a törvény kifejezetten tiltja.

e) Ön elfogadja, hogy a Szoftvert kizárólag olyan módon használja fel, amely megfelel az alkalmazandó jogszabályok előírásainak, amelyek alapján a Szoftvert használja, ideértve kivétel nélkül a szerzői jogról szóló törvényben és az egyéb szellemi alkotásokra vonatkozó jogszabályokban található korlátozásokat is.

f) Elfogadja, hogy a Szoftvert és annak funkcióit csak úgy használhatja, hogy azzal más Végfelhasználókat nem korlátoz e szolgáltatások elérésében. A Gyártó fenntartja magának a jogot az egyes Végfelhasználóknak nyújtott szolgáltatások hatókörének korlátozására annak érdekében, hogy a szolgáltatások használatát a lehető legnagyobb számú Végfelhasználó számára biztosíthassa. A szolgáltatások hatókörének korlátozása azt is magában foglalja, hogy a Gyártó teljes mértékben megakadályozhatja a Szoftver bármely funkciójának használatát, és törölheti a Szoftver egy adott funkciójával kapcsolatos Adatokat és információkat a Gyártó vagy harmadik fél által üzemeltetett szerverekről.

g) Ön beleegyezik abba, hogy nem folytat semmiféle olyan tevékenységet a Licenckulccsal kapcsolatban, amely megszegné a jelen Szerződés feltételeit, illetve amelynek következtében olyan személy kapná meg a Licenckulcsot, aki nem jogosult a Szoftver használatára. Ilyen tevékenység például a használt vagy nem használt Licenckulcs bármilyen formában való átadása, engedély nélküli másolása, megkettőzött vagy generált Licenkulcsok továbbadása, illetve a Szoftver használata olyan Licenkulccsal, amely nem a Gyártótól származik.

7. **Szerzői jogok**. A Szoftver és minden jogosultság, beleértve korlátozás nélkül a benne foglalt jogcímeket és szellemi tulajdonjogot, az ESET és/vagy a Licencet adó partnerei tulajdonát képezik. E jogokat a vonatkozó nemzetközi egyezmények rendelkezései és a használat helye szerinti ország alkalmazandó nemzeti jogszabályai védik. A Szoftver szerkezete, felépítése és kódja az ESET és/vagy a Licencet adó partnerei üzleti titkának és bizalmas információinak minősül. A 6(a) pontban foglalt esetet kivéve tilos a Szoftver másolása. A jelen Szerződés szerint másolt példányoknak is minden esetben tartalmazniuk kell a Szoftverrel megegyező szerzői jogokra és egyéb jogcímekre vonatkozó értesítéseket. Ha visszafordítja, visszafejti, vagy egyéb módon megkísérli a Szoftver forráskódjának megszerzését a jelen Szerződés rendelkezéseinek megszegésével, az úgy tekintendő, hogy az ezúton szerzett összes információ létrejöttének pillanatában automatikusan és visszavonhatatlanul a Gyártóra átruházza azt, a Gyártónak a jelen Szerződés megsértésével kapcsolatos jogaival együtt.

8. **Fenntartott jogok**. A Gyártó fenntartja magának a Szoftverre vonatkozó összes jogot, azokat kivéve, amelyeket Ön a Szoftver Végfelhasználójaként a jelen Szerződés keretei között gyakorolhat.

9. **Többnyelvű verzió, több adathordozón biztosított szoftver, több másolat**. Ha a Szoftver több platformot vagy nyelvet támogat, vagy ha Ön több példánnyal rendelkezik, a Szoftvert csak annyi számítógéprendszeren és azokkal a verziókkal használhatja, amelyekre a Licencet megszerezte. Ön nem jogosult a Szoftver nem használt verzióit vagy példányait értékesíteni, bérbe adni, haszonbérbe adni vagy a használatát továbbadni, kölcsönadni, illetve

más személyre átruházni.

10. **A Szerződés hatálybalépése és megszűnése.** A jelen Szerződés attól a dátumtól érvényes, amikor Ön elfogadja a Szerződés feltételeit. Ön a Szerződést bármikor megszüntetheti a Szoftver, az összes biztonsági másolat és a gyártótól vagy üzleti partnereitől kapott kapcsolódó anyag végleges törlésével, megsemmisítésével vagy a saját költségen történő visszaküldésével. A Szoftver és bármely funkciójának használatára vonatkozó jog az EOL szabályzat hatálya alá tartozhat. Miután a Szoftver vagy bármely funkciója eléri az EOL szabályzatban meghatározott Életciklus végét, megszűnik a Szoftver használatára vonatkozó joga. A Szerződés megszűnésének módjától függetlenül a 7., 8., 11., 13., 19. és 21. pontban foglalt rendelkezések korlátlan ideig érvényben maradnak.

11. **VÉGFELHASZNÁLÓI JOGNYILATKOZATOK**. VÉGFELHASZNÁLÓKÉNT ÖN TUDOMÁSUL VESZI, HOGY A SZOFTVERT ANNAK „ADOTT ÁLLAPOTÁBAN”, MINDENFÉLE KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁS NÉLKÜL KAPJA, AZZAL, HOGY AZ ALKALMAZANDÓ JOGSZABÁLYOK ÁLTAL MEGENGEDETT MÉRTÉKIG SEM A GYÁRTÓ, A LICENCET ADÓ PARTNEREI VAGY LEÁNYVÁLLALATAI, SEM A SZERZŐI JOGOK JOGOSULTJAI NEM VÁLLALNAK KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁST, KÜLÖNÖSKÉPPEN, DE NEM KIZÁRÓLAGOSAN ADÁSVÉTELHEZ KAPCSOLÓDÓ JÓTÁLLÁST, MEGHATÁROZOTT CÉLRA VALÓ ALKALMASSÁGOT, VALAMINT ARRA VONATKOZÓ JOGSZAVATOSSÁGOT, HOGY A SZOFTVER NEM SÉRTI HARMADIK SZEMÉLYEK SZABADALMI, SZERZŐI, VÉDJEGYRE VONATKOZÓ VAGY EGYÉB JOGAIT. SEM A GYÁRTÓ, SEM MÁS FÉL NEM VÁLLAL JÓTÁLLÁST AZÉRT, HOGY A SZOFTVERBEN TALÁLHATÓ FUNKCIÓK MEGFELELNEK AZ ÖN ELVÁRÁSAINAK, ILLETVE HOGY A SZOFTVER MŰKÖDÉSE ZAVARTALAN ÉS HIBAMENTES LESZ. A KÍVÁNT EREDMÉNY MEGVALÓSÍTÁSÁRA ALKALMAS SZOFTVER KIVÁLASZTÁSA, TELEPÍTÉSE ÉS HASZNÁLATA, ILLETVE A SZOFTVERREL ÖN ÁLTAL ELÉRT EREDMÉNY TELJES MÉRTÉKBEN AZ ÖN FELELŐSSÉGE ÉS KOCKÁZATA.

12. **További kötelezettségvállalás kizárása**. A jelen Szerződés a benne kifejezetten felsoroltakon kívül a Gyártóra és a Licencet adó partnereire nem ró további kötelezettségeket.

13. **KORLÁTOZOTT FELELŐSSÉGVÁLLALÁS**. AZ ALKALMAZANDÓ JOGSZABÁLYOK ÁLTAL MEGENGEDETT MÉRTÉKIG A GYÁRTÓ, ILLETVE ALKALMAZOTTAI ÉS LICENCET ADÓ PARTNEREI SEMMILYEN ESETBEN SEM FELELŐSEK BÁRMIFÉLE BEVÉTEL- VAGY NYERESÉGKIESÉSÉRT, MEGHIÚSULT ÉRTÉKESÍTÉSI LEHETŐSÉGÉRT, ADATVESZTÉSÉRT, HELYETTESÍTŐ TERMÉKEK VAGY SZOLGÁLTATÁSOK BESZERZÉSÉBŐL FAKADÓ KÖLTSÉGEKÉRT, TULAJDONBAN BEKÖVETKEZETT VAGY SZEMÉLYT ÉRINTŐ KÁRÉRT, ÜZLETI FORGALOM KIESÉSÉÉRT, ÜZLETI INFORMÁCIÓ ELVESZTÉSÉRT VAGY BÁRMIFÉLE SPECIÁLIS, KÖZVETLEN, KÖZVETETT, ESETI, GAZDASÁGI, FEDEZETI, BÜNTETŐJOGI VAGY KÖVETKEZMÉNYKÁRÉRT, FÜGGETLENÜL A KÁROKOZÁS MIKÉNTJÉTŐL, ÉS ATTÓL, HOGY AZ SZERZŐDÉSBŐL, SZÁNDÉKOS KÁROKOZÁSBÓL, GONDATLANSÁGBÓL, VAGY MÁS, FELELŐSSÉGET MEGALAPOZÓ TÉNYBŐL ERED, HA EZEK A SZOFTVER TELEPÍTÉSÉNEK, A HASZNÁLATÁNAK VAGY HASZNÁLHATATLANSÁGÁNAK OKÁN MERÜLTEK FEL, MÉG ABBAN AZ ESETBEN IS, HA A GYÁRTÓT VAGY A LICENCET ADÓ PARTNEREIT, ILLETVE LEÁNYVÁLLALATAIT ELŐZŐLEG ÉRTESÍTETTÉK AZ ILYEN KÁR BEKÖVETKEZTÉNEK LEHETŐSÉGÉRŐL. MIVEL EGYES ORSZÁGOK ÉS JOGSZABÁLYOK NEM TESZIK LEHETŐVÉ A FELELŐSSÉG KIZÁRÁSÁT, A KORLÁTOZÁSÁT VISZONT IGEN, A GYÁRTÓ, ANNAK ALKALMAZOTTAI ÉS A LICENCET ADÓ PARTNEREI, ILLETVE LEÁNYVÁLLALATAI FELELŐSSÉGE A LICENCÉRT FIZETETT DÍJ MÉRTÉKÉRE KORLÁTOZÓDIK.

14. A jelen Szerződés egyetlen rendelkezése sem érinti annak a félnek a jogait, aki a jogszabályok értelmében fogyasztónak minősül.

15. **Terméktámogatás**. Az ESET vagy az ESET által meghatalmazott harmadik felek jótállás vagy jognyilatkozatok nélkül, saját döntésüknek megfelelően terméktámogatást nyújtanak. Nem biztosítunk terméktámogatást, miután a Szoftver vagy bármely funkciója elérte az EOL szabályzatban meghatározott Életciklus végét. A terméktámogatás előkészületeként a Végfelhasználónak biztonsági másolatot kell készítenie az összes meglévő adatról, szoftverről és a program összetevőiről. Az ESET vagy/és az ESET által meghatalmazott harmadik felek nem vállalnak felelősséget az adatok, a tulajdon, a szoftver vagy a hardver terméktámogatás következtében keletkező sérüléséért vagy elvesztéséért, illetve a veszteség miatt. Az ESET vagy/és az ESET által meghatalmazott harmadik

felek fenntartják a jogot, hogy eldönthessék, miszerint a probléma megoldása túllépi-e a terméktámogatás hatáskörét. Az ESET fenntartja a jogot, hogy saját hatáskörében elutasítsa, felfüggessze vagy befejezze a terméktámogatás nyújtását. Technikai terméktámogatás céljából szükség lehet Licencadatokra, Adatokra és egyéb adatokra az Adatvédelmi szabályzatnak megfelelően.

16. **A licenc átadása.** A szoftver egyik számítógéprendszerről átvihető egy másikra, feltéve ha az nem ellentétes a Szerződés feltételeivel. Ha nem ütközik a Szerződés feltételeivel, a Végfelhasználó csak a Gyártó jóváhagyásával jogosult véglegesen átadni a Licencet és a jelen Szerződésből fakadó minden jogosultságot másik Végfelhasználónak azzal a feltétellel, hogy (i) az eredeti Végfelhasználó nem tartja meg a Szoftver egyetlen másolatát sem; (ii) a jogosultságok átadása közvetlen, vagyis az eredeti Végfelhasználóról az új Végfelhasználóra történik; (iii) az új Végfelhasználónak vállalnia kell a jelen Szerződés szerint az eredeti Végfelhasználót érintő minden jogosultságot és kötelezettséget; (iv) az eredeti Végfelhasználónak át kell adnia az új Végfelhasználó részére a Szoftver eredetiségének ellenőrzését lehetővé tevő összes dokumentációt a 17. pontban leírtak szerint.

17. **A Szoftver eredetiségének ellenőrzése.** A Végfelhasználó a Szoftver használatára vonatkozó jogosultságát az alábbi módok valamelyikén igazolhatja: (i) a Gyártó vagy a Gyártó által kinevezett harmadik fél által kibocsátott licenctanúsítvánnyal; (ii) írásbeli licencszerződéssel, amennyiben készült ilyen szerződés; (iii) a Gyártó által e-mailben küldött licencadatokkal (felhasználónév és jelszó). A Szoftver eredetiségének ellenőrzése céljából szükség lehet Licencadatokra és a Végfelhasználó személyazonosítására alkalmas adatokra az Adatvédelmi szabályzatnak megfelelően.

18. **Licencek adása hatóságok és az Amerikai Egyesült Államok kormánya számára.** A Szoftver a jelen Szerződésben rögzített licencjogosultságokkal és korlátozásokkal biztosítható a hatóságok, többek között az Amerika Egyesült Államok kormánya számára.

19. **A kereskedelmi felügyeleti törvények betartása**.

a) Ön vállalja, hogy nem fogja közvetve vagy közvetlenül exportálni, újraexportálni, továbbítani vagy más módon elérhetővé tenni a Szoftvert, nem fogja semmilyen módon használni, illetve nem vesz részt olyan tevékenységben, amelynek következtében az ESET vagy holdingtársaságai, leányvállalatai és holdingtársaságainak leányvállalatai, valamint a holdingtársaságai által irányított jogalanyok („Társult vállalatok”) megsértenének kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük. Kereskedelmi felügyeleti törvénynek minősül

i. minden olyan törvény, amely szabályozást, korlátozást, illetve licencelési követelményeket szab meg áruk, szoftverek, technológiai termékek, illetve szolgáltatások exportálásának, újraexportálásának vagy továbbításának vonatkozásában, és amelyet az Amerikai Egyesült Államok, Szingapúr, az Egyesült Királyság, az Európai Unió vagy bármely tagállama, illetve bármely olyan ország kormányzata, állami vagy szabályozó hatósága rendelt vagy fogadott el, ahol a Szerződés értelmében kötelezettségeket kell végrehajtani, illetve ahol az ESET vagy bármely társult vállalata be van jegyezve vagy működik, valamint

ii. minden olyan gazdasági, pénzügyi, kereskedelmi vagy egyéb jellegű szankció, korlátozás, embargó, importálási vagy exportálási tilalom, tiltás források vagy eszközök továbbításának vagy szolgáltatások nyújtásának vonatkozásában, illetve ezekkel egyenértékű intézkedés, amelyet az Amerikai Egyesült Államok, Szingapúr, az Egyesült Királyság, az Európai Unió vagy bármely tagállama, illetve bármely olyan ország kormányzata, állami vagy szabályozó hatósága rendelt vagy fogadott el, ahol a Szerződés értelmében kötelezettségeket kell végrehajtani, illetve ahol az ESET vagy bármely társult vállalata be van jegyezve vagy működik.

(a fenti i. és ii. pontban említett jogi aktusok együttesen „Kereskedelmi szabályozási törvények”).

b) Az ESET jogában áll azonnali hatállyal felfüggeszteni vagy felmondani a jelen Feltételek szerinti kötelezettségeit abban az esetben, ha:

i. Az ESET – észszerű feltételezés révén – megállapítja, hogy a Felhasználó megsértette vagy nagy valószínűséggel megsértette a Szerződés 19 a) cikkelyét; illetve

ii. a Végfelhasználó, illetve a Szoftver kereskedelmi felügyeleti törvények hatálya alá esik, és ennek eredményeképpen az ESET – észszerű feltételezés révén – megállapítja, hogy a Szerződés szerinti kötelezettségeinek további teljesítése következtében az ESET vagy Társult vállalatai megsérthetnek kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük.

c) A Szerződés egyik rendelkezése sem azzal a szándékkal jött létre és nem értelmezhető úgy, hogy bármely felet ráveszi vagy kötelezi a vonatkozó kereskedelmi felügyeleti törvényekkel össze nem egyeztethető vagy azok értelmében büntetendő vagy tiltott cselekedek végrehajtására vagy bizonyos cselekedek mellőzésére (illetve arra, hogy beleegyezzenek ilyen cselekedek végrehajtásába vagy bizonyos cselekedek mellőzésébe).

20. **Értesítések**. Minden értesítést, a visszaküldendő Szoftvert és Dokumentációt a következő címre kell küldeni: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Az ESET fenntartja a jogot arra, hogy értesítse Önt a jelen Szerződés, az Adatvédelmi szabályzat, az EOL szabályzat és a Dokumentáció bármilyen módosításáról a Szerződés 22. cikkelye szerint. Az ESET küldhet Önnek e-maileket, alkalmazáson belüli értesítéseket a Szoftveren keresztül, illetve közzétehetünk közleményeket a webhelyünkön. Ön beleegyezik abba, hogy elektronikus formában jogi tájékoztatást fog kapni az ESET-től, beleértve a Feltételek, a Különleges feltételek vagy az Adatvédelmi irányelvek módosításával kapcsolatos értesítéseket, olyan szerződéses ajánlatokat/jóváhagyásokat vagy meghívásokat, amelyeket kezelnie kell, értesítéseket és egyéb jogi közleményeket. Az ilyen elektronikus kommunikációt írásban átvettnek kell tekinteni, kivéve akkor, ha a vonatkozó jogszabályok más kommunikációs formát írnak elő.

21. **Alkalmazandó jog**. A jelen Szerződésre a Szlovák Köztársaság törvénye az irányadó, és a szerződés a szerint értelmezendő. A Végfelhasználó és a Gyártó ezennel megállapodnak abban, hogy az alkalmazandó jog és az ENSZ által elfogadott „Nemzetközi árukereskedelmi szerződésekről szóló egyezmény” ütközése esetén az ütköző rendelkezések nem alkalmazhatók. A Gyártóval fennálló, illetve a Szoftver használatával kapcsolatos minden jogvita vagy követelés tekintetében Ön kifejezetten aláveti magát a Pozsonyi I. sz. Kerületi Bíróság kizárólagos joghatóságának, továbbá kifejezetten aláveti magát a nevezett bíróság illetékességének az ilyen jogviták rendezésében.

22. **Általános rendelkezések**. Amennyiben a jelen Szerződés bármely rendelkezése érvénytelen vagy kikényszeríthetetlen, az nem érinti a Szerződés többi részének érvényességét. A többi rendelkezés továbbra is érvényes és végrehajtható marad az itt lefektetett feltételek szerint. A jelen Szerződés angol nyelven íródott. Amennyiben a Szerződésről bármilyen fordítás készül kényelmi okokból vagy bármely más célból, illetve bármilyen ellentmondás van a jelen Szerződés különböző nyelvi változatai között, az angol változat az irányadó.

Az ESET fenntartja a jogot arra, hogy bármikor módosítsa a Szoftvert és felülvizsgálja a jelen Feltételek pontjait, a függelékeket, a mellékeleteket, az Adatvédelmi szabályzatot, az EOL szabályzatot és a dokumentációt, illetve azok bármely részét a releváns dokumentum frissítésével (i) a Szoftver vagy az ESET megváltozott üzleti eljárásainak megfelelően, (ii) törvényi, szabályozási vagy biztonsági okokból vagy (iii) a visszaélések vagy károk megakadályozása érdekében. A Szerződés módosításáról Ön minden esetben értesítést fog kapni e-mailben, alkalmazáson belüli értesítés útján vagy egyéb elektronikus úton. Ha nem ért egyet a Szerződés javasolt módosításaival, a 10. cikkely szerint felmondhatja a módosításról szóló értesítés kézhezvételétől számított 30 napon belül. Hacsak nem mondja fel a Szerződést ezen határidőn belül, a javasolt változtatások elfogadottnak tekinthetők és kötelezővé válnak Önre nézve attól a naptól kezdve, amikor az értesítést kézhez kapta a változásról.

Az Ön és a Gyártó között létrejött jelen Szerződés jelenti a Szoftverre vonatkozó teljes szerződést, és hatályon kívül helyezi a Szoftverre vonatkozóan tett minden korábbi jognyilatkozatot, megállapodást, kötelezettségvállalást, kommunikációt vagy hirdetést.

EULAID: EULA-PRODUCT-LG-MAC; 3537.0

Adatkezelési 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;
  - Összeomlási memóriaképek és a bennük található információk.

Más célból nem kívánunk adatokat gyűjteni, viszont néha lehetetlen ezt elkerülni. Előfordulhat, hogy maguk a kártevők tartalmaznak véletlenül begyűjtött adatokat (amelyek begyűjtéséről Önnek tudomása van, vagy azt jóváhagyta), illetve hogy fájlnevek vagy URL-címek részét képezik. Nem célunk, hogy az ilyen információk

rendszereink vagy folyamataink részét képezzék, illetve nem dolgozzuk fel őket a jelen Adatvédelmi szabályzatban leírtak szerint.

- Licencelési információkra, például licencazonosítóra és személyes adatokra – például név, vezetéknév, cím, e-mail-cím – szükséges számlázási célokra, a licenc eredetiségének ellenőrzéséhez, valamint a szolgáltatások biztosításához.
- Szervizelés, illetve segítségnyújtás biztosításához szükség lehet az Ön által leadott terméktámogatási kérelmekben foglalt elérhetőségekre és adatokra. Attól függően, hogy Ön milyen csatornát választ a velünk történő kapcsolatfelvételre, összegyűjthetjük az Ön e-mail-címét, telefonszámát, a licencelési információkat, a termékadatokat és a támogatási eset leírását. Egyéb információk megadására is megkérhetjük a terméktámogatás megkönnyítése céljából.

Az adatok bizalmas kezelése

Az ESET világszerte jelen van a kapcsolt vállalkozások, illetve partnerek révén, amelyek forgalmazói, szolgáltatói és terméktámogatási hálózatunk részét képezik. A kapcsolt vállalkozások és partnerek megkaphatják, illetve visszaküldhetik az ESET által feldolgozott információkat a Végfelhasználói licencszerződés teljesítése céljából, így például a szolgáltatások, a terméktámogatás és a számlázás biztosítása érdekében. Az Ön tartózkodási helye és a kiválasztott szolgáltatások alapján előfordulhat, hogy kötelességünk továbbítani az adatokat olyan országba, amely nem rendelkezik az Európai Bizottság megfelelőségi határozatával. Ilyen esetben is adatvédelmi jogszabályok szabályozzák az adatátvitelt, és csak szükség esetén kerül rá sor. Kivétel nélkül minden esetben általános szerződési feltételeket, kötelező erejű vállalati szabályokat vagy egyéb megfelelő védintézkedéseket kell alkalmazni.

Mindent megteszünk annak megakadályozása érdekében, hogy a szükségesnél hosszabb ideig történjen meg az adatok tárolása, amíg szolgáltatásokat nyújtunk a Végfelhasználói szoftverlicenc-szerződés szerint. A megőrzési időtartam hosszabb is lehet, mint az Ön licencének érvényessége, ami lehetőséget ad az egyszerű és kényelmes megújításra. Sor kerülhet a minimalizált és álnevesített statisztikai adatok, valamint az ESET LiveGrid® rendszerből származó egyéb adatok statisztikai célból történő további feldolgozására.

Az ESET megfelelő technikai és szervezeti intézkedésekkel biztosít a potenciális kockázatoknak megfelelő védelmi szintet. Mindent megteszünk azért, hogy a feldolgozó rendszerek és a szolgáltatások folyamatosan biztosítsák az adatok bizalmas kezelését, az integritást, a hozzáférhetőséget és a terhelhetőséget. Ha azonban sor kerül az adatok megsértésére, ami veszélyezteti az Ön jogait és szabadságát, készen állunk értesíteni a felügyeleti hatóságot és az érintetteket. Ön mint adatalany jogosult panaszt benyújtani egy felügyeleti hatósághoz.

Az adatalany jogai

Az ESET vállalatra a szlovák törvények az irányadók, és az Európai Unió tagjaként kötelességünk betartani az adatvédelmi rendelkezéseket. A vonatkozó adatvédelmi törvényekben rögzített feltételek szerint Önt adatalanyként a következő jogok illetik meg:

- jogosult kérelmezni a személyes adataihoz való hozzáférést az ESET vállalattól;
- jogosult személyes adatai helyesbítésére, ha azok pontatlanok (arra is jogosult, hogy kiegészítse a hiányos személyes adatokat);
- jogosult személyes adatai törlését kérelmezni;
- jogosult személyes adatai feldolgozásának korlátozását kérelmezni;
- jogosult tiltakozni az adatfeldolgozás ellen

- jogosult panaszt emelni; valamint
- joga van az adathordozhatósághoz.

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