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. 2023.03.19.

ESET Endpoint Antivirus for macOS

Az ESET Endpoint Antivirus for macOS 6 egy újszerű megoldást jelentő integrált biztonsági programcsomag. A ThreatSense® keresőmotor legújabb, kombinált verziója gyorsan 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 6 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 (korábbi nevén ESET Security Management Center) szoftverrel, együtt lehetővé teszi tetszőleges számú munkaállomás egyszerű kezelését, házirendek és szabályok alkalmazását, észlelések figyelését és bármely hálózati számítógép távoli felügyeletét.

A 6-os verzió újdonságai

Az ESET Endpoint Antivirus for macOS grafikus felhasználói felületét teljesen átalakítottuk annak érdekében, hogy könnyebben áttekinthető és egyszerűbben használható legyen. A 6-os verzióban bevezetett számos újítás közül néhány:

- ESET Enterprise Inspector – az ESET Endpoint Antivirus for macOS 6.9-es verziójától az ESET Endpoint Antivirus for macOS csatlakoztatható az ESET Enterprise Inspectorhoz. Az ESET Enterprise Inspector (EEI) 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 Enterprise Inspectorról, a telepítéséről és a funkcióiról bővebben az ESET Enterprise Inspector súgójában tájékozódhat.
- **64 bites architektúra támogatása**
- **Webhozzáférés-védelem** – A böngészők és a távoli szerverek közötti kommunikációt figyeli
- **E-mail védelem** – A POP3 és az IMAP protokollon keresztül érkező e-mailek ellenőrzését biztosítja
- **Adathalászat elleni védelem** – Megvédi Önt a jelszavak és más bizalmas adatok megszerzésére irányuló támadásoktól oly módon, hogy korlátozza a hozzáférést azokhoz a kártékony webhelyekhez, amelyek szabályszerű webhelyeknek adják ki magukat
- **Eszközfelügyelet** – Lehetővé teszi a kiterjesztett szűrők és/vagy engedélyek ellenőrzését, tiltását vagy módosítását, valamint annak megadását, hogy a felhasználó hogyan érhet el és használhat külső eszközöket. Ez a funkció a 6.1-es és újabb verziókban érhető el.
- **Bemutató üzemmód** – Lehetővé teszi az ESET Endpoint Antivirus for macOS futtatását a háttérben, és letiltja az előugró ablakokat és ütemezett feladatokat

- **Megosztott helyi gyorsítótár** – Lehetővé teszi az ellenőrzés sebességének javítását virtualizált környezetekben

Rendszerkövetelmények

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

	Rendszerkövetelmények:
Processzorarchitektúra	Intel 64-bit, Apple ARM 64 bites
Operációs rendszer	macOS 10.12 és újabb macOS Server 10.12 és újabb
Memória	300 MB
Szabad tárhely	200 MB

A meglévő Intel-támogatás mellett az ESET Endpoint Antivirus for macOS 6.10.900.0-s és újabb verziói támogatják az Apple ARM chipet is a Rosetta 2 segítségével

Az ESET PROTECT ismertetése

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

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

Az ESET PROTECT a következő összetevőkből áll:

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

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

- ESET Management Ügynök – Az ESET Management Ügynök megkönnyíti a kommunikációt az ESET PROTECT Szerver és kliensszámítógépek között. Az Ügynököt telepíteni kell a kliensszámítógépre annak érdekében, hogy létrejöjjön a kommunikáció a számítógép és az ESET PROTECT Szerver között. Mivel a kliensszámítógépen található, és több biztonsági forgatókönyvet tud tárolni, az ESET Management Ügynök használatakor sokkal

gyorsabban lehet reagálni az új kártevőkre. Az ESET PROTECT Webkonzol segítségével telepíthető az ESET Management Ügynök az Active Directory vagy az ESET RD-érzékelő által beazonosított felügyelet nélküli számítógépekre. Manuálisan is telepíthető az ESET Management Ügynök kliensszámítógépekre szükség esetén.

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

- Apache HTTP-proxy – Ez a szolgáltatás az ESET PROTECT rendszerrel együtt használható a következőkhöz:

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

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

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

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

- ESET PROTECT Virtual Agent Host – Az ESET PROTECT egyik összetevője, amely az ügynökök virtualizálásával lehetővé teszi az ügynök nélküli virtuális gépek felügyeletét. A megoldás révén lehetővé válik az automatizálás, a dinamikus csoportfelhasználás és az olyan szintű feladatkezelés, mint amit az ESET Management Ügynök nyújt a fizikai számítógépeken. A Virtuális ügynök összegyűjti az információk a virtuális gépekről, és elküldi őket az ESET PROTECT Szervernek.

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

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

- ESET Business Account – Az ESET üzleti termékek új licencelési portálja lehetővé teszi a licencek kezelését. A jelen dokumentum ESET Business Account című szakaszában találja meg a termék aktiválására vonatkozó útmutatót, vagy nézze meg az ESET Business Account Felhasználói útmutatójában az ESET Business Account használatára vonatkozó bővebb tudnivalókat. Ha már rendelkezik ESET által kiadott felhasználónévvel és jelszóval, amelyeket licenckulcsra szeretne konvertálni, olvassa el a Régi licencadatok konvertálása című szakaszt.

- ESET 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 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 online felhasználói útmutatójában talál.

Az ESET PROTECT CLOUD ismertetése

az ESET PROTECT CLOUD lehetővé teszi, hogy egyetlen központi helyről felügyeljen ESET-termékeket munkaállomásokon és szervereken hálózati környezetben anélkül, hogy szükség lenne fizikai vagy virtuális szerverre, mint az ESET PROTECT 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

Távoli telepítés

A telepítés előtt

macOS 10.15 és régebbi verziók

Azt javasoljuk, hogy az ESET Endpoint Antivirus for macOS macOS 10.13 vagy újabb rendszerre való telepítése előtt a célszámítógépeken engedélyezze az ESET-kernelbővítményeket, a macOS 10.14-es vagy újabb verziója esetén pedig a teljes lemezhozzáférést is. Ha a telepítés után engedélyezi ezeket a funkciókat, akkor a felhasználók a **Rendszerkiterjesztés letiltva** és **A számítógép részben védett** értesítést fogják kapni addig, amíg az ESET-kernelbővítményeket és a teljes lemezhozzáférést nem engedélyezi.

Az ESET-kernelbővítmények és a Teljes lemezhozzáférés távoli engedélyezéséhez regisztrálnia kell számítógépét egy MDM- (mobileszköz-felügyelet) szerveren, amilyen például a Jamf.

ESET-rendszerbővítmények engedélyezése

A kernelkiterjesztések távoli engedélyezése az eszközén:

- Ha a Jamf-et használja MDM-ként, olvassa el a kapcsolódó tudásbáziscikkünket.
- Ha egy másik MDM-szolgáltatást használ, töltse le a .plist konfigurációs fájlt. Hozzon létre két UUID-azonosítót egy tetszőleges UUID-generátorral, és egy szövegszerkesztővel cserélje le a karakterláncokat az `illessze be ide az UUID 1 azonosítóját` és az `illessze be ide az UUID 2 azonosítóját` szövegre a letöltött konfigurációs profilban. Telepítse központilag a .plist konfigurációs profilt tartalmazó fájlt az MDM-szerver segítségével. Regisztrálnia kell számítógépét az MDM-szerveren ahhoz, hogy telepíteni tudja a konfigurációs profilokat a számítógépekre.

Teljes lemezhozzáférés engedélyezése

A macOS 10.14 rendszerben **A számítógép részben védett** értesítést küldi az ESET Endpoint Antivirus for macOS a telepítés után. Az ESET Endpoint Antivirus for macOS összes funkciójának eléréséhez és az értesítés megjelenítésének megakadályozásához engedélyeznie kell a **teljes lemezhozzáférést** az ESET Endpoint Antivirus for macOS szolgáltatásnak a termék telepítése előtt. A **teljes lemezhozzáférés** távoli engedélyezése:

- Ha a Jamf-et használja MDM-ként, olvassa el a kapcsolódó tudásbáziscikkünket.
- Ha egy másik MDM-szolgáltatást használ, töltse le a .plist konfigurációs fájlt. Hozzon létre két UUID-

azonosítót egy tetszőleges UUID-generátorral, és egy szövegszerkesztővel cserélje le a karakterláncokat az `illessze be ide az UUID 1 azonosítóját` és az `illessze be ide az UUID 2 azonosítóját` szövegre a letöltött konfigurációs profilban. Telepítse központilag a .plist konfigurációs profilt tartalmazó fájlt az MDM-szerver segítségével. Regisztrálnia kell számítógépét az MDM-szerveren ahhoz, hogy telepíteni tudja a konfigurációs profilokat a számítógépekre.

macOS Big Sur (11)

Azt javasoljuk, hogy az ESET Endpoint Antivirus for macOS macOS Big Sur rendszerre való telepítése előtt a célszámítógépeken engedélyezze az ESET-rendszerbővítményeket és a Teljes lemezhozzáférést. Ha a telepítés után engedélyezi ezeket a funkciókat, akkor a felhasználók a **Rendszerkiterjesztés letiltva** és **A számítógép részben védett** értesítést fogják kapni addig, amíg az ESET-kernelbővítményeket és a Teljes lemezhozzáférést nem engedélyezi. A rendszerbővítmények csak az ESET Endpoint Antivirus for macOS telepítése előtt engedélyezhetők távolról.

Az ESET-rendszerbővítmények és a Teljes lemezhozzáférés távoli engedélyezéséhez regisztrálnia kell számítógépét egy MDM- (mobileszköz-felügyelet) szerveren, amilyen például a Jamf.

ESET-rendszerbővítmények engedélyezése

A rendszerbővítmények távoli engedélyezése az eszközén:

- Ha a Jamf-et használja MDM-ként, olvassa el a kapcsolódó tudásbáziscikkünket.
- Ha másik MDM-et használ, töltse le a .plist konfigurációs profilt. Telepítse a .plist konfigurációs profilfájlt az MDM-kiszolgáló segítségével. Regisztrálnia kell számítógépét az MDM-szerveren ahhoz, hogy telepíteni tudja a konfigurációs profilokat a számítógépekre. Saját konfigurációs profil létrehozásához használja az alábbi beállításokat:

Csapatazonosító (TeamID)	`P8DQRXPVLP`

Csomagazonosító (BundleID)	`com.eset.endpoint`
	`com.eset.network`
	`com.eset.firewall`
	`com.eset.devices`

Teljes lemezhozzáférés engedélyezése

Teljes lemezhozzáférés engedélyezése távolról:

- Ha a Jamf-et használja MDM-ként, olvassa el a kapcsolódó tudásbáziscikkünket.
- Ha egy másik MDM-szolgáltatást használ, töltse le a .plist konfigurációs fájlt. Telepítse a .plist konfigurációs profilfájlt az MDM-szerver segítségével. Regisztrálnia kell számítógépét az MDM-szerveren ahhoz, hogy telepíteni tudja a konfigurációs profilokat a számítógépekre. Saját konfigurációs profil létrehozásához használja az alábbi beállításokat:

ESET Endpoint Antivirus	
Azonosító	`com.eset.eea.6`
Azonosító típusa	`bundleID`

Kódkövetelmény	`identifier "com.eset.eea.6" 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 Endpoint Antivirus és ESET Endpoint Security	
Azonosító	`com.eset.devices`
Azonosító típusa	`bundleID`
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	`Allow`

ESET Endpoint Antivirus és ESET Endpoint Security	
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`

Telepítés

Telepítés előtt létrehozhat egy előre beállított ESET Endpoint Antivirus for macOS-konfigurációval rendelkező távoli telepítőcsomagot, amelyet később az ESET PROTECT vagy MDM használatával telepíthet.

- Hozzon létre egy távoli telepítőcsomagot.

Végezze el távolról az ESET Endpoint Antivirus for macOS telepítését úgy, hogy létrehoz egy **szoftvertelepítési feladatot** az ESET felügyeleti rendszer segítségével:

- Szoftvertelepítési feladat – ESET PROTECT
- Szoftvertelepítési feladat – ESET Security Management Center

Telepítés után

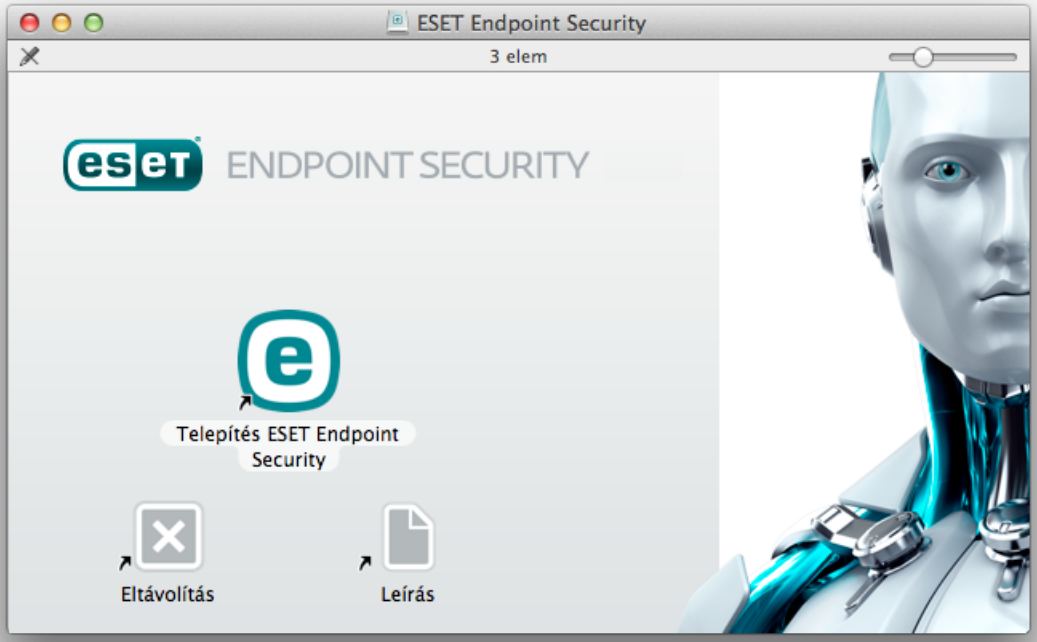
A felhasználók a következő értesítést fogják kapni: **Az „**ESET Endpoint Antivirus for macOS**” hálózati tartalmat szeretne szűrni**. Amikor a felhasználók megkapják az értesítést, kattintson az **Engedélyezés** gombra. Ha a **Tiltás** gombra kattint, a Webhozzáférés-védelem nem fog működni.

Távoli telepítőcsomag létrehozása

Telepítőcsomag létrehozása az Apple Remote Desktop telepítéséhez

1. Töltse le a szabványos telepítőcsomagot az ESET webhelyéről:
ESET Endpoint Antivirus for macOS

2. Az ESET Endpoint Antivirus for macOS telepítőjének elindításához kattintson duplán a letöltött fájlra.



1. Kattintson a **Telepítés**ESET Endpoint Antivirus for macOS gombra.

2. Amikor a rendszer kéri, az **Engedélyezés** gombra kattintva engedélyezze a telepítőnek annak meghatározását, hogy a szoftver telepíthető-e.

3. Kattintson a **Tovább** gombra. Ha távoli telepítőcsomagot hoz létre, a rendszer nem telepíti az ESET Endpoint Antivirus for macOS szolgáltatást.

4. Tekintse át a rendszerkövetelményeket, majd kattintson a **Folytatás** gombra.

5. Olvassa el az ESET szoftverlicenc-szerződését, majd – ha elfogadja – kattintson a **Folytatás** → **Elfogadom** gombra.

6. A **Telepítési mód** lépésnél válassza ki a **Távoli** lehetőséget.

7. Válassza ki a telepíteni kívánt termékösszetevőket. Alapértelmezés szerint mindegyik összetevő ki van jelölve. Kattintson a **Tovább** gombra.

8. A **Proxykiszolgáló** lépésnél válassza ki azt a beállítást, amely megfelel az internetkapcsolatnak. Ha nem tudja, melyik az, használja az alapértelmezett rendszerbeállításokat. Kattintson a **Tovább** gombra. Ha

proxykiszolgálót használ, a következő lépésnél meg kell adnia a proxycímet, a felhasználónevet és a jelszót.

9. Válassza ki, hogy ki módosíthassa a program konfigurációját. Csak kiváltságos felhasználók és csoportok módosíthatják. Alapértelmezés szerint a Rendszergazda csoport van kiválasztva kiváltságosként. Jelölje be az **Összes felhasználó megjelenítése** vagy az **Összes csoport megjelenítése** jelölőnégyzetet az összes virtuális felhasználó és csoport, például a programok és folyamatok megjelenítéséhez.

10. Engedélyezze az ESET LiveGrid szolgáltatást a célszámítógépen, ha ez releváns.

11. Engedélyezze a kéretlen alkalmazások észlelését a célszámítógépen, ha ez releváns.

12. Válasszon tűzfalmódot:
Automatikus üzemmód – Ez az alapértelmezett üzemmód. Ez az üzemmód azoknak a felhasználóknak ajánlott, akik a tűzfal egyszerű és kényelmes használatát részesítik előnyben, és nincs szükségük szabályok definiálására. Az automatikus üzemmód nem korlátozza az adott rendszer szokványos kimenő forgalmát, de letiltja a nem a hálózati oldalról kezdeményezett összes kapcsolatot. Ebben az üzemmódban egyéni szabályokat is megadhat.

Interaktív üzemmód – Ez az üzemmód lehetővé teszi a tűzfal egyéni konfigurációjának a kialakítását. Ha a program olyan kommunikációt észlel, amelyhez nincs szabály definiálva, egy párbeszédpanelen jelenti az ismeretlen kapcsolatot. A párbeszédpanelen engedélyezheti vagy letilthatja a kommunikációt, döntését pedig a tűzfal új szabályaként is mentheti. Ha új szabály létrehozása mellett dönt, a program a szabály alapján az összes hasonló típusú kommunikációt engedélyezi vagy letiltja a jövőben.

13. Mentse a telepítőfájlt a számítógépére. Ha korábban létrehozott már telepítési fájlt az alapértelmezett helyen, a folytatás előtt módosítania kell a célmappa helyét, vagy törölnie kell a korábbi fájlokat. Ezzel befejeződik a távoli telepítés első fázisa. A helyi telepítő kilép, majd távoli telepítési fájlokat hoz létre a kiválasztott célmappában.

A távoli telepítési fájlok a következők:

- *esets_setup.dat* – A telepítő Beállítások szakaszában megadott beállítási adatok
- *program_components.dat* – A kiválasztott programösszetevők beállítási adatai. (Ez a fájl nem kötelező. Akkor jön létre, ha úgy dönt, hogy nem telepít bizonyos ESET Endpoint Antivirus for macOS-összetevőket.)
- *esets_remote_install.pkg* – Távoli telepítőcsomag
- *esets_remote_uninstall.sh* – Távoli eltávolítási parancsfájl

Az Apple Remote Desktop telepítése

1. Nyissa meg az Apple Remote Desktop alkalmazást, és csatlakozzon a célszámítógéphez. További információt erről az Apple Remote Desktop dokumentációjában talál.

2. Másolja a következő fájlokat az Apple Remote Desktop **Fájlok vagy mappák másolása** funkciójának használatával a célszámítógép */tmp* mappájába:

Ha minden összetevőt telepít, másolja át a következőt:
– *esets_setup.dat*

Ha nem telepíti az összes termékösszetevőt, a következőket másolja át:
– *esets_setup.dat*

– *product_components.dat*

3. A **Csomagok telepítése** paranccsal telepítse a *esets_remote_install.pkg* fájlt a célszámítógépre.

Az Apple Remote Desktop távoli eltávolítása

1. Nyissa meg az Apple Remote Desktop alkalmazást, és csatlakozzon a célszámítógéphez. További információt erről az Apple Remote Desktop dokumentációjában talál.

2. Másolja az *esets_remote_uninstall.sh* parancsfájlt az Apple Remote Desktop **Fájlok vagy mappák másolása** funkciójának használatával a célszámítógép */tmp* mappájába.

3. Az Apple Remote Desktop alkalmazásban küldje a következő **UNIX-héjparancsot** a célszámítógépre:

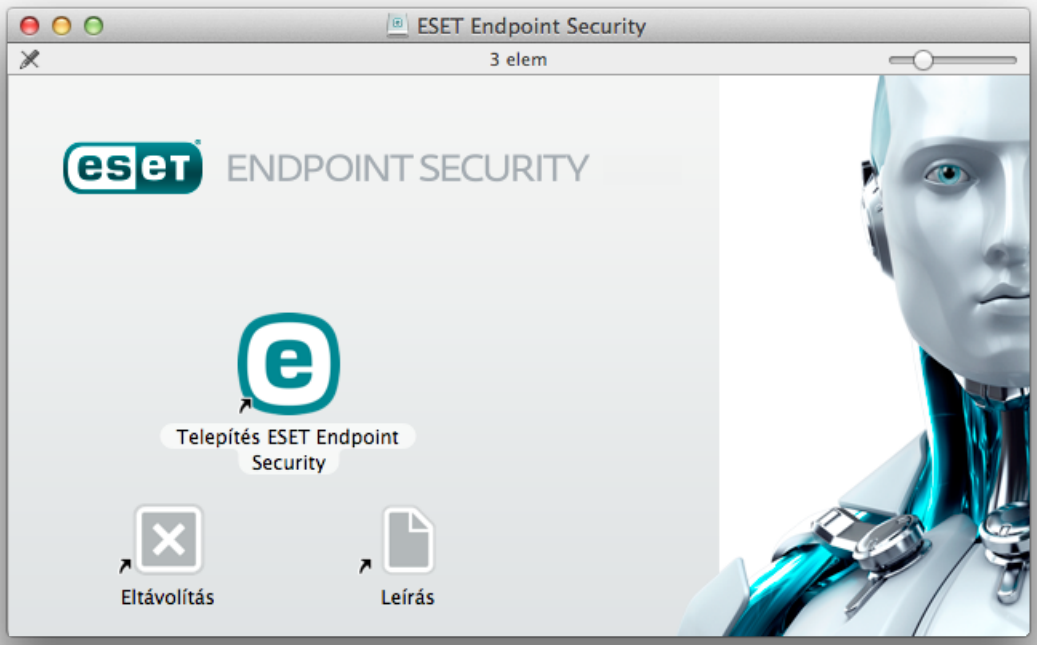
```
/tmp/esets_remote_uninstall.sh
```

Az eltávolítási folyamat befejeződése után a konzol megjelenik az Apple Remote Desktop alkalmazásban a célszámítógépen.

Telepítés

A telepítővarázsló végigvezeti az alapvető telepítési folyamaton. Részletes útmutatásért tekintse meg a telepítésről szóló tudásbáziscikkünket.

1. Az ESET Endpoint Antivirus for macOS telepítőjének elindításához kattintson duplán a letöltött fájlra.



1. A telepítés megkezdéséhez kattintson az ESET Endpoint Antivirus for macOS **telepítése** gombra.

Telepítés a .pkg fájlból
A macOS rendszerben az ESET-termékek telepítésekor és elindításakor internetelérés szükséges a Macen ahhoz, hogy engedélyezni lehessen az Apple-nek az ESET-kernelbővítmények hitelesítését.

2. Amikor a rendszer kéri, az **Engedélyezés** gombra kattintva engedélyezze a telepítőnek annak meghatározását, hogy a szoftver telepíthető-e.

3. Ha még nem tette meg, távolítsa el a meglévő biztonsági alkalmazásokat, például a vírusirtót, a kémprogramvédelmet vagy a tűzfalat a számítógépről. Ha nincs telepítve más biztonsági alkalmazás, kattintson a **Folytatás** gombra.

4. Tekintse át a rendszerkövetelményeket, majd kattintson a **Folytatás** gombra.

5. Olvassa el az ESET szoftverlicenc-szerződését, majd – ha elfogadja – kattintson a **Folytatás** → **Elfogadom** gombra.

6. Válassza ki a kívánt telepítési típust.

- Tipikus telepítés
- Egyéni telepítés
- Távoli telepítés

Verziófrissítés
A telepítés kezdeti szakaszában a telepítő automatikusan újabb termékverziót keres az interneten. Ha újabb verziót talál, felkínálja, hogy a telepítési folyamat folytatása előtt töltse le a legújabb verziót.

Tipikus telepítés

A tipikus telepítési mód a legtöbb felhasználónak megfelelő beállítási lehetőségeket tartalmaz. Ezek a beállítások maximális biztonságot nyújtanak kiváló rendszerteljesítmény mellett. A tipikus telepítés az alapértelmezett beállítás, amely azoknak ajánlott, akiknek nincsenek különleges követelményeik az adott beállítások esetén.

1. Az **ESET LiveGrid** ablakban válassza ki a kívánt beállítást, majd kattintson a **Folytatás** gombra. Ha később módosítani szeretné a beállítást, a **LiveGrid beállításaiban** ezt megteheti. Az ESET Live Gridről a Szószedetben talál további információkat.
2. A **Kéretlen alkalmazások** ablakban válassza ki a kívánt beállítást (lásd: Mit nevezünk kéretlen alkalmazásnak?), majd kattintson a **Folytatás** gombra. Ha később módosítani szeretné a beállítást, használja a **További beállítások** szakaszt.

3. Kattintson a **Telepítés** gombra. Ha a rendszer felszólítja a macOS-jelszó megadására, írja be, majd kattintson a **Szoftver telepítése** gombra.

Az ESET Endpoint Antivirus for macOS telepítése után:

macOS Big Sur (11)

1. Engedélyezze a rendszerbővítményeket.

2. Engedélyezze a Teljes lemezhozzáférést.

3. Engedélyezze az ESET számára proxykonfigurációk hozzáadását. A következő értesítést fogja kapni: **Az „**ESET Endpoint Antivirus for macOS**” hálózati tartalmat szeretne szűrni**. Amikor megkapja ezt az értesítést, kattintson a **Engedélyezés** gombra. Ha a **Tiltás** gombra kattint, a Webhozzáférés-védelem nem fog működni.

macOS 10.15 és régebbi verziók

1. A macOS 10.13-as vagy újabb verziójában a **Rendszerkiterjesztés letiltva** értesítést küldi a rendszer, az ESET Endpoint Antivirus for macOS pedig **A számítógép nem áll védelem alatt** értesítést jeleníti meg. Az ESET Endpoint Antivirus for macOS összes funkciójának használatbavételéhez engedélyeznie kell a kernelbővítményeket a készüléken. A kernelbővítmények engedélyezéséhez lépjen a **Rendszerbeállítások** > **Biztonság és adatvédelem** lapra, majd kattintson az **Engedélyezés** elemre az **ESET, spol. s.r.o. fejlesztőtől származó rendszerszoftverek engedélyezéséhez** Bővebb információkért tekintse meg tudásbáziscikkünket.

2. A macOS 10.14-es és újabb verziójában **A számítógép részben védett** értesítést küldi az ESET Endpoint Antivirus for macOS. Az ESET Endpoint Antivirus for macOS összes funkciójának használatbavételéhez engedélyeznie kell a **Teljes hozzáférés a lemezhez** funkció az ESET Endpoint Antivirus for macOS számára. Nyissa meg a **Rendszerbeállítások** > **Biztonság és adatvédelem** ablakot. Lépjen az **Adatvédelem** lapra, majd jelölje be a **Teljes hozzáférés a lemezhez** jelölőnégyzetet. A lakatot ábrázoló ikonra kattintva engedélyezze a szerkesztést. Kattintson a plusz ikonra, majd válassza ki az ESET Endpoint Antivirus for macOS alkalmazást. A számítógép ezután felszólítja az újraindításra. Kattintson a **Később** elemre. Egyelőre ne indítsa újra a számítógépet. Kattintson az **Újrakezdés** elemre az ESET Endpoint Antivirus for macOS értesítési ablakában, vagy indítsa újra a számítógépet. Bővebb információkért tekintse meg tudásbáziscikkünket.

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

Egyéni telepítés

Az egyéni telepítési mód tapasztalt felhasználóknak készült, akik a telepítés során módosítani szeretnék a további beállításokat.

- **Programösszetevők**
  Az ESET Endpoint Antivirus for macOS lehetővé teszi a termék telepítését egyes alapösszetevői (például a Web- és e-mail védelem) nélkül. Ha el szeretne távolítani a telepítésből egy összetevőt, törölje a neve mellett lévő jelölőnégyzet bejelölését.

- **Proxyszerver**
  Ha proxyszervert használ, válassza ki a **Proxyszervert használok** beállítást a paraméterek megadásához. A következő ablakban írja be a proxyszerver IP- vagy URL-címét a **Cím** mezőbe. A Port mezőben adja meg azt a portot, amelyen a proxyszerver fogadja a kapcsolatokat (alapértelmezés szerint a 3128-as). Hitelesítést kérő proxyszerver esetén be kell írnia egy érvényes **felhasználónevet** és **jelszót**, mert csak így lesz jogosult a szerver használatára. Ha nem használ proxyszervert, a **Nem használok proxyszervert** opciót jelölje be. Ha nem biztos abban, hogy proxyszervert használ-e, a **Rendszerbeállítások használata (javasolt)** opciót bejelölve használhatja az aktuális rendszerbeállításokat.

• **Jogosultságok**
A következő lépésben meghatározhatja a jogosult felhasználókat vagy csoportokat, akik módosíthatják a programbeállításokat. A bal oldali felhasználólistából jelölje ki a felhasználókat, és **adja hozzá** őket a **Jogosult felhasználók** listájához. Az összes felhasználó megjelenítéséhez válassza ki **Az összes felhasználó megjelenítése** beállítást. Ha üresen hagyja a Jogosult felhasználók listáját, az összes felhasználó jogosultnak tekintendő.

• **ESET LiveGrid®**
Az ESET Live Gridről a Szószedetben talál további információkat.

• **Kéretlen alkalmazások**
A kéretlen alkalmazásokról a Szószedetben talál további információkat.

Az ESET Endpoint Antivirus for macOS telepítése után:

macOS Big Sur (11)

1. Engedélyezze a rendszerbővítményeket.

2. Engedélyezze a Teljes lemezhozzáférést.

3. Engedélyezze az ESET számára proxykonfigurációk hozzáadását. A következő értesítést fogja kapni: **Az „**ESET Endpoint Antivirus for macOS**” hálózati tartalmat szeretne szűrni**. Amikor megkapja ezt az értesítést, kattintson a **Engedélyezés** gombra. Ha a **Tiltás** gombra kattint, a Webhozzáférés-védelem nem fog működni.

macOS 10.15 és régebbi verziók

1. A macOS 10.13-as és újabb vagy újabb verziójában a **Rendszerkiterjesztés letiltva** értesítést küldi a rendszer, az ESET Endpoint Antivirus for macOS pedig **A számítógép nem áll védelem alatt** értesítést jeleníti meg. Az ESET Endpoint Antivirus for macOS összes funkciójának használatbavételéhez engedélyeznie kell a kernelbővítményeket a készüléken. A kernelbővítmények engedélyezéséhez lépjen a **Rendszerbeállítások** > **Biztonság és adatvédelem** lapra, majd kattintson az **Engedélyezés** elemre az **ESET, spol. s.r.o. fejlesztőtől származó rendszerszoftverek engedélyezéséhez** Bővebb információkért tekintse meg tudásbáziscikkünket.

2. A macOS 10.14-es és újabb verziójában **A számítógép részben védett** értesítést küldi az ESET Endpoint Antivirus for macOS. Az ESET Endpoint Antivirus for macOS összes funkciójának használatbavételéhez engedélyeznie kell a **Teljes hozzáférés a lemezhez** funkció az ESET Endpoint Antivirus for macOS számára. Nyissa meg a **Rendszerbeállítások** > **Biztonság és adatvédelem** ablakot. Lépjen az **Adatvédelem** lapra, majd jelölje be a **Teljes hozzáférés a lemezhez** jelölőnégyzetet. A lakatot ábrázoló ikonra kattintva engedélyezze a szerkesztést. Kattintson a plusz ikonra, majd válassza ki az ESET Endpoint Antivirus for macOS alkalmazást. A számítógép ezután felszólítja az újraindításra. Kattintson a **Később** elemre. Egyelőre ne indítsa újra a számítógépet. Kattintson az **Újrakezdés** elemre az ESET Endpoint Antivirus for macOS értesítési ablakában, vagy indítsa újra a számítógépet. Bővebb információkért tekintse meg tudásbáziscikkünket.

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

Rendszerbővítmények engedélyezése helyileg

A macOS 11-ben (Big Sur) a kernelkiterjesztéseket rendszerbővítmények váltották fel. Ezekhez a felhasználó jóváhagyása szükséges az új, harmadik féltől származó rendszerbővítmények betöltése előtt.

Az ESET Endpoint Antivirus for macOS macOS Big Sur (11) vagy újabb rendszerre való telepítése után a Rendszerkiterjesztés letiltva értesítést küldi a rendszer, az ESET Endpoint Antivirus for macOS pedig A számítógép nem áll védelem alatt értesítést jeleníti meg. Az ESET Endpoint Antivirus for macOS összes funkciójának eléréséhez engedélyeznie kell a rendszerbővítményeket az eszközén.

Frissítsen az előző macOS-verzióról a Big Surre.
Ha már elvégezte az ESET Endpoint Antivirus for macOS telepítését, és frissíteni fog a macOS Big Sur rendszerre, a frissítés után manuálisan engedélyeznie kell az ESET-kernelbővítményeket. Az ügyfélszámítógéphez fizikai hozzáférés szükséges – ha távolról éri el, az Engedélyezés gomb le van tiltva.

Amikor az ESET-termék telepítését végzi a macOS Big Sur vagy újabb rendszerre, manuálisan kell engedélyeznie az ESET-rendszerbővítményeket. Az ügyfélszámítógéphez fizikai hozzáférés szükséges – ha távolról éri el, az Engedélyezés gomb le van tiltva.

Rendszerbővítmények manuális engedélyezése

1. Kattintson **A Rendszerbeállítások megnyitása** elemre vagy a **Biztonsági beállítások megnyitása** elemre az egyik riasztási párbeszédablakban.

2. A bal alsó sarokban lévő lakatra kattintva engedélyezze a módosításokat a beállítási ablakban.

3. Használja a Touch ID-t, vagy kattintson a **Jelszó használata** gombra, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.

4. Kattintson a **Részletek** elemre.

5. Válassza ki mindhárom ESET Endpoint Antivirus for macOS**.app** lehetőséget.

6. Kattintson az **OK** gombra.

Részletes útmutatót ehhez a tudásbáziscikkünkben talál. (A tudásbáziscikkek nem minden nyelven érhetők el.)

Teljes lemezhozzáférés engedélyezése helyileg

A macOS 10.14 rendszerben **A számítógép részben védett** értesítést küldi az ESET Endpoint Antivirus for macOS. Az ESET Endpoint Antivirus for macOS összes funkciójának eléréséhez engedélyeznie kell a **Teljes lemez hozzáférést** az ESET Endpoint Antivirus for macOS számára.

1. Kattintson **A Rendszerbeállítások megnyitása** szövegre a riasztási párbeszédpanelen.

2. A bal alsó sarokban található lakatra kattintva engedélyezze a módosításokat a beállítási ablakban.

3. Használja a Touch ID-t, vagy kattintson a **Jelszó használata** gombra, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.

4. Válassza ki az ESET Endpoint Antivirus for macOS**.app** elemet a listában.

5. Ekkor megjelenik az ESET Endpoint Antivirus for macOS újraindítását lehetővé tevő értesítés. Kattintson a Később gombra.

6. Válassza ki az ESET **Valós idejű fájlrendszer-védelem** elemet a listában.

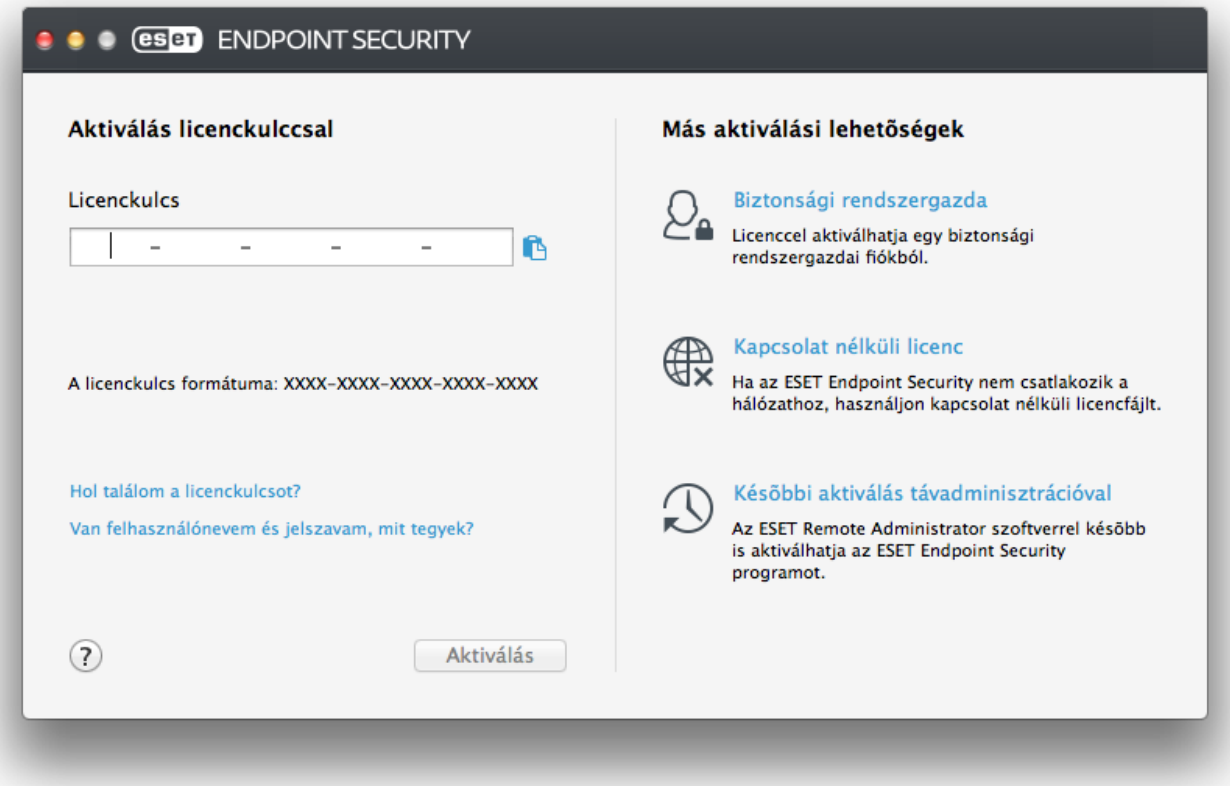
> **Az ESET Valós idejű fájlrendszer-védelem nem található meg**
> Ha a **Valós idejű fájlrendszer-védelem** lehetőség nem szerepel a listában, engedélyeznie kell az ESET-termék rendszerbővítményeit.

7. Kattintson az Újrakezdés gombra az ESET Endpoint Antivirus for macOS riasztási párbeszédpanelén, vagy indítsa újra a számítógépet. További információkért tekintse meg tudásbáziscikkünket.

Licenc aktiválása

A telepítés végeztével a rendszer kéri a szoftver licencének aktiválását. Többféle aktiválási mód közül választhat. Az adott aktiválási mód elérhetősége az országtól, valamint a termék forgalmazási módjától (CD/DVD, az ESET weboldala stb.) függően eltérhet.

Ha közvetlenül a programból szeretné aktiválni az ESET Endpoint Antivirus for macOS licencét, kattintson az ESET Endpoint Antivirus for macOS ikonra a macOS menüsorában (a képernyő tetején), majd kattintson a **Licenc aktiválása** elemre. A programot a főmenüből is aktiválhatja a **Súgó** > **A licenc kezelése** vagy a **Védelem állapota** > **Licenc aktiválása** részen.



Az ESET Endpoint Antivirus for macOS aktiválásához az alábbi lehetőségek közül választhat:

- **Aktiválás licenckulccsal** – A licenctulajdonos azonosítására és a licenc aktiválására szolgáló egyedi,XXXX-XXXX-XXXX-XXXX-XXXX formátumú karakterlánc. A licenckulcs a licenc online megvásárlását követően kapott e-mailben, illetve a csomagban lévő licenckártyán található.
- **Biztonsági rendszergazda** – Az ESET License Administrator portálon hitelesítő adatokkal (e-mail-cím és jelszó) létrehozott fiók. Ezzel a módszerrel több licencet kezelhet egyetlen helyről.
- **Kapcsolat nélküli licenc** – Egy automatikusan létrehozott, a licencadatok megadása végett az ESET-szoftverbe átvitt fájl. A kapcsolat nélküli licencfájl az ESET License Administrator portálon hozható létre, és olyan környezetekben használható, ahol az alkalmazás nem csatlakozhat licencet adó szolgáltatóhoz.

Később is aktiválhatja a klienst, ha számítógépe egy felügyelt hálózat tagja, és rendszergazdája az ESET Remote Administrator segítségével szándékozik aktiválni a szoftvert.

> **Csendes aktiválás**
> Az ESET Remote Administrator képes értesítés nélkül, a rendszergazda által elérhetővé tett licenceket használva aktiválni a kliensszámítógépeket.

Az ESET Endpoint Antivirus for macOS 6.3.85.0 (vagy újabb) verziója tartalmazza a terminál használatával történő licencaktiválási lehetőséget. Ehhez adja ki a következő parancsot:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Az `XXXX-XXXX-XXXX-XXXX-XXXX` karakterláncot helyettesítse az ESET Endpoint Antivirus for macOS aktiválásához már használt vagy az ESET License Administrator alkalmazásban regisztrált licenckulccsal. A parancs az „OK” állapotot adja vissza, illetve az aktiválás meghiúsulása esetén hibaüzenetet jelenít meg.

Eltávolítás

Az ESET Endpoint Antivirus for macOS eltávolítója többféleképpen indítható el:

- Nyissa meg az ESET Endpoint Antivirus for macOS telepítőfájlját (*.dmg*), és kattintson duplán az **Eltávolítás** elemre.
- Indítsa el a **Finder** eszközt, nyissa meg az **Alkalmazások** mappát a merevlemezen, nyomja le a CTRL billentyűt, és kattintson az **ESET Endpoint Antivirus for macOS** ikonra, majd válassza a **Csomagtartalom megjelenítése** beállítást. Nyissa meg a **Contents** > **Helpers** mappát, és kattintson duplán az **Uninstaller** ikonra.

> **Eltávolítás**
> Az eltávolítási folyamat során többször is meg kell adnia a rendszergazdai jelszót az ESET Endpoint Antivirus for macOSteljes körű eltávolításához.

Alapbeállítások áttekintése

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 főmenüből az alábbi csoportok érhetők el:

- **Védelem állapota** – A számítógép, a webhozzáférés- és az e-mail védelem állapotáról nyújt információkat.
- **Számítógép ellenőrzése** – Ebben a csoportban konfigurálhatja és indíthatja el a kézi indítású számítógép-ellenőrzést.
- **Frissítés** – A modulok frissítéseiről jelenít meg információkat.
- **Beállítások** – Itt konfigurálhatja a számítógép biztonsági szintjét.
- **Eszközök** – Hozzáférést biztosít a Naplófájlok, a Feladatütemező, a Karantén, a Futó folyamatok és a program egyéb funkcióihoz.
- **Súgó** – Ezt a lehetőséget választva elérheti a súgófájlokat, az internetes tudásbázist, a terméktámogatási űrlapot és egyéb programinformációkat.

Billentyűparancsok

Az ESET Endpoint Antivirus for macOS alkalmazásban használható billentyűparancsok közé tartoznak az alábbiak:

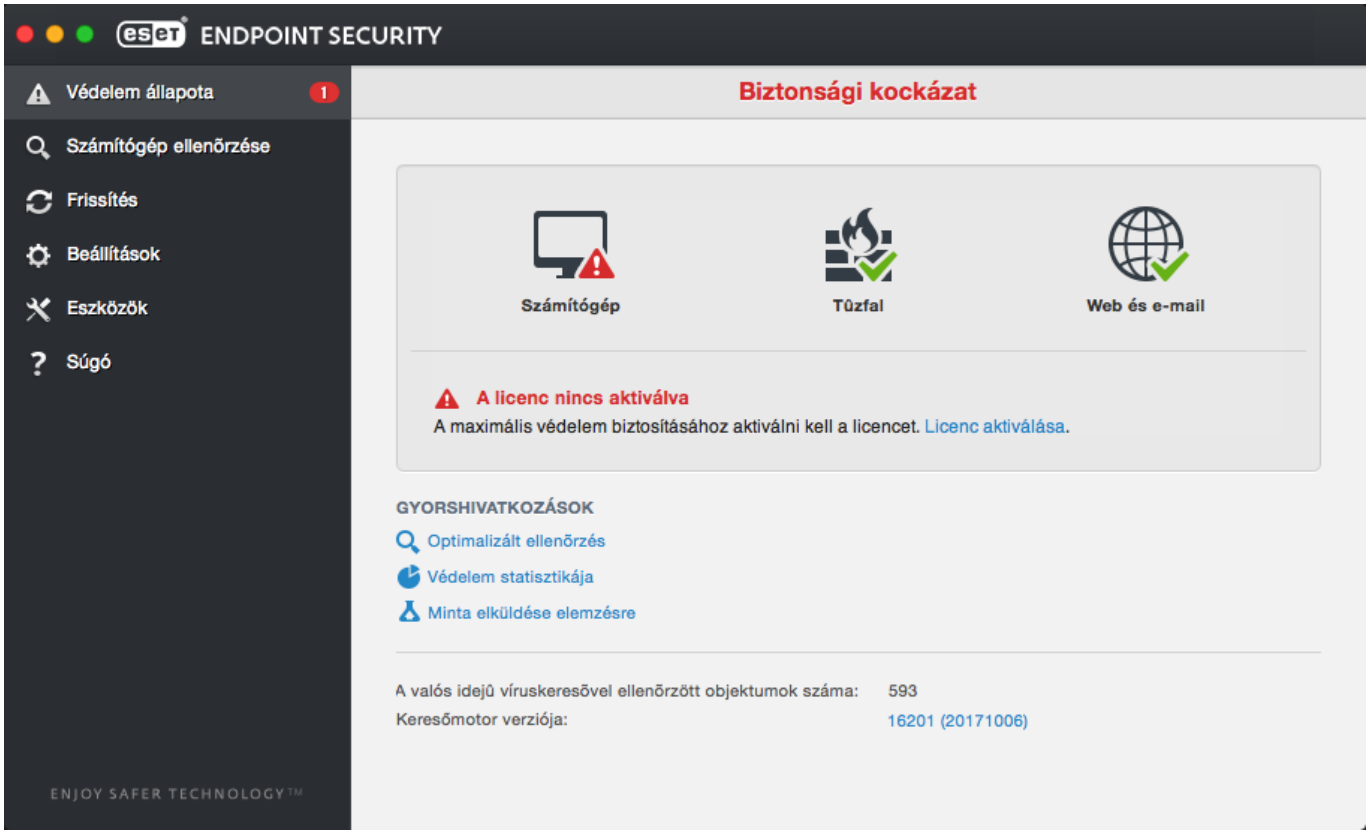
- *cmd+,* – az ESET Endpoint Antivirus for macOS beállításainak megadása;
- *cmd+O* – az ESET Endpoint Antivirus for macOS grafikus felhasználói felülete főablakának átméretezése az alapértelmezett méretre, és a képernyő közepére helyezése;
- *cmd+Q* – az ESET Endpoint Antivirus for macOS grafikus felhasználói felülete főablakának elrejtése. Ezt a macOS menüsorán (a képernyő tetején) található ESET Endpoint Antivirus for macOS ikonra kattintva nyithatja meg;
- *cmd+W* – az ESET Endpoint Antivirus for macOS grafikus felhasználói felülete főablakának bezárása.

Az alábbi billentyűparancsok csak akkor működnek, ha engedélyezi a **Szokásos menü használata** funkciót a **Beállítások** > **Alkalmazásbeállítások megadása** > **Interfész** csoportban:

- *cmd+alt+L* – a **Naplófájlok** csoport megnyitása;
- *cmd+alt+S* – a **Feladatütemező** csoport megnyitása;
- *cmd+alt+Q* – a **Karantén** csoport megnyitása.

A rendszer működésének ellenőrzése

A védelem állapotának megjelenítéséhez a főmenüben kattintson a **Védelem állapota** kategóriára. Az elsődleges ablakban ekkor megjelenik az ESET Endpoint Antivirus for macOS moduljainak a működésére vonatkozó állapotösszegzés.



Teendők, ha a program nem megfelelően működik

Amikor egy modul megfelelően működik, megjelenik egy zöld pipát tartalmazó ikon. Vörös felkiáltójel vagy narancsszínű értesítő ikon jelzi, ha egy modul nem működik megfelelően. A modulra vonatkozó további információk és a hiba javítására szolgáló megoldás is látható a program főablakában. Az egyes modulok állapotának módosításához kattintson az adott értesítési üzenet alatti kék hivatkozásra.

Ha a javasolt megoldásokkal nem oldható meg a probléma, megoldást kereshet az ESET tudásbázisában, illetve felkeresheti az ESET terméktámogatását. A terméktámogatási munkatárs gyorsan válaszol a kérdéseire, és segít az ESET Endpoint Antivirus for macOS alkalmazással kapcsolatos hibák elhárításában.

A számítógép védelme

A számítógép konfigurációja a **Beállítások** > **Számítógép** csoportban található, és megjeleníti a **Valós idejű fájlrendszervédelem** állapotát. Az egyes modulok kikapcsolásához állítsa a kívánt modult **LETILTVA** állapotra. Ne feledje, hogy ez gyengítheti a számítógép védelmét. Az egyes modulok részletes beállításainak megjelenítéséhez kattintson a **Beállítások** hivatkozásra.

Vírus- és kémprogramvédelem

A vírusvédelem a lehetséges fenyegetéseket jelentő fájlok módosításával megakadályozza a kártevők bejutását a rendszerbe. Ha a program kártékony kódot észlel, a víruskereső modul letiltja, majd megtisztítja, törli vagy karanténba helyezi a hordozó fájlt.

Általános

Az **Általános** csoportban (**Beállítások** > **Alkalmazásbeállítások megadása** > **Általános**) az alábbi típusú alkalmazások észlelését engedélyezheti:

- A **kéretlen alkalmazások** nem feltétlenül kártevők, de hátrányosan befolyásolhatják a számítógép teljesítményét. Ezek az alkalmazások általában engedélyt kérnek a telepítésükhöz. Miután a számítógépre kerülnek, a rendszer a telepítésük előtti állapotához képest eltérően kezd viselkedni. A legjelentősebb változások közé tartozik például a nem kívánt előugró ablakok megjelenése, a rejtett folyamatok aktiválása és futtatása, a rendszererőforrások nagyobb mértékű igénybevétele, a keresési eredmények módosítása, valamint a távoli szerverekkel kommunikáló alkalmazások.

- **Veszélyes alkalmazások** – A kereskedelemben kapható olyan törvényes szoftverek, amelyekkel a támadók visszaélhetnek, ha a felhasználó beleegyezése nélkül telepítik azokat. Ebbe a kategóriába tartoznak például a távoli elérésre szolgáló eszközök, és ez az oka annak, hogy a beállítás alapértelmezés szerint le van tiltva.

- **Gyanús alkalmazások** – Ezek olyan programok, amelyeket tömörítőprogramokkal vagy védelmi modulokkal tömörítettek. Az észlelés alól kibúvókat kereső kártevőkészítők gyakran használnak ilyen típusú programokat. A tömörítők futásidejű önkicsomagoló végrehajtható fájlok, amelyek többféle kártevőtípust tartalmaznak egyetlen csomagban. A leggyakoribb tömörítők az UPX, a PE_Compact, a PKLite és az ASPack. Ugyanaz a kártevő eltérően is észlelhető, ha másik tömörítővel van tömörítve. A tömörítők képesek „aláírásaikat” megváltoztatni, így nehezebb felismerni és eltávolítani a kártevőt.

A fájlrendszer beállítását vagy a webre és az e-mailekre vonatkozó kivételeket a **Beállítások** gombra kattintva adhatja meg.

Kivételek

A Kivételek csoportban megadhatja egyes fájlok, mappák, alkalmazások vagy IP/IPv6-címek kizárását az ellenőrzésből.

A **Fájlrendszer** lapon szereplő fájlokat és mappákat a rendszer a következő ellenőrzések mindegyikéből kizárja: rendszer-indításkori, valós idejű és kézi indítású (számítógép-ellenőrzés).

- **Elérési út** – A kizárt fájlok és mappák elérési útja

- **Kártevő** – Ha a kizárt fájl mellett egy kártevő neve látható, az azt jelenti, hogy a fájlt nem teljesen, hanem csak az adott kártevőt érintő ellenőrzésből zárja ki. Ha a fájlt később egy másik kártevő is megfertőzi, a vírusvédelmi modul ezt észlelni fogja.

- [+] – Új kivétel létrehozása. Írja be az objektum elérési útját (használhatja a *** és a *?* helyettesítő karaktert is), vagy jelölje ki a mappát, illetve a fájlt a fastruktúrában.

- [−] – A kijelölt bejegyzések eltávolítása

- **Alapbeállítás** – A kivételek visszaállítása a legutóbbi mentett állapotra.

A **Web és e-mail** lapon kizárhat a protokollszűrésből egyes **alkalmazásokat** vagy **IP/IPv6-címeket**.

Rendszerindításkori védelem

A Rendszerindításkor futtatott fájlok ellenőrzése automatikusan megvizsgálja a fájlokat a rendszer indításakor. A program alapértelmezés szerint rendszeresen, ütemezett feladatként futtatja ezt az ellenőrzést a felhasználó bejelentkezése vagy a modulok sikeres frissítése után. Ha módosítani szeretné a ThreatSense motor rendszerindításkori ellenőrzésre vonatkozó paraméterbeállításait, kattintson a **Beállítások** gombra. A ThreatSense motor beállításáról ebben a szakaszban olvashat bővebben.

Valós idejű fájlrendszervédelem

A valós idejű fájlrendszervédelem ellenőrzi az összes típusú adathordozót, és különféle események hatására ellenőrzést indít el. Az ellenőrzés a ThreatSense technológiát alkalmazza (leírása A ThreatSensekeresőmotor beállításai című témakörben található). Előfordulhat, hogy a valós idejű fájlrendszervédelem működése eltér az újonnan létrehozott, illetve a meglévő fájlok esetén. Az újonnan létrehozott fájlok még pontosabban ellenőrizhetők.

A program alapértelmezés szerint minden fájlt ellenőriz azok **megnyitásakor**, **létrehozásakor** vagy **futtatásakor**. Ajánlott az alapértelmezett beállítások megtartása, amelyek maximális szinten biztosítják a számítógép valós idejű védelmét. A valós idejű védelem indítása a rendszerindításkor történik, és folyamatos ellenőrzést biztosít. Különleges esetekben (például egy másik valós idejű víruskeresővel való ütközés esetén) a valós idejű védelem leállítható, ha a (képernyő tetején található) menüsor ESET Endpoint Antivirus for macOS ikonjára ⓔ kattint, és **A valós idejű fájlrendszervédelem letiltása** lehetőséget választja. A valós idejű fájlrendszervédelem a program főablakában is leállítható (kattintson a **Beállítások** > **Számítógép** elemre, és állítsa a **Valós idejű fájlrendszervédelem** beállítást **LETILTVA** értékre).

Az alábbi típusú adathordozók kizárhatók a Real-time ellenőrzésből:

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

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

A valós idejű fájlrendszervédelem további beállításainak módosításához válassza a **Beállítások** > **Alkalmazásbeállítások megadása** lehetőséget (vagy nyomja le a *cmd+,* billentyűparancsot), és kattintson a **Valós idejű védelem** elemre, majd a **Beállítások** gombra a **További beállítások** felirat mellett (a További ellenőrzési beállítások című részben ismertetett módon).

További beállítások

Ebben az ablakban meghatározhatja, hogy a ThreatSense keresőmotor milyen objektumtípusokat ellenőrizzen. Az **Önkicsomagoló tömörített fájlok**, a **Futtatás közbeni tömörítők** és a **Kiterjesztett heurisztika** részletes leírását „A ThreatSense keresőmotor beállításai” című témakör tartalmazza.

A **tömörített fájlok alapértelmezett beállításainak** módosítását csak adott hiba megoldásához ajánljuk, mivel

ronthatja a rendszer teljesítményét, ha a többszörösen tömörített fájlokhoz magasabb értékeket állít be.

Futtatott fájlok **ThreatSense-paraméterei** – Alapértelmezés szerint a program **kiterjesztett heurisztikát** használ a fájlok futtatásakor. Kifejezetten javasoljuk, hogy a rendszer teljesítményére gyakorolt hatás csökkentése végett hagyja engedélyezve az optimalizálást és az ESET LiveGrid® rendszert.

Hálózati kötetek kompatibilitásának növelése – Ezzel az opcióval javíthatja a teljesítményt a fájlok hálózaton keresztül történő elérésekor. Ha a hálózati meghajtók elérésekor a teljesítmény csökkenését tapasztalja, érdemes engedélyeznie ezt az opciót. Ez a funkció rendszerfájl-koordinátort használ az OS X 10.10 és újabb verzión. Vegye figyelembe, hogy nem minden alkalmazás támogatja a fájlkoordinátort, a Microsoft Word 2011 például nem támogatja, a Word 2016 viszont igen.

Mikor érdemes módosítani a valós idejű védelem beállításait?

A valós idejű védelem a biztonságos rendszerek fenntartásának legfontosabb összetevője, amely paramétereinek módosításakor körültekintően kell eljárni. Azt javasoljuk, hogy csak különleges esetekben válassza a módosítást, például ha a beállítások miatt a program ütközik egy másik alkalmazással vagy egy másik vírusvédelmi program valós idejű víruskeresőjével.

Az ESET Endpoint Antivirus for macOS a telepítése után minden beállítást optimalizál, hogy a lehető legmagasabb szintű védelmet biztosítsa a rendszer számára. Az alapértelmezett beállítások az **Alapbeállítás** gombbal állíthatók vissza, amely a **Valós idejű védelem** ablak bal alsó részén található (**Beállítások** > **Alkalmazásbeállítások megadása** > **Valós idejű védelem**).

A valós idejű védelem ellenőrzése

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

Ha az ESET Security Management Center használata nélkül szeretné ellenőrizni a valós idejű védelem állapotát, a **Terminál** használatával távolból csatlakozzon a kliensszámítógéphez, és adja ki a következő parancsot:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

A valós idejű víruskereső állapota a következőképpen jelenik meg: `RTPStatus=Enabled` vagy `RTPStatus=Disabled`.

A terminálvizsgálat eredménye az alábbi állapotokat foglalja magában:

- a kliensszámítógépen telepített ESET Endpoint Antivirus for macOS verziója;
- a keresőmotor dátuma és verziószáma;

- a frissítési szerver elérési útja.

> **Terminálhasználat**
> A Terminál segédprogram használatát csak tapasztalt felhasználóknak ajánljuk.

Teendők, ha a valós idejű védelem nem működik

Ez a témakör a valós idejű védelem használata során előforduló problémákat és azok elhárítási módját ismerteti.

A valós idejű védelem le van tiltva

Ha a valós idejű védelmet a felhasználó elővigyázatlanul letiltotta, újra kell aktiválni. A valós idejű védelem újbóli aktiválásához a főmenüből kattintson a **Beállítások** > **Számítógép** elemre, és a **Valós idejű fájlrendszervédelem** lehetőséget állítsa **ENGEDÉLYEZVE** értékre. A valós idejű védelmet az alkalmazásbeállítások között is engedélyezheti a **Valós idejű védelem** párbeszédpanelen **A valós idejű fájlrendszervédelem engedélyezése** jelölőnégyzet bejelölésével.

A valós idejű védelem nem észleli és nem tisztítja meg a fájlokat a fertőzésektől

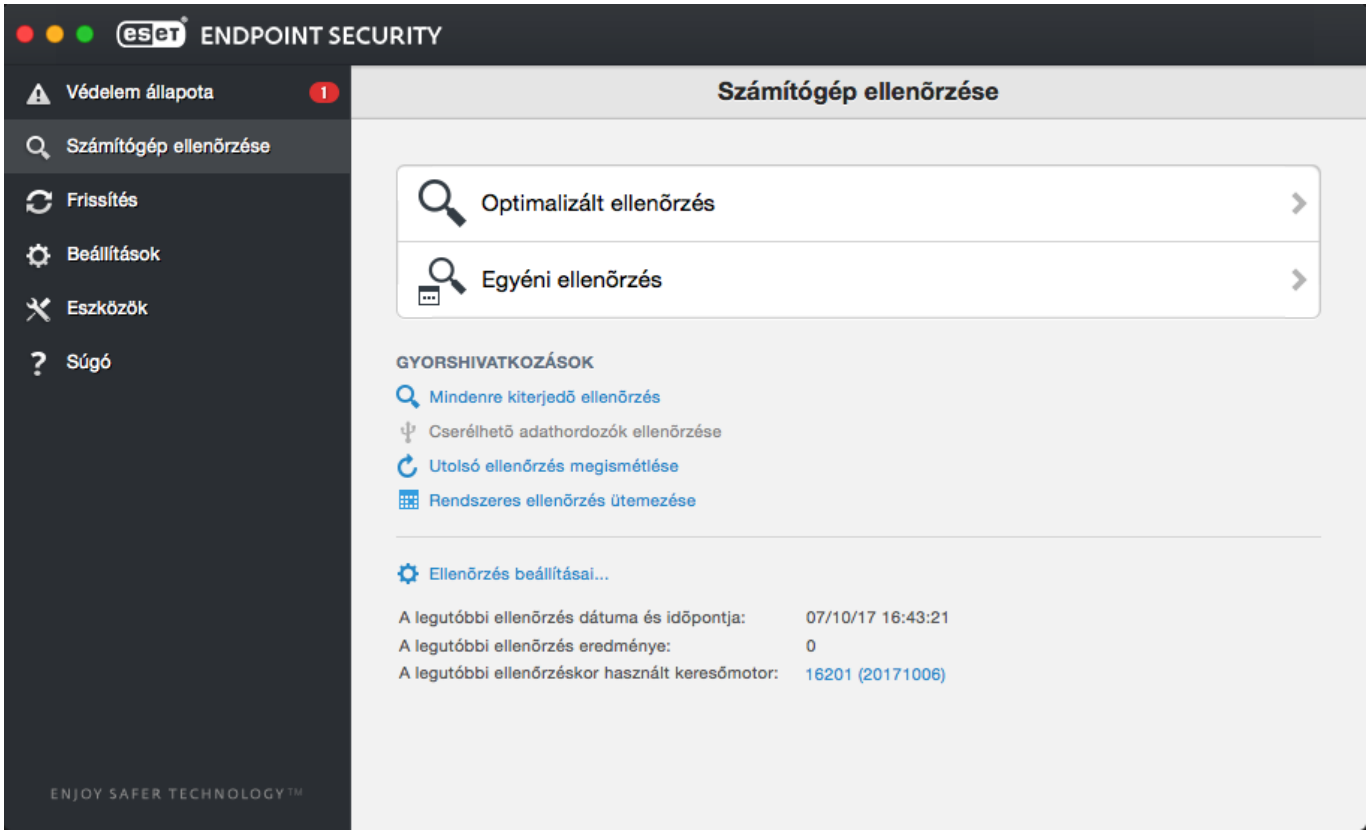
Győződjön meg arról, hogy a számítógépen nincs másik víruskereső program telepítve. Ha egyszerre két valós idejű védelmi szolgáltatást nyújtó eszköz van engedélyezve, azok ütközésbe kerülhetnek egymással. Ajánlatos az esetleges további víruskereső programokat eltávolítani a rendszerből.

A valós idejű védelem nem indul el

Ha a rendszer indításakor nem indul el a valós idejű védelem, annak oka az egyéb programokkal való ütközés lehet. Ha ilyen hibát tapasztal, forduljon az ESET terméktámogatásához.

Kézi indítású számítógép-ellenőrzés

Ha a számítógép gyaníthatóan megfertőződött (a szokásostól eltérő módon viselkedik), **optimalizált ellenőrzés** futtatásával ellenőrizheti, hogy tartalmaz-e fertőzéseket. A maximális védelem biztosításához a számítógép-ellenőrzéseket nem csak fertőzés gyanúja esetén kell futtatni, hanem érdemes a szokásos biztonsági intézkedések részeként, rendszeres időközönként elvégezni. A rendszeres ellenőrzésekkel felismerhetők azok a fertőzések, amelyeket a valós idejű víruskereső nem észlelt a lemezre mentéskor. Ez akkor fordulhat elő, ha a fertőzés időpontjában a valós idejű víruskereső ki volt kapcsolva, illetve a modulok nem voltak naprakészek.



A kézi indítású számítógép-ellenőrzést ajánlott legalább havonta egyszer futtatni. Az ellenőrzés az **Eszközök** lapon lévő **Feladatütemező** lehetőséget választva állítható be.

A kijelölt fájlokat és mappákat áthúzhatja az asztalról vagy a **Finder** ablakból az ESET Endpoint Antivirus for macOS főképernyőjére, a Dock ikonjára, a menüsor ikonjára (a képernyő tetején) vagy az alkalmazás ikonjára (az */Applications* (Alkalmazások) mappában).

Az ellenőrzés típusa

Kétféle kézi indítású számítógép-ellenőrzés lehetséges: az **Optimalizált ellenőrzés** lehetőséget választva gyorsan, az ellenőrzési paraméterek konfigurálása nélkül ellenőrizheti a rendszert; míg az **Egyéni ellenőrzés** esetén választhat az előre definiált ellenőrzési profilok közül, illetve kijelölhet ellenőrizendő célterületeket.

Optimalizált ellenőrzés

Az optimalizált ellenőrzéssel gyorsan elindítható a számítógép ellenőrzése, és felhasználói beavatkozás nélkül megtisztíthatók a fertőzött fájlok. Fő előnye az egyszerű kezelhetősége anélkül, hogy részletesen be kellene állítani az ellenőrzést. Az optimalizált ellenőrzés az összes mappa minden fájlját ellenőrzi, és automatikusan megtisztítja vagy törli az észlelt kártevőket tartalmazó fájlokat. A megtisztítás szintje automatikusan az alapértelmezett értékre van állítva. A megtisztítás típusairól a Megtisztítás című témakörben olvashat bővebben.

Egyéni ellenőrzés

Az **egyéni ellenőrzés** lehetővé teszi az ellenőrzési paraméterek, többek között az ellenőrizendő célterületek és az ellenőrzési módok megadását. Az egyéni ellenőrzés futtatásának előnye a paraméterek részletes beállításának lehetősége. A különböző beállítások a felhasználó által definiált ellenőrzési profilokba menthetők, ami az

ugyanolyan paraméterekkel végzett gyakori ellenőrzések során lehet hasznos.

Az ellenőrizendő célterületek kijelöléséhez válassza ki a **Számítógép ellenőrzése** > **Egyéni ellenőrzés** elemet, majd a fastruktúrában jelölje ki az **ellenőrizendő célterületeket**. Az ellenőrizendő célterületek pontosabban is meghatározhatók az ellenőrzésben szerepeltetni kívánt mappa vagy fájl(ok) elérési útjának megadásával. Ha csak információszerzés céljából, megtisztítás nélkül szeretné ellenőrizni a rendszert, jelölje be a **Csak ellenőrzés megtisztítás nélkül** jelölőnégyzetet. Ezenkívül három megtisztítási szint közül is választhat a **Beállítások** > **Megtisztítás** lehetőséget kiválasztva.

> **Egyéni ellenőrzés**
> A számítógép egyéni ellenőrzése csak a víruskereső programok használatában tapasztalattal rendelkező felhasználóknak ajánlott.

Ellenőrizendő célterületek

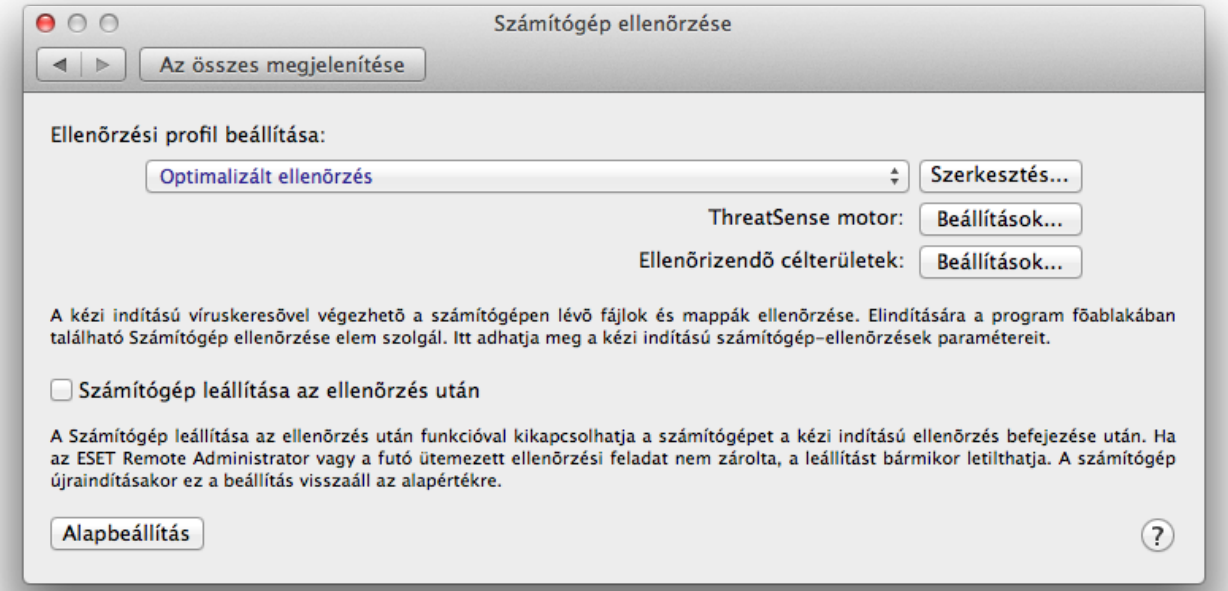
Az ellenőrizendő célterületek fastruktúrája lehetővé teszi azoknak a fájloknak és mappáknak a kijelölését, amelyekben víruskeresést szeretne végezni. A profil beállításainak megfelelően mappákat is kijelölhet.

Az ellenőrizendő célterületek pontosabban definiálhatók az ellenőrzésben szerepeltetni kívánt mappa vagy fájl(ok) elérési útjának megadásával. Az ellenőrizendő célterületeket a számítógépen elérhető összes mappát tartalmazó fastruktúrás listából választhatja ki az adott fájlhoz vagy mappához tartozó jelölőnégyzet bejelölésével.

Ellenőrzési profilok

A kívánt ellenőrzési beállításokat mentheti, és a későbbi ellenőrzésekhez használhatja. A rendszeresen használt ellenőrzésekhez ajánlott egy másik profilt létrehozni (különböző ellenőrizendő célterületekkel, ellenőrzési módszerekkel és más paraméterekkel).

Új profil létrehozásához a főmenüben válassza a **Beállítások** > **Alkalmazásbeállítások megadása** lehetőséget. (vagy nyomja le a *cmd+,* billentyűparancsot), majd a **Számítógép ellenőrzése** elemet, és kattintson az aktuális profilok listája mellett lévő **Szerkesztés** gombra.



Ha segítségre van szüksége az igényeinek megfelelő ellenőrzési profil létrehozásával kapcsolatban, olvassa el az ellenőrzési beállítások egyes paramétereinek a leírását A ThreatSense keresőmotor beállításai című részben.

> **Példa**
>
> Tegyük fel, hogy saját ellenőrzési profilt szeretne létrehozni, és az Optimalizált ellenőrzés konfigurációja részben megfelel az elképzeléseinek, nem kívánja azonban ellenőrizni a futtatás közbeni tömörítőket és a veszélyes alkalmazásokat, emellett automatikus megtisztítást szeretne alkalmazni. A **Kézi indítású víruskereső profillistája** ablakban írja be a profil nevét, kattintson a **Hozzáadás** gombra, és az **OK** gombra kattintva erősítse meg a műveletet. Ezt követően a **ThreatSense keresőmotor** és a **Ellenőrizendő célterületek** beállításával adja meg a követelményeinek megfelelő paramétereket.

Ha a kézi indítású ellenőrzés végrehajtása után le szeretné állítani az operációs rendszert és a számítógépet, jelölje be a **Számítógép leállítása az ellenőrzés után** jelölőnégyzetet.

A ThreatSense keresőmotor beállításai

A ThreatSense az ESET saját technológiája, amely számos összetett kártevő-észlelési módszer együtteséből áll. A technológia proaktív, ami azt jelenti, hogy az új kártevők elterjedésének korai szakaszában is védelmet nyújt. Számos módszer (kódelemzés, kódemuláció, általános definíciók stb.) 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 elkerülhető a rootkitek okozta fertőzés is.

A ThreatSense technológia beállítási lehetőségeivel több ellenőrzési paraméter megadható, például az alábbiak:

- Az ellenőrizendő fájltípusok és kiterjesztések
- Különböző észlelési módszerek kombinációja

- A megtisztítás mértéke stb.

A beállítási ablak megnyitásához válassza a **Beállítások > Alkalmazásbeállítások megadása** lehetőséget (vagy nyomja le a *cmd+,* billentyűparancsot), majd kattintson a ThreatSense motor **Beállítások** gombjára a **Rendszerindításkori védelem**, a **Valós idejű védelem** és a **Számítógép ellenőrzése** modul esetében, amelyek mind a ThreatSense technológiát használják (lásd alább). A különböző biztonsági körülmények eltérő konfigurációkat igényelhetnek. Ennek érdekében a ThreatSense külön beállítható az alábbi védelmi modulokhoz:

- **Rendszervédelem** – A fájlok automatikus ellenőrzése rendszerindításkor
- **Valós idejű védelem** – Valós idejű fájlrendszervédelem
- **Számítógép ellenőrzése** – Kézi indítású számítógép-ellenőrzés
- **Webhozzáférés-védelem**
- **E-mail-védelem**

A ThreatSense paraméterei minden modulhoz speciálisan optimalizáltak, és módosításuk jelentősen befolyásolhatja a rendszer működését. Ha például engedélyezi, hogy a program mindig ellenőrizze a futtatás közbeni tömörítőket, vagy bekapcsolja a kiterjesztett heurisztikát a Valós idejű fájlrendszervédelem modulban, a rendszer lelassulhat. Ezért a Számítógép ellenőrzése modul kivételével az összes modul esetében ajánlott a ThreatSense paramétereit az alapértelmezett értékeken hagyni.

Objektumok

Az **Objektumok** csoportban megadhatja, hogy mely fájlokat ellenőrizze a keresőmotor.

- **Szimbolikus hivatkozások** – Az olyan szöveges karakterláncot tartalmazó fájlok ellenőrzése, amelyeket a rendszer egy fájlra vagy könyvtárra mutató elérési útként értelmez (csak számítógép-ellenőrzés esetén).
- **E-mail fájlok** – (Nem érhető el a valós idejű védelem esetén.) Az e-mail fájlok ellenőrzése.
- **Postaládák** – (Nem érhető el a valós idejű védelem esetén.) A rendszerben található felhasználói postaládák ellenőrzése. E funkció helytelen használata ütközést okozhat a levelezőprogrammal. A funkció előnyeiről és hátrányairól olvashat ebben a tudásbáziscikkben.
- **Tömörített fájlok** – (Nem érhető el a valós idejű védelem esetén.) A tömörített fájlokba (.rar, .zip, .arj, .tar stb.) tömörített fájlok ellenőrzése.
- **Önkicsomagoló tömörített fájlok** – (Nem érhető el a valós idejű védelem esetén.) Az önkicsomagoló tömörített fájlokban található fájlok ellenőrzése.
- **Futtatás közbeni tömörítők** – A normál tömörítettfájl-típusoktól eltérően a fájlokat a memóriába tömörítő, futtatás közbeni tömörítők ellenőrzése. Ha ezt a beállítást választja, a program a normál statikus tömörítőket (például UPX, yoda, ASPack, FGS) is ellenőrzi.

Beállítások

A **Beállítások** csoportban a rendszer ellenőrzésekor használandó módszereket adhatja meg. A választható lehetőségek az alábbiak:

- **Heurisztika** – A heurisztika a programok (kártékony) tevékenységének felismerésére szolgáló algoritmust használ. Fő előnye, hogy a korábban még nem létező, új kártevő szoftvereket is képes felismerni.

- **Kiterjesztett heurisztika** – A kiterjesztett heurisztika az ESET saját, a számítógépes férgek és trójai programok felismerésére optimalizált, magas szintű programozási nyelveken fejlesztett heurisztikus algoritmusa. A kiterjesztett heurisztikának köszönhetően a program észlelési képessége jelentősen megnőtt.

Megtisztítás

A megtisztítási beállítások határozzák meg, hogy a víruskereső milyen módon tisztítja meg a fertőzött fájlokat. A megtisztításnak három szintje van:

- **Nincs megtisztítás** – A program nem tisztítja meg automatikusan a fertőzött fájlokat, hanem megjelenít egy figyelmeztető ablakot, és a felhasználó választhat a műveletek közül.

- **Szokásos módon megtisztít** – A program megkísérli a fertőzött fájlok automatikus megtisztítását vagy törlését. Ha a megfelelő művelet automatikus kiválasztására nincs lehetőség, felkínál néhány utóműveletet. A program akkor is megjeleníti az utóműveleteket, ha nem sikerült egy előre megadott művelet végrehajtása.

- **Automatikusan megtisztít** – A program megtisztítja vagy törli az összes fertőzött fájlt (a tömörített fájlokat is beleértve). A rendszerfájlok kivételt képeznek. Ha egy fájl nem tisztítható meg, a program értesíti erről a felhasználót, és kéri, hogy adja meg a végrehajtandó művelet típusát.

> **Szokásos módon megtisztít – tömörített fájlok megtisztítása**
> Az alapértelmezett megtisztítási szint használata esetén a program csak akkor törli a kártevőt tartalmazó teljes tömörített fájlt, ha az abban lévő összes fájl fertőzött. A program nem törli a tömörített fájlt, ha az szabályos, valamint fertőzött fájlokat is tartalmaz. Ha az Automatikusan megtisztít módban a program egy fertőzött tömörített fájlt észlel, akkor is törli a teljes tömörített fájlt, ha nem fertőzött fájlokat is tartalmaz.

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.

A program alapértelmezés szerint kiterjesztéstől függetlenül ellenőrzi az összes fájlt. Az ellenőrzésből kizárt fájlok listájára bármilyen kiterjesztés felvehető. A  és  gombbal engedélyezheti vagy letilthatja adott kiterjesztésű fájlok ellenőrzését.

A fájlok ellenőrzésből való kizárására akkor lehet szükség, ha bizonyos fájltípusok ellenőrzése akadályozza a program megfelelő működését. Ajánlott lehet például a *log*, *cfg* és *tmp* kiterjesztés kizárása. A fájlkiterjesztéseket a következő formátumban kell megadni:

log

cfg

tmp

Korlátok

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

- **Maximális méret:** Az ellenőrizendő objektumok maximális méretének megadására szolgál. A víruskereső modul csak a megadott méretnél kisebb objektumokat fogja ellenőrizni. Az alapértelmezett érték módosítására általában nincs szükség, ezért nem javasoljuk azt. A beállítás módosítása csak olyan tapasztalt felhasználóknak javasolt, akik megfelelő indokkal rendelkeznek a nagyobb méretű objektumok ellenőrzésből való kizárásához.

- **Maximális ellenőrzési idő:** Itt az objektumok ellenőrzésére szánt maximális időtartamot adhatja meg. A felhasználó által megadott érték esetén a víruskereső modul leállítja az objektum ellenőrzését, függetlenül attól, hogy az ellenőrzés befejeződött-e, vagy sem.

- **Maximális beágyazási szint:** Itt adhatja meg a tömörített fájlok ellenőrzésének maximális mélységét. Nem javasoljuk az alapértelmezett 10-es érték módosítását, mivel erre a szokásos körülmények között nincs szükség. Ha az ellenőrzés a többszörösen tömörített fájlok száma miatt idő előtt megszakad, a tömörített fájl ellenőrizetlen marad.

- **Maximális fájlméret:** Itt adhatja meg az ellenőrizendő tömörített fájlok között található fájlok (kibontás utáni) maximális méretét. Ha az ellenőrzés a korlát következtében idő előtt megszakad, a tömörített fájl ellenőrizetlen marad.

Egyebek

Optimalizálás engedélyezése

Az optimalizálás engedélyezése esetén a program a legoptimálisabb beállításokat használja, hogy az ellenőrzési sebesség csökkenése nélkül a leghatékonyabb ellenőrzési szintet biztosítsa. A különböző védelmi modulok intelligensen végzik az ellenőrzést, kihasználva a különböző ellenőrzési módszereket. Az optimalizálás nincs szigorúan definiálva a terméken belül. Az ESET fejlesztési csoportja folyamatosan új módosításokat valósít meg, amelyeket a szokásos frissítéseken keresztül az ESET Endpoint Antivirus for macOS programba integrál. Az optimalizálás letiltása esetén a program csak a felhasználók által az adott modul ThreatSense-alapbeállításaiban megadott beállításokat alkalmazza az ellenőrzések végrehajtásakor.

Alternatív adatfolyam ellenőrzése (csak kézi indítású víruskereső esetén)

A fájlrendszer által használt változó adatfolyamok (erőforrás/adatelágazások) olyan fájl- és mappatársítások, amelyek a szokásos ellenőrzési technikák számára láthatatlanok maradnak. Számos fertőzés úgy próbálja meg elkerülni az észlelést, hogy változó adatfolyamként jelenik meg.

A program fertőzést észlelt

A fertőzések számos különböző ponton keresztül juthatnak be a rendszerbe: weboldalakról, megosztott mappákból, e-mailen keresztül vagy cserélhető számítógépes eszközökről (USB-eszközökről, külső lemezekről, CD

vagy DVD lemezekről stb.).

Ha a számítógép fertőzés jeleit mutatja, azaz például működése lelassul vagy gyakran lefagy, ajánlatos elvégeznie az alábbi lépéseket:

1. Kattintson a **Számítógép ellenőrzése** elemre.

2. Kattintson az **Optimalizált ellenőrzés** hivatkozásra (további információ található az Optimalizált ellenőrzés című fejezetben).

3. Az ellenőrzés végeztével a naplóban megtekintheti az ellenőrzött, a fertőzött és a megtisztított fájlok számát.

Ha csak a lemez bizonyos részét kívánja ellenőrizni, kattintson az **Egyéni ellenőrzés** hivatkozásra, és jelölje ki az ellenőrizendő célterületeket.

Annak szemléltetéséhez, hogy miként kezeli az ESET Endpoint Antivirus for macOS a fertőzéseket, tegyük fel, hogy az alapértelmezett megtisztítási szintet alkalmazó valós idejű fájlrendszerfigyelő fertőzést talál. Ilyenkor a valós idejű védelem megkísérli a fájl megtisztítását vagy törlését. Ha nincs előre meghatározva a végrehajtandó művelet a valós idejű védelmi modul számára, a program egy riasztási ablakban kérni fogja a művelet megadását. Rendszerint a **Megtisztítás**, a **Törlés** és a **Nincs művelet** közül választhat. Nem ajánlott a **Nincs művelet** beállítást választani, mert a fertőzött fájlok ebben az esetben fertőzött állapotban maradnak. A beállítás használata abban a helyzetben ajánlott, ha az adott fájl biztosan ártalmatlan, és a program hibásan észlelte azt fertőzöttnek.

Megtisztítás és törlés
Megtisztítást akkor érdemes alkalmazni, ha a fájlt olyan vírus támadta meg, amely kártékony kódot csatolt hozzá. Ilyen esetben először a fertőzött fájlt megtisztítva kísérelje meg visszaállítani annak eredeti állapotát. Ha a fájl kizárólag kártékony kódból áll, akkor a program törli azt.

Tömörített fájlokban lévő fájlok törlése
Az alapértelmezett megtisztítási szint használata esetén a program csak akkor törli a teljes tömörített fájlt, ha kizárólag fertőzött fájlokat tartalmaz. Más szóval a program nem törli a tömörített fájlokat abban az esetben, ha azok ártalmatlan, nem fertőzött fájlokat is tartalmaznak. Az **automatikus megtisztítással** járó ellenőrzés végrehajtásakor körültekintően kell eljárni, mert ebben az esetben a program akkor is törli a tömörített fájlt, ha csak egyetlen fertőzött fájlt tartalmaz (a benne lévő többi fájl állapotától függetlenül).

Webhozzáférés- és e-mail-védelem

A webhozzáférés- és e-mail védelem eléréséhez a főmenüben kattintson a **Beállítások** > **Web és e-mail** elemre. Az egyes modulok részletes beállításait is elérheti innen a **Beállítások gombra kattintva.**

> **Ellenőrzési kivételek**
> Az ESET Endpoint Antivirus for macOS nem ellenőrzi a következő titkosított protokollokat: HTTPS, POP3S és IMAPS.

- **Webhozzáférés-védelem** – A böngészők és a távoli szerverek közötti kommunikációt figyeli.

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

- **Adathalászat elleni védelem** – A webhelyekről és tartományokból származó minden potenciális adathalászati támadást letilt.

Webhozzáférés-védelem

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

Webszűrés a HTTP-kommunikáció portszámai és/vagy az URL-címek megadásával állítható be.

Portok

A **Portok** lapon adhatók meg a HTTP-kommunikációhoz használt portszámok. Alapértelmezés szerint a 80-as, a 8080-as és a 3128-as portszám van beállítva.

URL-listák

Az **URL-listák** csoportban adhatók meg a letiltandó, engedélyezendő, illetve az ellenőrzésből kizárandó HTTP-címek. A tiltólistán szereplő webhelyeket nem fogja tudni elérni. A kizárt címek listáján szereplő webhelyek elérése közben a program nem keres kártékony kódokat.

Ha csak az **Engedélyezett URL-cím** listán szereplő címekhez szeretne hozzáférést biztosítani, jelölje be az **URL-címek korlátozása** jelölőnégyzetet.

A lista aktiválásához válassza a listanév melletti **Engedélyezve** lehetőséget. Ha értesítést szeretne megjeleníteni az aktuális listán szereplő címek beírásakor, válassza az **Értesítve** lehetőséget.

Az URL-listák készítésekor 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.

E-mail-védelem

Az e-mail-védelem biztosítja a POP3 és az IMAP protokollon keresztül érkező e-mailek ellenőrzését. 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 levelezőprogram használatakor mindig megtörténik.

ThreatSense keresőmotor: Beállítások – A speciális víruskeresési beállításokkal megadhatja az ellenőrizendő célterületek körét, az észlelési módszereket stb. A **Beállítások** gombra kattintva megnyithatja a részletes vírusellenőrzési beállításokat tartalmazó ablakot.

Címkeüzenet hozzáfűzése az e-mail lábjegyzetéhez – Egy-egy e-mail ellenőrzése után lehet, hogy a program az

ellenőrzés eredményét ismertető értesítést is hozzáfűz az üzenethez. Nem lehet kizárólag az értesítésekre támaszkodni, mivel a címkék a hibásan formázott HTML-üzenetekben eltűnhetnek, illetve egyes vírusok meg tudják hamisítani őket. A választható lehetőségek az alábbiak:

- **Soha** – A program nem fűz értesítő szöveget az üzenetekhez.
- **Csak a fertőzött e-mailekhez** – A program csak a kártevő szoftvert tartalmazó levelekhez fűz értesítő szöveget.
- **Az összes ellenőrzött e-mailhez** – Az ESET Endpoint Antivirus for macOS minden ellenőrzött levélhez értesítő szöveget fűz.

Megjegyzés hozzáfűzése a fogadott és elolvasott fertőzött e-mailek tárgyához – Jelölje be ezt a jelölőnégyzetet, ha azt szeretné, hogy az e-mailek védelmét ellátó funkció vírusra 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.

A fertőzött e-mailek tárgyához hozzáfűzendő szöveg – A sablon szerkesztésével módosíthatja a fertőzött e-mail tárgyában szereplő előtag formátumát.

- %avstatus% – Megadja az e-mail fertőzési állapotát (például: tiszta, fertőzött...)
- %virus% – Megadja a kártevő nevét
- %product% – Megadja az ESET-termék nevét (ebben az esetben ESET Endpoint Antivirus for macOS)
- %product_url% – Megadja az ESET webhelyének linkjét (www.eset.com)

Az ablak alsó szakaszában engedélyezheti vagy letilthatja a POP3 és az IMAP protokollon keresztül érkező e-mailek ellenőrzését. Erről az alábbi témakörökben olvashat bővebben:

- POP3-protokollszűrés
- IMAP-protokollszűrés

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 protokollszűrés megfelelő működéséhez ellenőrizze, hogy a modul engedélyezve van-e. Az automatikus POP3-protokollszűréshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 110-es porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. A portszámokat vesszővel elválasztva kell megadni.

Ha a **POP3-protokollszűrés engedélyezése** be van jelölve, a program a POP3 protokollon zajló teljes forgalmon végez ellenőrzést.

IMAP-protokollszűrés

Az Internet Message Access Protocol (IMAP) protokoll az e-mailek fogadására szolgál. Az IMAP protokollnak számos előnye van a POP3 protokollal szemben – például több levelezőprogram is csatlakozhat ugyanahhoz a postaládához egy időben, miközben az üzenetek állapota (például hogy elolvasták, megválaszolták vagy törölték-e) megőrződik és egységesen látszik. Az ESET Endpoint Antivirus for macOS a 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. A portszámokat vesszővel elválasztva kell megadni.

Ha az **IMAP-protokollszűrés engedélyezése** be van jelölve, a program az IMAP protokollon zajló teljes forgalmon végez ellenőrzést.

Adathalászat elleni védelem

Az adathalászat kifejezés olyan bűnözői tevékenységre utal, amely pszichológiai manipulációt alkalmaz (vagyis bizalmas információk kiszolgáltatására veszi rá a felhasználót). Az adathalászattal megszerezni kívánt bizalmas adatok közé tartoznak többek között a bankszámlaszámok, a hitelkártyaszámok, a PIN-kódok, illetve a felhasználónevek és a jelszók.

Azt javasoljuk, hogy hagyja bekapcsolva az Adathalászat elleni védelem funkciót (**Beállítások** > **Alkalmazásbeállítások megadása** > **Adathalászat elleni védelem**). A rendszer a veszélyes webhelyekről vagy tartományokból érkező minden lehetséges adathalászati támadást letilt, és a támadásról figyelmeztető értesítést jelenít meg.

Eszközfelügyelet

Az ESET Endpoint Antivirus for macOS lehetővé teszi a kiterjesztett szűrők és engedélyek ellenőrzését, tiltását vagy módosítását, valamint annak megadását, hogy a felhasználó hogyan érhet el és használhat egy adott adathordozót. Ez a lehetőség különösen hasznos lehet akkor, ha a számítógép rendszergazdája meg kívánja akadályozni, hogy a felhasználók kéretlen tartalmú eszközöket használjanak.

Eszközfelügyelet a macOS 11-es és újabb verzióiban

A macOS 11-es és újabb verzióira telepített ESET Endpoint Antivirus for macOS csak adathordozók ellenőrzését végzi el (pl. USB-meghajtók, CD/DVD...).

Támogatott külső eszközök a macOS 10.15-ös és régebbi verziói esetén:

- Lemezes tárhely (HDD, USB flash meghajtó)
- CD/DVD

- USB-nyomtató
- Képeszköz
- Soros port
- Hálózat
- Hordozható eszköz

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

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

Szabályszerkesztő

Az eszközfelügyelet beállítási lehetőségei a **Beállítások** > **Alkalmazásbeállítások megadása** > **Eszközfelügyelet** részen adhatók meg.

Az eszközfelügyelet engedélyezése lehetőségre kattintva kapcsolhatja be az Eszközfelügyelet funkciót az ESET Endpoint Antivirus for macOS alkalmazásban. Az Eszközfelügyelet funkció engedélyezését követően kezelheti és szerkesztheti az eszközfelügyeleti szabályokat. A szabály engedélyezéséhez vagy letiltásához jelölje be az adott szabály neve melletti jelölőnégyzetet.

Szabályokat a + vagy a − gomb használatával vehet fel vagy távolíthat el. A szabályok prioritási sorrendben vannak felsorolva úgy, hogy a legnagyobb prioritású szabályok vannak a lista tetején. A sorrend átrendezéséhez húzzon egy szabályt az új helyére, vagy kattintson a ⚙ gombra, és válasszon ki egy lehetőséget.

Az ESET Endpoint Antivirus for macOS automatikusan észleli az összes aktuálisan behelyezett eszközt a paramétereikkel együtt (eszköz típusa, gyártó, modell, sorozatszám). A szabályok kézi létrehozása helyett kattintson a **Felismerés** lehetőségre, jelölje ki az eszközt, és a szabály létrehozásához kattintson a **Folytatás** elemre.

Adott eszközök engedélyezhetők vagy letilthatók a felhasználójuk vagy a felhasználócsoport szerint, illetve a szabály konfigurációjában megadható számos paraméter alapján. A szabálylista az adott szabályokra vonatkozó leírásokat, többek között az eszköz típusát, a napló részletességét és az eszköz számítógéphez való csatlakoztatása után végrehajtandó műveletet tartalmazza.

Név
A **Név** mezőbe írt leírás segítségével a szabály könnyebben azonosítható. A **Szabály engedélyezve** jelölőnégyzettel engedélyezheti vagy letilthatja a szabályt – ez akkor lehet hasznos, ha nem szeretné véglegesen törölni.

Eszköz típusa
A legördülő menüben válassza ki a külső eszköz típusát. Az eszközök típusára vonatkozó információt az operációs rendszerből gyűjti össze a program. A tárolóeszközök közé tartoznak az USB-n vagy FireWire-eszközön keresztül csatlakoztatott külső lemezek vagy a hagyományos memóriakártya-olvasók. Képeszközök többek között a képolvasók és a fényképezőgépek. Mivel ezek az eszközök csak a saját műveleteikről adnak meg információkat, a felhasználókról nem, csak globálisan tilthatók le.

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

Olvasás/Írás – Teljes hozzáférést engedélyez az eszközhöz.

Csak olvasás – Csak olvasási hozzáférést engedélyez az eszközhöz.

Tiltás – Letiltja a hozzáférést az eszközhöz.

Feltételek típusa
Az **Eszközcsoport** vagy az **Eszköz** közül választhat. Az alább látható további paraméterek szabályok pontosításához és adott eszközök testreszabásához használhatók.

Gyártó – Szűrés a gyártó neve vagy azonosítója szerint.

Típus – Az eszköz elnevezése

Sorozatszám – A külső eszközök rendszerint saját sorozatszámmal rendelkeznek. CD/DVD esetén ez nem a CD/DVD-meghajtó, hanem az adathordozó sorozatszáma.

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

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

Naplózás részletessége

Mindig – Az összes esemény naplózása

Diagnosztikai – A program pontos beállításához szükséges információk naplózása

Tájékoztató – Tájékoztató jellegű üzenetek, valamint a fenti rekordok rögzítése

Figyelmeztetés – Kritikus figyelmeztetések és figyelmeztető üzenetek rögzítése

Nincs – Nem jönnek létre naplók

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

Szerkesztés... – Az **Identitásszerkesztő** megnyitása, ahol felhasználókat vagy csoportokat jelölhet ki. A felhasználók listájának megadásához jelölje ki őket a bal oldali **Felhasználók** listában, és kattintson a

Hozzáadás gombra. Ha felhasználókat szeretne eltávolítani, jelölje ki a nevüket a **kijelölt felhasználók** listájában, és kattintson az **Eltávolítás** gombra. Az összes felhasználó megjelenítéséhez válassza **Az összes felhasználó megjelenítése** beállítást. Ha a lista üres, minden felhasználó engedélyezve lesz.

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

Eszközök

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

Naplófájlok

A Naplófájlok lap a fontos programeseményekről tájékoztatást, az észlelt kártevőkről áttekintést nyújt. A naplózás fontos szerepet tölt be a rendszerelemzésben, a kártevők felismerésében és a hibaelhárításban. A program a naplózást a háttérben aktívan, felhasználói beavatkozás nélkül végzi. Az információkat az aktuális naplórészletességi beállításoknak megfelelően rögzíti. A szöveges üzenetek és a naplófájlok közvetlenül az ESET Endpoint Antivirus for macOS-programkörnyezetből is megtekinthetők, de ugyanitt nyílik lehetőség a naplófájlok archiválására is.

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

1. **Észlelt kártevők** – A fertőzések észlelésével kapcsolatos eseményekre vonatkozó információk.

2. **Események** – A program az ESET Endpoint Antivirus for macOS által elvégzett összes műveletet rögzíti az eseménynaplókban.

3. **Számítógép ellenőrzése** – Ezt a lehetőséget választva megjelenítheti az összes befejezett ellenőrzés eredményét. Az egyes bejegyzésekre duplán kattintva megjelennek az adott számítógép-ellenőrzés részletes adatai.

4. **Eszközfelügyelet** – A számítógéphez csatlakoztatott cserélhető adathordozókra vagy eszközökre vonatkozó bejegyzéseket tartalmaz. A program csak a megfelelő eszközfelügyeleti szabállyal rendelkező eszközöket jegyzi fel a naplófájlba. Ha a szabály nem felel meg egy csatlakoztatott eszköznek, létrejön egy naplóbejegyzés az eszközhöz. Itt láthatók bizonyos adatok, többek között az eszköz típusa, a sorozatszám, a gyártó neve és az adathordozó mérete (ha van).

5. **Szűrt webhelyek** – Ebben a listában láthatók a Webhozzáférés-védelem vagy a. Ezekben a naplókban látható az idő, az URL-cím, az állapot, az IP-cím, a felhasználó és az adott webhely felé kapcsolatot megnyitó alkalmazás.

Kattintson a jobb gombbal bármely naplófájlra, és a **Másolás** parancsot kiválasztva másolja a naplófájl tartalmát a vágólapra.

Naplókezelés

Az ESET Endpoint Antivirus for macOS naplózási beállításai a program főablakában érhetők el. Kattintson a **Beállítások** > **Alkalmazásbeállítások megadása** > **Eszközök** > **Naplófájlok** elemre. A naplófájlokhoz az alábbi beállításokat adhatja meg:

- **Régi naplóbejegyzések automatikus törlése** – A program automatikusan törli a megadott napnál régebbi naplóbejegyzéseket.
- **Naplófájlok automatikus optimalizálása** – Ha a nem használt bejegyzések száma meghaladja a megadott százalékot, a program automatikusan elvégzi a naplófájlok töredezettségmentesítését.

A grafikus felhasználói felületen megjelenített minden idevonatkozó információ, kártevőre és eseményre utaló üzenet tárolható olvasható formában, például egyszerű szöveges vagy CSV- (vesszővel tagolt) fájlokban. Ha elérhetővé szeretné tenni ezeket a fájlokat külső gyártó eszközeiben történő feldolgozáshoz, jelölje be a **Szöveges fájlokba történő naplózás engedélyezése jelölőnégyzetet.**

A naplófájlok célmappájának a megadásához kattintson a **Beállítások** elemre a **További beállítások** mellett.

A **Szöveges naplófájlok**: **Szerkesztés** csoportban kiválasztott beállítások alapján a következő információkat tartalmazó naplókat mentheti:

- Az *Érvénytelen felhasználónév és jelszó*, *A modulok frissítése nem sikerült* és hasonló eseményeket a program az *eventslog.txt* fájlba írja
- A rendszerindításkori és a valós idejű ellenőrzés, valamint a számítógép-ellenőrzés által észlelt kártevőket a *threatslog.txt* nevű fájlban tárolja.
- Az összes befejezett ellenőrzés eredményét *scanlog.SZÁM.txt* formátumban tárolja.
- A rendszer az eszközfelügyelet által letiltott minden eszközt feljegyez a devctllog.txt fájlba.

Az **Alapértelmezett számítógép-ellenőrzési naplórekordok** szűrőinek a beállításához kattintson a **Szerkesztés** gombra, és jelölje be a kívánt naplótípusokat, vagy törölje a jelölésüket. A naplótípusokról további tudnivalókat talál a Napló szűrése című témakörben.

Napló szűrése

A naplók fontos rendszereseményekre vonatkozó információkat tartalmaznak. A naplószűrési funkció lehetővé teszi az adott eseményekre vonatkozó rekordok megjelenítését.

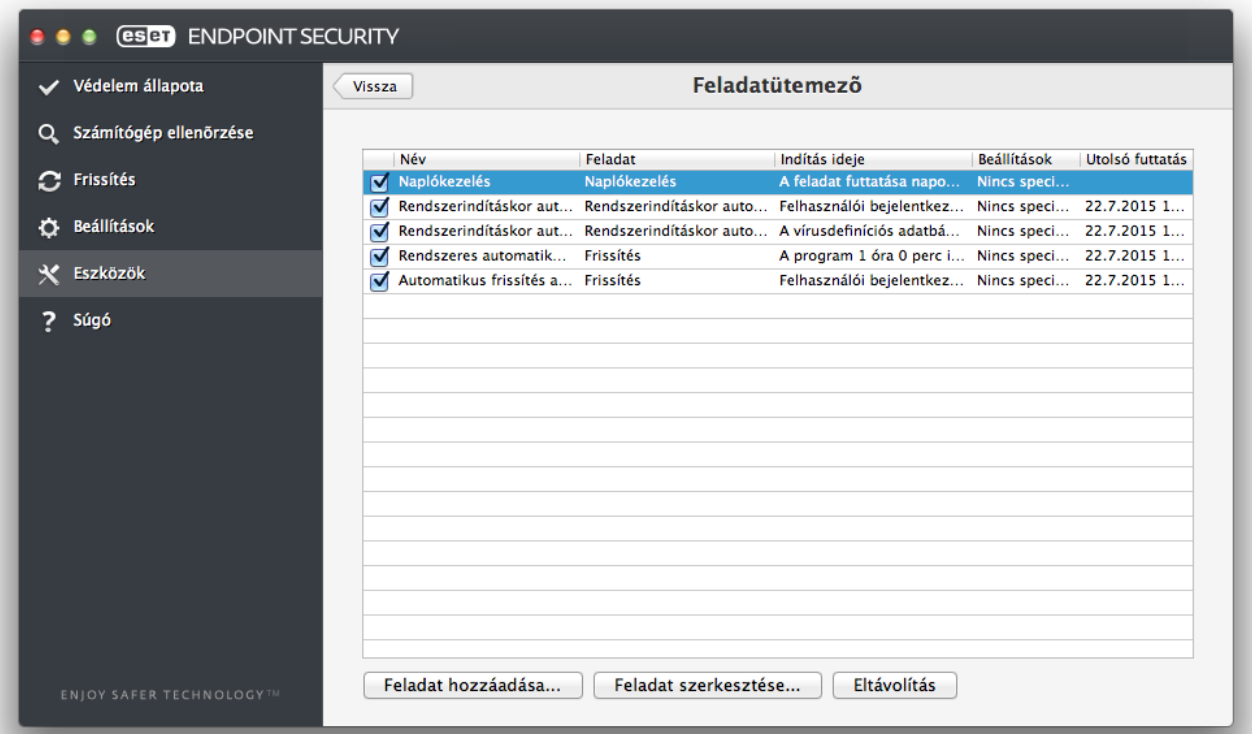
A leggyakrabban használt bejegyzéstípusok:

- **Kritikus figyelmeztetések** – Kritikus fontosságú rendszerhibák (például a vírusvédelmi szolgáltatás indítási hibája)

- **Hibák** – *Fájlletöltési* és kritikus hibákra vonatkozó hibaüzenetek
- **Figyelmeztetések** – Figyelmeztető üzenetek
- **Tájékoztató bejegyzések** – Sikeres frissítésekre, riasztásokra és hasonlókra vonatkozó tájékoztató üzenetek
- **Diagnosztikai bejegyzések** – A program és a fentebb ismertetett bejegyzések finomhangolásához felhasználható információk

Feladatütemező

A **Feladatütemező** az ESET Endpoint Antivirus for macOS főmenüjében található az **Eszközök** csoportban. A **Feladatütemező** valamennyi ütemezett feladat és beállított tulajdonságainak (például előre definiált dátum, időpont és ellenőrzési profil) összesített listáját tartalmazza.



A Feladatütemező bizonyos feladatok előre definiált beállításokkal és tulajdonságokkal történő indítását és kezelését végzi. Ilyen beállítás például a feladatindítás ideje, futtatásának gyakorisága, az ellenőrzési beállításokat tartalmazó profil stb.

A Feladatütemező alapértelmezés szerint az alábbi ütemezett feladatokat jeleníti meg:

- Naplókezelés (a **Rendszerfeladatok megjelenítése** funkciónak a feladatütemező beállításaiban történő engedélyezése után)
- Rendszerindításkor futtatott fájlok ellenőrzése a felhasználó bejelentkezése után

- Rendszerindításkor futtatott fájlok ellenőrzése a keresőmodulok sikeres frissítésekor
- Rendszeres automatikus frissítés
- Automatikus frissítés a felhasználó bejelentkezése után

A már meglévő (alapértelmezett és felhasználó által) ütemezett feladatok beállításainak módosításához nyomja le a CTRL billentyűt, jelölje ki a módosítani kívánt feladatot, és válassza a **Szerkesztés** parancsot, vagy jelölje ki a feladatot, és kattintson a **Feladat szerkesztése** gombra.

Új feladatok létrehozása

Ha új feladatot szeretne létrehozni a Feladatütemezőben, kattintson a **Feladat hozzáadása** gombra, vagy nyomja le a Control billentyűt, kattintson az üres mezőbe, és a helyi menüben válassza a **Hozzáadás** parancsot. Négyféle ütemezett feladat közül lehet választani:

- **Alkalmazás futtatása**
- **Frissítés**
- **Kézi indítású számítógép-ellenőrzés**
- **Rendszerindításkor automatikusan futtatott fájlok ellenőrzése**

Felhasználó által megadott feladatok

Alapértelmezés szerint az alkalmazásokat egy egyedi, ESET által létrehozott felhasználó futtatja, aki korlátozott jogokkal rendelkezik. Ha módosítani szeretné az alapértelmezett felhasználót, a parancs elé írja be a nevet, utána pedig egy kettőspontot (:). A **root** felhasználót is használhatja.

Példa: Feladat futtatása felhasználóként

Ebben a példában beütemezzük, hogy a Számológép alkalmazás elinduljon a megadott időben **UserOne** nevű felhasználóként:
1. A **Feladatütemezõben** válassza ki a **Feladat hozzáadása** elemet.
2. Írja be a feladat nevét. Az **Alkalmazás futtatása** esetén adja meg az **Ütemezett feladat** beállítást. A **Feladat futtatása** ablakban válassza ki az **Egyszer** beállítást a feladat egyszer történő futtatásához. Kattintson a **Tovább** gombra.
3. Kattintson a Tallózás gombra, majd válassza ki a Számológép alkalmazást.
4. Írja be a **UserOne:** nevet az alkalmazás elérési útvonala elé (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator'), majd kattintson a **Tovább** gombra.
5. Adja meg a feladat végrehajtási idejét, majd kattintson a **Tovább** gombra.
6. Válasszon ki egy alternatív lehetőséget, ha a feladat nem futtatható, majd kattintson a **Tovább** gombra.
7. Kattintson a **Befejezés** elemre.
8. Az ESET Feladatütemező el fogja indítani a Számológép alkalmazást a megadott időpontban.

Felhasználónévre vonatkozó korlátozások

Szóközök és térközkarakterek nem használhatók felhasználónév előtt. A felhasználónévben sem használhatók szóközök. Helyette üres karaktert használjon.

Ellenőrzés könyvtártulajdonosként

Ellenőrizhet könyvtárakat mint könyvtártulajdonos:
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done

A /tmp mappa is ellenőrizhető aktuálisan bejelentkezett felhasználóként:
root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

Példa: Frissítési feladat

A következő példában adott időpontban induló frissítési feladatot hozunk létre.
1. Válassza ki a **Frissítés** parancsot az **Ütemezett feladat** legördülő menüben.
2. Írja be a feladat nevét a **Feladat neve** mezőbe.
3. Válassza ki a feladat gyakoriságát a **Feladat futtatása** legördülő listában. A kiválasztott gyakoriságtól függően különböző frissítési paramétereket kell megadni. A **Felhasználó által megadva** beállítás választása esetén a program kérni fogja a dátum és idő megadását cron formátumban (további részletek a Felhasználó által megadott feladat létrehozása című témakörben találhatók).
4. A következő lépésben válasszon ki egy lehetőséget arra az esetre, ha a feladat nem hajtható végre vagy nem fejezhető be az ütemezett időpontban.
5. Kattintson a **Befejezés** elemre. A program felveszi az új ütemezett feladatot a jelenleg ütemezett feladatok listájára.

Az ESET Endpoint Antivirus for macOS a megfelelő működés biztosításához alapértelmezés szerint előre megadott ütemezett feladatokat tartalmaz. Ezeket a feladatokat nem célszerű módosítani, ezért rejtett állapotban vannak. Ha meg szeretné tekinteni a feladatokat, lépjen a főmenübe, kattintson a **Beállítások** > **Alkalmazásbeállítások megadása** > **Feladatütemező** elemre, majd válassza ki a **Rendszerfeladatok megjelenítése** lehetőséget.

Felhasználó által megadott feladat létrehozása

Amikor a Feladat futtatása legördülő listában a feladat típusaként a Felhasználó által megadva elemet választja, meg kell adnia néhány speciális paramétert.

A **felhasználó által megadott** feladat dátumát és időpontját éves kiterjesztett cron (6 mezőből álló, térközzel elválasztott) formátumban kell megadni:

```
perc(0-59) óra(0-23) hónap napja(1-31) hónap(1-12) év(1970-2099) hét napja(0-7)(vasárnap = 0 vagy 7)
```

Példa:

```
30 6 22 3 2012 4
```

Az alábbi speciális karakterek támogatottak a cron kifejezésekben:

- csillag (`*`) – a kifejezés megegyezik a mező összes értékével; a harmadik mezőben (hónap napja) lévő csillag például mindennapot jelent
- kötőjel (`-`) – tartományokat határoz meg; például `3–9`
- vessző (`,`) – lista elemeit választja el; például `1,3,7,8`

- perjel (/) – tartománynövekményeket határoz meg; például a 3-28/5 a harmadik mezőben (hónap napja) a hónap harmadik napját, majd minden 5. napot jelent.

A program nem támogatja a napneveket ((Monday-Sunday)) és a hónapneveket ((January-December)).

> **Felhasználó által megadott feladatok**
> Ha meghatározza mind a hónap, mind a hét napját, a program csak akkor hajtja végre a parancsot, ha a két mező megegyezik.

LiveGrid®

A LiveGrid® korai riasztási rendszerrel biztosítható, hogy az ESET azonnal és folyamatosan értesüljön az új fertőzésekről. A kétirányú LiveGrid® korai riasztási rendszer egyedüli célja, hogy minél hatékonyabb védelmet biztosítson a felhasználóknak. Az új kártevőkről úgy értesülhetünk a megjelenésüket követően a leghamarabb, ha a lehető legtöbb ügyfelünkkel tartunk fenn kapcsolatot, és az általuk gyűjtött információkat felhasználjuk a keresőmotorok folyamatos frissítéséhez. Válasszon a LiveGrid® alábbi két beállítása közül:

1. Dönthet úgy, hogy nem engedélyezi a LiveGrid® korai riasztási rendszert. A szoftver funkciói megmaradnak, bizonyos esetekben azonban előfordulhat, hogy az ESET Endpoint Antivirus for macOS a keresőmodulok frissítésénél gyorsabban reagál az új kártevőkre.

2. Beállíthatja a LiveGrid® korai riasztási rendszert úgy is, hogy az anonim információkat küldjön az új kártevőkről, valamint arról, hogy a kártevőt hordozó új kód melyik fájlban található. A szoftver ezt az információt el tudja küldeni az ESET víruslaborjába további elemzés céljából. A kártevők tanulmányozása az ESET segítségére szolgál a vírusdefiníciós adatbázis frissítésében, és javítja a kártevő-észlelési képességünket.

A LiveGrid® korai riasztási rendszer összegyűjti a számítógép újonnan észlelt kártevőkkel kapcsolatos adatait. Ez az információ tartalmazhatja a kártevőt magában foglaló fájl mintáját vagy másolatát, a fájl elérési útját és nevét, a dátumot és az időt, azt a folyamatot, amelynek során a kártevő megjelent a számítógépen, valamint a számítógép operációs rendszerére vonatkozó adatokat.

Noha nem kizárt, hogy így a felhasználó néhány személyes adata (például egy elérési úton szereplő felhasználónév) vagy a számítógép bizonyos adatai esetenként eljuthatnak az ESET víruslaborjába, az adatok felhasználásának célja kizárólag az új kártevőkkel szembeni új megoldások kidolgozása.

Ha el szeretné érni a LiveGrid® beállításait a főmenüből, válassza a **Beállítások** > **Alkalmazásbeállítások megadása** > **LiveGrid®** lehetőséget. A LiveGrid® aktiválásához jelölje be **Az ESET LiveGrid® megbízhatósági rendszer engedélyezése (javasolt)** jelölőnégyzetet, majd kattintson a **Beállítások** gombra a **További beállítások** mellett.

Gyanús fájlok

Az ESET Endpoint Antivirus for macOS alapértelmezés szerint elküldi a gyanús fájlokat alapos elemzésre az ESET víruslaborjába. Ha nem szeretné automatikusan elküldeni a fájlokat, törölje a **Gyanús fájlok elküldése (Beállítások** > **Alkalmazásbeállítások megadása** > **LiveGrid® > Beállítások)** jelölőnégyzet bejelölését.

Ha gyanús fájlt talál, elküldheti elemzésre a víruslaborunknak. Ehhez a program főablakában kattintson az **Eszközök** > **Fájl elküldése elemzésre** hivatkozásra. Ha az egy kártékony alkalmazás, a felismerését felvesszük a legközelebbi frissítésbe.

Anonim statisztikai adatok küldése – Az ESET LiveGrid® korai riasztási rendszer az újonnan felfedezett

kártevőkkel kapcsolatos információkat gyűjt a számítógépről. Az információk közé tartozik a kártevő neve, az észlelés dátuma és időpontja, az ESET biztonsági termék verziószáma, az operációs rendszer verziója és a területi beállítások. Ezeket a statisztikai adatokat a program általában naponta egy vagy két alkalommal küldi el az ESET szerverére.

Példa: Elküldött statisztikai csomag

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

Kivétel szűrő – Ezzel a funkcióval bizonyos fájltípusok kizárhatók az elküldésből. Az olyan fájlokat érdemes kizárni, amelyek bizalmas információkat tartalmazhatnak (például a dokumentumok vagy a táblázatok). A leggyakoribb fájltípusok (.doc, .rtf stb.) alapértelmezés szerint ki vannak zárva. A kizárt fájlok listája szükség szerint bővíthető.

E-mail-cím (nem kötelező) – E-mail-címét akkor használjuk, ha az elemzéshez további információra van szükségünk. Az ESET munkatársai csak akkor keresik, ha a gyanús fájlokkal kapcsolatban további információra van szükség.

Karantén

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

Bármilyen fájlt karanténba helyezhet. A szóban forgó fájlt akkor érdemes karanténba helyezni, ha viselkedése gyanús, a víruskereső azonban nem észleli. A karanténba helyezett fájlok elemzés céljából elküldhetők az ESET víruslaborjának.

A karanténmappában lévő fájlokat egy táblázat jeleníti meg, amelyben látható a karanténba helyezés dátuma és időpontja, a fertőzött fájl eredeti helyének elérési útja, a fájl bájtban megadott mérete, a karanténba helyezés oka (például a felhasználó vette fel az objektumot) és az észlelt fertőzések száma. A karanténmappa (*/Library/Application Support/Eset/esets/cache/quarantine*) az ESET Endpoint Antivirus for macOS eltávolítása után is a rendszerben marad. A karanténba helyezett fájlok tárolása biztonságos titkosított formában történik, és a fájlok az ESET Endpoint Antivirus for macOS telepítése után ismét visszaállíthatók.

Fájlok karanténba helyezése

Az ESET Endpoint Antivirus for macOS automatikusan karanténba helyezi a törölt fájlokat (ha nem törölte a beállítás bejelölését a riasztási ablakban). A Karantén ablakban a Karantén elemre kattintva kézzel is felvehet bármilyen fájlt a karanténba. A fájlt a karanténba küldheti úgy is, hogy lenyomja a CTRL billentyűt, a fájlra kattint, és a Szolgáltatások > ESET Endpoint Antivirus for macOS – Fájlok karanténba helyezése parancsot választja.

Visszaállítás a karanténból

A karanténba helyezett fájlok visszaállíthatók az eredeti helyükre. Ehhez jelölje ki a fájlt, és kattintson a **Visszaállítás** gombra. A visszaállítást a helyi menüből is elvégezheti. Nyomja le a CTRL billentyűt, kattintson az adott fájlra a Karantén ablakban, és kattintson a **Visszaállítás** parancsra. A **Visszaállítás megadott helyre** beállítást használva az eredeti helyétől eltérő helyre is visszaállíthatja a fájlt.

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 nyomja le a CTRL billentyűt és kattintson a fájlra, majd válassza a helyi menü **Elemzésre küldés** parancsát.

Jogosultságok

Az ESET Endpoint Antivirus for macOS beállításai nagyon fontosak lehetnek szervezete biztonsági házirendje szempontjából. A jogosulatlan módosítások veszélyeztethetik a rendszer stabilitását és védelmét. Ezért lehetősége van kiválasztani, hogy mely felhasználók rendelkezzenek a programkonfiguráció szerkesztésére vonatkozó engedéllyel.

A jogosult felhasználók a **Beállítások** > **Alkalmazásbeállítások megadása** > **Felhasználó** > **Jogosultságok** részen konfigurálhatók.

A rendszer maximális biztonsága érdekében fontos, hogy a program megfelelően legyen konfigurálva. A jogosulatlan módosítások fontos adatok elvesztésével járhatnak. A jogosult felhasználók listájának megadásához egyszerűen jelölje ki őket a bal oldali **Felhasználók** listában, és kattintson a **Hozzáadás** gombra. Felhasználó eltávolításához jelölje ki a nevét a jobb oldali **Jogosult felhasználók** listában, és kattintson az **Eltávolítás** gombra. Az összes felhasználó megjelenítéséhez válassza **Az összes felhasználó megjelenítése** beállítást.

> **Üres a jogosult felhasználók listája**
> Ha a jogosult felhasználók listája üres, a rendszer összes felhasználója számára engedélyezett a programbeállítások szerkesztése.

Bemutató üzemmód

A **bemutató üzemmód** azoknak a felhasználóknak hasznos, akiknek fontos a szoftverek megszakítás nélküli használata, és nem szeretnék, hogy előugró ablakok zavarják meg őket, illetve szeretnék minimalizálni a processzor terhelését. A bemutató üzemmód olyan bemutatók során használható, amelyeket nem szakíthat meg semmiféle vírusvédelmi művelet. Engedélyezése esetén minden előugró ablak le van tiltva, és az ütemezett feladatok nem futnak. A rendszervédelem változatlanul működik a háttérben, felhasználói beavatkozást azonban nem igényel.

A bemutató üzemmód engedélyezéséhez válassza a **Beállítások** > **Alkalmazásbeállítások megadása** > **Bemutató üzemmód** > **Bemutató üzemmód engedélyezése** lehetőséget.

Jelölje be a **Bemutató üzemmód automatikus engedélyezése teljes képernyős módban jelölőnégyzetet**, ha azt

szeretné, hogy az alkalmazások teljes képernyős módban történő futtatásakor a program automatikusan bemutató üzemmódra váltson. A szolgáltatás engedélyezésekor a bemutató üzemmód elindul, valahányszor elindít egy teljes képernyős alkalmazást, és automatikusan leáll, ha kilép az alkalmazásból. Ez különösen hasznos a bemutatók indításakor.

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

A bemutató üzemmód engedélyezése lehetséges biztonsági kockázatot is jelent, amelyre az ESET Endpoint Antivirus for macOS védelmének állapotát jelző, a tálcán narancssárga színűre váltó állapotikon figyelmeztet.

Futó folyamatok

A **Futó folyamatok** listája megjeleníti a számítógépen futó folyamatokat. Az ESET Endpoint Antivirus for macOS részletes információkkal szolgál a futó folyamatokról a felhasználók védelmének biztosításához az ESET LiveGrid® technológiával.

- **Folyamat** – A számítógépen éppen futó folyamat neve. A számítógépen futó összes folyamat megtekintéséhez használható az aktivitásfigyelő (helye: */Applications/Utilities*).

- **Kockázati szint** – A legtöbb esetben az ESET Endpoint Antivirus for macOS az ESET LiveGrid® technológiát használva, heurisztikus szabályokkal kockázati szinteket rendel az objektumokhoz (fájlokhoz, folyamatokhoz stb.), ennek során megvizsgálva az egyes objektumok jellemzőit, majd súlyozva a kártékony tevékenységek előfordulásának lehetőségét. Ezeken a heurisztikus szabályokon alapulva a program kockázati szintet rendel az objektumokhoz. A zöld színnel megjelölt ismert alkalmazások egészen biztosan nem fertőzöttek (engedélyezőlistán vannak), ezért a szűrésből kizártak. Ez növeli a kézi indítású és a valós idejű ellenőrzés sebességét is. Az alkalmazás nem feltétlenül kártékony szoftver, ha a jelölése ismeretlen (sárga). Ezek rendszerint csak újabb alkalmazások. Ha nem biztos egy fájlban, elküldheti elemzésre az ESET víruslaborjába. Ha a fájl kártékony alkalmazás, bekerül a vírusdefiníciós adatbázis valamelyik későbbi frissítésébe.

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

- **Észlelés ideje** – Az az időtartam, amióta az ESET LiveGrid® technológia észlelte az alkalmazást.

- **Alkalmazáscsomag azonosítója** – A gyártó vagy az alkalmazásfolyamat neve.

Ha az ablak alján egy adott folyamatra kattint, az alábbi információk jelennek meg róla.

- **Fájl** – Alkalmazás helye a számítógépen.

- **Fájlméret** – A fájl mérete a lemezen.

- **Fájlleírás** – A fájl jellemzői az operációs rendszer leírása alapján.

- **Alkalmazáscsomag azonosítója** – A gyártó vagy az alkalmazásfolyamat neve.

- **Fájlverzió** – Az alkalmazás gyártójától származó információ.

- **Terméknév** – Az alkalmazás és/vagy a gyártó cég neve.

Felhasználói felület

A felhasználói felület beállításai lehetővé teszik, hogy a felhasználó a saját igényei szerint alakítsa ki munkakörnyezetét. A beállítások eléréséhez a főmenüben válassza a **Beállítások** > **Alkalmazásbeállítások megadása** > **Interfész** lehetőséget.

- Az ESET Endpoint Antivirus for macOS nyitóképernyőjének rendszerindításkor történő megjelenítéséhez jelölje be a **Nyitóképernyő megjelenítése indításkor** jelölőnégyzetet.

- Az **Alkalmazás elhelyezése a Dockban** opcióval megjelenítheti az ESET Endpoint Antivirus for macOS ikonját a macOS Dockban, és a *cmd+tab* billentyűkombinációt lenyomva válthat az ESET Endpoint Antivirus for macOS és más futó alkalmazások között. A módosítások az ESET Endpoint Antivirus for macOS újraindítása után lépnek érvénybe (általában a számítógép újraindítását követően).

- A **Szokásos menü használata** opció lehetővé teszi bizonyos billentyűparancsok használatát (lásd Billentyűparancsok) és a szokásos menüelemek megtekintését (Felhasználói felület, Beállítások és Eszközök) a macOS menüsorán (a képernyő tetején).

- Az **Eszköztippek megjelenítése** funkció engedélyezésével megjelenítheti az eszköztippeket, amikor a kurzort az ESET Endpoint Antivirus for macOS bizonyos beállításai fölé viszi.

- A **Rejtett fájlok megjelenítése** beállítással megjelenítheti és kijelölheti a rejtett fájlokat a **Számítógép ellenőrzése** funkció **Ellenőrizendő célterületek** beállításában.

- Alapértelmezés szerint az ESET Endpoint Antivirus for macOS ikon megjelenik a menüsor extrái között a macOS menüsorának jobb oldalán (a képernyő tetején). Ha le szeretné tiltani, törölje az **Ikon megjelenítése a menüsáv extrái között** opció bejelölését. A módosítás az ESET Endpoint Antivirus for macOS újraindítása után lép érvénybe (általában a számítógép újraindítását követően).

Riasztások és értesítések

A **Riasztások és értesítések** csoportban beállíthatja, hogy az ESET Endpoint Antivirus for macOS hogyan kezelje a kártevőriasztásokat, valamint a védelmi állapotra vonatkozó és a rendszerértesítéseket.

A **Riasztások megjelenítése** opció kikapcsolásakor a szoftver egyetlen riasztást sem jelenít meg – mindez azonban csak az események szűk körére alkalmazható beállítás. A legtöbb felhasználó számára javasolt, hogy hagyja bekapcsolva ezt az opciót (alapértelmezett beállítás). A további beállítások ismertetése ebben a fejezetben található.

Az **Értesítések megjelenítése az asztalon** jelölőnégyzet bejelölésével engedélyezi azoknak a riasztási ablakoknak az asztalon való megjelenítését (alapértelmezés szerint a képernyő jobb felső sarkában), amelyek nem igényelnek felhasználói beavatkozást. Az **Értesítések automatikus bezárása ezt követően:** X **másodperc** érték módosításával meghatározhatja az értesítés megjelenésének időtartamát (ez alapértelmezés szerint 5 másodperc).

Az ESET Endpoint Antivirus for macOS 6.2-es verziójától kezdve letilthatja azt is, hogy egyes **védelmi állapotok** megjelenjenek a program főképernyőjén (a **Védelem állapota** ablakban). Erről a Védelmi állapotok című

témakörben olvashat bővebben.

Riasztások megjelenítése

Az ESET Endpoint Antivirus for macOS értesítési ablakokat jelenít meg az új programverziókról, az operációs rendszer új frissítéseiről, egyes programösszetevők letiltásáról, naplók törléséről stb. Az egyes értesítéseket a **Ne jelenjen meg többet ez a párbeszédpanel** jelölőnégyzet bejelölésével tilthatja le az adott párbeszédpaneleken.

A **párbeszédpanelek listája** (a **Beállítások** > **Alkalmazásbeállítások megadása** > **Riasztások és értesítések** > **Riasztások megjelenítése: Beállítások...** csoportban) megjeleníti az ESET Endpoint Antivirus for macOS által kiváltott összes riasztási párbeszédpanel listáját. Az egyes értesítések engedélyezéséhez vagy letiltásához jelölje be a **Párbeszédpanel neve** melletti jelölőnégyzetet. Ha a párbeszédpanel be van jelölve, az adott értesítés mindig megjelenik, és a **megjelenítési feltételek** nem érvényesülnek. Ha nem szeretne értesítést kapni a listában található bizonyos eseményekről, törölje a jelet a jelölőnégyzetből. Ezenkívül meghatározhatja azt is, hogy milyen **megjelenítési feltételek** mellett menjenek végbe bizonyos műveletek.

Védelmi állapotok

Az ESET Endpoint Antivirus for macOS védelmi állapota az állapotok be- vagy kikapcsolásával módosítható a **Beállítások** > **Alkalmazásbeállítások megadása...** > **Riasztások és értesítések** > **Megjelenítés a Védelem állapota képernyőn: Beállítások** részen. A különféle programfunkciók állapota az ESET Endpoint Antivirus for macOS főképernyőjén (a **Védelem állapota** ablakban) jeleníthető meg vagy rejthető el.

Az alábbi programfunkciók védelmi állapotát rejtheti el:

- Adathalászat elleni védelem
- Webhozzáférés-védelem
- E-mail védelem
- Bemutató üzemmód
- Operációsrendszer-frissítés
- Licenc lejárata
- A számítógép újraindítása szükséges

Helyi menü

Ha elérhetővé szeretné tenni az ESET Endpoint Antivirus for macOS szolgáltatásait a helyi menüből, kattintson a **Beállítások** > **Alkalmazásbeállítások megadása** > **Helyi menü** lehetőségre, és jelölje be az **Integrálás a helyi menübe** jelölőnégyzetet. A módosítások a kijelentkezéskor vagy a számítógép újraindításakor lépnek érvénybe. A helyi menü beállításai elérhetők az asztalon és a **Finder** ablakában, amikor lenyomja a CTRL billentyűt, és egy fájlra vagy mappára kattint.

Frissítés

Az ESET Endpoint Antivirus for macOS rendszeres frissítésével tartható fenn a biztonság maximális szintje. A Frissítés modul a legfrissebb keresőmodulok letöltésével biztosítja, hogy a program mindig naprakész legyen.

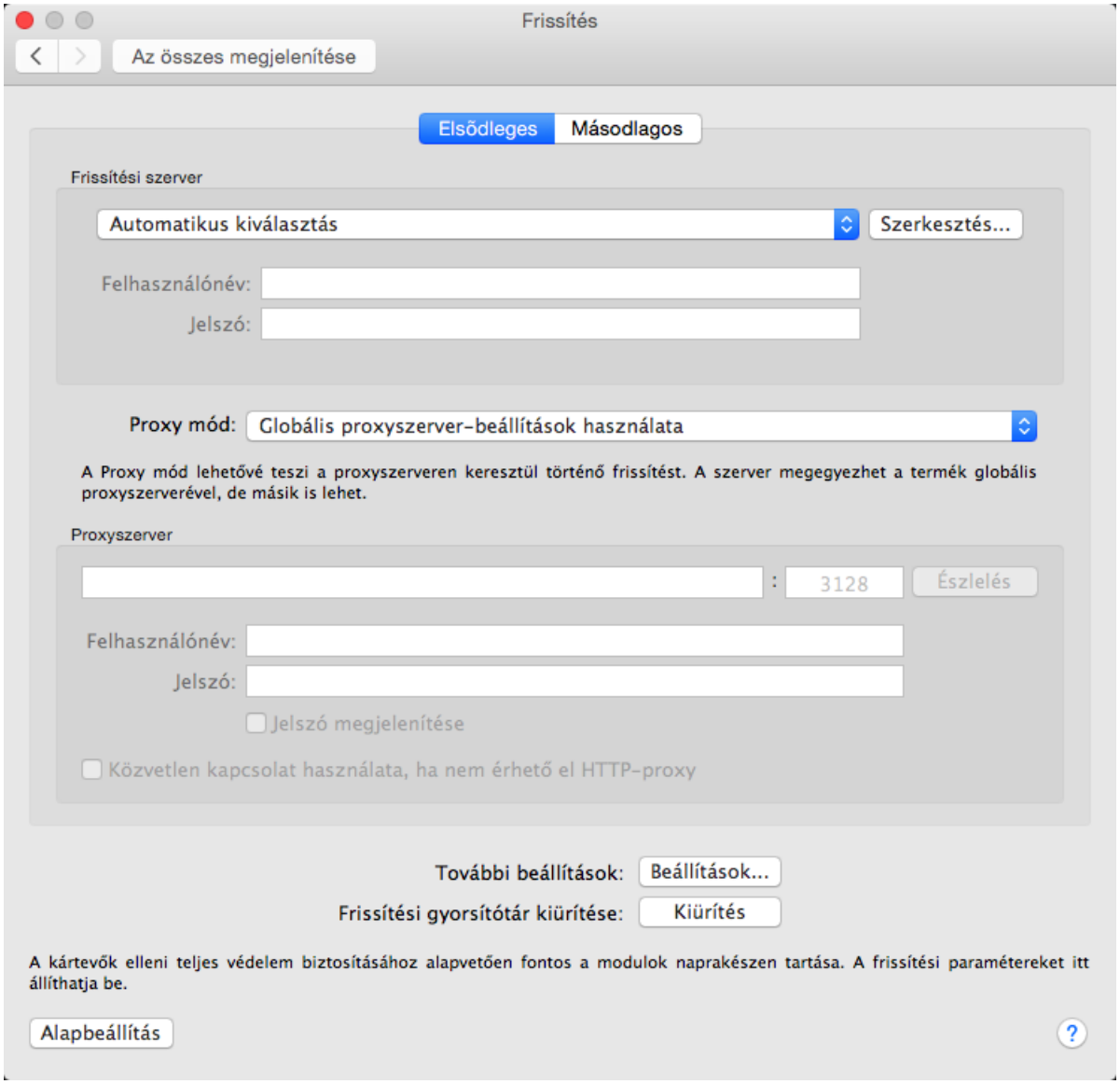
A főmenü **Frissítés** parancsára kattintva megjelenítheti az aktuális frissítési állapotot, beleértve az utolsó sikeres frissítés dátumát és időpontját, valamint azt, hogy szükség van-e frissítésre. A frissítési folyamat kézi indításához kattintson a **Modulok frissítése** hivatkozásra.

Ha szokásos körülmények között, a frissítések megfelelő letöltése esetén rendelkezik a legújabb modulokkal, a Frissítés ablakban a *Nincs szükség frissítésre – a telepített modulok aktuálisak* üzenet jelenik meg. Ha a modulok nem frissíthetők, javasoljuk, hogy ellenőrizze a frissítési beállításokat – e hiba leggyakoribb oka a helytelenül megadott licencadatok vagy a helytelenül konfigurált kapcsolatbeállítások.

A **Update** ablakban látható a keresőmotor verziószáma is. Ez a verziószámjelzés az ESET webhelyével van összekapcsolva, ahol láthatók a keresőmotor frissítési adatai.

Frissítési beállítások

A frissítési beállításoknál adhatja meg a frissítési forrás információit, például a frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat. A **Frissítési szerver** legördülő lista alapértelmezés szerinti **Automatikus kiválasztás** beállítása biztosítja, hogy a program – a lehető legkisebb hálózati forgalom mellett – automatikusan letöltse a frissítési fájlokat az ESET szerveréről.



A rendelkezésre álló frissítési szerverek listája a **Frissítési szerver** legördülő listában található. Új frissítési szerver felvételéhez kattintson a **Szerkesztés gombra,** adja meg az új szerver címét a **Frissítési szerver** beviteli mezőben, és kattintson a **Hozzáadás** gombra.

Az ESET Endpoint Antivirus for macOS lehetővé teszi egy másik vagy feladatátvételi frissítési szerver megadását. Az **Elsődleges** szerver lehet a tükörszerver, és a **Másodlagos szerver** a szokásos ESET frissítési szerver. A másodlagos szerver nem lehet azonos az elsődlegessel, ellenkező esetben nem használható. Ha nem ad meg másodlagos frissítési szervert, felhasználónevet és jelszót, a feladatátviteli frissítési funkció nem fog működni. Választhatja az Automatikus kiválasztás lehetőséget is, és a megfelelő mezőkben megadhatja a felhasználónevet és a jelszót ahhoz, hogy az ESET Endpoint Antivirus for macOS automatikusan kiválassza a legalkalmasabb használandó frissítési szervert.

A **Proxy mód** lehetővé teszi a keresőmodulok frissítését proxyszerveren (például helyi HTTP-proxyn) keresztül. A szerver megegyezhet a kapcsolatot igénylő összes programfunkcióhoz megfelelő globális proxyszerverrel, de lehet attól eltérő is. A globális proxyszerver beállításait már a telepítés során, illetve a Proxyszerver beállítása részen meg kell adni.

Kliens beállítása csak a frissítések letöltésére egy proxyszerverről:

1. A legördülő listában válassza a **Kapcsolódás proxyszerveren keresztül** elemet.

2. Az **Észlelés** gombra kattintva engedélyezheti az ESET Endpoint Antivirus for macOS alkalmazásnak az IP-cím és a portszám kitöltését (**3128** alapértelmezés szerint).

3. Ha a proxyszerver hitelesítést igényel, a megfelelő mezőkben adjon meg egy érvényes **felhasználónevet** és **jelszót**.

Az ESET Endpoint Antivirus for macOS a macOS rendszerbeállításaiból ismeri fel a proxybeállításokat. Ezek a macOS rendszerben a > **System Preferences** (Rendszerbeállítások) > **Network** (Hálózat) > **Advanced** (Speciális) > **Proxies** (Proxyk) részen állíthatók be.

Ha engedélyezi a **Közvetlen kapcsolat használata, ha nem érhető el HTTP-proxy** opciót, az ESET Endpoint Antivirus for macOS megkísérel proxy használata nélkül automatikusan csatlakozni a frissítési szerverekhez. Ez az opció MacBookkal rendelkező mobilfelhasználóknak javasolt.

Ha a keresőmodulok frissítéseinek letöltése során problémát tapasztal, a **Frissítési gyorsítótár kiürítése gombra kattintva törölje az ideiglenes frissítési fájlokat**.

További beállítások

Ha le szeretné tiltani az egyes sikeres frissítések után megjelenő értesítéseket, válassza ki a **Sikeres frissítésről szóló értesítések megjelenítésének mellőzése** opciót.

Engedélyezze az előzetes frissítéseket a végső tesztelésen átesett fejlesztési modulok letöltéséhez. Az előzetes frissítések gyakran a termékhibák javításait tartalmazzák. A késleltetett frissítések letöltése a kiadásukat követő néhány órán belül valósul meg, így biztosítva, hogy a kliensek frissítéseit addig ne töltsék le a felhasználók, amíg a hibáikat ki nem javítják.

Az ESET Endpoint Antivirus for macOS pillanatfelvételeket készít a kereső- és programmodulokról a **Frissítési fájlok visszaállítása** funkcióhoz való használatra. Hagyja bekapcsolva a **Frissítési fájlok pillanatképének létrehozása** funkciót ahhoz, hogy az ESET Endpoint Antivirus for macOS automatikusan rögzítse ezeket a pillanatképeket. Ha egy új keresőmodul és/vagy a programmodulok egyik új frissítése feltehetően nem stabil, illetve sérült, a Frissítési fájlok visszaállítása funkciót használva visszaállhat az előző verzióra, és adott időszakra letilthatja a frissítéseket. Másik lehetőségként engedélyezheti a korábban letiltott frissítéseket, ha bizonytalan időre elhalasztotta őket. Amikor a Frissítési fájlok visszaállítása funkcióval visszaáll egy korábbi frissítésre, használja a Felfüggesztési időszak beállítása a következőre legördülő listát annak az időszaknak a megadásához, amely során fel szeretné függeszteni a frissítéseket. Ha a Visszavonásig lehetőséget választja, a szokásos frissítések addig nem folytatódnak, amíg kézzel vissza nem állítja őket. Körültekintően járjon el, amikor megadja a frissítések felfüggesztésének időtartamát.

A keresőmotor elavulási idejének beállítása automatikusan – Ez a funkció lehetővé teszi a maximális időtartam megadását (napokban), amely után a keresőmodulokat elavultként fogja jelenteni. Az alapértelmezett érték 7 nap.

Frissítési feladatok létrehozása

A keresőmodulok frissítését a Frissítés > **UModulok frissítése** elemre kattintva indíthatja el.

A frissítések ütemezett feladatokként is futtathatók. Ha ütemezett feladatot szeretne beállítani, az **Eszközök** lapon válassza a **Feladatütemező** eszközt. Az ESET Endpoint Antivirus for macOS programban alapértelmezés szerint az alábbi feladatok aktívak:

- **Rendszeres automatikus frissítés**
- **Automatikus frissítés a felhasználó bejelentkezése után**

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

Operációsrendszer-frissítések

A macOS-rendszerfrissítések szolgáltatás fontos szerepet játszik a felhasználók védelmében a kártevő szoftverek ellen. Javasoljuk, hogy a maximális védelem biztosítása érdekében a kiadásukat követően rögtön telepítse ezeket a frissítéseket. Az ESET Endpoint Antivirus for macOS a fontossági szintnek megfelelően értesítést küld a hiányzó frissítésekről. Az értesítések megjelenítéséhez módosíthatja a frissítések fontosságának szintjét a **Beállítások** > **Alkalmazásbeállítások megadása** > **Riasztások és értesítések > Beállítások részen az Operációsrendszer-frissítések melletti Megjelenítési feltételek** legördülő menüben.

- **Az összes frissítés megjelenítése** – Értesítés jelenik meg, valahányszor egy rendszerfrissítés hiányzik
- **Csak a javasoltak megjelenítése** – Csak a javasolt frissítésekről kap értesítést

Ha nem szeretne értesítéseket kapni a hiányzó frissítésekről, törölje az **Operációsrendszer-frissítések** felirat melletti jelölőnégyzet bejelölését.

Az értesítési ablakban látható a macOS operációs rendszerhez elérhető frissítések és a macOS natív eszközzel (Szoftverfrissítések) frissített alkalmazások áttekintése. A frissítést futtathatja közvetlenül az értesítési ablakból vagy az ESET Endpoint Antivirus for macOS alkalmazás **Védelem állapota** részén **A hiányzó frissítések telepítése** elemre kattintva.

Az értesítési ablakban látható az alkalmazás neve, verziószáma, mérete, a tulajdonságok (jelzők) és a rendelkezésre álló frissítések további adatai. A **Jelzők** oszlop az alábbi információkat tartalmazza:

- **[javasolt]** – Az operációs rendszer gyártója javasolja, hogy a rendszer biztonsága és stabilitása érdekében telepítse ezt a frissítést

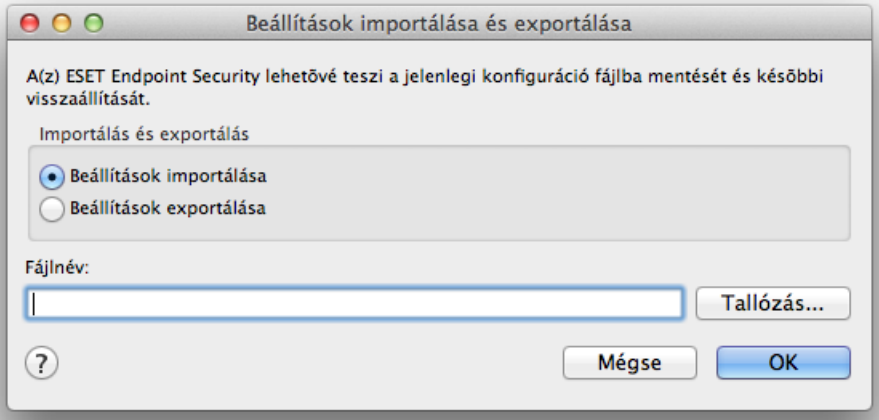
- **[újraindítás]** – A telepítést követően újra kell indítani a számítógépet
- **[leállítás]** – A telepítést követően le kell állítani, majd újra be kell kapcsolni a számítógépet

Az értesítési ablakban láthatók a „softwareupdate” nevű parancssori eszközzel lekért frissítések. Ezek a frissítések eltérhetnek a Szoftverfrissítések (Software updates) alkalmazás által megjelenített frissítésektől. Ha a hiányzó szoftverfrissítéseket megjelenítő ablakban látható összes frissítést, valamint a Szoftverfrissítések alkalmazásban nem látható frissítéseket is szeretné telepíteni, a „softwareupdate” nevű parancssori eszközt kell használnia. Az eszközről a „softwareupdate” kézikönyvében olvashat bővebben, ha beírja a `man softwareupdate` kifejezést a **Terminál** ablakba. Ez csak tapasztalt felhasználóknak javasolt.

Beállítások importálása és exportálása

Meglévő konfiguráció importálásához vagy az ESET Endpoint Antivirus for macOS konfigurációjának exportálásához válassza a **Beállítások** parancsot, és kattintson a **Beállítások importálása és exportálása hivatkozásra.**

Importálásra és exportálásra akkor lehet szükség, ha az ESET Endpoint Antivirus for macOS aktuális konfigurációjáról későbbi használat céljából biztonsági másolatot kell készítenie. A beállítások exportálása azok számára is hasznos, akik az ESET Endpoint Antivirus for macOS előnyben részesített beállításait több rendszerben is szeretnék használni. A kívánt beállításokat egyszerűen átviheti egy konfigurációs fájl importálásával.



Ha konfigurációt szeretne importálni, válassza a **Beállítások importálása** lehetőséget, és a **Tallózás** gombra kattintva keresse meg az importálni kívánt konfigurációs fájlt. Ha exportálni szeretne, válassza a **Beállítások exportálása** elemet, és a tallózási funkcióval jelöljön ki egy helyet a számítógépen, ahová menteni szeretné a fájlt.

Proxyszerver beállítása

A proxyszerver beállításai a **Beállítások** > **Alkalmazásbeállítások megadása** > **Proxyszerver** részen adhatók meg. A proxyszerver megadása ezen a szinten meghatározza az ESET Endpoint Antivirus for macOS összes funkciójának globális proxyszerver-beállítását. Az itt található paramétereket fogja használja az internetkapcsolatot igénylő összes modul. Az ESET Endpoint Antivirus for macOS támogatja a Basic Access és az NTLM (NT LAN Manager) típusú hitelesítést.

A proxyszerver-beállítások megadásához ezen a szinten jelölje be a **Proxyszerver használata** opciót, és a **Proxyszerver** mezőben adja meg a proxyszerver IP-címét vagy URL-címét. A Port mezőben adja meg azt a portot, amelyen a proxyszerver fogadja a kapcsolatokat (alapértelmezés szerint a (3128-as port). Az **Észlelés** gombra kattintva engedélyezheti, hogy a program töltse ki mindkét mezőt.

Ha a proxyszerver hitelesítést igényel, a megfelelő mezőkben adjon meg egy érvényes **felhasználónevet** és **jelszót**.

Megosztott helyi gyorsítótár

A megosztott helyi gyorsítótár használatának engedélyezéséhez kattintson a Beállítások > Alkalmazásbeállítások megadása > Megosztott helyi gyorsítótár elemre, és jelölje be a Gyorsítótárazás engedélyezése az ESET Megosztott helyi gyorsítótár használatával jelölőnégyzetet. A funkció használatával javíthatja a virtualizált környezetek teljesítményét oly módon, hogy kiküszöböli az ismétlődő ellenőrzést a hálózatban. Ezzel biztosítható, hogy minden egyes fájlt csak egyszer ellenőrizzen a program, tárolásuk pedig a megosztott gyorsítótárban történjen. Ha engedélyezve van, információkat menthet a helyi gyorsítótárba a hálózaton lévő fájlok és mappák ellenőrzéseiről. Új ellenőrzés végrehajtásakor az ESET Endpoint Antivirus for macOS megkeresi az ellenőrzött fájlokat a gyorsítótárban. Ha talál egyezést, az egyező fájlokat kizárja az ellenőrzésből.

A megosztott helyi gyorsítótár beállításai közé tartoznak az alábbiak:

- **Szerver címe** – Annak a számítógépnek a neve vagy IP-címe, amelyen a gyorsítótár található.
- **Port** – A kapcsolathoz használt port száma (alapértelmezés szerint a (3537-es)
- **Jelszó** – A megosztott helyi gyorsítótár jelszava (nem kötelező)

> **Részletes útmutató**
> Az ESET Megosztott helyi gyorsítótár telepítésére és beállítására vonatkozó részletes utasításokat az ESET Megosztott helyi gyorsítótár felhasználói útmutatójában talál. (Az útmutató csak angol nyelven áll rendelkezésre.)

Végfelhasználói licencszerződés

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

Végfelhasználói licencszerződés

Jelen végfelhasználói licencszerződés (a továbbiakban „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; a továbbiakban „ESET” vagy „Gyártó”), másfelől Ön mint természetes vagy jogi személy (a továbbiakban „Ön” vagy „Végfelhasználó”) között jött létre, Ön jogosult a jelen Szerződés 1. pontjában meghatározott Szoftver használatára. A jelen Szerződés 1. pontjában meghatározott Szoftver az alábbiakban megadott feltételeknek megfelelően adathordozón tárolható, e-mailben küldhető, az internetről vagy a Gyártó szervereiről letölthető, illetve más forrásokból beszerezhető.

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

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

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

1. **Szoftver**. A jelen Szerződésben a „Szoftver" kifejezés a következőt jelenti: (i) a jelen Szerződéshez 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 (a továbbiakban „Dokumentáció"); (iv) a Szoftver másolatai, lehetséges hibáinak javításai, kiegészítései, bővítményei, módosított verziói, összetevőinek frissítései (ha vannak), amelyekhez a Gyártó a jelen Szerződés 3. pontja szerint Önnek használati engedélyt adott. A Szoftver kizárólag végrehajtható tárgykód formájában szerezhető be.

2. **Telepítés, Számítógép és Licenckulcs**. Az adathordozón biztosított, e-mailben küldött vagy az internetről, illetve a Gyártó szervereiről letöltött vagy más forrásból megszerzett Szoftvert telepíteni kell. A Szoftvert megfelelően konfigurált számítógépre kell telepíteni, amely legalább a Dokumentációban közölt követelményeknek megfelel. A telepítési módszer leírása a Dokumentációban található. A Szoftvert futtató Számítógépre nem telepíthető olyan számítógépes program vagy hardver, amely kedvezőtlen hatással lehet a Szoftverre. A Számítógép olyan hardver – korlátozás nélkül ideértve a személyi számítógépeket, laptopokat, munkaállomásokat, 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, és megfelel az itt előírt összes feltételnek, a Gyártó az alábbi jogokat (a továbbiakban „Licenc") biztosítja az Ön számára:

a) **Telepítés és használat.** Nem kizárólagos és nem átruházható jogot szerez a Gyártótól arra, hogy a Szoftvert egy számítógép merevlemezére vagy más tartós adattárolásra alkalmas adathordozóra telepítse, a Szoftvert számítógépes rendszerek memóriájába telepítse, és ott tárolja, valamint megjelenítse azt.

b) **A 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) (a továbbiakban „Levelezőprogram") keresztül fogad e-mailt. Ha egy Levelezőprogram e-mailt fogad, majd azt automatikusan továbbítja több felhasználónak, akkor a Végfelhasználók számának meghatározása az alapján történik, hogy ténylegesen hány felhasználó kapja meg a továbbítással az e-mailt. Ha a levelezési szerver levelezési kapuként

működik, a Végfelhasználók száma megegyezik azon 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) **Business Edition.** A Szoftver Business Edition verzióját kell beszerezni a Szoftver levelezési szervereken, levelezési átjárókon vagy internetes átjárókon való használatához.

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

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

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

g) **A licenc 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 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 időről időre kiadni a Szoftver frissítéseit („Frissítések”). Ez a funkció a Szoftver általános beállításai között engedélyezve van, és a Frissítések ezért automatikusan települnek, kivéve ha a Végfelhasználó letiltotta a Frissítések automatikus telepítését. A frissítések biztosításához szükség van a Licenc eredetiségének ellenőrzésére, ideértve a Számítógépre vonatkozó információkat és/vagy annak ellenőrzését, hogy megfelel-e az Adatvédelmi szabályzatnak az a platform, amelyre a Szoftver telepítve van.

b) **Kártevők és információk továbbítása a Gyártónak.** A Szoftver olyan funkciókat tartalmaz, amelyek mintákat gyűjtenek a vírusokról és egyéb kártékony számítógépes programokról, a gyanús, problémás, kéretlen vagy veszélyes objektumokról, többek között fájlokról, URL-címekről, IP-csomagokról vagy Ethernet-keretekről (a továbbiakban „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, illetve a szoftver működésével és funkcióival, valamint a helyi hálózaton található eszközökkel kapcsolatos adatokkal (ideértve a típust, a gyártót, a modellt és/vagy az eszköz nevét) (a továbbiakban „Adatok”) együtt. Ezek az Adatok és Kártevők magukban foglalhatják a Végfelhasználóval vagy a Szoftvert futtató számítógép más felhasználóival kapcsolatos adatokat (beleértve a véletlenszerűen vagy nem szándékosan megszerzett személyes adatokat is), valamint a kártevők által érintett fájlokat a kapcsolódó metaadatokkal együtt.

Az információkat és a kártevőket a szoftver következő funkciói gyűjthetik:

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

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

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

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

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

Az adatvédelemről, a személyes adatok védelméről és az Önt mint adatalanyt megillető jogokról az Adatvédelmi szabályzat tartalmaz részletes információkat, amely a Gyártó webhelyén található, és közvetlenül a telepítési eljárás során érhető el. A szoftver 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 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 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. 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 (a továbbiakban „Társult vállalatok”) megsértenének kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük. Kereskedelmi felügyeleti törvénynek minősül

i. minden olyan törvény, amely szabályozást, korlátozást, illetve 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 (a továbbiakban „Exportálási felügyeleti törvények”), valamint

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

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

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

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

c) A Szerződés egyik rendelkezése sem azzal a szándékkal jött létre és nem értelmezhető úgy, hogy bármely felet ráveszi vagy kötelezi a vonatkozó kereskedelmi felügyeleti törvényekkel össze nem egyeztethető vagy azok értelmében büntetendő vagy tiltott 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.

21. **Alkalmazandó jog**. A jelen Szerződésre a Szlovák Köztársaság törvénye az irányadó, és a szerződés a szerint értelmezendő. A Végfelhasználó és a Gyártó ezennel megállapodnak abban, hogy az alkalmazandó jog és az ENSZ által elfogadott „Nemzetközi árukereskedelmi szerződésekről szóló egyezmény” ütközése esetén az ütköző rendelkezések nem alkalmazhatók. A Gyártóval fennálló, illetve a Szoftver használatával kapcsolatos minden

jogvita vagy követelés tekintetében Ön kifejezetten aláveti magát a Pozsonyi I. sz. Kerületi Bíróság kizárólagos joghatóságának, továbbá kifejezetten aláveti magát a nevezett bíróság illetékességének az ilyen jogviták rendezésében.

22. **Általános rendelkezések**. Amennyiben a jelen Szerződés bármely rendelkezése érvénytelen vagy kikényszeríthetetlen, az nem érinti a Szerződés többi részének érvényességét. A többi rendelkezés továbbra is érvényes és végrehajtható marad az itt lefektetett feltételek szerint. Amennyiben bármilyen ellentmondás van a jelen Szerződés különböző nyelvi változatai között, az angol változat az irányadó. Jelen Szerződés csak írásban módosítható, amely módosításokat a Gyártó meghatalmazott képviselőjének vagy egy olyan személynek kell aláírnia, aki ügyvédi meghatalmazással kifejezetten eljárhat ebben a hatáskörben.

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

EULA ID: BUS-STANDARD-20-01

Privacy Policy

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