

Sicontact Kft. – ESET Magyarország

Javaslatok a magasabb szintű védelem kialakításához és az ESET termékek biztonságosabb, hatékonyabb használatához

Tartalom

Termékek élettartama	4
Ajánlott ESET beállítások és javaslatok a zsarolóvírusok és más kártevők elleni magasabb szintű védelem érdekében	4
Az ESET PROTECT Hub.....	9
Előfizetés hozzáadása	9
Irányítópult	10
Automatikus deaktiválás.....	10
Az ESET Business Account.....	11
Előfizetés hozzáadása	11
Automatikus deaktiválás.....	12
Az ESET Business Account használatának előnyei:	13
ESET Endpoint (EEA és EES) és ESET Server Security (ESS) ajánlott beállítások	14
Keresőmotor beállítások (EEA, EES, ESS):	14
Valós idejű fájlrendszervédelem (EEA, EES, ESS):	14
Felhőalapú védelem (EEA, EES, ESS):	16
Minták elküldése.....	16
Hálózati hozzáférés-védelem -> Megbízható zóna (EEA, EES, ESS):	17
Bejövő RDP-kapcsolatok korlátozása (EEA, ESS).....	17
E-mail védelem (EES)	18
Védett böngésző (EES)	19
Az Eszközfelügyelet engedélyezése (EEA, EES, ESS):	19
A Dokumentumvédelem engedélyezése (EEA, EES, ESS):	20
Automatikus frissítések (EEA, EES, ESS).....	21
A beállítások jelszavas védelme (EEA, EES, ESS):	21
ESET Server Security for Microsoft Windows Server ajánlott beállítások	22
„Emelt szintű jogosultságok” fiók beállítása:	22
Tűzfal.....	23

ESET PROTECT On-Prem javaslatok és ajánlott beállítások	25
ESET PROTECT On-Prem letöltés:	25
A tanúsítványok biztonsági mentése:	25
Adatbázis mentés.....	26
ESET Bridge Proxy	26
ESET Business Account, ESET PROTECT Hub fiók.....	27
ESET PROTECT On-Prem felhasználók	27
Natív és tartományi felhasználó hozzáadása az ESET PROTECT On-Prem-hez:.....	28
ESET PROTECT On-Prem e-mail értesítések beállítása	28
Az SMTP beállítása:	29
Az értesítések beállítása:	29
ESET PROTECT On-Prem naplófájlok.....	29
Windows:	29
Linux:	29
Automatikus házirend.....	30
Házirend jelzők.....	30
Házirend felülbírállás mód.....	30
ESET Management Agent telepítési, beállítási tippek	32
Telepítés.....	32
Rendszerkövetelmények.....	32
Linux, MacOS	32
Agent Live Installer létrehozása	32
Beállítások.....	34
Kapcsolati intervallum beállítása	35
Minden telepített szoftver jelentése	36
Operációs rendszer frissítésének szükségessége.....	37
Jelszavas védelem	37
Távoli kliensek kapcsolódása a helyi ESET PROTECT On-Prem szerverhez.....	38
Naplófájlok.....	38
ESET PROTECT Cloud.....	39
Védelem beállítása.....	39
AD szinkronizáció	40
Sebezhetőségek és hibajavítások kezelése (Vulnerability és Patch Management).....	40
Aktiválás	41

Házirend beállítása.....	44
Mobile Device Management	46
Licencelés.....	46
Mobileszközök migrációja felhőbe	46
Migráció On-Prem rendszerből felhőbe	47
ESET Secure Authentication.....	47
ESET Cloud Office Security.....	48
ECOS aktiválása.....	48
ECOS megnyitása	48
Bérlő hozzáadása	49
Bérlők aktiválása	50
Házirend beállítások	51
ESET Inspect.....	56

Termékek élettartama

A fejlődő fenyegetésekre válaszul az ESET-termékeket is frissítenünk kell. Az ESET korábbi verziójú termékei nem garantálják az élvonalbeli védelmet, az új operációs rendszerek kompatibilitását, ezért az ESET a termékek élettartamának végére vonatkozóan új irányelvet vezetett be.

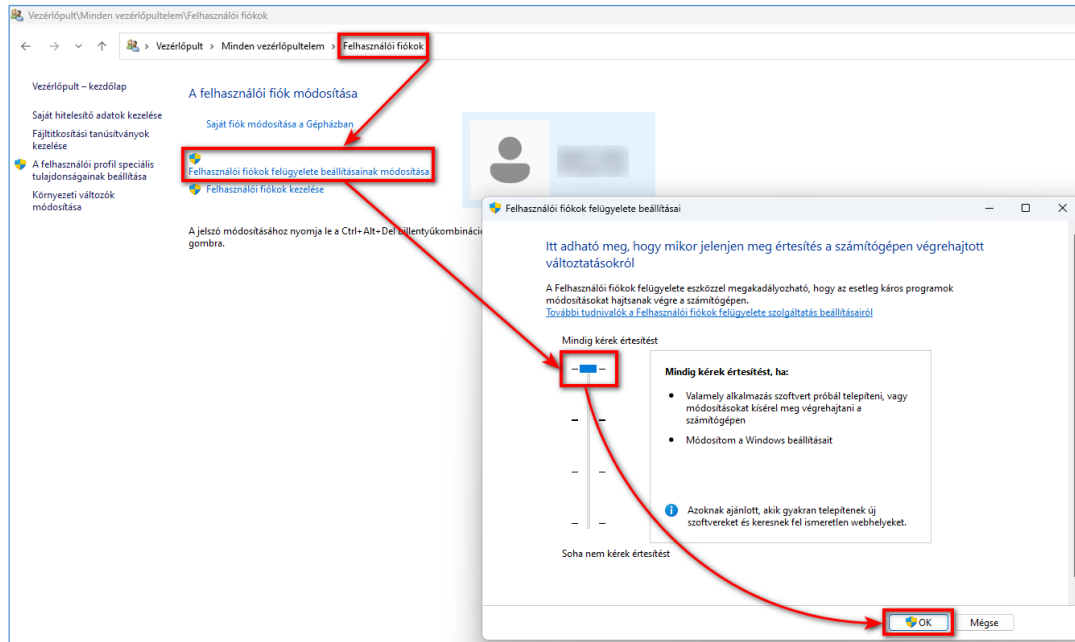
Minden szükséges információt megtalál az alábbi oldalon: <https://support-eol.eset.com/hu/>

A vállalati termékeink élettartamáról részletesen az alábbi oldalon tájékozódhat:
https://support-eol.eset.com/hu/policy_business/product_tables.html

Ajánlott ESET beállítások és javaslatok a zsarolóvírusok és más kártevők elleni magasabb szintű védelem érdekében

1. Az ESET védelmi szoftver beállításait minden esetben lássa el egyedi, erős jelszóval. Ezzel megakadályozhatja, hogy a támadók a kártékony kód futtatása előtt kikapcsolják vagy töröljék az alkalmazást.
2. Elsősorban vállalatoknál, a távoli munkavégzéshez használt, az internet felé nyitott Távoli-asztal, azaz RDP (Remote Desktop Protocol) hozzáférések sok esetben gyenge, nem egyedi jelszavát feltörve a hackerek olyan jogosultságokat szerezhetnek, amelyekkel bejuthatnak valamelyik számítógépbe, ahol ezután trójai program futtatásával megkezdik az adott gép, illetve a hálózaton található többi eszköz támadását. A távoli munkavégzés biztosítására az internet felé publikált RDP helyett használjon VPN kapcsolatot. Ne publikálja ki a **3389-es** portot az internet felé. Abban az esetben, ha az RDP nem az alapértelmezett 3389-es porton érhető el, hanem másikon, szintén nem javasoljuk az internet felé történő publikálását.
3. A hozzáféréseket minden esetben védje erős, legalább 15–20 karakter hosszú, egyedi jelszavakkal.
4. Amennyiben megoldható, javasoljuk, hogy használjon (**VPN, RDP, Windows bejelentkezés, OWA esetén**) kétfaktoros hitelesítést is (pl.: ESET Secure Authentication).
5. Biztonsági szoftverek esetén az ESET legújabb frissítéseinek telepítése, valamint a legújabb termékverzió használata.
6. Az operációs rendszer (Windows, Linux, MacOS), a böngészők és a további telepített szoftverek frissítése, naprakészen tartása. A biztonsági szint maximalizálása érdekében egyáltalán nem javasoljuk az operációs rendszer automatikus frissítésének kikapcsolását.
7. Régebbi asztali operációs rendszeren (Windows 8.1, 8, 7 SP1) a legfrissebb ESET Endpoint védelem telepítése már nem támogatott, javasoljuk, hogy frissítse operációs rendszerét Windows 11-re.
8. Régebbi szerver operációs rendszeren (Windows Server 2012 R2, 2012 és 2008 R2) a legfrissebb ESET Server Security védelem telepítése már nem támogatott, javasoljuk, hogy frissítse szerver operációs rendszerét újabb verzióra.
9. Készítsen rendszeresen offline biztonsági mentést adatairól, amelyek segítségével egy esetleges fertőzés esetén azok visszaállíthatók.

10. A Windows beállításainál az UAC-ot (User Account Control = Felhasználói fiókok felügyelete) hagyja bekapcsolva (Vezérlőpult/Felhasználói fiókok/Felhasználói fiókok felügyelete beállításainak módosítása).



11. Az ESET védelmi megoldásainak beállításánál kapcsolja be

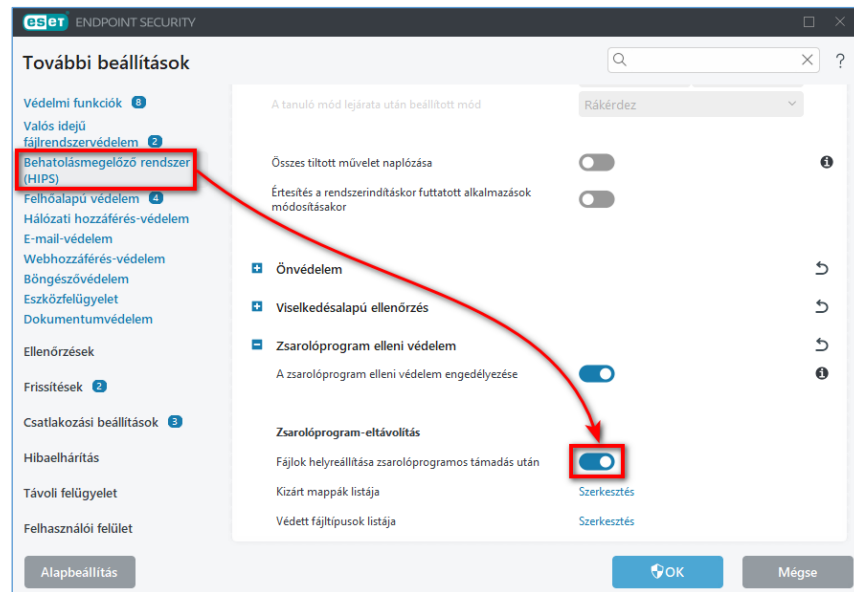
- a kéréslen és veszélyes alkalmazások keresését
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_protections.html#s-vedelmi-beallitasok
- a Futtatás közbeni tömörítőket és a Kiterjesztett heurisztika/DNA-vírusdefiníciókat
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_threat_sense.html
- a Zsarolóprogram elleni védelmet
Leírás: https://help.eset.com/ees/13/hu-HU/idh_hips_main.html#s-zsaroloprogram-elleni-vedelem
https://help.eset.com/glossary/hu-HU/technology_ransomware_protection.html
- a Zsarolóprogram-eltávolítást - **ÚJ FUNKCIÓ!**
Leírás: https://help.eset.com/ees/13/hu-HU/idh_hips_main.html#s-zsaroloprogram-eltavolitas
Feltétel: minimum az ESET Endpoint Security/Antivirus 12-es verziója és ESET PROTECT Advanced vagy magasabb licenccsomag

Technikai feltételek:

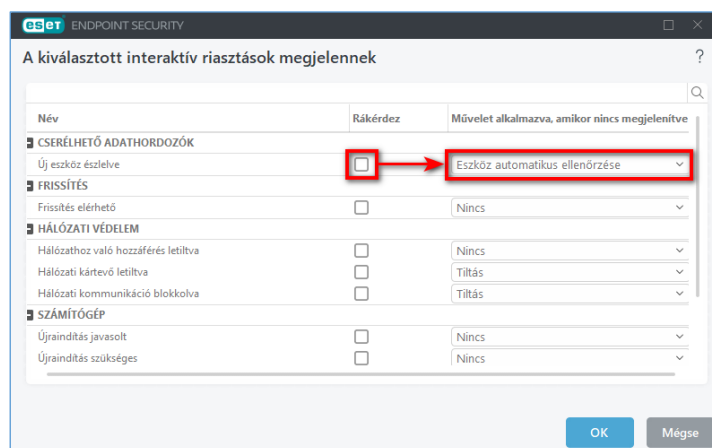
- csak NTFS fájlrendszer támogatott
- USB- és hálózati meghajtók nem támogatottak

A funkció működését megtekintheti az alábbi YouTube videóban:

<https://www.youtube.com/watch?v=ifMOvoHEVbQ>

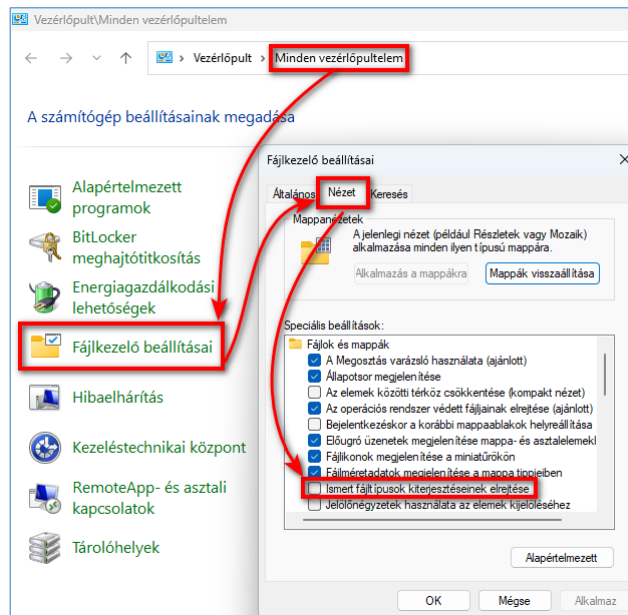


- a Felhő alapú LiveGrid és LiveGuard Advanced (amennyiben rendelkezik megfelelő licenccel) megbízhatósági rendszert.
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_charon.html
<https://help.eset.com/elga/en-US/?overview.html>
- a Dokumentumvédelmet
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_dmon.html
- a Brute force támadás elleni védelmet
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_epfw_brute_force_attack_protection.html
- az Automatikus termékfrissítést
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_update_source.html#s-frissitesek
- A csatlakoztatott eszközök automatikus ellenőrzését
Az ESET Endpoint Security lehetővé teszi a cserélhető adathordozók (CD, DVD, USB stb.) automatikus ellenőrzését a számítógépbe való behelyezésük során. Ez különösen hasznos lehet akkor, ha a számítógép rendszergazdája meg kívánja akadályozni, hogy a felhasználók kéretlen tartalmú cserélhető adathordozót helyezzenek a számítógépbe.
Leírás: https://help.eset.com/ees/13/hu-HU/idh_config_rem_media_amon.html



- HIPS-szabályok konfigurálása az ESET üzleti termékeiben a zsarolóvírusok elleni védelem érdekében:
<https://support.eset.com/en/kb6119-configure-hips-rules-for-eset-business-products-to-protect-against-ransomware>

12. Futtasson heti egy alkalommal ütemezett, teljes számítógép ellenőrzést, amely megtalálja azokat a kártevőket is, amelyeket esetleg a valós idejű ellenőrzés nem talált meg.
13. Tiltson le minden makró, kivéve a digitálisan aláírtakat.
14. Csökkentse a támadási felületet azáltal, hogy kikapcsol vagy eltávolít minden szükségtelen szolgáltatást és szoftvert.
15. Kapcsolja ki az operációs rendszer „Automatikus lejátszás” funkcióját. Ezzel megakadályozhatja az ártalmas folyamatok automatikus futtatását olyan külső adathordozókról, mint például az USB memóriakártyák vagy a pendrive-ok.
16. Állítsa be levelezőszerverét úgy, hogy blokkolja a kétes eredetű, .exe, .com, .bat, .lnk, .vbs, .scr vagy .zip kiterjesztésű mellékleteket.
17. Állítson be szoftverkorlátozási házirendeket, amelyekkel megakadályozható, hogy futtatható fájlok lehessenek indíthatók olyan kártevő folyamatok futtatására gyakran használt helyekről, mint pl. **a ProgramData, AppData, Temp és a Windows\SysWOW64.**
18. Soha ne nyisson meg kettős kiterjesztésű fájlokat (pl. táblázat.xlsx.exe)
19. Állítsa be a Windowsban a fájl kiterjesztések megjelenítését. Ezáltal csökkentheti az esélyét olyan mellékletek megnyitásának, amelyek potenciálisan zsarolóvírust tartalmazhatnak (pl. .exe, vbs, scr, zip)



20. Ne engedélyezze a PowerShell script-ek futtatását olyan gépeken, ahol az nem szükséges.
21. Az SMB-portokat ne érje el az internet, ha nem szükséges.
Zárja be a **135-139-es és 445-ös** fájlmegosztó portokat.
22. Tiltson le a **gyakori nem használt** és alapértelmezett fiókokat, például **rendszergazda, admin vagy root** fiókokat)
23. Használjon tartalom szkennelést és szűrést a levelezőszerverein. Így a bejövő e-mail-ek vizsgálhatók lesznek az ismert kártevőkre, megakadályozva így minden fenyegetést, amely veszélyt jelenthet.
24. Rendszeresen képezze munkatársait, hogy fel tudják ismerni és kezelni tudják az adathalász vagy zsaroló támadásokat.

25. Kerülje a jogosultságoknál a szerepkörhalmozást és minden felhasználóval kapcsolatban kövesse a „legsúlyosabb jogosultság” elvét, azaz minden munkatárs csak azokkal a jogosultságokkal rendelkezzen, amelyek a munkája végzéséhez elengedhetetlenek.

Az ESET PROTECT Hub

Az ESET PROTECT Hub 2026-ban átveszi a jelenlegi licenckezelő portál az ESET Business Account helyét. Fő célja, hogy egy helyről legyen elérhető az ESET minden felhős szolgáltatása. Az ESET Business Account továbbra is használható, oda már korábban regisztrált ügyfelek részére, azonban új fiók regisztráció automatikusan az ESET PROTECT Hub-ban jön már létre. Az ESET Business Account fiókok át lesznek migrálva az ESET PROTECT Hub-ba, erről minden felhasználó értesítést fog kapni. Jelenleg viszonteladói szerepkör nem érhető el az ESET PROTECT Hub-on.

Bővebb információ: https://help.eset.com/protect_hub/public/hu-HU/index.html

Bejelentkezési link: <https://protecthub.eset.com/>

A használata ingyenes, mindössze egy e-mail címre és a vállalata néhány adatára van szükség.

FONTOS! Ne regisztráljon ugyanazzal az e-mail címmel, mint amellyel korábban már volt ESET Business Account fiókja.

Azok a felhasználók, akiknek korábban volt már ESET Business Account fiókjuk, az alábbi linkek tudnak belépni:

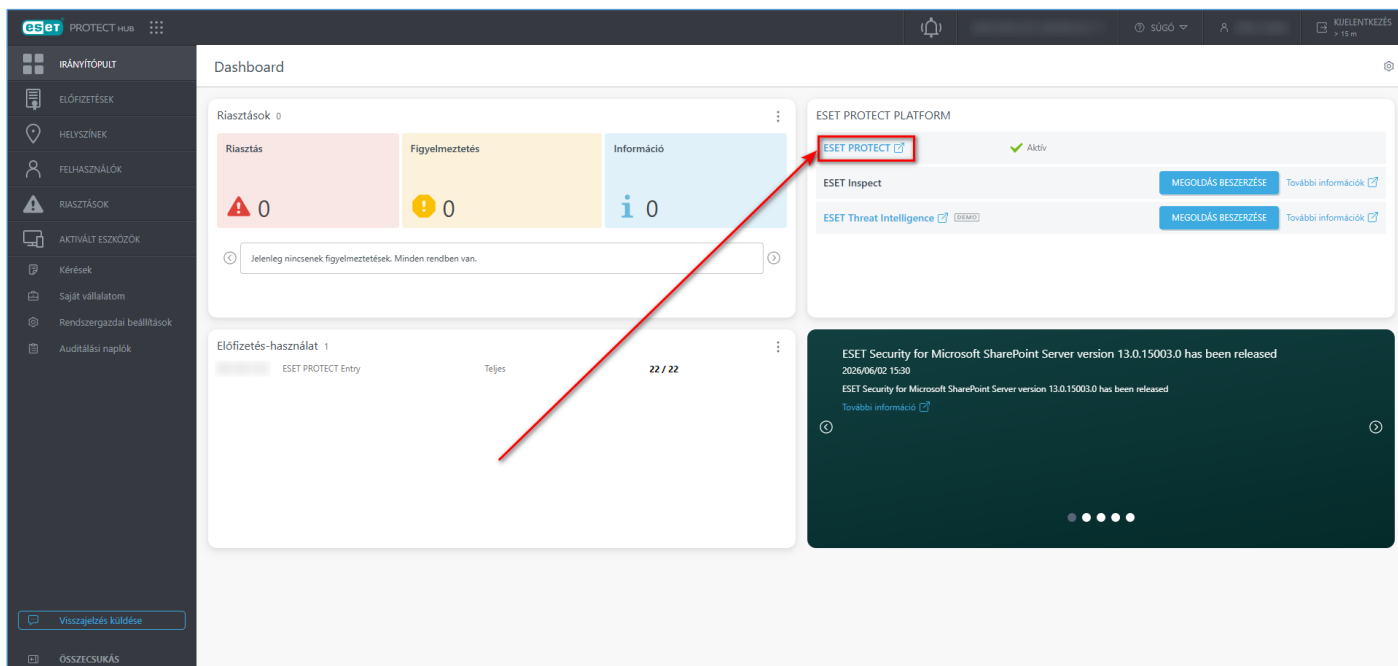
<https://eba.eset.com/>

Előfizetés hozzáadása

The screenshot displays the ESET PROTECT Hub interface. On the left sidebar, the 'ELŐFIZETÉSEK' (Subscriptions) menu item is highlighted with a red box. A red arrow points from this menu item to the '+ ELŐFIZETÉS HOZZÁADÁSA' (Add Subscription) button located at the bottom of the main content area. This button triggers a modal window titled 'Előfizetés hozzáadása' (Add Subscription). Inside the modal, there is a text field labeled 'Aktiválási kulcs' (Activation key) containing the value 'ABCD-EFGH-IJKL-MNOP-QRST'. A red arrow points from this text field to the '+ ELŐFIZETÉS HOZZÁADÁSA' button at the bottom right of the modal.

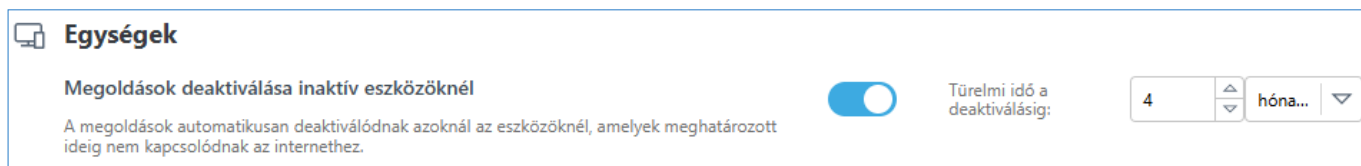
Irányítópult

A felhős központi menedzsmen felületek az irányítópultról indíthatók el, ha rendelkezik a megfelelő előfizetési csomaggal és az előfizetését hozzáadta az ESET PROTECT Hub-hoz az aktiválási kulcs segítségével.



Automatikus deaktiválás

Az EBA-hoz hasonlóan az ESET PROTECT Hub-hoz nem kapcsolódó munkaállomások deaktiválásra kerülnek a megadott időtartam után. Így az adott időintervallumon kívül be nem jelentkező gépek által lefoglalt helyek automatikusan felszabadításra kerülnek az előfizetési készletből.



Az ESET Business Account

FONTOS!

Ahogy azt az előző szekcióban említettük, az ESET Business Account-ot le fogja váltani az ESET PROTECT Hub.

Az ESET vállalati ügyfelei a megvásárolt előfizetéshez tartozó előfizetési helyek felhasználását az ESET Business Account (EBA) szolgáltatásban felügyelhetik.

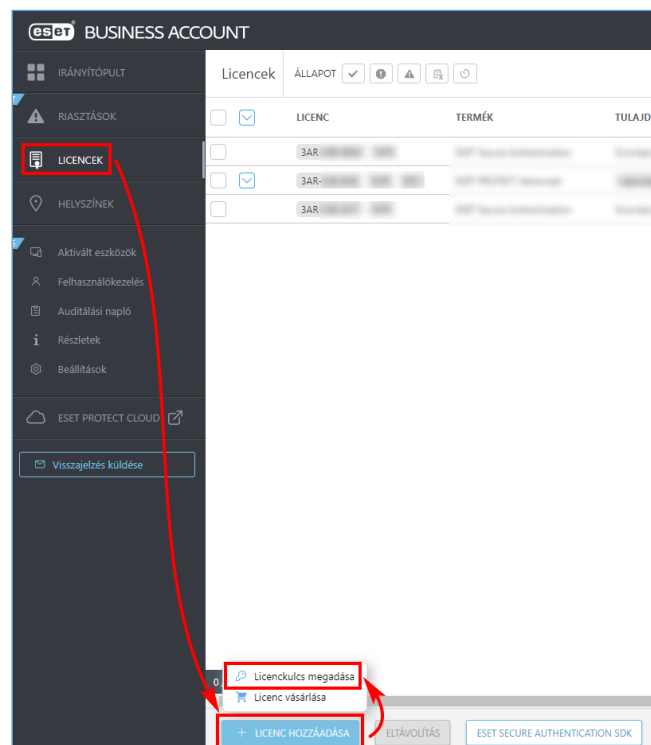
Bővebb információ:

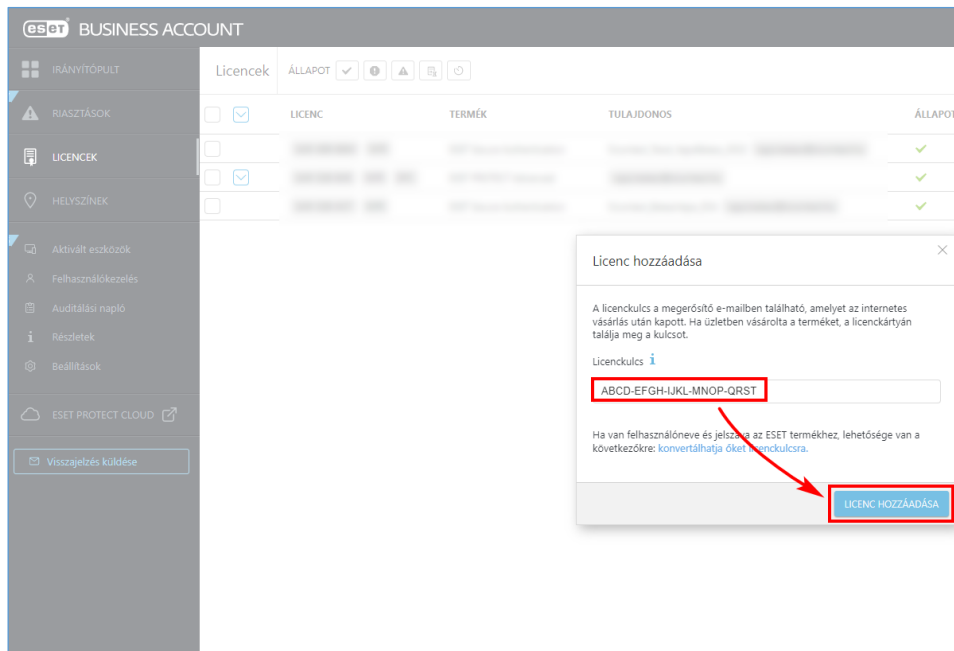
<https://help.eset.com/eba/hu-HU/>

A szolgáltatás ingyenesen használható, mindössze egy fiók létrehozására van szükség egy tetszőleges e-mail cím és jelszó megadásával: <https://help.eset.com/eba/hu-HU/eba-portal.html>

Előfizetés hozzáadása

Meglévő fiókjához hozzá tudja adni a megvásárolt előfizetését, előfizetéseit, ezután láthatóvá válik, hogy az adott előfizetéshez tartozó előfizetési helyekből mennyi, milyen eszközökön került felhasználásra. Lehetősége van a már nem használt vagy leselejtezett eszközök által lefoglalt helyek felszabadítására is.





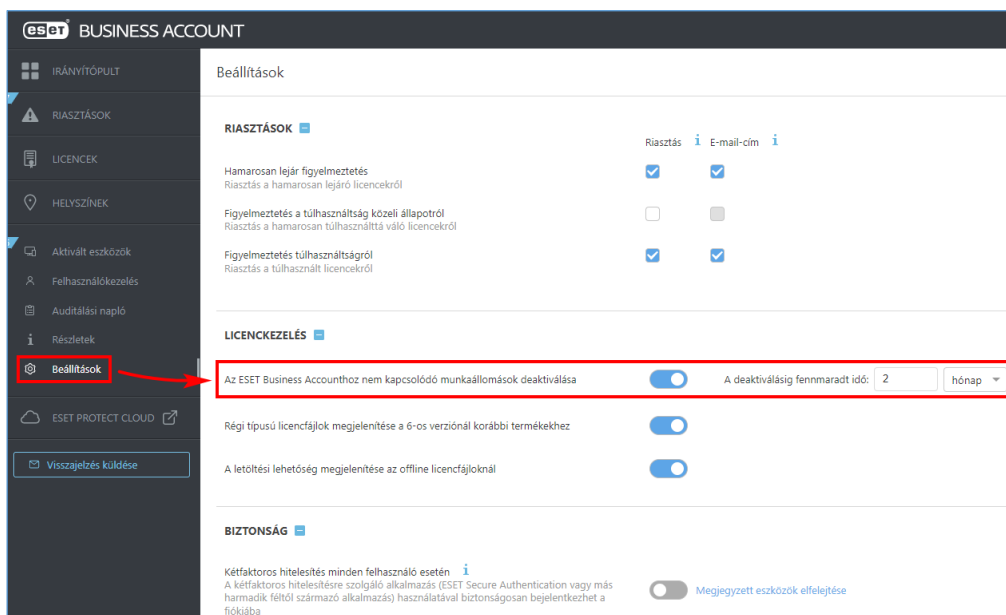
Részletes segítség:

<https://help.eset.com/eba/hu-HU/?import-licenses.html>

<https://help.eset.com/eba/hu-HU/?deactivate-licenses-on-security-products.html>

Automatikus deaktiválás

Előfordulhat, hogy az elromlott vagy leselejtezett gépeken a vírusirtó szabályos eltávolításának elmaradása miatt beragad az adott gép által használt előfizetés, így az feleslegesen foglal helyet az előfizetésből. Az így kialakuló túlhasználatot az ESET Business Accounttal meg lehet előzni, ha bekapcsolja az EBA-hoz nem kapcsolódó munkaállomások deaktiválását a megadott időtartam után. Így az adott időintervallumon kívül be nem jelentkező gépeken lefoglalt előfizetési hely automatikusan felszabadításra kerül.



Abban az esetben, ha az előfizetéssel különböző telephelyeken használt eszközöket kellene aktiválni egy harmadik személy által, akkor ezt egy ESET Business Account fiók segítségével az aktiválási kulcs kiadása nélkül is megteheti. Ehhez telephelyeket és felhasználókat kell létrehozni az ESET Business Accountban. A felhasználókhöz különböző jogosultságokat rendelhet, hozzárendelheti őket telephelyekhez, a telephelyekhez pedig előfizetési helyeket oszthat ki a teljes előfizetésből. Ezáltal az adott telephelyen az adott felhasználó az ESET Business Account fiókja használatával tudja aktiválni az ESET termékeket a hozzá rendelt telephelyhez kiosztott előfizetési helyek mértékéig. Erről az alábbi oldalakon tudhat meg többet:

<https://help.eset.com/eba/hu-HU/?sites.html>

<https://help.eset.com/eba/hu-HU/?users.html>

<https://help.eset.com/eba/hu-HU/?associate-user-with-sites.html>

https://help.eset.com/ees/12/hu-HU/idh_wizard_activation_sec_admin.html

Az ESET Business Account használatának előnyei:

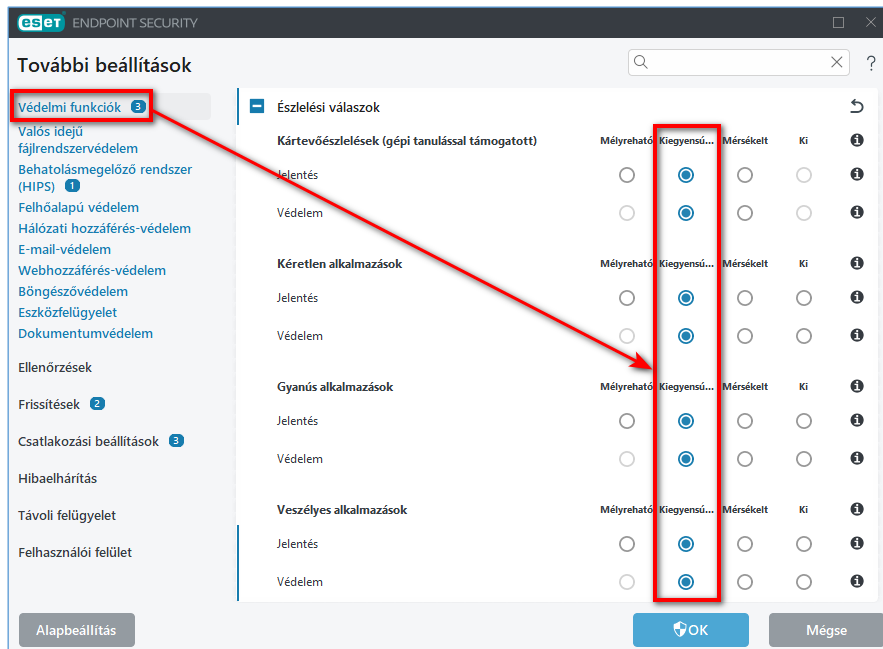
- Nem kell bővíteni az előfizetést, csak akkor, ha valóban fel vannak használva a rendelkezésre álló előfizetési helyek
- Könnyen át lehet tekinteni az előfizetés kihasználtságát, így akár költséget is lehet megtakarítani a felesleges bővítés elkerülésével
- Az aktivált eszközök áttekintésével meg lehet akadályozni az előfizetés jogosulatlan felhasználását, illetve a már leselejtezett, nem használt, tönkrement gépek által felhasznált előfizetési helyeket könnyen fel lehet szabadítani
- Az egyes helyszíneken az aktiváláshoz nem kell kiadni az aktiválási kulcsot, amivel jelentősen csökkenthető a jogosulatlan felhasználás kockázata
- Automatizálni lehet a rég nem használt, illetve a már leselejtezett eszközökön lekötött előfizetési hely deaktiválását

ESET Endpoint (EEA és EES) és ESET Server Security (ESS) ajánlott beállítások

A gyári beállításokon felül ajánlott több védelmi modult engedélyezni. Az engedélyezés után a védelmi program több erőforrást vehet igénybe így előfordulhat, hogy az adott funkció engedélyezése után egyes régebbi hardverű, gyengébb erőforrással rendelkező kliensgépek lelassulhatnak, ezeken érdemes előbb tesztelni az új védelmi beállításokat.

Keresőmotor beállítások (EEA, EES, ESS):

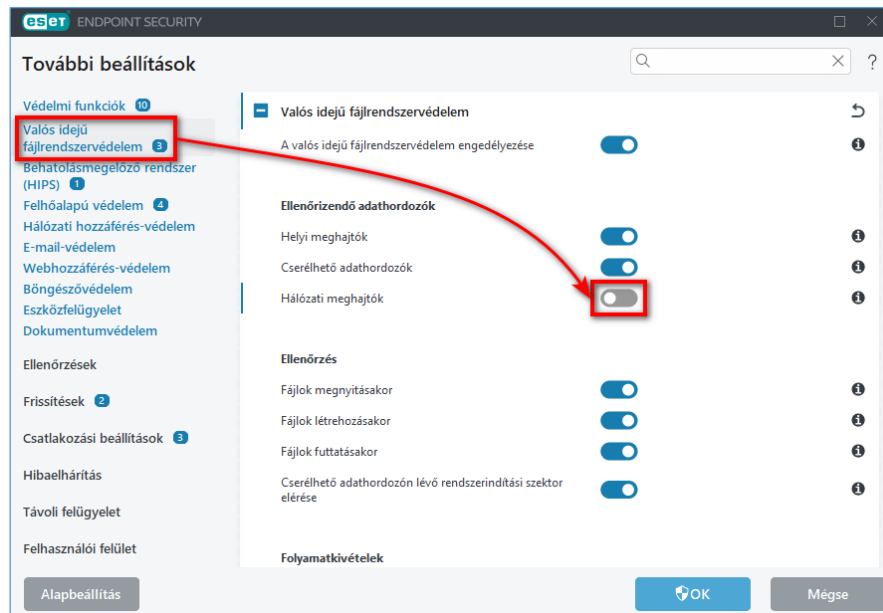
Kártevők és gyanús alkalmazások mellett ajánlott a kórtelen- és veszélyes alkalmazások keresésének engedélyezése. A kategóriákat állítsa kiegyensúlyozottra.



A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_protections.html

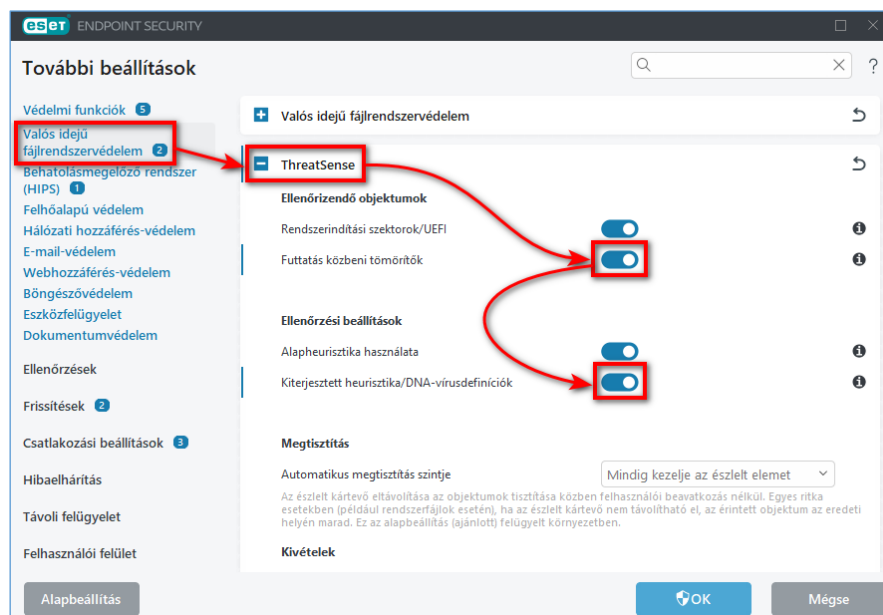
Valós idejű fájlrendszervédelem (EEA, EES, ESS):

- **Hálózati meghajtók** ellenőrzését abban az esetben érdemes kikapcsolni, ha a hálózatra csatlakoztatott minden munkaállomáson és szerveren már telepítve van az ESET védelem.



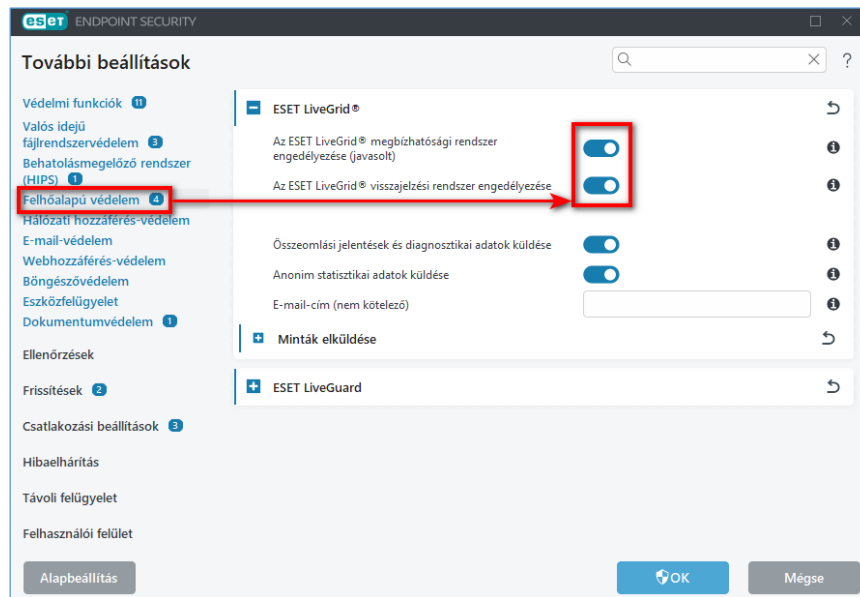
Ajánlott ThreatSense-paraméterek bekapcsolása:

- Futtatás közbeni tömörítők engedélyezése
- Kiterjesztett heurisztika/DNA-vírusdefiníciók engedélyezése



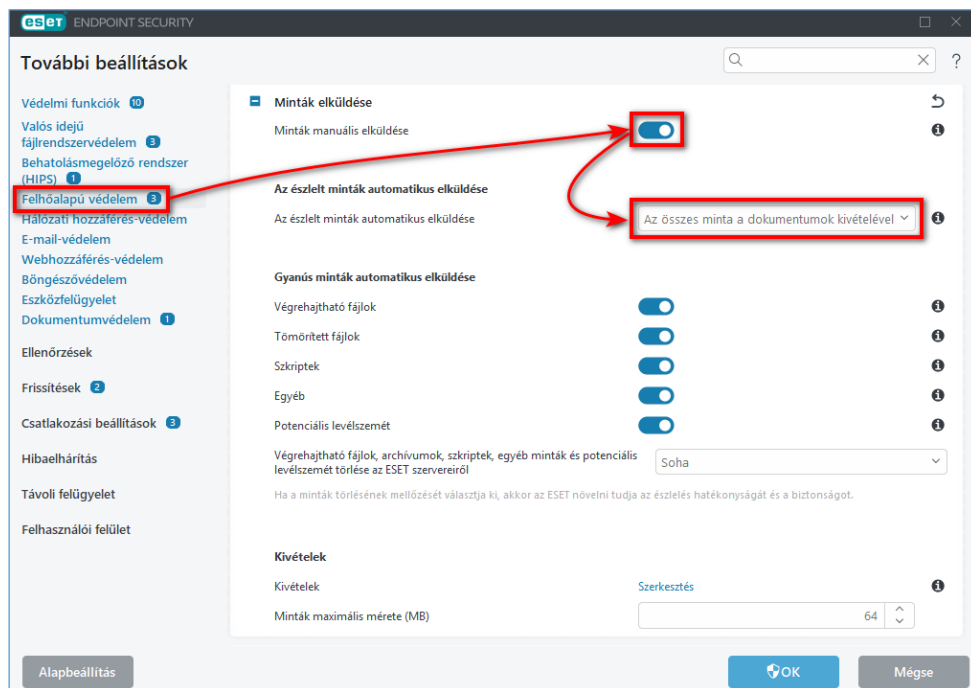
A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_threat_sense.html

Felhőalapú védelem (EEA, EES, ESS):



Minták elküldése

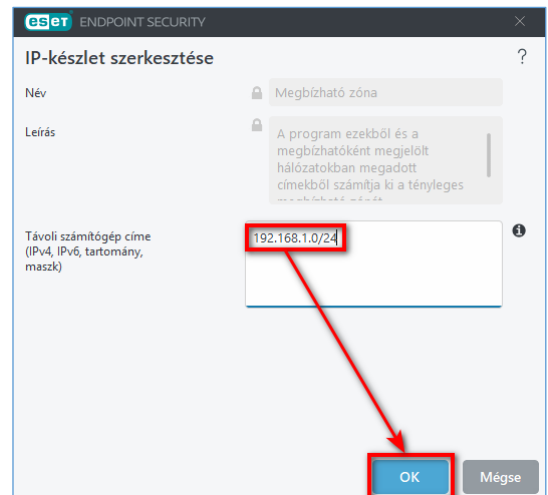
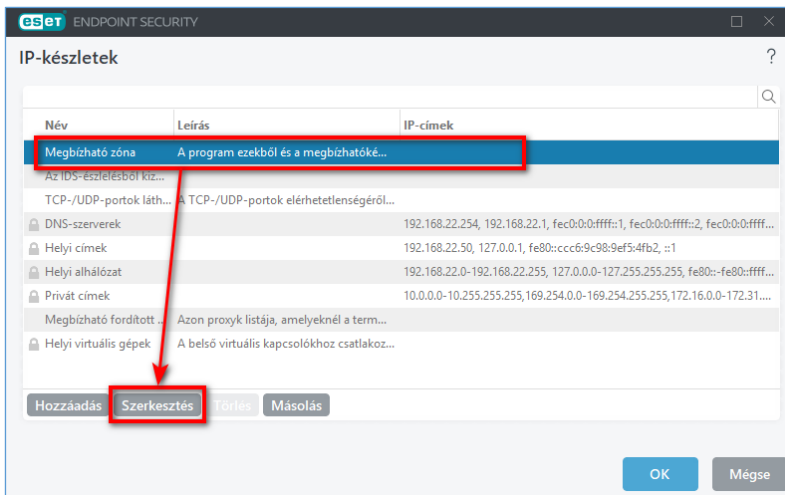
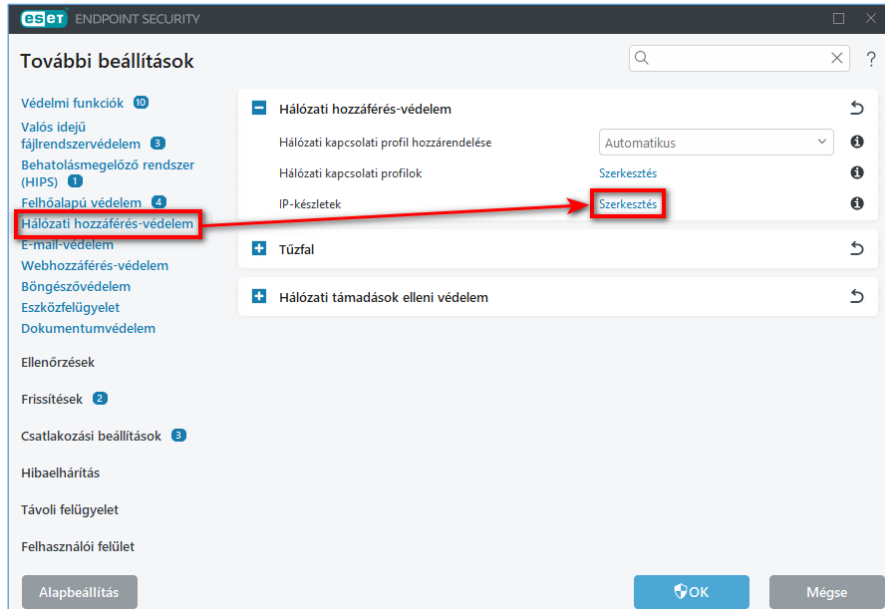
ESET LiveGrid® visszajelzési rendszer az újonnan felfedezett kártevőkkel kapcsolatos információkat gyűjt a számítógépről. Hatékonyabb és gyorsabb vírusfelismerés és eltávolítás érdekében javasolt ennek a funkciónak a bekapcsolása.



A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_charon.html

Hálózati hozzáférés-védelem -> Megbízható zóna (EEA, EES, ESS):

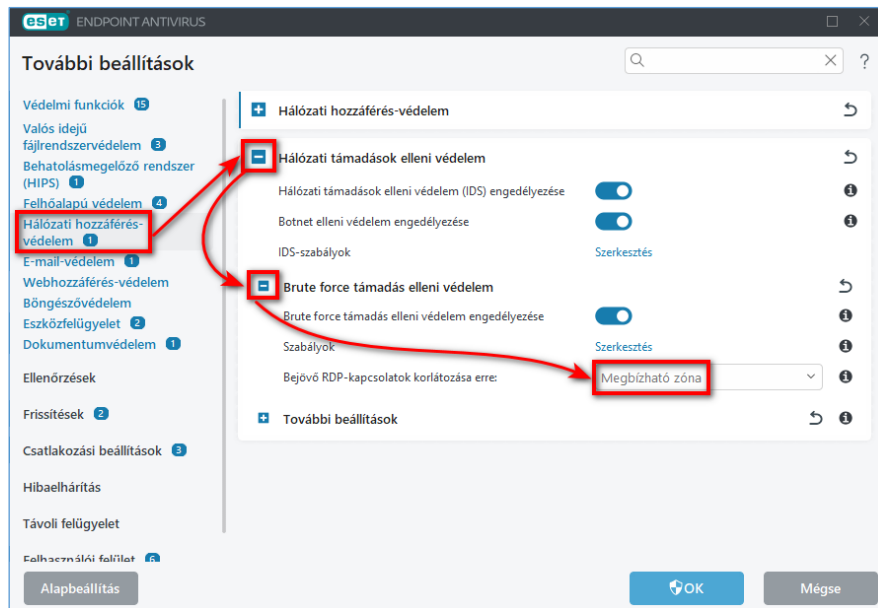
A megfelelő hálózati működés érdekében javasolt a megbízható zóna felvétele. A Megbízható zóna olyan hálózati címek csoportja, ahol a számítógép és a számítógépen tárolt megosztott fájlok láthatók, és a rendszer erőforrásai elérhetők a hálózat többi felhasználója számára.



A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_epfw_network_protection.html

Bejövő RDP-kapcsolatok korlátozása (EEA, ESS)

Lehetővé teszi az RDP-kapcsolatok korlátozását megbízható hálózatokra. Adja meg az IP készletek menüpontban a megbízható zónát (előző szekcióban leírtak szerint), ahonnan az ESET védelme elfogadja az RDP kapcsolódást. Ez a funkció csak ESET PROTECT Essential licenc-el aktivált védelmeken, ESET Endpoint Antivirus és ESET Server Security termékeken érhető el.



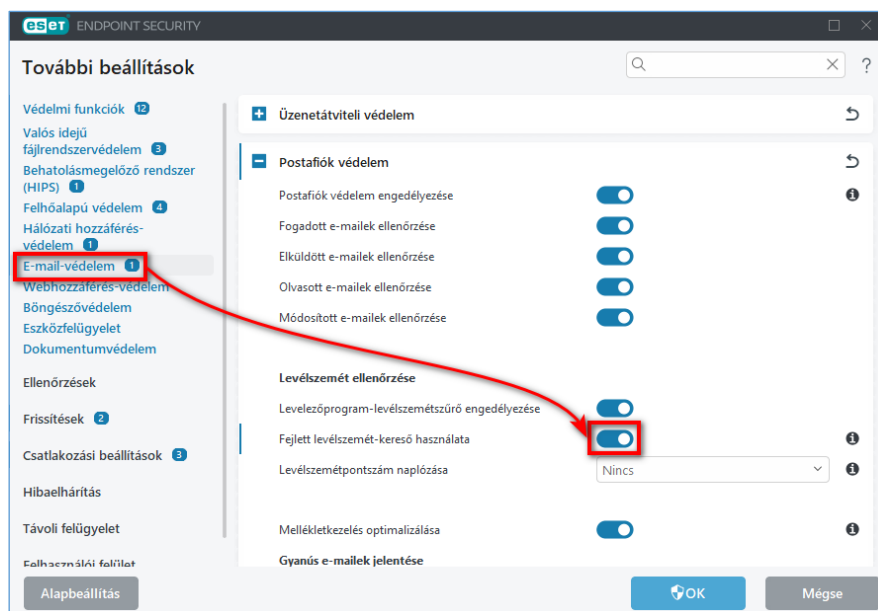
A fent említett funkciók leírása:

https://help.eset.com/eea/13/hu-HU/idh_config_epfw_brute_force_attack_protection.html

https://help.eset.com/efsw/13.0/en-US/idh_config_epfw_brute_force_attack_protection.html

E-mail védelem (EES)

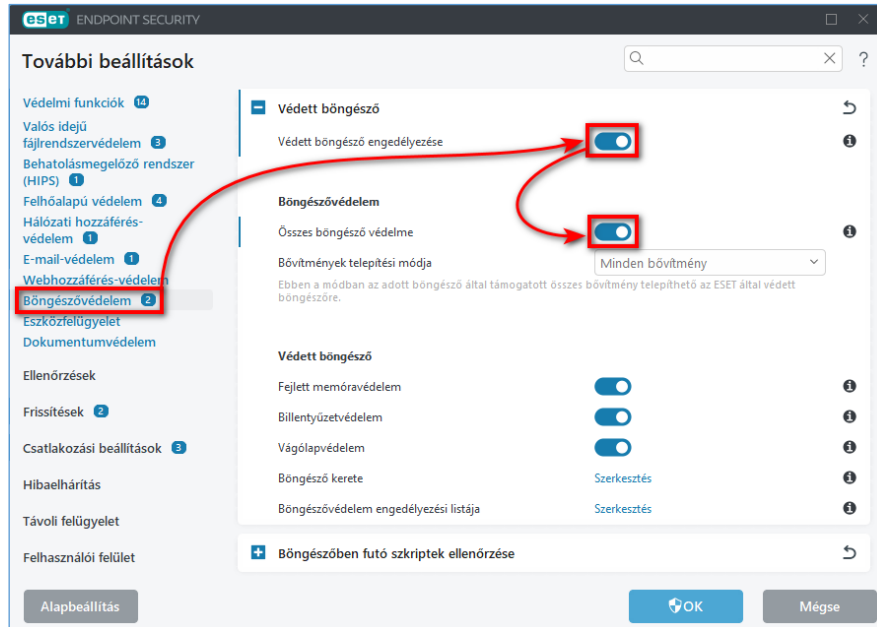
A fejlett levélszemét-kereső bekapcsolásával hatékonyabb a végponton történő levélszemétszűrés. Ez a funkció csak az Endpoint Security termékben érhető el.



A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_emon_clients.html

Védett böngésző (EES)

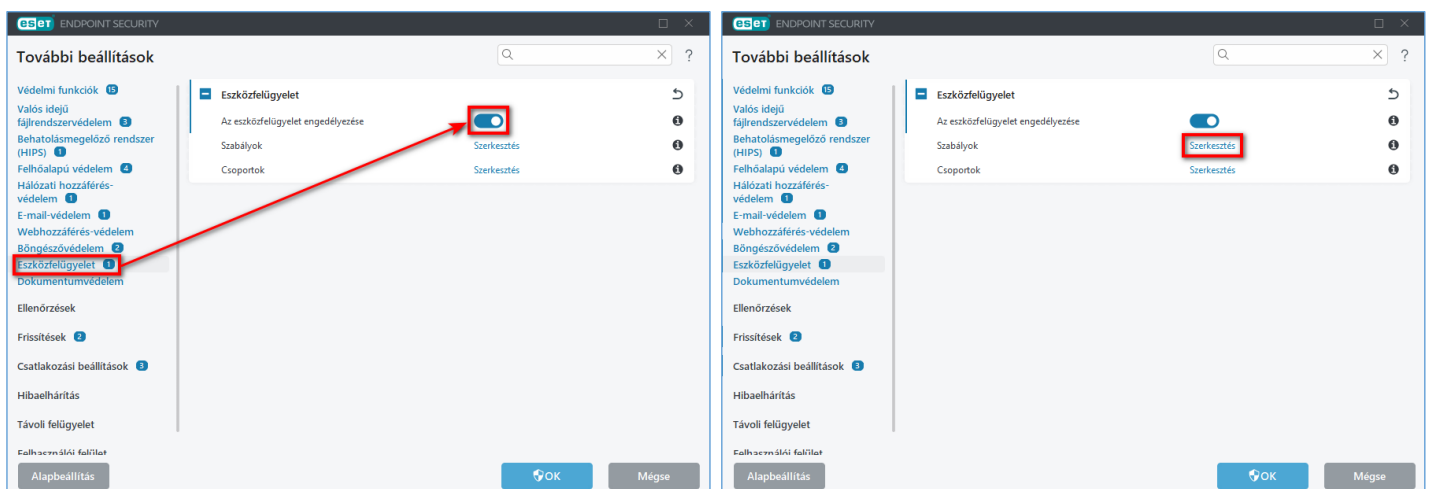
A Védett böngésző a védelem egy újabb rétege, amellyel megóvhatja pénzügyi adatait az online tranzakciók során. Ez a funkció csak az Endpoint Security termékben érhető el. A funkció bekapcsolása után a számítógépet újra kell indítani.

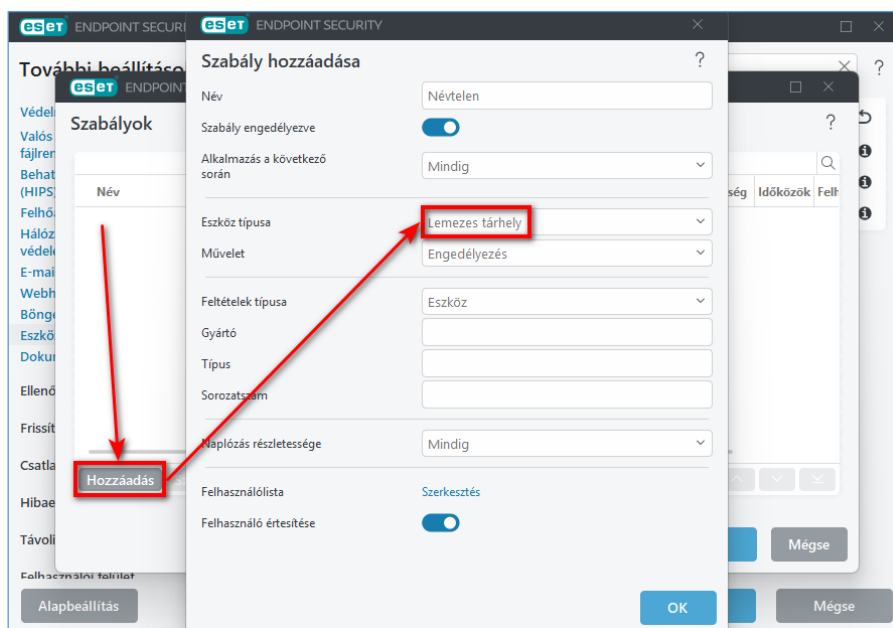


A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_sb.html

Az Eszközfelügyelet engedélyezése (EEA, EES, ESS):

Az ESET termékek lehetővé teszik a cserélhető adathordozók (CD/DVD/USB/mobil stb.) felügyeletét. Ezzel a modullal és a szabályokkal megadható, hogy a felhasználó hogyan érhet el és használhat egy adott eszközt.

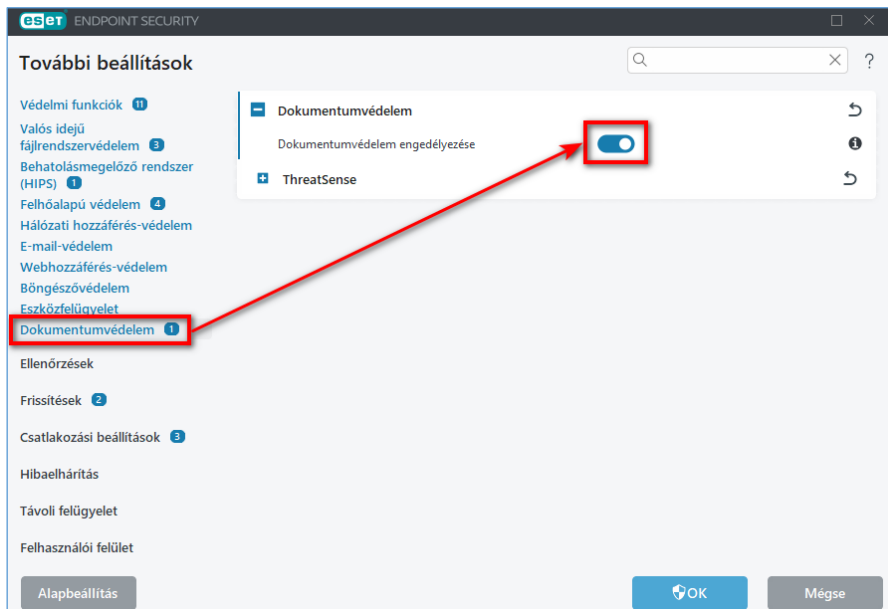




A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_devmon.html

A Dokumentumvédelem engedélyezése (EEA, EES, ESS):

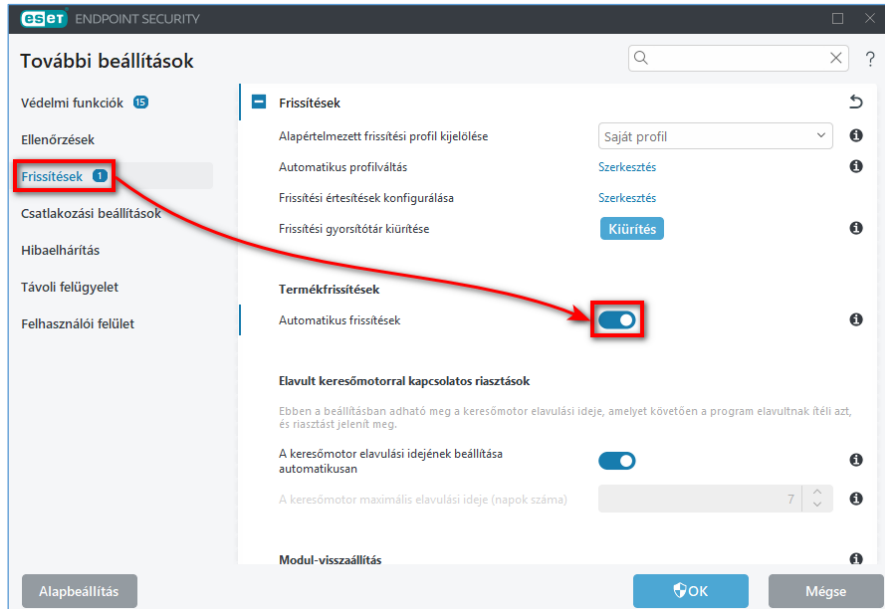
A dokumentumvédelmi szolgáltatás még azt megelőzően ellenőrzi a Microsoft Office-dokumentumokat, valamint az automatikusan letöltött fájlokat, mielőtt megnyitná azokat.



A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_dmon.html

Automatikus frissítések (EEA, EES, ESS)

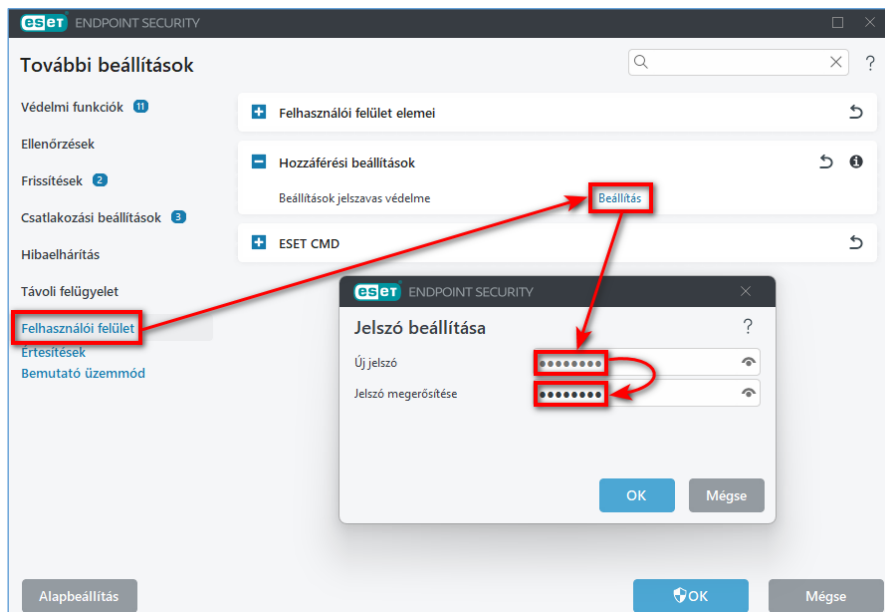
Annak érdekében, hogy mindig az ESET végpontvédelem legfrissebb verziója fusson a védett eszközön, kapcsolja be az automatikus frissítéseket.



A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_config_update_mode.html

A beállítások jelszavas védelme (EEA, EES, ESS):

Erősen ajánlott a végpontvédelem jelszavas védelme a jogosulatlan módosítások ellen.

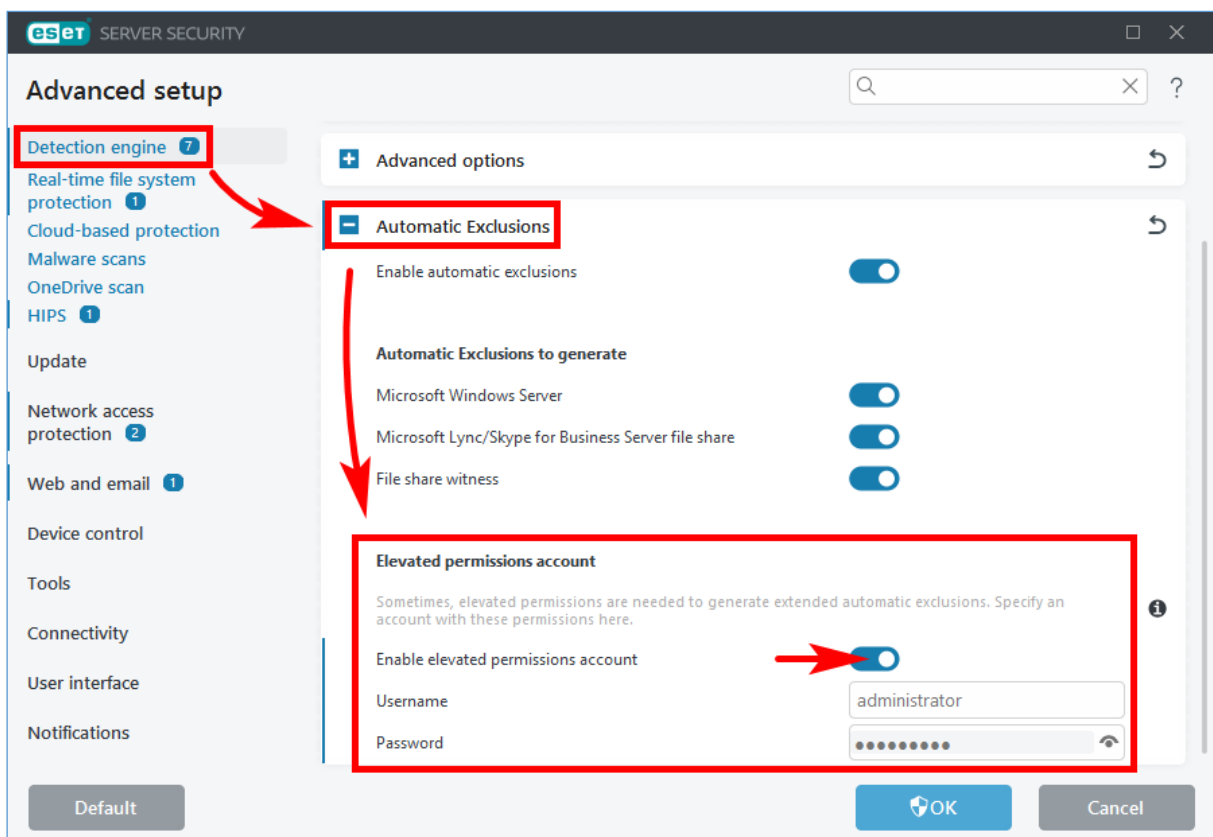


A fent említett funkciók leírása: https://help.eset.com/ees/13/hu-HU/idh_change_password.html

ESET Server Security for Microsoft Windows Server ajánlott beállítások

„Emelt szintű jogosultságok” fiók beállítása:

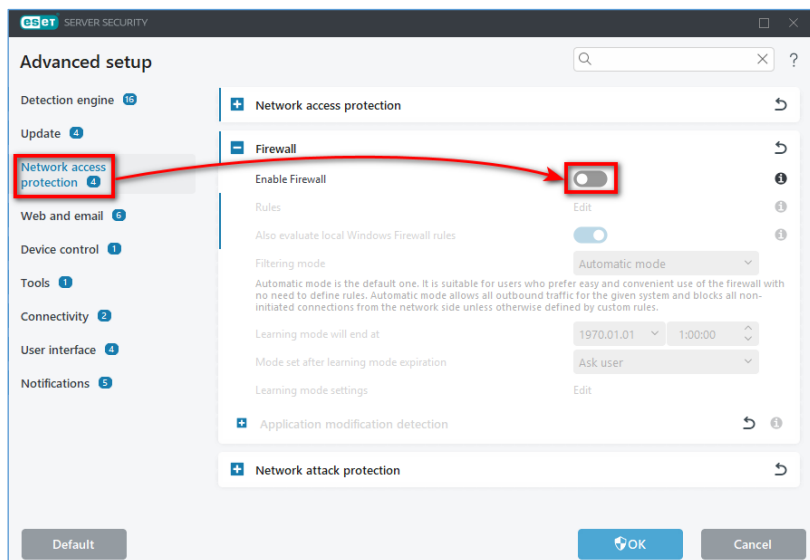
Ez a funkció lehetővé teszi az ESET Server Security számára, hogy további kizárásokat hozzon létre olyan erőforrásokra vonatkozóan, mint a hálózati megosztások, a Microsoft SQL Server adatbázisfájlok helyei vagy a Skype for Business fájlmegosztó tárhelye. Az automatikus kizárások funkciójának kiterjesztéséhez engedélyezze az ESET Server Security További beállításainál (Advanced Setup) az „emelt szintű jogosultságok” fiókot (Enable elevated permissions account), és adja meg a tartományi vagy helyi rendszergazdai fiók felhasználónevét és jelszavát. Ha kívánja, létrehozhat egy új, erre a célra szolgáló fiókot is, de győződjön meg arról, hogy a fiók tagja legyen a tartományi beépített rendszergazdák (BA) csoportjának vagy a helyi Rendszergazdák csoportnak.



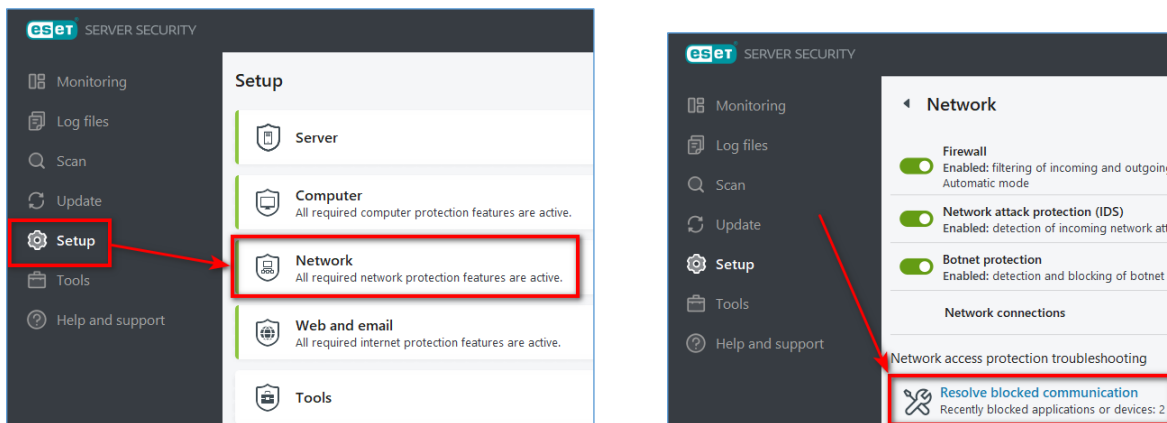
További információk: https://help.eset.com/efsw/13.0/en-US/idh_config_server_autoexclude.html

Tűzfal

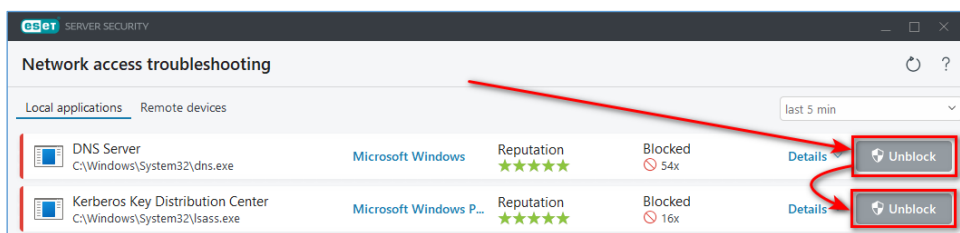
Az ESET Server Security új verziója már tartalmazza az ESET Endpoint Security-ben is használt tűzfalat. A modul az ESET PROTECT Entry vagy magasabb licenc-el aktiválható. Alapértelmezettként kikapcsolt állapotban van.

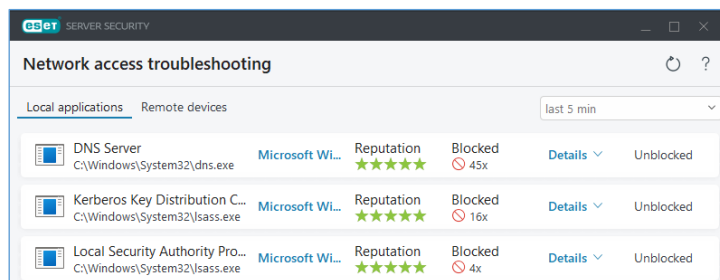


Ha úgy dönt, hogy bekapcsolja a tűzfalat, akkor az blokkolhat olyan kommunikációt mely a hálózat működésére hatással lehet. Ezeket fel kell venni a tűzfal szabályok közé. A blokkolt kommunikációt megtekintheti az ESET Server Security grafikus felületén a Setup -> Network -> Resolve blocked communication menüpontban.



Az Unblock gombra kattintva létrejön a megfelelő tűzfal szabály, és a kommunikáció engedélyezve lesz.





ESET PROTECT On-Prem javaslatok és ajánlott beállítások

ESET PROTECT On-Prem letöltés:

- Windows: <https://www.eset.com/hu/vallalati/letoltes/eset-protect/#all-in-one>
- VA (Virtual Appliance - Rocky Linux 9): <https://www.eset.com/hu/vallalati/letoltes/eset-protect/#virtual>
- Különálló komponensek: <https://www.eset.com/hu/vallalati/letoltes/eset-protect/#standalone>

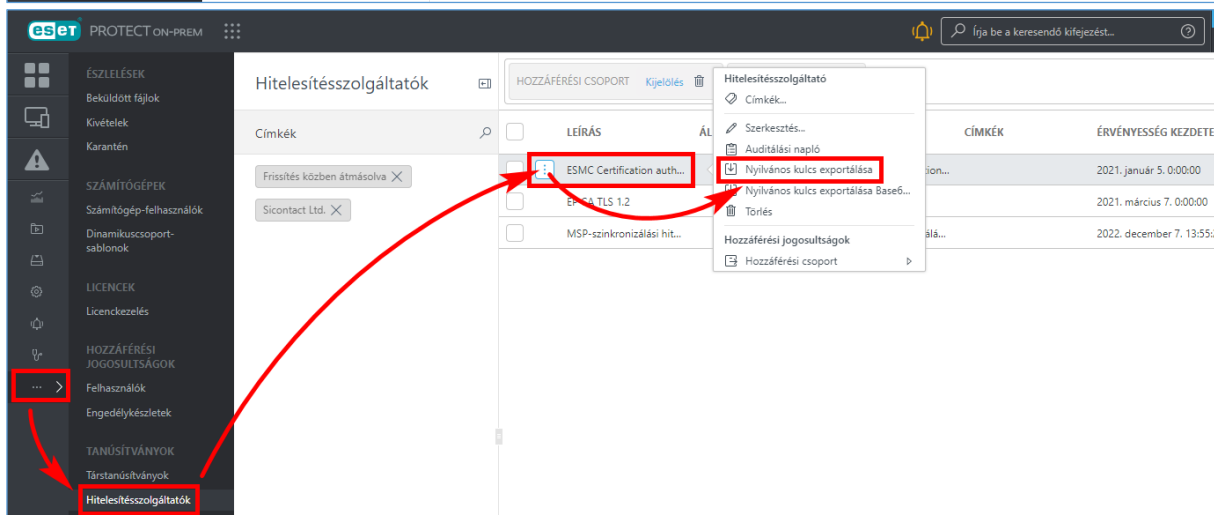
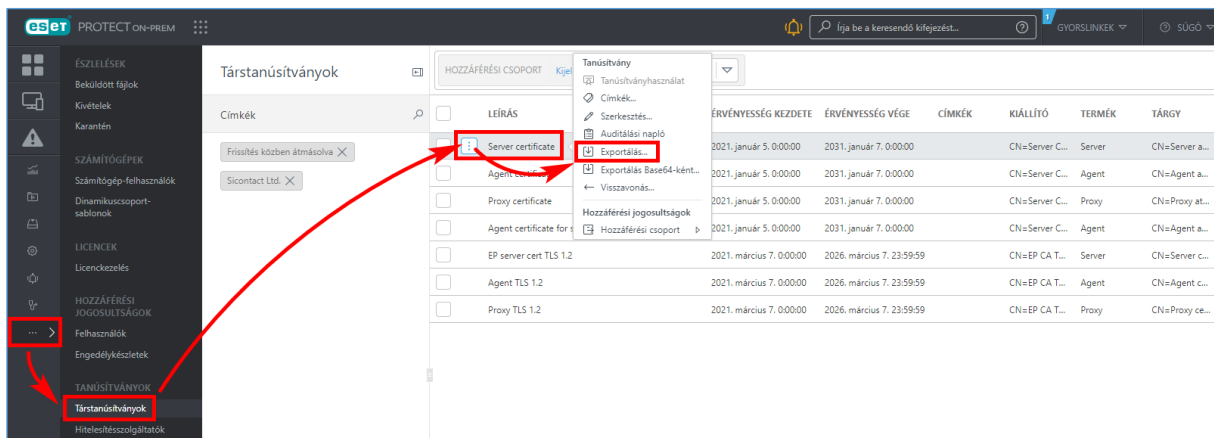
A tanúsítványok biztonsági mentése:

Annak érdekében, hogy az összes összetevő megfelelően tudjon kommunikálni, minden társtanúsítványnak érvényesnek kell lennie, és ugyanazon hitelesítésszolgáltatónak kell aláírnia, ezért ahhoz, hogy a szervert migrálni lehessen, exportálnia kell az összes használt társtanúsítványt valamint a hitelesítésszolgáltatókat.

Első bejelentkezés után exportálja ki a hitelesítésszolgáltatókat és a társtanúsítványokat. Windows szerver esetén készítsen másolatot a **startupconfiguration.ini** fájlról.

Fájl helye:

%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\
startupconfiguration.ini



Adatbázis mentés

Készítsen biztonsági másolatot az adatbázisról, VA esetén pedig készítsen snapshotot az egész virtuális szerverről.
Útmutató: https://help.eset.com/protect_install/13.0/en-US/db_backup.html

ESET Bridge Proxy

Telepítéskor javasolt az ESET Bridge Proxy szolgáltatás használata. Feladata a frissítések, valamint a telepítési csomagok gyorsítótárazása az ESET Management Agent és a végpontvédelmek számára.

The image shows two side-by-side windows from the ESET PROTECT installation process. The left window, titled 'ESET PROTECT On-Prem Setup', is in the 'Components' step, showing a list of components to install. The 'ESET Bridge Proxy' checkbox is selected and highlighted with a red box. The right window, titled 'ESET PROTECT Server Appliance', shows configuration fields. A red arrow points from the 'ESET Bridge Proxy' checkbox in the left window to the 'ENABLE ESET BRIDGE PROXY' checkbox in the right window, which is also selected and highlighted with a red box. Other fields like 'HOSTNAME', 'PASSWORD', 'LOCALE', 'WINDOWS DOMAIN', and 'WINDOWS DOMAIN CONTROLLER' are visible but not highlighted.

Mikor javasolt: https://help.eset.com/protect_install/13.0/en-US/when_to_start_using_http_proxy.html

Részletes áttekintés: <https://help.eset.com/ebe/4.2/en-US/index.html>

Önálló telepítő: <https://www.eset.com/hu/vallalati/letoltes/eset-protect/#standalone>

ESET Business Account, ESET PROTECT Hub fiók

Az ESET PROTECT On-Prem szervertől adja hozzá a meglévő előfizetését regisztrált ESET Business Account (EBA) vagy ESET PROTECT Hub (EPH) fiókkal.

Előfizetés hozzáadása

Az előfizetések ESET PROTECT On-Prem szolgáltatásban való közvetlen hozzáadására már nincs lehetőség. Most már az ESET PROTECT Hub, az ESET Business Account vagy az ESET MSP Administrator szolgáltatásban lehet hozzáadni az előfizetéseket, majd szinkronizálni kell az ESET PROTECT On-Prem segítségével.

A következő opciók egyikével adhatja hozzá az előfizetést:

☒ Jelentkezzen be a fiókjába: ESET PROTECT Hub, ESET Business Account vagy ESET MSP Administrator

☐ Offline aktiválási fájl beszurása

Szinkronizálja az előfizetéseket az ESET PROTECT Hub, ESET Business Account vagy ESET MSP Administrator szolgáltatásból az ESET PROTECT On-Prem szolgáltatásban lévő statikus csoportra frissítéséhez.

☒ E-mail cím

☒ Jelszó

[Elfelejttem a jelszavam](#)

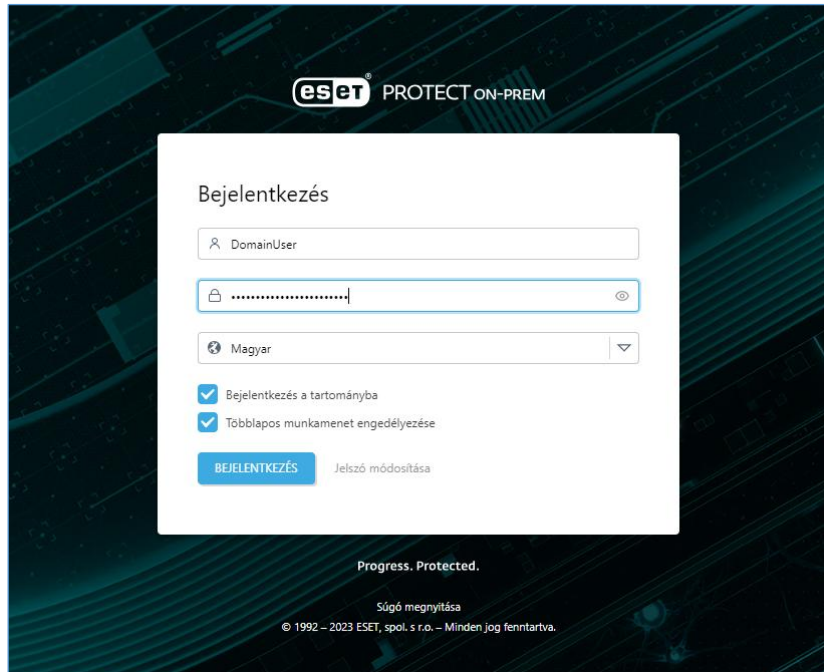
ELŐFIZETÉSEK HOZZÁADÁSA

MÉGSE

Segédlet: https://help.eset.com/protect_admin/13.0/en-US/?license_security_admin.html

ESET PROTECT On-Prem felhasználók

A webkonzol belépéséhez **ne használja az alapértelmezett Administrator fiókot**, hanem hozzon létre másik felhasználót/felhasználókat kétfaktoros hitelesítéssel.

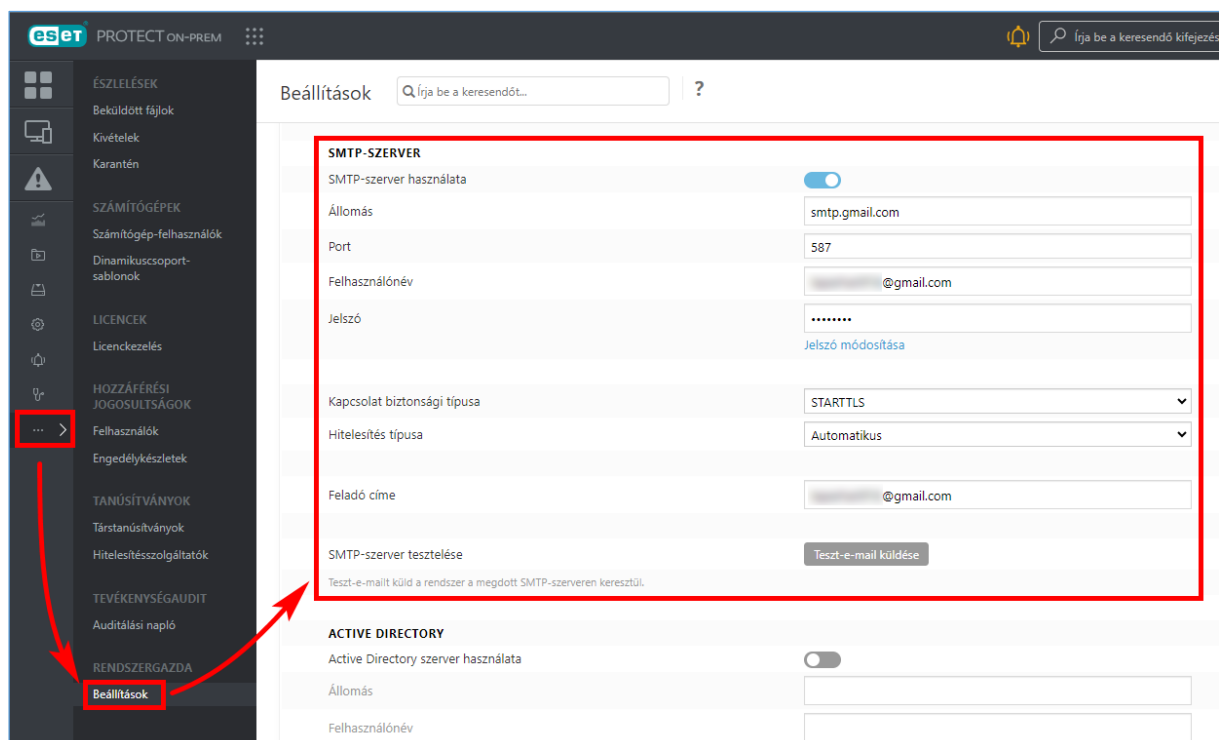


Natív és tartományi felhasználó hozzáadása az ESET PROTECT On-Prem-hez:

https://help.eset.com/protect_admin/13.0/en-US/admin_ar_users.html

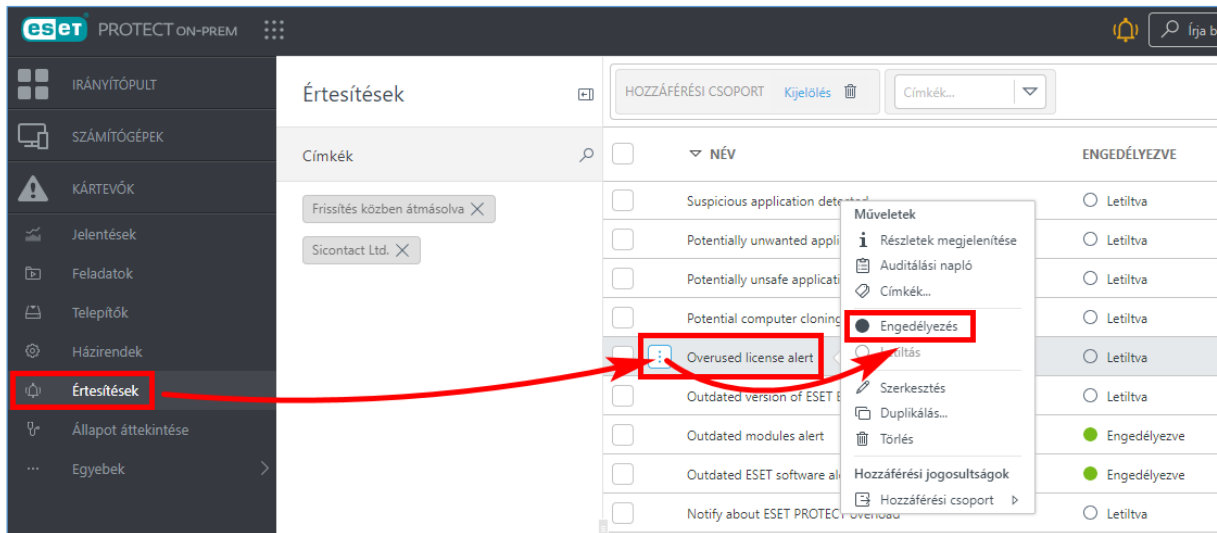
ESET PROTECT On-Prem e-mail értesítések beállítása

Beállíthatja az automatikus értesítéseket bizonyos események, például észlelt fenyegetések, elavult végpontok és egyébek alapján.



Az SMTP beállítása:

https://help.eset.com/protect_admin/13.0/en-US/smtp_server.html



Az értesítések beállítása:

https://help.eset.com/protect_admin/13.0/en-US/admin_ntf_notifications.html

ESET PROTECT On-Prem naplófájlok

Minden ESET PROTECT összetevő naplózást végez. A naplófájlok helye az összetevőtől függően változik.

Windows:

- ESET PROTECT On-Prem szerver naplófájlok:
C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\
- ESET PROTECT On-Prem Web Console és Apache Tomcat:
C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs\

Linux:

- ESET PROTECT On-Prem szerver naplófájlok
/var/log/eset/RemoteAdministrator/Server/
/var/log/eset/RemoteAdministrator/EraServerInstaller.log
- ESET PROTECT On-Prem Web Console és Apache Tomcat
/var/log/tomcat/

További részletek a naplófájlokról:

https://help.eset.com/protect_install/13.0/en-US/log_file.html

Automatikus házirend

Ha az alábbi felugró ablak jelenik meg az ESET PROTECT On-Prem rendszerben, akkor javasoljuk, hogy az utólagos házirend szerkeszthetőség és átláthatóság miatt kattintson a házirend elutasítása gombra.



Házirend jelzők

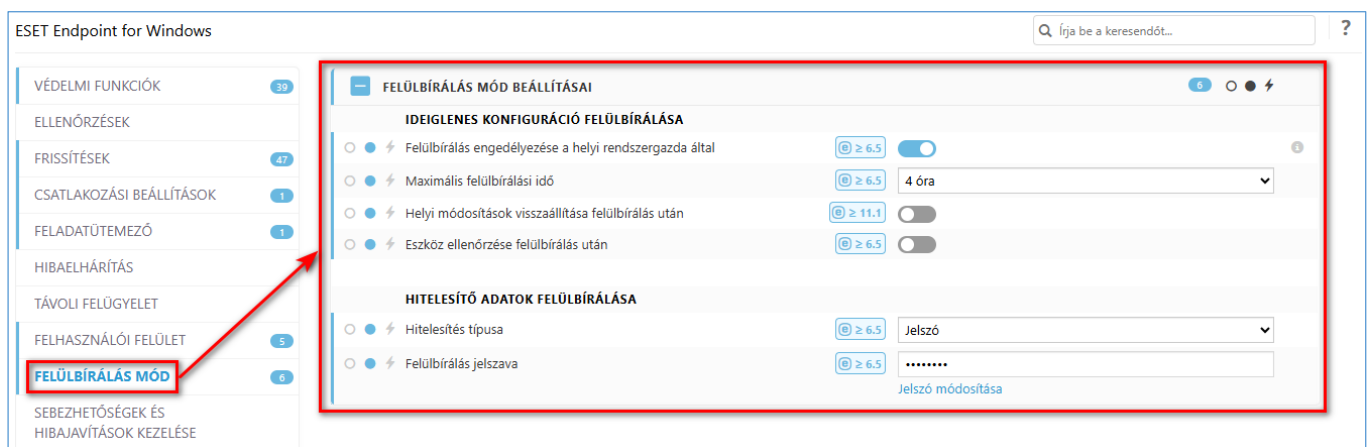
A házirend beállításainak 3 lehetséges opciója van:

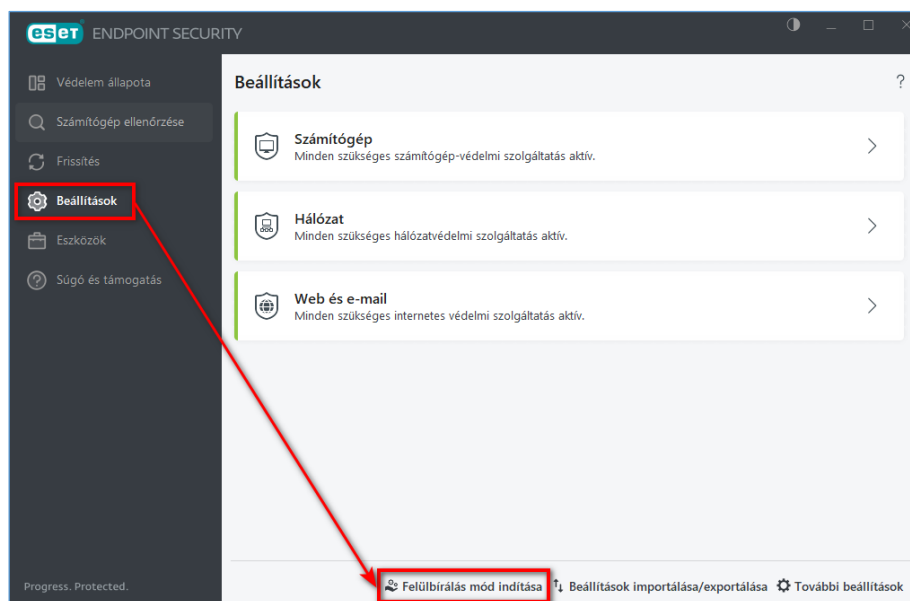
- - Ezt a beállítást nem a házirend adja meg, módosítható lesz a végponton ☒
- - Ezt a beállítást a házirend adja meg, zárolva (nem módosítható) lesz a végponton ☐ , csak másik házirend tudja felülrírni a kiértékelési szabályok alapján.
- ⚡ - Ezt a beállítást a házirend kényszeríti ki, zárolva (nem módosítható) lesz a végponton, és más házirend sem tudja felülrírni ☐

Segédlet: https://help.eset.com/protect_admin/13.0/en-US/admin_pol_flags.html

Házirend felülbírlás mód

A felülbírlási mód lehetővé teszi a rendszergazda számára a kliens számítógépen, hogy módosítsa a telepített ESET termék beállításait, még akkor is, ha ezekre a beállításokra van érvényes házirend.
A felülrírási mód engedélyezhető az AD-felhasználók számára, vagy jelszóval védhető.
A funkció négy óránál hosszabb időtartamra nem engedélyezhető.





Segédlet: https://help.eset.com/protect_admin/13.0/en-US/admin_pol_override.html

ESET Management Agent telepítési, beállítási tippek

Telepítés

Rendszerkövetelmények

A Microsoft által már nem támogatott régebbi operációs rendszereknél (Windows 7 SP1, Windows 8 és 8.1, Windows Server 2008 R2, Windows Server 2012 és Windows Server 2012 R2) szintén telepíthető a legújabb 13-as verziójú ESET Management Agent.

A rendszerkövetelményekről az alábbi oldalon tájékozódhat:

https://help.eset.com/protect_install/13.0/en-US/windows.html

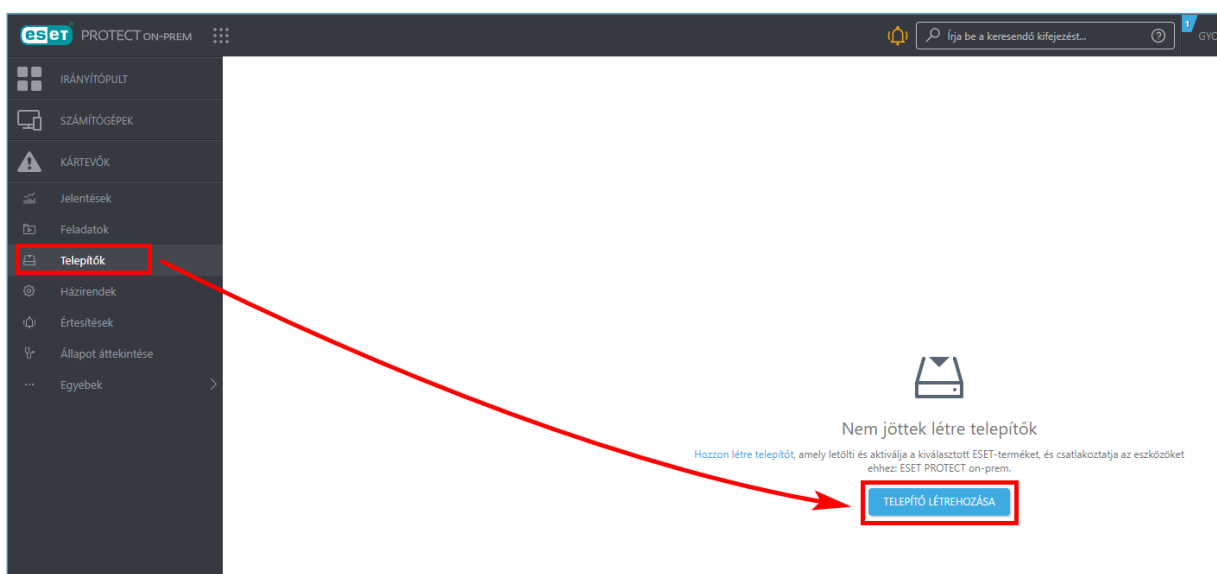
Linux, MacOS

Abban az esetben, ha a klienseken Linux vagy MacOS operációs rendszer fut, a telepítéshez az alábbi tudásbázis cikkben talál segítséget:

<https://support.eset.com/en/kb7750-deploy-the-eset-management-agent-to-a-macos-client-using-agent-live-installer>

Agent Live Installer létrehozása

Az ESET PROTECT On-Prem server és a kliensek közötti kommunikáció az ESET Management Agent-en keresztül történik. Az EM Agent vagy egy külön telepítővel (Agent Live telepítő) vagy egy teljes telepítőcsomaggal (Agent és végpontvédelem) telepíthető a kliensekre. Mindkét esetben ügyeljen arra, hogy ha nincs a helyi hálózatban elérhető DNS szerver (melynek segítségével fel tudják oldani a szerver nevét a kliensek), akkor az alábbi képeken látható „Szerver hosztneme” mezőben az alapértelmezetten szereplő FQDN nevet (pl. epva.local.hu) cserélje le az ESET PROTECT On-Prem szerver IP címére.



eset PROTECT ON-PREM

IRÁNYÍTÓPULT
SZÁMÍTÓGÉPEK
KÁRTEVŐK
Jelentések
Feladatok
Telepítők
Házirendek
Értesítések
Állapot áttekintése
Egyebek

Telepítő létrehozása

Telepítők > ESET Management Agent

Alap

Windows

macOS

Linux

Terjesztés

- ☐ Telepítő letöltése vagy az ESET Remote Deployment Tool használata
- ☒ Az ügynök telepítése először (Agent szkript telepítő)
- ☐ GPO vagy SCCM használata a telepítéshez

Komponensek

- ☒ Management Agent

Termékfejlesztési program Javasolt

- ☒ Részvétel a termékfejlesztési programban

Szülőcsoport
/Mind

Szerver hosztneve (nem kötelező)

epva.local.hu

Port
2222

Társtanúsítvány

eset PROTECT ON-PREM

IRÁNYÍTÓPULT
SZÁMÍTÓGÉPEK
KÁRTEVŐK
Jelentések
Feladatok
Telepítők
Házirendek
Értesítések
Állapot áttekintése
Egyebek

Telepítő létrehozása

Telepítők > ESET Management Agent

Alap

☒ Management Agent

Termékfejlesztési program Javasolt

- ☒ Részvétel a termékfejlesztési programban

Szülőcsoport
/Mind

Szerver hosztneve (nem kötelező)

192.168.10.2

Port
2222

Társtanúsítvány

- ☒ ESET PROTECT-tanúsítvány
- ☐ Egyéni tanúsítvány

ESET PROTECT-tanúsítvány

Leírás Agent certificate,
Kiadó CN=Server Certification Authority;C=US;
Alany CN=Agent at *;C=US;
Termék Agent,
Érvényesség kezdete Tue Jan 05 2021,
Érvényesség vége Tue Jan 07 2031.

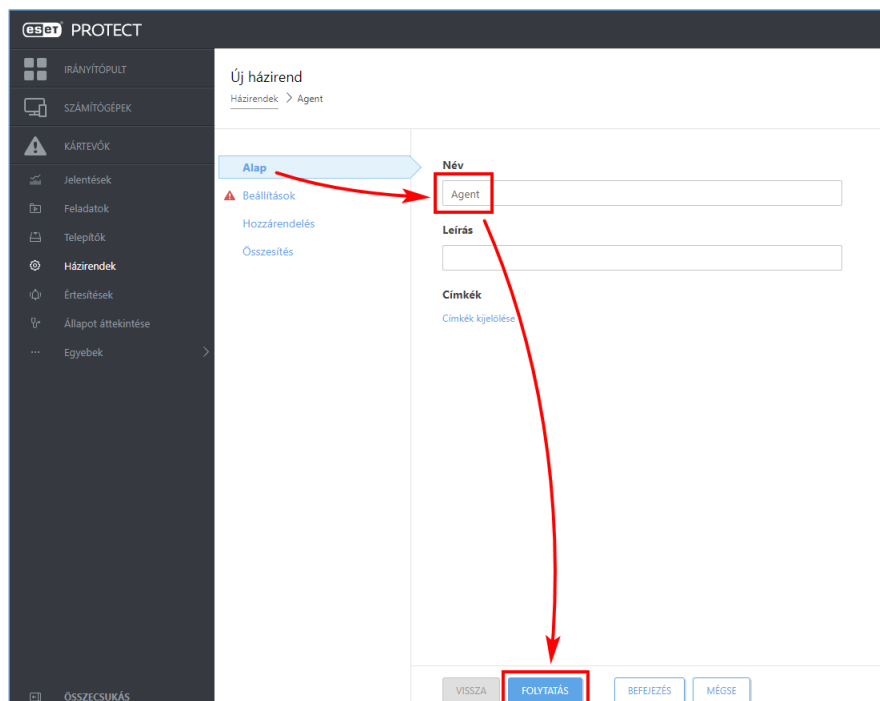
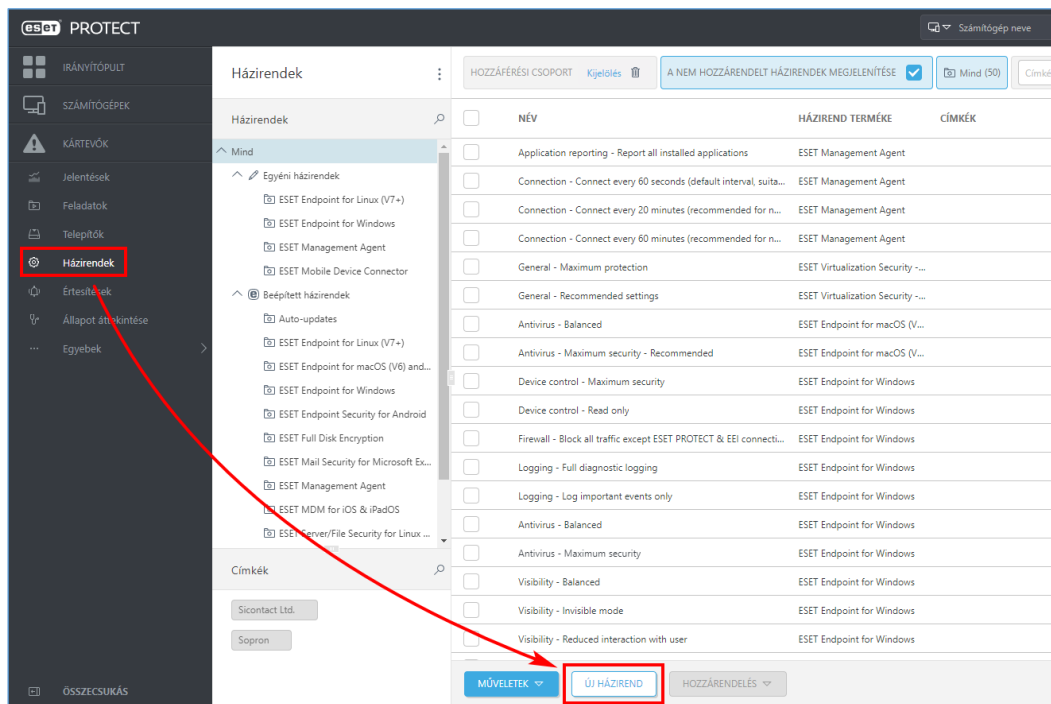
Tanúsítvány jelszava

További beállítások testreszabása

VISSZA FOLYTATÁS MENTÉS & LETÖLTÉS MEGSE

Beállítások

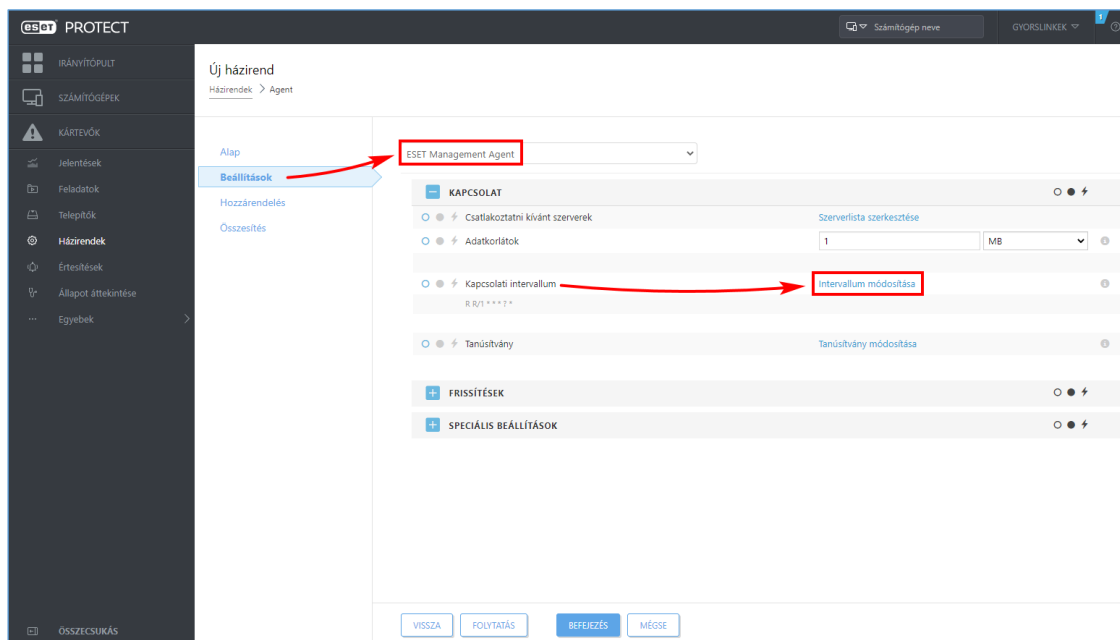
Az ESET Management Agent beállításainak finomhangolásával optimalizálni lehet az ESET PROTECT On-Prem szerver terhelését, illetve bizonyos funkciók használatával további információkhoz is juthat a kliens gépekkel kapcsolatban. Az EM Agent-ek beállításait csakúgy, mint a végpontvédelmek esetében, házirenddel lehet megadni. Az EM Agent házirend létrehozásához kattintson a Házirendek menüpontra az ESET PROTECT On-Prem webkonzol bal oldali menüjében, majd alul hozzon létre egy új házirendet, amelyet nevezzen el tetszőlegesen és kattintson a Folytatás gombra:

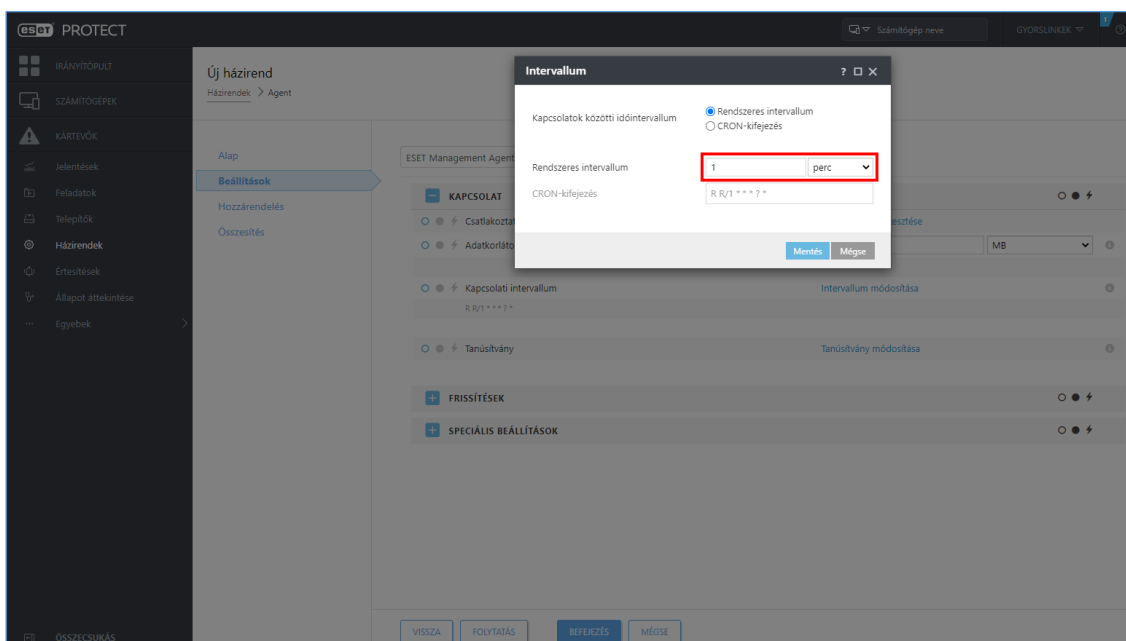


A Beállítások részre ugorva a fenti legördülő menüből válassza az „ESET Management Agent” lehetőséget. Ekkor megjelennek az EM Agent-re vonatkozó beállítási lehetőségek.

Kapcsolati intervallum beállítása

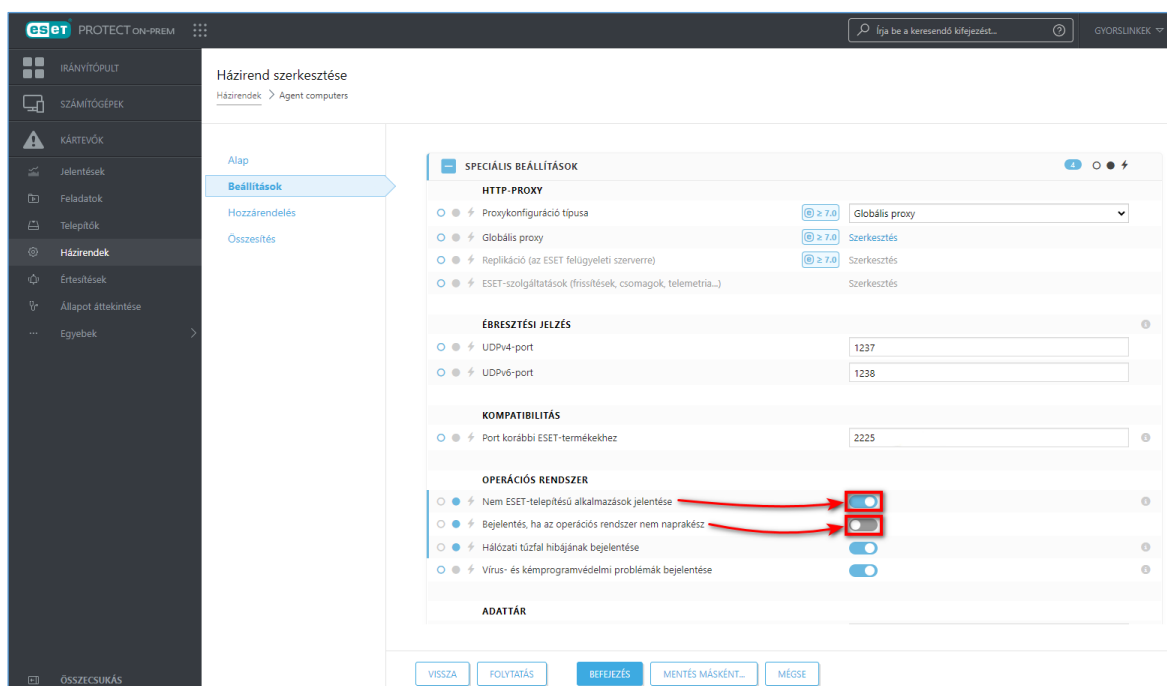
A Kapcsolat részen a Kapcsolati intervallum sorban az Intervallum módosítása felírra kattintva tudja beállítani, hogy a kliensekre telepített EM Agent-ek milyen időközönként kapcsolódjanak az ESET PROTECT On-Prem szerverhez. Ez az idő intervallum alapértelmezetten 1 perc, amely abban az esetben, ha az ESET PROTECT On-Prem szervernek a dokumentációban javasolt erőforrások lettek rendelkezésre bocsájtva a telepítéskor, 1000 kliensig megfelelő. 1000-tól 5000 kliensig 5 percre, 5000 kliens felett pedig 10 percre érdemes növelni a kapcsolati intervallumot. Bevezetéskor, teszteléskor azonban érdemes lecsökkenteni a minimális 10 másodperce.





Minden telepített szoftver jelentése

Az EM Agent alapértelmezetten elküldi az ESET PROTECT On-Prem szervernek, hogy az adott kliensen milyen ESET végpontvédelmi termék melyik verziója van telepítve, valamint azt is, hogy milyen operációs rendszer fut rajta. Ezeknek az információknak a körét azonban ki lehet bővíteni azzal is, hogy az egyes klienseken milyen egyéb alkalmazások vannak telepítve. Ehhez be kell kapcsolni az EM Agent házirendben a „Nem ESET-telepítésű alkalmazások jelentése” funkciót.

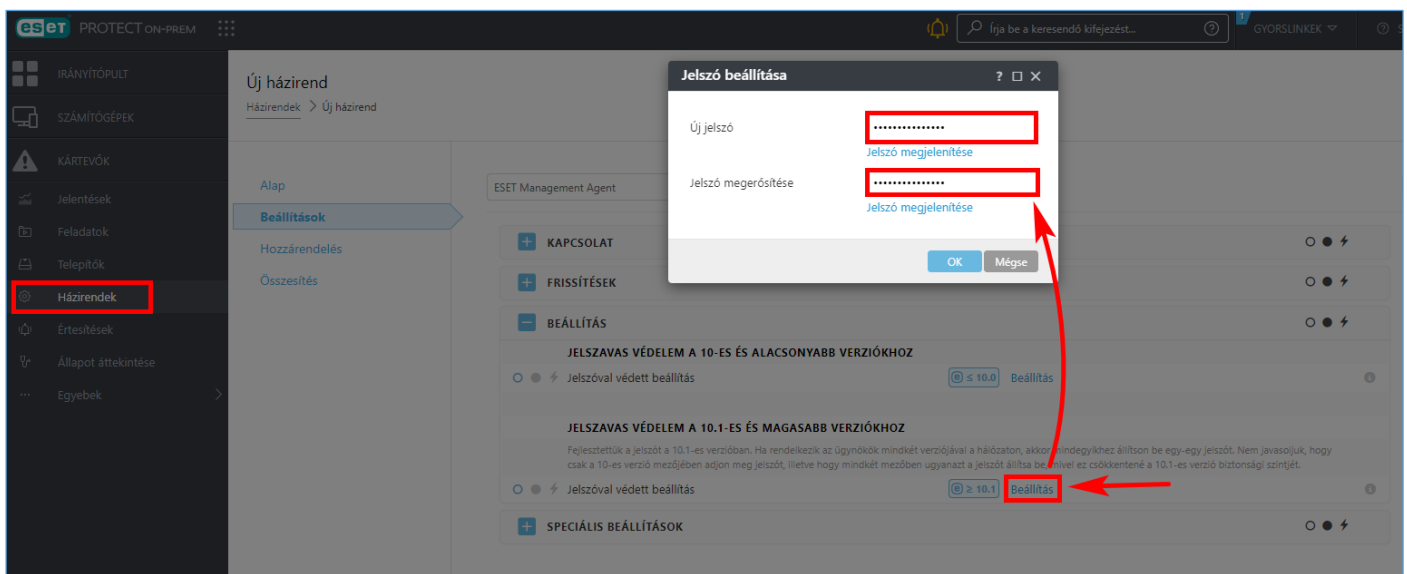


Operációs rendszer frissítésének szükségessége

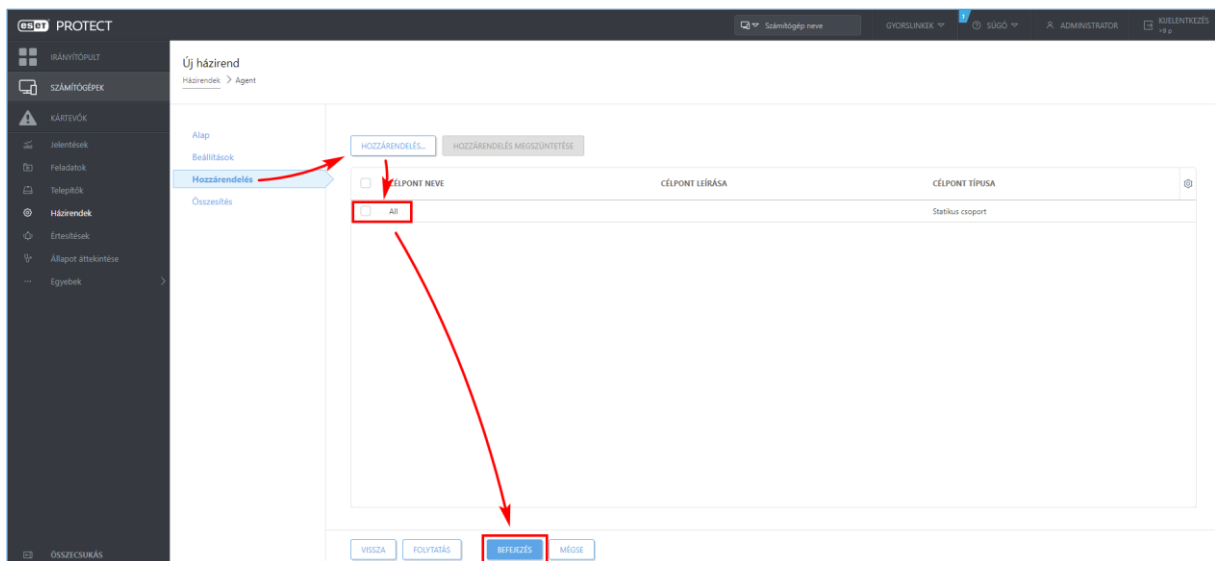
Az EM Agent az operációs rendszer állapotát is jelenti a központi menedzsment felé, azaz jelzi, ha szükség van a frissítésre. Amennyiben a kliens gépek frissítését központilag kezelik, akkor ezt a funkciót ki lehet kapcsolni a „Bejelentés, ha az adott operációs rendszer nem naprakész” sorban található kapcsoló kikapcsolásával (lásd a fenti képen).

Jelszavas védelem

Olyan környezetekben, ahol indokolt a még magasabb szintű biztonság, az EM Agent esetleges eltávolítása ellen a beépített védelmi megoldásokon túl jelszó megadásának előírásával is lehet védekezni.



Az előzőekben elvégzett beállítások elvégzése után, az érvényesüléshez hozzá kell rendelni az elkészült házirendet a megfelelő csoporthoz (pl. All) vagy eszközhöz. A Befejezés gombra kattintva mentheti a házirendet.



Távoli kliensek kapcsolódása a helyi ESET PROTECT On-Prem szerverhez

Abban az esetben, ha vannak olyan kliensek, amelyek távolról kapcsolódnak az ESET PROTECT On-Prem szerverhez, a megvalósításhoz kövesse az alábbi tudásbázis cikk útmutatását:

<https://support.eset.com/en/kb8146-configure-network-to-allow-clients-to-remotely-connect-to-eset-protect>

Ilyenkor az ezekre a kliensekre telepítendő EM Agent telepítőjében a fentebb említett „Szerver hosztneve” mezőben az ESET PROTECT On-Prem szerver telephelyének külső IP-címét kell megadni.

Naplófájlok

Kapcsolódási és egyéb hibák kereséséhez ajánljuk az alábbi mappában található *status.html* és *trace.log* fájlok vizsgálatát: C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs

ESET PROTECT Cloud

Az ESET PROTECT Cloud használatát tekintve szinte megegyezik az ESET PROTECT On-Premmel. Az új funkciók, illetve újdonságok először a Cloud, majd később az On-Prem verzióban jelennek meg. Azonban van egy-két funkció, ami csak a Cloud-ban érhető el.

A teljesség igénye nélkül néhány ezek közül:

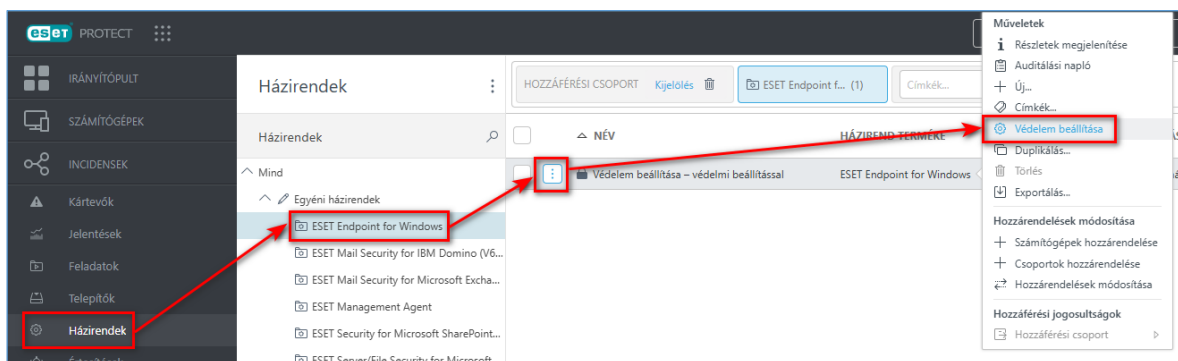
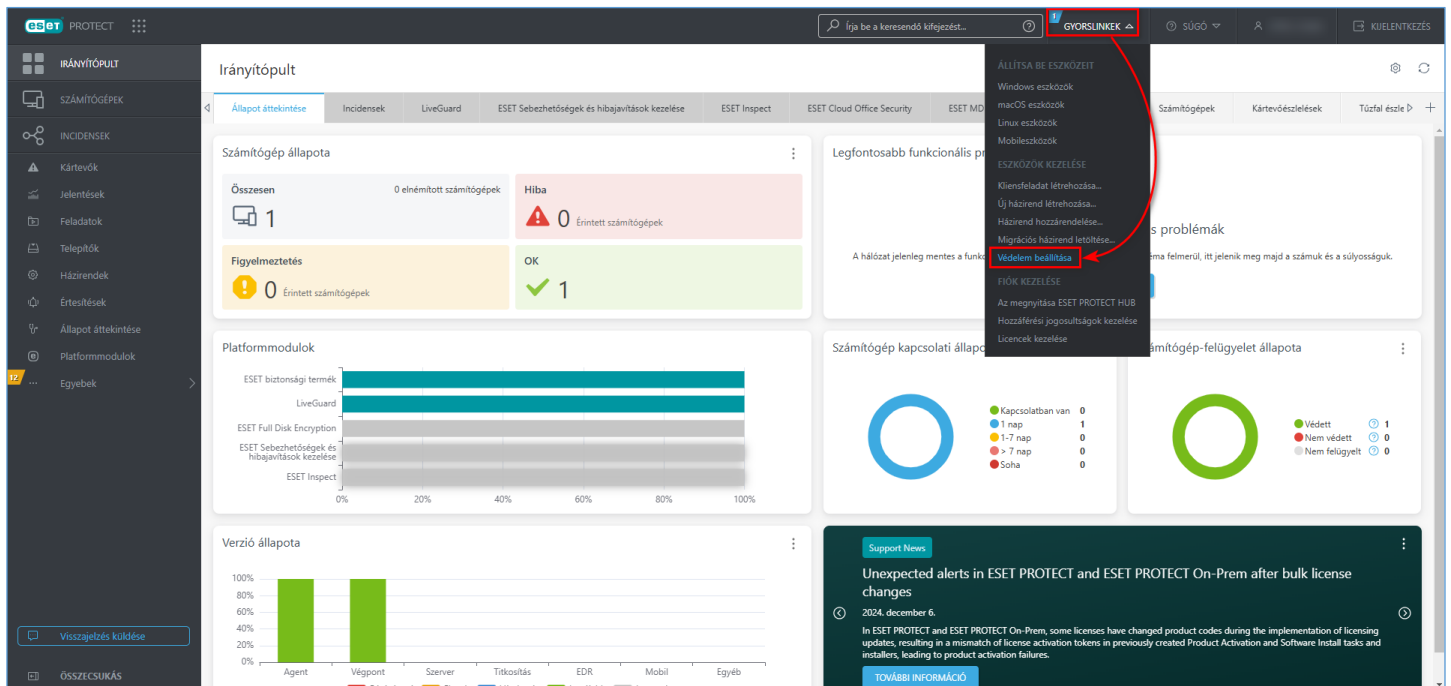
- Sebezhetőség és hibajavítások kezelése
- Mobile Device Management

A különbségekről bővebben: https://help.eset.com/protect_cloud/en-US/differences_onprem_cloud.html

Védelem beállítása

Az ESET PROTECT alapértelmezetten felajánlja a legalapvetőbb beállítások és funkciók használatának bekapcsolását házirendben. Azonban a jövőbeni átláthatóságot és szerkeszthetőséget szem előtt tartva erősen javasoljuk, hogy ezt **NE** a felajánlott ablakban tegye meg, hanem manuálisan végezze el. Ezért azt javasoljuk, hogy az alábbi képen látható módon, ne változtasson a beállításokon, hanem kattintson a „Később kérdezze meg” gombra.

Amennyiben szeretné mégis ezt használni, az ajánlott „Védelmi beállítása” ablak az alábbi helyeken újra megnyitható.



AD szinkronizáció

Mivel az ESET PROTECT Cloud nem kapcsolódik közvetlenül az Ön hálózatába, ezért az Active Directory-val való szinkronizálás közvetlenül nem lehetséges. A szinkronizálni, csak a felhasználókat vagy számítógépeket és csoportokat lehet. Ehhez külön program használata szükséges.

Leírás: <https://support.eset.com/en/kb7760-active-directory-scanner>
https://help.eset.com/protect_cloud/en-US/protect_cloud_synchronize_with_ad.html

Sebezhetőségek és hibajavítások kezelése (Vulnerability és Patch Management)

A modul aktívan monitorozza és javítja az operációs rendszerek és az alkalmazások sebezhetőségeit az összes végponton.

Ez a modul csak ESET PROTECT Complete és magasabb licenccsomaggal használható. Elérhető Windows, Linux és MacOS operációs rendszerre.

Leírás:

https://help.eset.com/protect_cloud/en-US/patch_management.html?vulnerabilities.html
https://help.eset.com/protect_cloud/en-US/patch_management.html?patch_management.html

Ismert sebezhetőségek listája:

https://help.eset.com/protect_cloud/en-US/patch_management.html?applications_vulnerabilities.html

Ismert hibajavítások listája:

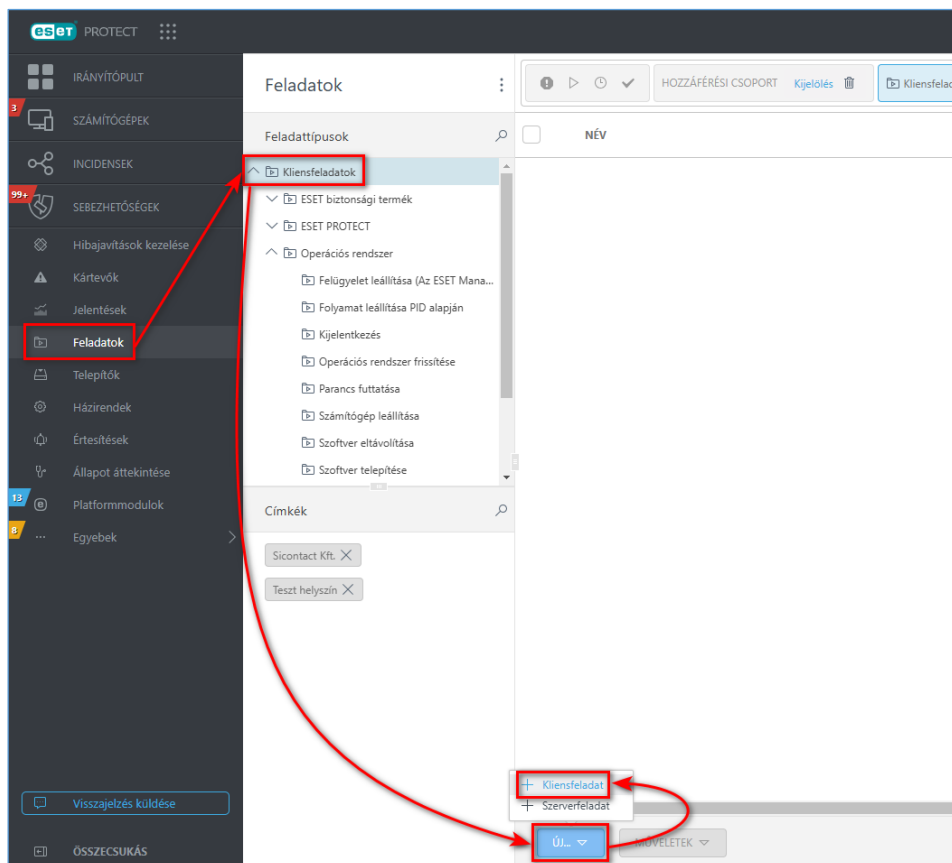
https://help.eset.com/protect_cloud/en-US/patch_management.html?applications_patch_management.html

Gyakran ismételt kérdések

https://help.eset.com/protect_cloud/en-US/patch_management.html?vulnerabilities_patch_management_faq.html

Kérjük, vegye figyelembe: A modul aktiválásakor ellenőrizze, hogy mely gépekhez rendeli hozzá, valamint amikor a házirendben megadja az automatikus újraindítás lehetőséget, ellenőrizze le, hogy a szerverek ne legyenek benne. A szervereken javasoljuk, hogy manuálisan futtassa az ellenőrzést és a hibajavítást.

Aktiválás



eset PROTECT

IRÁNYÍTÓPULT
SZÁMÍTÓGÉPEK
INCIDENSEK
SEBEZHETŐSÉGEK
Hibajavítások kezelése
Kártevők
Jelentések
Feladatok
Telepítők
Házirendek
Értesítések
Állapot áttekintése
Platformmodulok
Egyebek

Visszajelzés küldése
ÖSSZECSUKÁS

Új kliensfeladat

Feladatok > VAPM aktiválása

Alap
Beállítások
Összesítés

Név
VAPM aktiválása

Címkék
Címkék kiválasztása

Leírás

Feladatkategória
Minden feladat

Feladat
Termék aktiválása

VISSZA FOLYTATÁS BEFEJEZÉS MÉGSE

eset PROTECT

IRÁNYÍTÓPULT
SZÁMÍTÓGÉPEK
INCIDENSEK
SEBEZHETŐSÉGEK
Hibajavítások kezelése
Kártevők
Jelentések
Feladatok
Telepítők
Házirendek
Értesítések
Állapot áttekintése
Platformmodulok
Egyebek

Visszajelzés küldése
ÖSSZECSUKÁS

Új kliensfeladat

Feladatok > VAPM aktiválása

Alap
Beállítások
Összesítés

Termékaktiválási beállítások

ESET-licenc ⓘ
ESET Endpoint & Server Security for ESET PROTECT Complete, nyilvános azonosító tulajdonos
, lejárát 0:59:59

VISSZA FOLYTATÁS BEFEJEZÉS MÉGSE

Kérjük, válasszon licenct

Címkék

TERMÉKNÉV LICENCTÍPUS JELŐLŐI Nincs kiválasztva Címkék...

Szűrő hozzáadása

1 LICENCFELHASZNÁLÓ	2 NYILVÁNOS AZO...	CSOMAGNÉV	TERMÉKNÉV	EGYSÉGEK	ALEGYSÉGEK
☒	Sicontact Kft.	ESET PROTECT Advanced	ESET Mobile Threat Defense	1/10	
☐	Sicontact Kft.	ESET PROTECT Advanced	ESET LiveGuard Advanced for Endpoint Security + Server S...	1/10	
☐	Sicontact Kft.	ESET PROTECT Advanced	ESET Full Disk Encryption	1/10	
☐	Sicontact Kft.	ESET PROTECT Advanced	ESET Endpoint & Server Security for ESET PROTECT Advan...	5/10	
☐	Sicontact Kft.	ESET PROTECT Complete	ESET Endpoint & Server Security for ESET PROTECT Compl...	0/10	
☐	Sicontact Kft.	ESET PROTECT Complete	ESET LiveGuard Advanced for Endpoint Security + Server S...	0/10	
☐	Sicontact Kft.	ESET PROTECT Complete	ESET Mobile Threat Defense	0/10	
☐	Sicontact Kft.	ESET PROTECT Complete	ESET LiveGuard Advanced for Mail Security	0/12	0/12
☐	Sicontact Kft.	ESET PROTECT Complete	ESET Full Disk Encryption	0/10	
☒	Sicontact Kft.	ESET PROTECT Complete	ESET Vulnerability & Patch Management component	1/10	
☐	Sicontact Kft.	ESET PROTECT Complete	ESET Mail Security	0/12	0/12
☐	Sicontact Kft.	ESET PROTECT Advanced			

OK MEGSE

eset PROTECT

IRÁNYÍTÓPULT

SZÁMÍTÓGÉPEK

INCIDENSEK

SEBEZHETŐSÉGEK

Hibajavítások kezelése

Kártevők

Jelentések

Feladatok

Telepítők

Házirendek

Értesítések

Állapot áttekintése

Platformmodulok

Egyebek

Visszajelzés küldése

ÖSSZECSUKÁS

Új kliensfeladat

Feladatok > VAPM aktiválása

Alap

Beállítások

Összesítés

Termékaktiválási beállítások

ESET-licenc

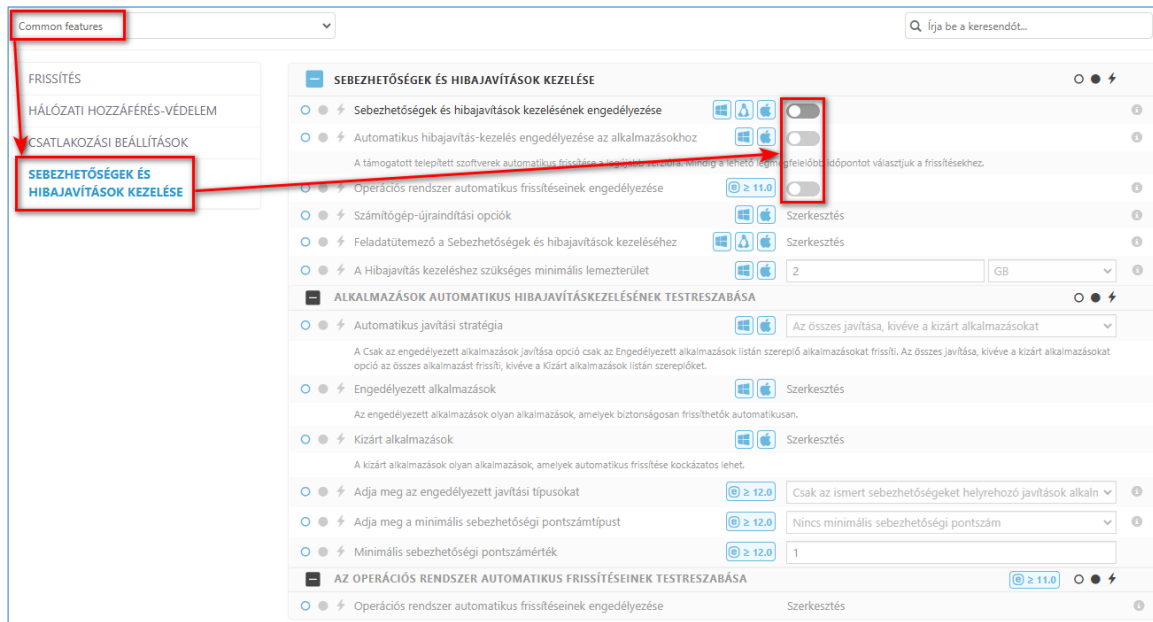
ESET Vulnerability & Patch Management component, nyilvános azonosító 3B8-EWF-XB3, tulajdonos Sicontact Kft. [toth.andras.boldizsar@sicontact.hu], lejárat 2026. január 18. 0:59:59

VISSZA FOLYTATÁS BEFEJEZÉS MEGSE

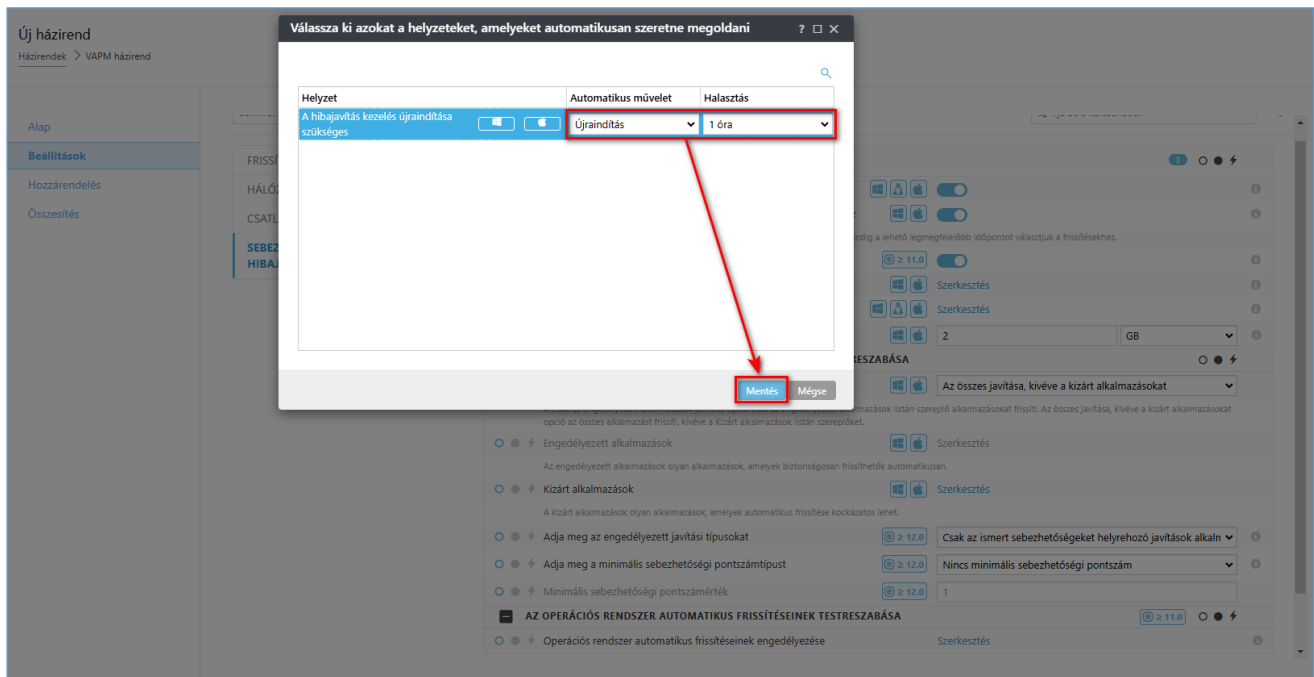
Triggerrel adja meg, hogy mely gépeken vagy csoportokon legyen aktiválva.

Házirend beállítása

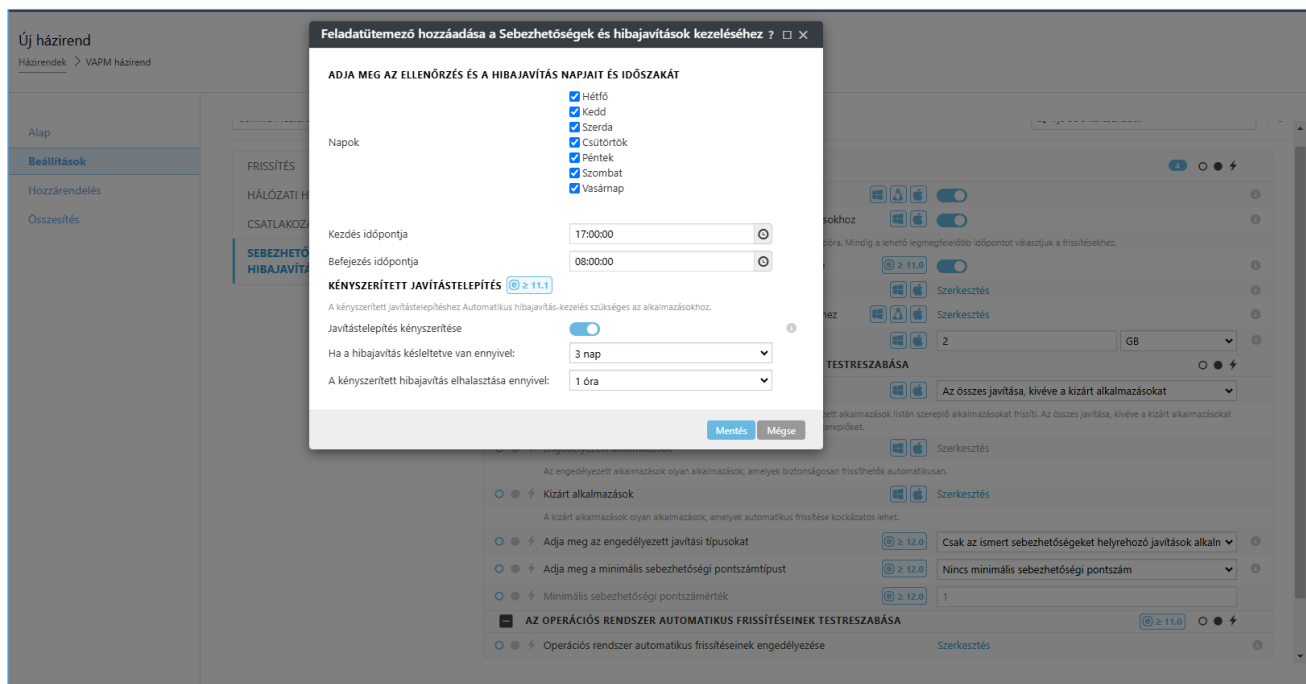
Készítsen új házirendet a funkció használatához, majd a termékeknél válassza a „Common features” lehetőséget, majd a „Sebezhetőségek és hibajavítások kezelése” menüpontot. Kapcsolja be az alábbi képen látható funkciókat:



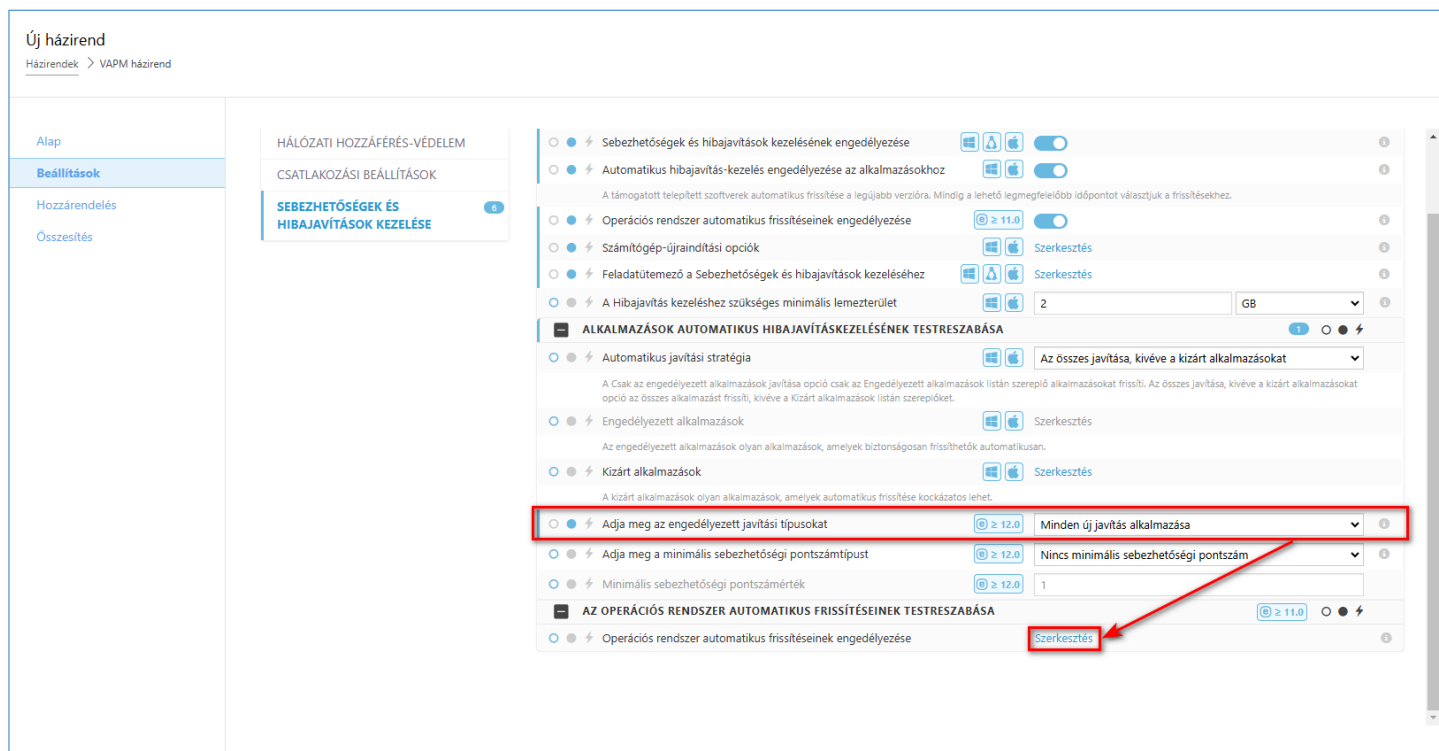
Adja meg a számítógép-újraindítási opciót:



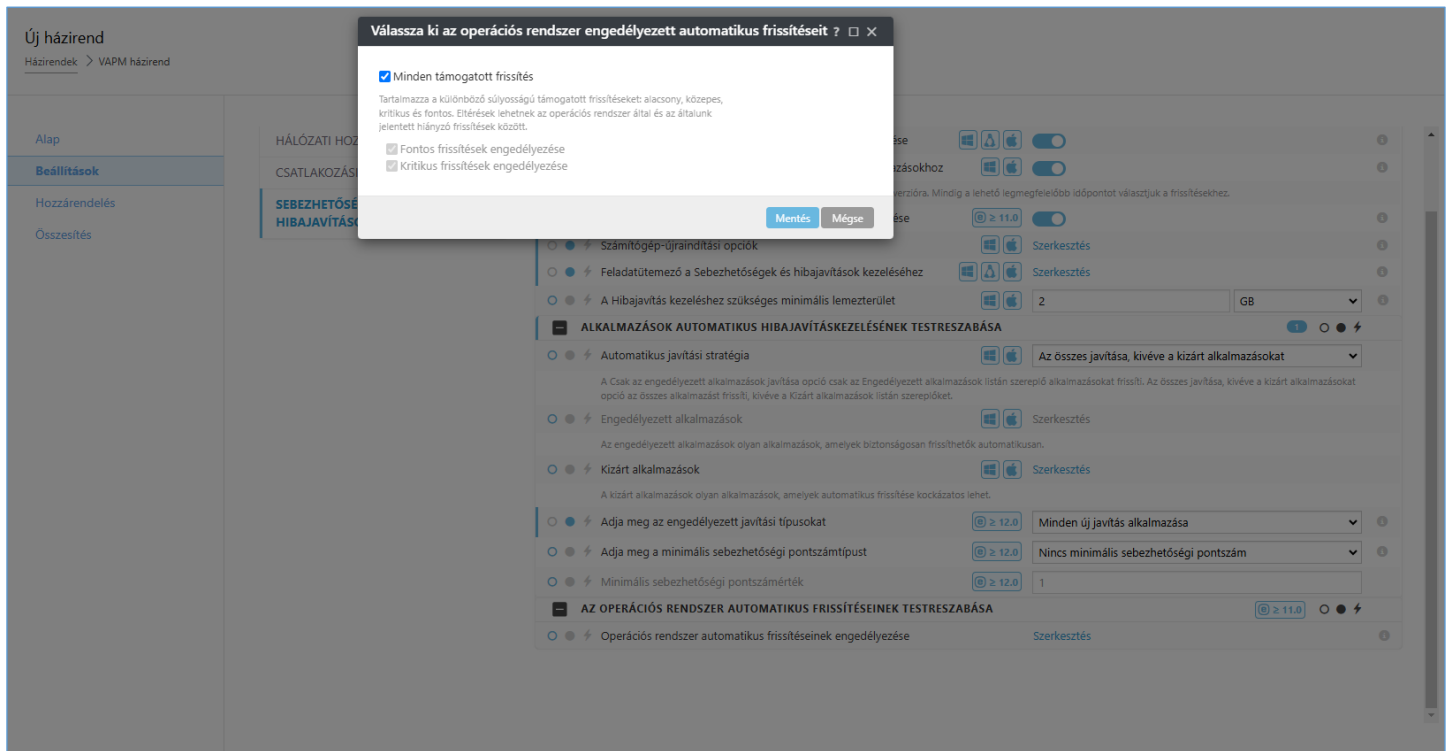
Adja meg a feladat ütemezését:



Állítsa be a javítási típusokat, majd kattintson alul a szerkesztés szövegre:



Kapcsolja be a funkciót a képen látható módon.



Végül rendelje hozzá gépekhez, csoportokhoz a házirendet.

Mobile Device Management

Az ESET PROTECT Cloud-ban lehetőség van mobil eszközök menedzselésére mind Android, mind iOS rendszerű készülékeket.

Kérjük, vegye figyelembe, hogy vírusvédelem csak Android rendszerű készülékeken érhető el, míg iOS rendszerű készülékeken csak a Mobile Device Management érhető el.

Leírás: https://help.eset.com/protect_cloud/en-US/?cloud_mobile_device_management.html

Licencelés

A mobil eszközök védelme bármelyik felhős licenccsomaggal elérhető. ESET PROTECT Essential és Entry csomagok esetén a mobil eszközök is egy helyet foglalnak a teljes licencből. Pl. egy 100 eszközös licenc esetén 10 db szerver 45 db munkaállomás és 45 db mobil eszköz aktiválható.

Ezzel szemben az ESET PROTECT Advanced vagy magasabb licenccsomag esetén grátiszként jelenik meg a mobil eszközök védelme. Ez előző példából kiindulva 100 eszközös licenc esetén 100 db munkaállomás vagy szerver aktiválható, és plusz 100 mobil eszköz.

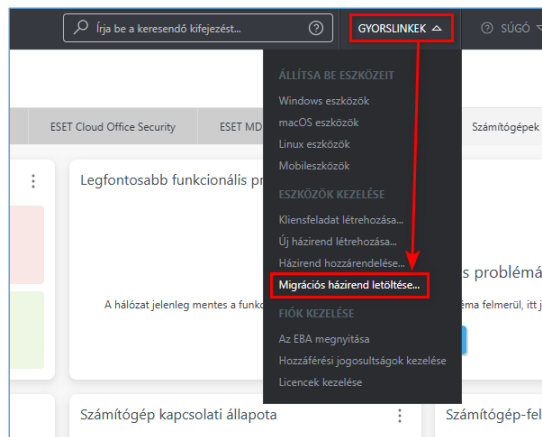
Mobil eszközök migrációja felhőbe

Ha korábban az ESET PROTECT On-Prem rendszerben menedzselte mobil eszközeit, lehetőség van migrálni azokat az ESET PROTECT Cloud rendszerbe. Migrálni csak Android rendszerű készülékeket lehet, iOS eszközöket manuálisan kell újra regisztrálni.

Leírás a migráció menetéről: https://help.eset.com/protect_cloud/en-US/?cmdm_migration_tool.html

Migráció On-Prem rendszerből felhőbe

Lehetőség van a számítógépeket migrálni az ESET PROTECT On-Prem rendszerből az ESET PROTECT Cloudba. Ehhez migrációs házirendet kell letölteni az ESET PROTECT Cloudból és importálni az ESET PROTECT On-Prem-be, majd hozzárendelni csoportokhoz vagy számítógépekhez.



Leírás: https://help.eset.com/protect_cloud/en-US/?cloud_migration.html

ESET Secure Authentication

Az ESET Secure Authentication problémamentes távoli hozzáférést biztosít a céges hálózathoz és adatokhoz. Egy erős mobilalapú megoldás, amely kétfaktoros, egyszer használatos egyedi kódos hitelesítésre (2FA-OTP) épül. Az egyszer használatos egyedi kódok (OTP) véletlenszerűen generáltak, tehát nem megjósolhatók vagy újra használhatók. Az ESET Secure Authentication natívan támogatja az Outlook Web Access/App (OWA) for Microsoft Exchange 2013-at, 2016-ot és 2019-et, valamint támogat olyan kritikus alkalmazásokat, mint az Exchange Control Panel, és az Exchange Administration Centre.

VPN eszközök széles körével, Microsoft SharePoint és Microsoft Dynamics CRM üzleti eszközökkel is használható. Erősíti értékes adatai külső hozzáféréseinek védelmét - RDP-n (Remote Desktop Protocol), Remote Desktop Web Access-en vagy VMWare Horizon View-n keresztül.

Az ESET Secure Authentication önállóan és az ESET PROTECT Elite csomag részeként is rendelhető.

Bővebb információ a következő oldalon olvasható:

<https://www.eset.com/hu/vallalati/megoldasok/tobbfaktoros-hitelesites/>

ESET Cloud Office Security

Hatékony védelem az e-mail-alapú támadásokkal és kártevőkkel szemben, Microsoft 365 alkalmazásokat (Exchange Online, Microsoft OneDrive) használó vállalkozások részére.

Az ESET Cloud Office Security megelőző védelmet biztosít a Microsoft 365 alkalmazások számára a rosszindulatú programok, kényszerített levelek és adathalász támadások ellen. Segítségével felügyelheti a karanténba került állományokat és e-maileket, illetve ellenőrizheti, hogy melyik felhasználót éri a legtöbbször támadási kísérlet. Emellett azonnal értesülhet róla, ha a rendszerbe kártékony kód érkezik, így pillanatok alatt beavatkozhat és megszüntetheti a fenyegetést.

Az licenc tartalmazza az ESET LiveGuard Advanced for Cloud Office Security felhőalapú sandbox technológiát, amely képes az eddig nem ismert, nulladik napi fenyegetések magasabb szintű elhárítására.

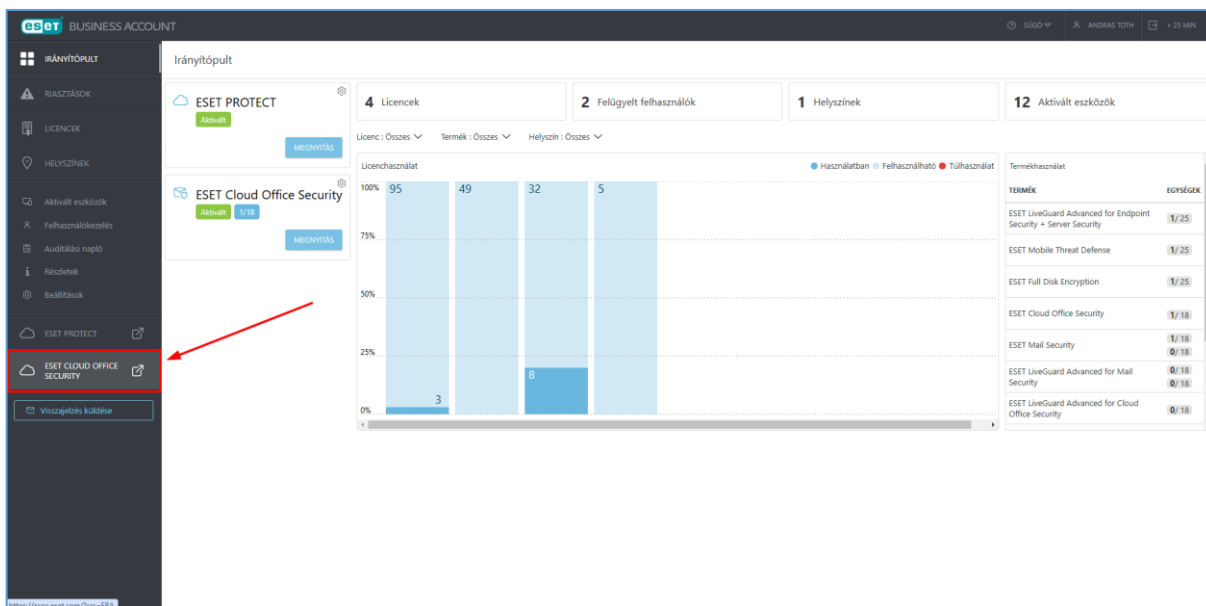
Az ESET Cloud Office Security megoldást egyszerűen kezelheti egy bárhonnal elérhető, felhőalapú management konzolon keresztül. A termék az ESET PROTECT Complete és Elite csomagokban érhető el.

Bővebb információt a következő oldalon talál:

<https://www.eset.com/hu/vallalati/felhoolapuvedelem/cloud-office-security>

ECOS aktiválása

Kérem, lépjen be az <https://protecthub.eset.com> vagy <https://eba.eset.com> weboldalon, attól függően, hogy mely licenckezelő felületet használja. Amennyiben még nem regisztrált, a <https://protecthub.eset.com> weboldalon teheti meg.



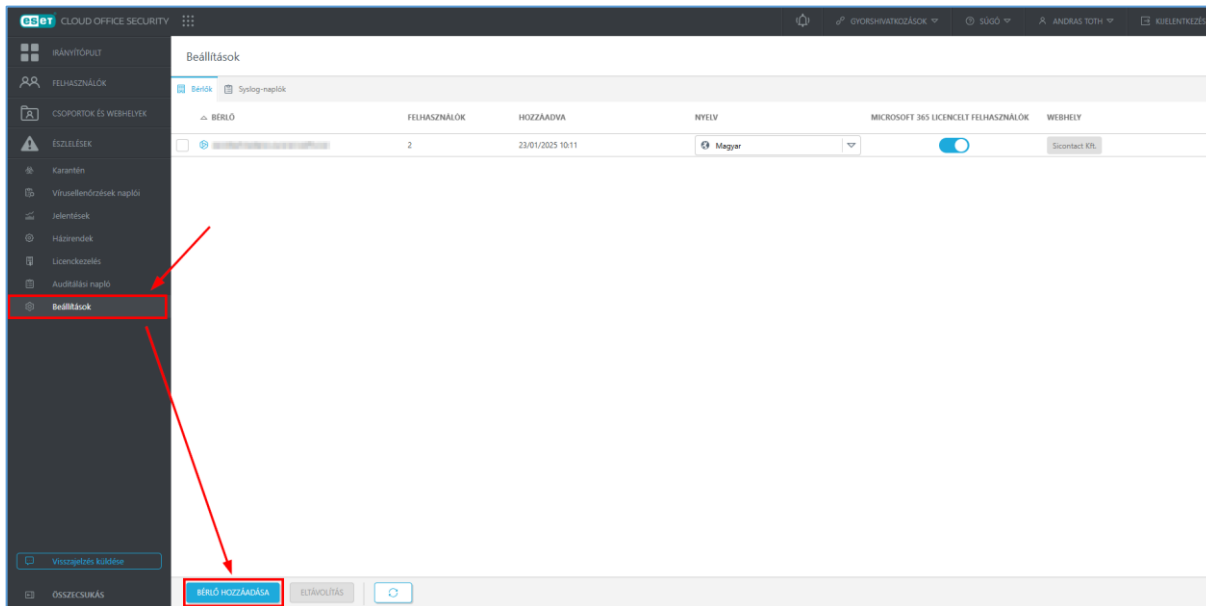
Bal oldal válassza az ESET CLOUD OFFICE SECURITY menüpontot és aktiválás során válassza ki a kívánt régiót (EU régiót).

ECOS megnyitása

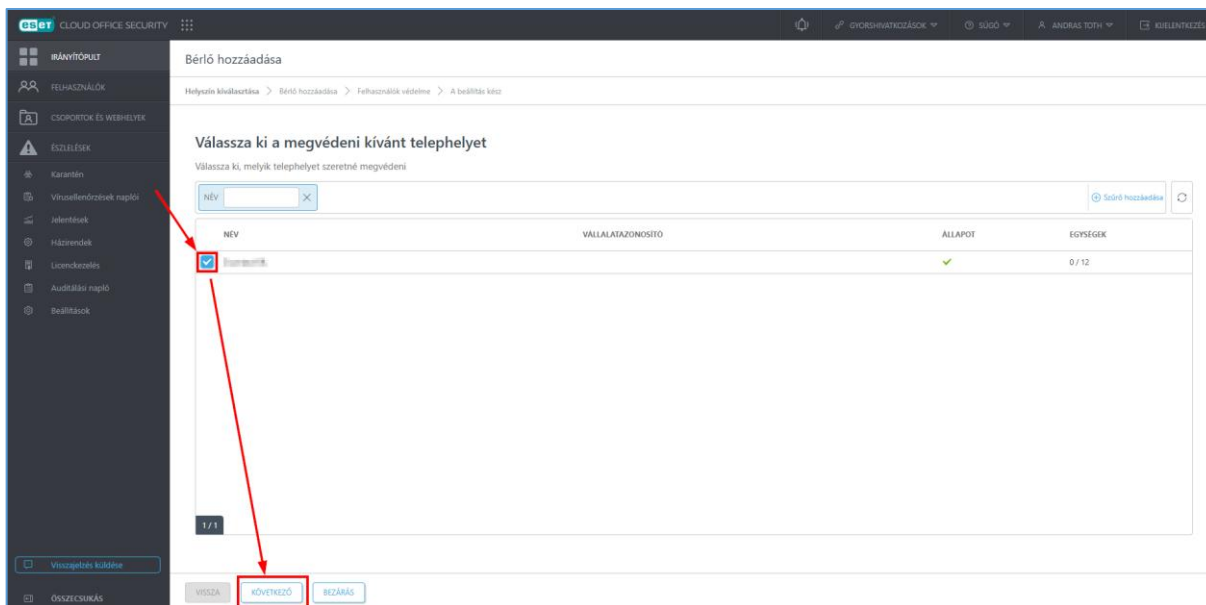
Amennyiben sikerült, szintén bal oldalt kattintson az ESET CLOUD OFFICE SECURITY menüpontra. (Ekkor megnyílik a *.ecos.eset.com weboldal.)

Bérlő hozzáadása

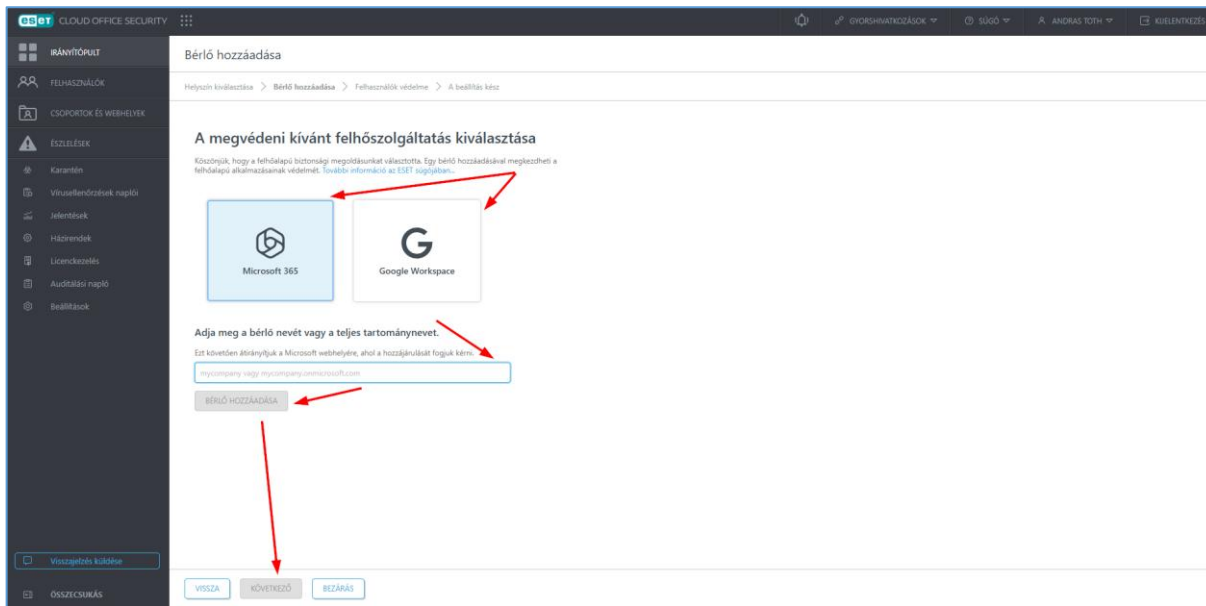
Megjelenő felületen, kérem, kattintson a Bérlő hozzáadása gombra. (Másik lehetőség bal oldalt a beállítások, majd alul a BÉRLŐ HOZZÁADÁSA gomb.)



Válassza ki az ECOS licenct és alul kattintson a KÖVETKŐZŐ gombra.



Válassza ki, a Microsoft 365 vagy a Google Workspace felhőszolgáltatást, adja meg a bérlő nevét/tartománynevet és kattintson a BÉRLŐ HOZZÁADÁSA gombra, majd a következő gombra. (Google Workspace választásakor kérem telepítse a marketplacen található ESET Cloud Office Security-t is.)



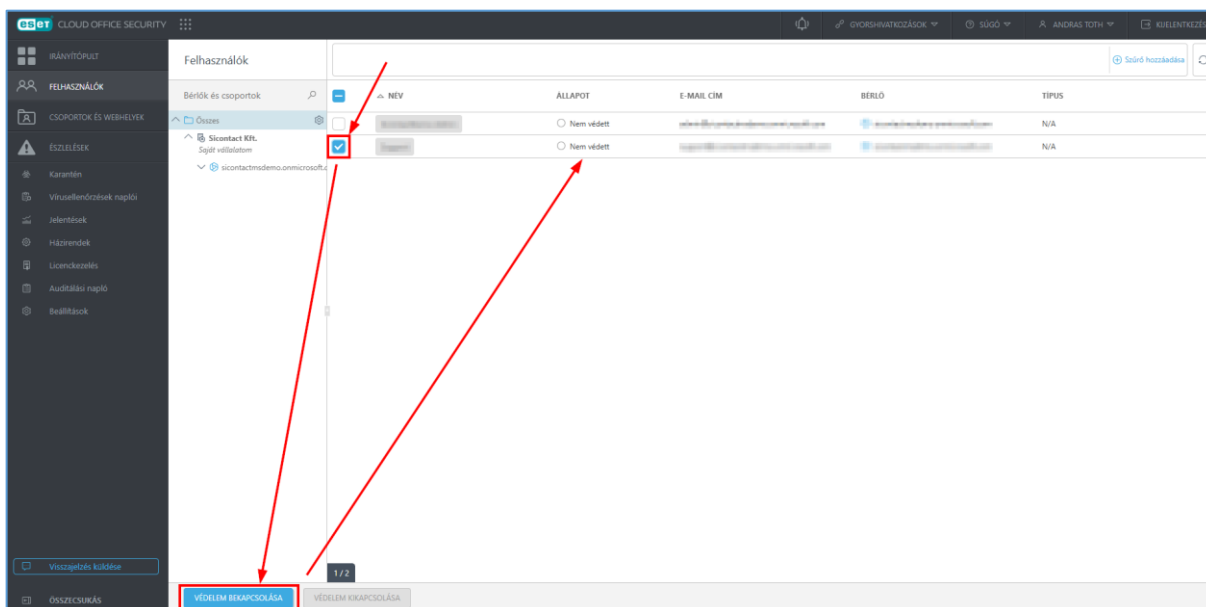
Ezután a rendszer átirányítja a Microsoft/Google weboldalára, kérem, adja meg a kért engedélyeket.

Végül a bérlői beállítás folyamatban üzenet jelenik meg. A rendszer jelzi, ha végzett a beállítással, bezárhatja az ablakot.

Bérlők aktiválása

Bal oldalt a FELHASZNÁLÓK menüpontra kattintva láthatók a felhasználók/csoportok. A jelölőnégyzeteket pipálva (vagy az oszlop tetején egy kattintással akár az összeset megjelölve), majd alul a VÉDELEM BEKACSPOLÁSA gombra kattintva a védelem aktiválható felhasználók/csoportok számára.

Ezután a Nem védett állapotot felváltja a Védett állapot.



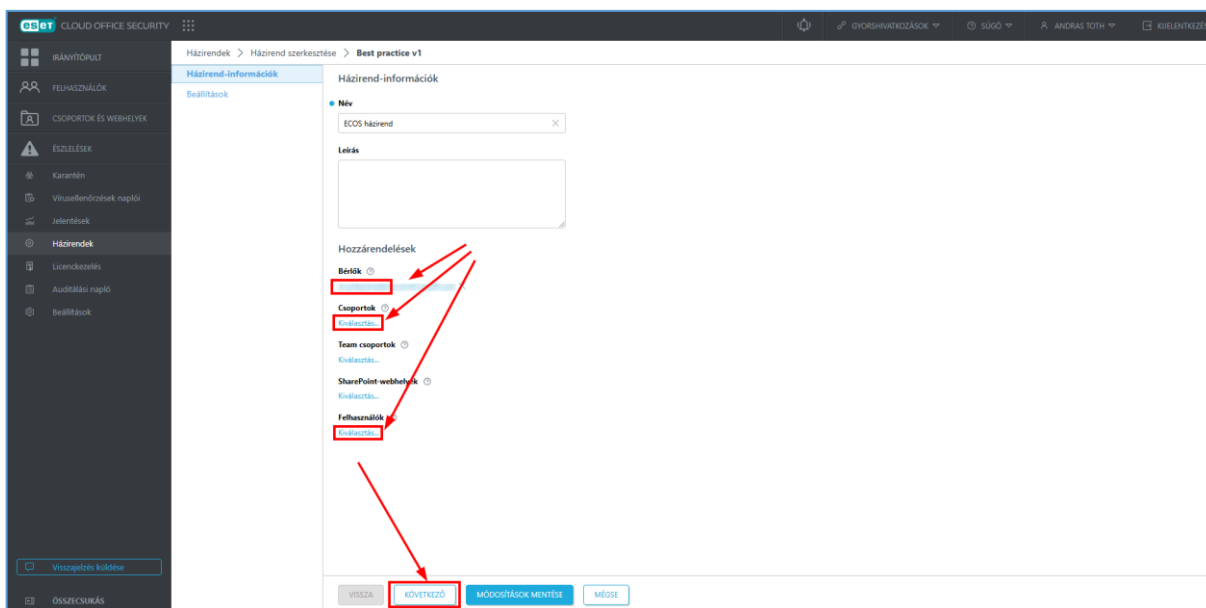
Házirend beállítások

Bal oldalt a Házirendek menüpontban látható az alapértelmezett házirend. Alul az ÚJ HÁZIREND gombra kattintva készíthető személyre szabott házirend.

Házirend-információk:

Elnevezés (és leírása megadása) után, kiválasztható, hogy Bérlőd(ke)t, Csoport(ka)t, Team csoport(ka)t, SharePoint-webhely(eke)t vagy Felhasználó(ka)t szeretnénk védeni. Bérldőket, Csoportokat vagy Felhasználókat javasoljuk a lehetőségek közül.

Alul a KÖVETKEZŐ gombra kattintva tovább léphet a Beállításokra.



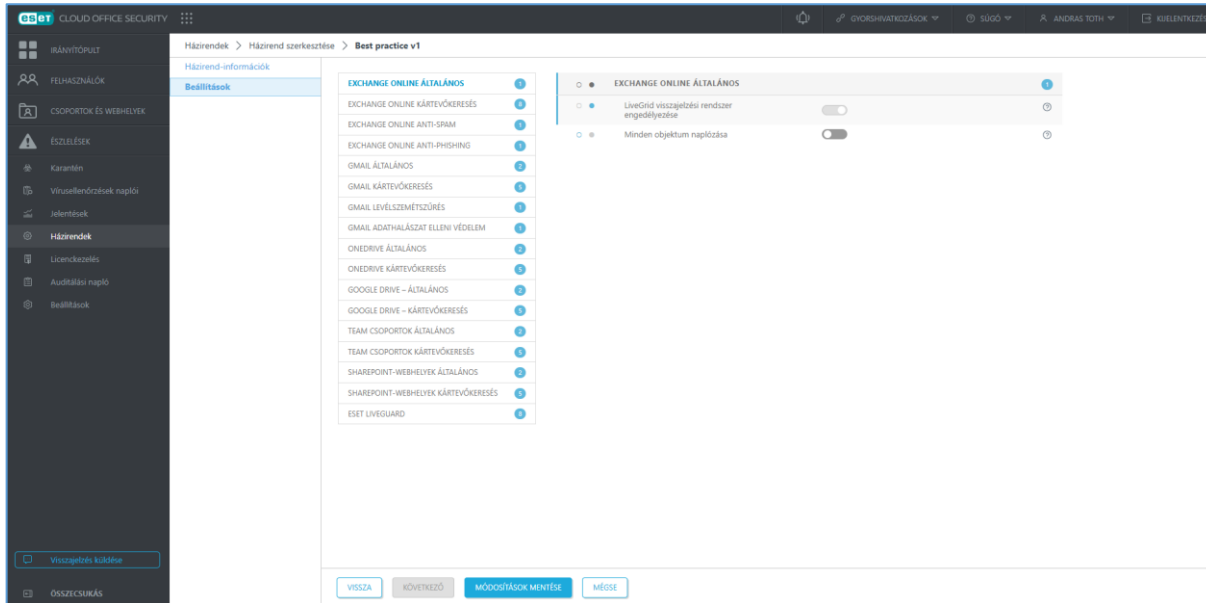
Beállítások:

Bizonyos beállítások több almenüpontban (Exchange, Gmail, OneDrive, Google Drive, Team csoportok, SharePoint, LiveGuard) is megjelennek. Így például, a Minden objektum naplózása kapcsolót érdemes kikapcsolva hagyni minden felhőszolgáltatásnál. Tehát nem csak például Gmail kártevőkeresésnél, hanem az összes többinél is (Exchange, OneDrive...etc.).

Ajánlott beállítások a következők:

Általános:

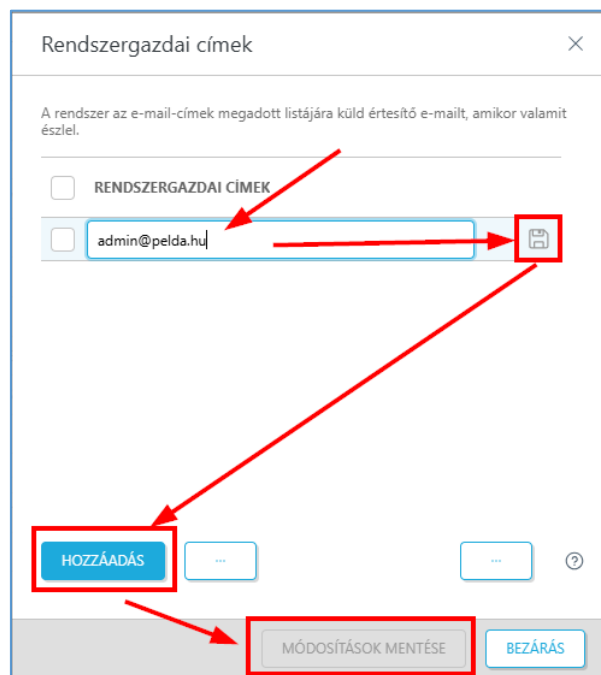
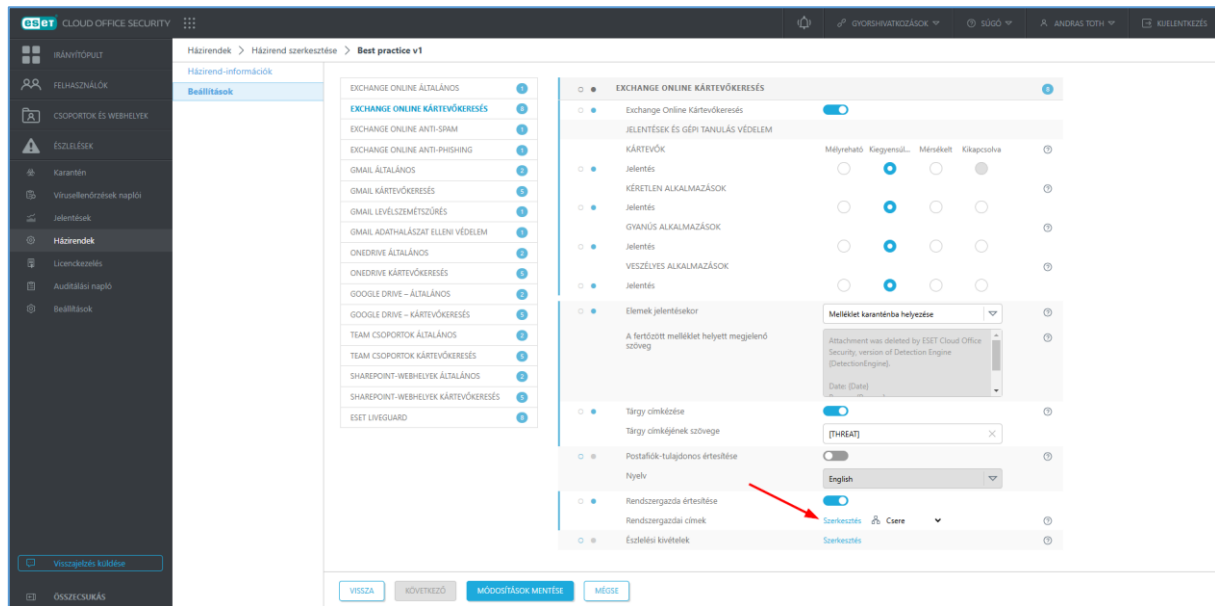
- LiveGrid visszajelzési rendszer engedélyezése → bekapcsolva.
- Minden objektum naplózása → kikapcsolva. (Kizárólag hibaelhárításhoz használt funkció.)



Kártevőkeresés:

- Kártevőkeresés (főmenüpont) → bekapcsolva
- Kártevők, Kéretlen alkalmazások, Gyanús alkalmazások, Veszélyes alkalmazásokat → állítsa Kiegyensúlyozott szintre.
- Elemek jelentésekor → Melléklet karanténba helyezése (emailéknél)/Karantén (a többi felhőszolgáltatásnál). Amennyiben magyar nyelvű üzenetet szeretne megjeleníteni, a Csere lehetőséget válassza, ekkor az alatta lévő Fájlt lecserélő szöveg(mező) szerkeszthető.
- Tulajdonos értesítése → kikapcsolva.
- Rendszergazda értesítése → bekapcsolva. Alatta a Szerkesztés felíratra beállíthatók a rendszergazdai email címek. Hozzáadás, email cím beírása, majd a sor végén mentés (floppy lemez) ikon. További email címeznél szintén hozzáadás, email cím beírása, majd sor végén mentés ikon. Végül módosítások mentése.

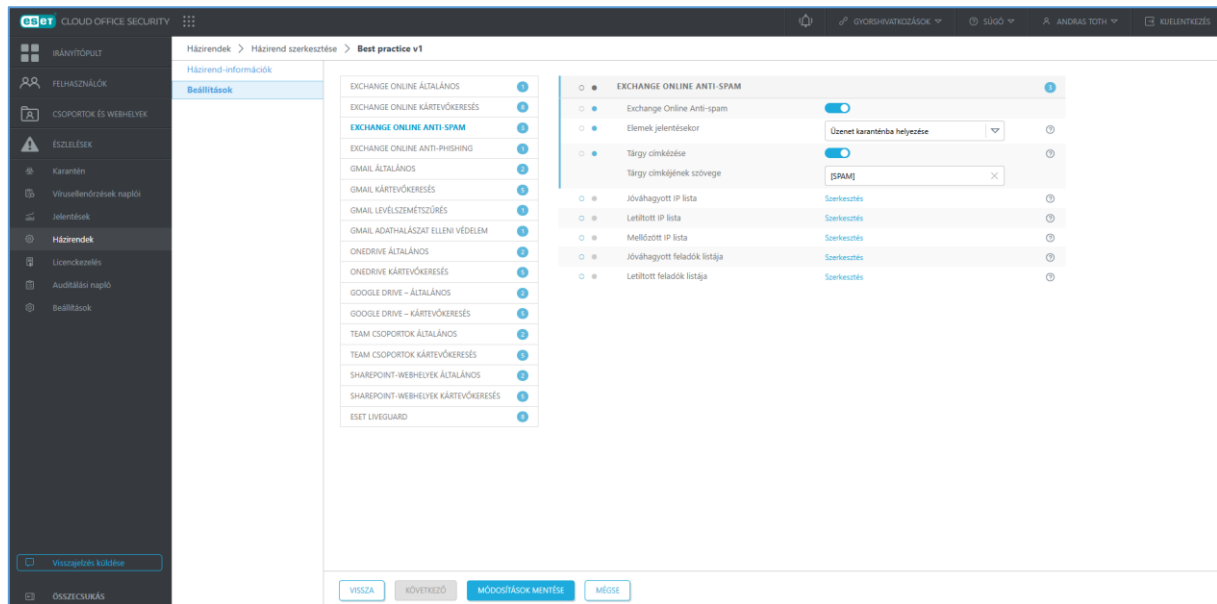
Fontos! Ezek az emailcímek csak a jelenlegi felhőszolgáltatásnál lesznek beállítva, ezért érdemes a rendszergazdai email címeket (jegyzetömbbe) felírni, és onnan másolni a többi felhőszolgáltatás Rendszergazdai címek beállításánál.



- Észlelési kivétele → szükség esetén fájlnev vagy hash alapján hozzáadható.

Anti-spam/levélszemétszűrés beállítások:

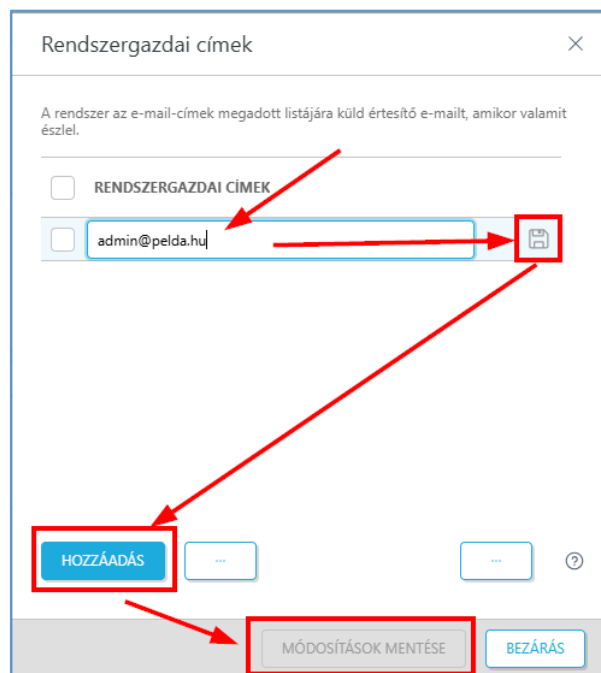
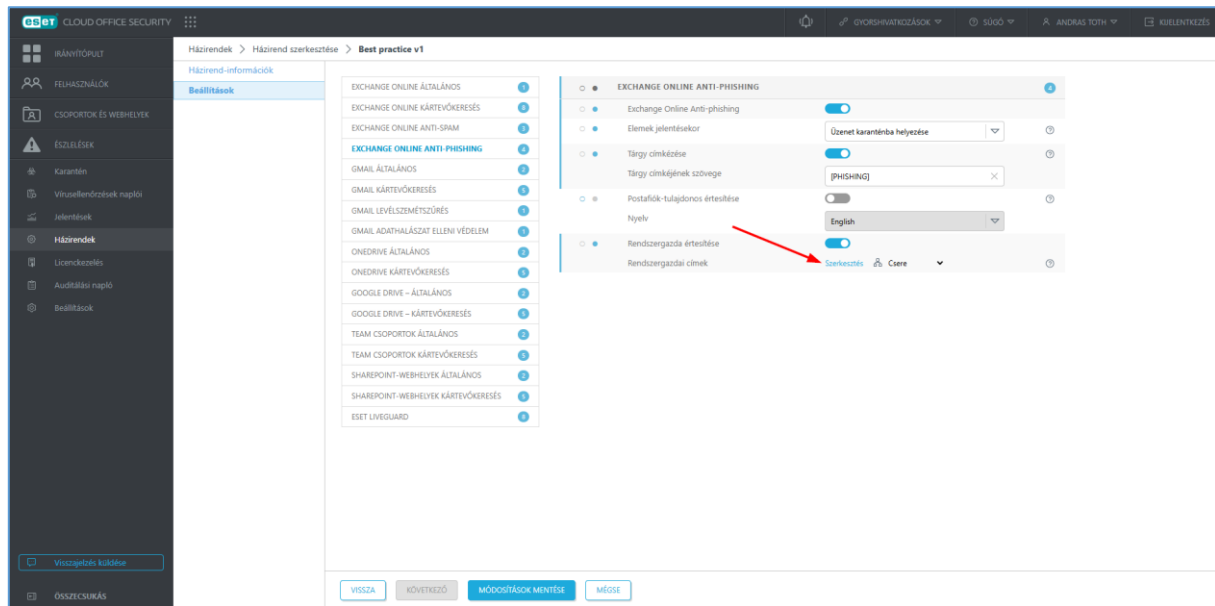
- Anti-spam/levélszemétszűrés → bekapcsolva
- Elemek jelentésekor → Üzenet karanténba helyezése
- Tárgy címkézése → bekapcsolva
- Tárgy címkéjének szövege → [SPAM] címke módosítható tetszés szerint, hogy könnyen felismerhető legyen a rendszergazdák számára.
- IP listák (Jóváhagyott IP lista, Letiltott IP lista, Mellőzött IP lista) és feladók listája (Jóváhagyott feladók listája, Letiltott feladók listája) tetszés szerint módosítható a Szerkesztés feliratra kattintva, majd hozzáadás, szövegmező kitöltése, mentés ikon, módosítások mentése.



Anti-phishing/Adathalászat elleni védelem:

- Anti-phishing/ Adathalászat elleni védelem → bekapcsolva
- Elemek jelentésekor → Üzenet karanténba helyezése
- Tárgy címkézése → bekapcsolva
- Tárgy címkéjének szövege → [SPAM] címke módosítható tetszés szerint, hogy könnyen felismerhető legyen a rendszergazdák számára.
- Postafiók-tulajdonos értesítése → kikapcsolva
- Rendszergazda értesítése → bekapcsolva. Alatta a Szerkesztés feliratra beállíthatók a rendszergazdai email címek. Hozzáadás, email cím beírása, majd a sor végén mentés (floppy) ikon. További email címeknél szintén hozzáadás, email cím beírása, majd sor végén mentés ikon. Végül módosítások mentése.

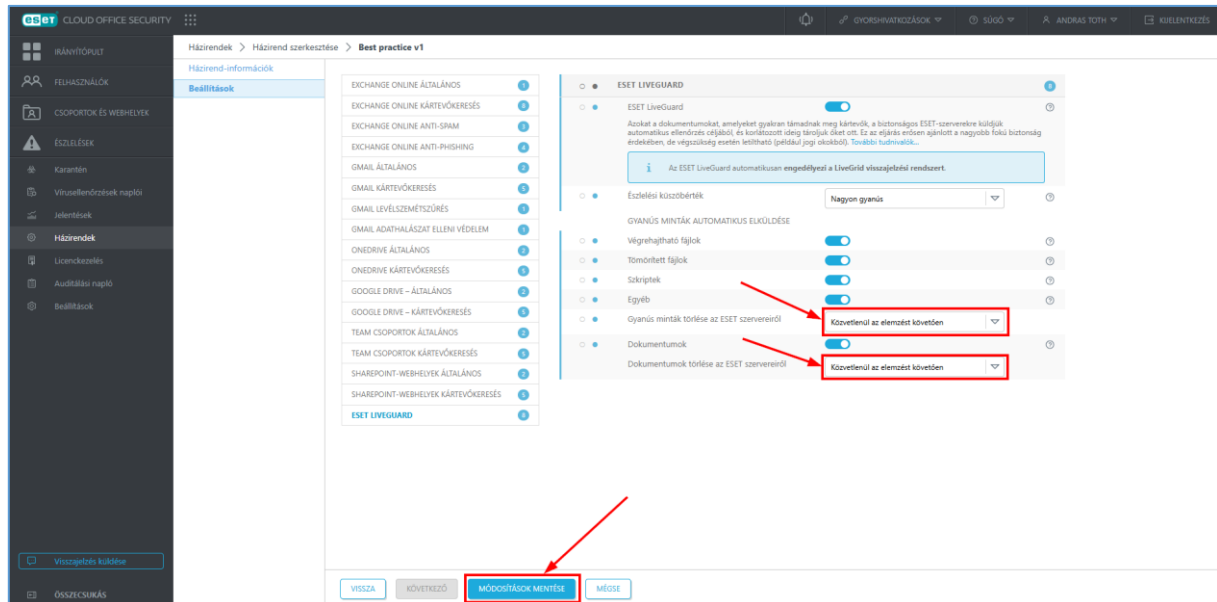
Fontos! Ezek az emailcímek csak a jelenlegi felhőszolgáltatásnál lesznek beállítva, ezért érdemes a rendszergazdai email címeket jegyzetömbbe felírni, és onnan másolni a többi felhőszolgáltatás Rendszergazdai címek beállításánál.



ESET LiveGuard:

- ESET LiveGuard → bekapcsolva
- Észlelési küszöbérték → Nagyon gyanús vagy Kártékony szintre javasolt beállítani.
- Végrehajtható fájlok, Tömörített fájlok, Szekretek, Egyéb → javasolt bekapcsolni, (természetesen állítható tetszés szerint), sor végi kérdőjelek jelzik mely kiterjesztésekre vonatkoznak.
- Gyanús minták törlése az ESET szervereiről → Közvetlenül az elemzést követően. Így jobban megfelelhet az Ön szervezetének előírásainak.
- Dokumentumok → amennyiben bizalmas dokumentumokról van szó(Microsoft Office, PDF fájlok) természetesen kikapcsolható

- Dokumentumok törlése az ESET szervereiről → Közvetlenül az elemzést követően. Így jobban megfelelhet az Ön szervezetének előírásainak és a gyanús dokumentum is ellenőrzésre kerülhet.



Végezetül a **MÓDOSÍTÁSOK MENTÉSE** gombra kattintva mentheti a házirendet.

ESET Inspect

Az ESET kiterjesztett észlelési és elhárítási (EDR/XDR) funkciója lehetővé teszi a megszokottól eltérő viselkedések és biztonsági események gyors és hatékony azonosítását, valamint fejlett kockázatértékelést, incidenskezelést, vizsgálati és kárelhárítási képességeket biztosít. Használatához ESET végpontvédelmi termék megléte szükséges. A szoftver az ESET PROTECT Elite licenccsomag részeként érhető el.

Bővebb információ a következő oldalon olvasható:

<https://www.eset.com/hu/vallalati/megoldasok/kiterjesztett-eszeles-es-elharitas>

Amennyiben bármilyen kérdés felmerül Önben, vagy visszajelzése lenne a segédlettel, termékekkel kapcsolatban, vegye fel a kapcsolatot velünk elérhetőségeink egyikén.

E-mail: support@sicontact.hu

Telefon: +36-1/346-70-48