kaspersky

Kaspersky Endpoint Security 14.1 for Windows

© 2026 AO Kaspersky Lab

Tartalmat

Kaspersky Endpoint Security for Windows súgó
- Újdonságok
- Javított problémák
- Gyakori kérdések

Kaspersky Endpoint Security for Windows
- Az alkalmazási üzemmódjai: Standard, EDR Agent, Light Agent
- Forgalmazási készlet
- Hardveres és szoftveres rendszerkövetelmények
- Az operációs rendszer típusától függően elérhető alkalmazásfunkciók összehasonlítása.
- Az alkalmazásfunkciók összehasonlítása a kezelőeszközök alapján.
- Kompatibilitás más alkalmazásokkal

Az alkalmazás telepítése és eltávolítása
- Üzembe helyezés a Kaspersky Security Centeren keresztül
  - Az alkalmazás normál telepítése
  - Telepítőcsomag létrehozása
  - Az adatbázisok frissítése a telepítőcsomagban
  - Távoli telepítés feladat létrehozása
- Az alkalmazás telepítése helyben, a Varázsló segítségével
- Az alkalmazás távoli telepítése a Rendszerközpont beállításkezelő segítségével
- A setup.ini fájl telepítései beállításainak leírása
- Alkalmazásösszetevők módosítása
- Az alkalmazás korábbi verziójának frissítése
  - Az alkalmazás frissítése újraindítás nélkül
  - Az alkalmazás SMU-frissítése
- Az alkalmazás eltávolítása

Az alkalmazás licencelése
- A végfelhasználói licencszerződésről
- A licenc
- A licenctanúsítványról
- Az előfizetés
- Tudnivalók a licenckulcsról
- Az aktiváló kód
- A kulcsfájl
- Alkalmazások funkcionalitásának összehasonlítása a munkaállomási licenctípustól függően
- Alkalmazások funkcionalitásának összehasonlítása a kiszolgálói licenctípustól függően
- Alkalmazás aktiválása
- Licenckulcs eltávolítása
- A licencadatok megtekintése
- Licenc vásárlása
- Előfizetés megújítása

Első lépések
- Tudnivalók a Kaspersky Endpoint Security for Windows adminisztrációs bővítményről
- Az adminisztrációs bővítmény különböző verzióival való munkavégzés különleges szempontjai

Különleges szempontok a külső szolgáltatásokkal való interakcióhoz használt titkosított protokollok használatakor
Az alkalmazás felülete
Alkalmazásikon a tálca értesítési területén
Egyszerűsített alkalmazásfelület
Az alkalmazás felülete megjelenítésének beállítása
Az alkalmazás használatra való előkészítése
A rendszabályok kezelése
Rendszabály létrehozása
Szabályzat exportálása és importálása
Biztonságiszint-jelző
Feladatkezelés
Helyi alkalmazásbeállítások megadása.
A Kaspersky Endpoint Security elindítása és leállítása
A számítógép védelmének és felügyeletének szüneteltetése és folytatása
Konfigurációs fájl létrehozása és használata
Az alapértelmezett alkalmazásbeállítások visszaállítása
A Kaspersky Endpoint Security teljesítménye és kompatibilitása más alkalmazásokkal
Az energiatakarékos mód be- és kikapcsolása
Erőforrások más alkalmazásoknak történő átadásának engedélyezése és letiltása
Ajánlott eljárások a Kaspersky Endpoint Security teljesítményének optimalizálásához
Kártevő vizsgálata
Számítógép vizsgálata
Cserélhető meghajtók vizsgálata a számítógéphez történő csatlakoztatásukkor
Vizsgálat a háttérben
Vizsgálat a helyi menüből
Alkalmazás integritás-ellenőrzése
A vizsgálat hatókörének szerkesztése
Ütemezett vizsgálat futtatása
Vizsgálat futtatása más felhasználóként
Vizsgálatoptimalizáció
Adatbázisok és alkalmazás-szoftvermodulok frissítése
Adatbázis- és alkalmazásmodul frissítésének lehetőségei
Frissítés a kiszolgáló tárhelyéből
Megosztott mappából való frissítés
Frissítés a Kaspersky Update Utility használatával
Frissítés mobil módban
A frissítési feladatok elindítása és leállítása
Frissítési feladat elindítása másik felhasználói fiók jogosultságaival
Frissítési feladat futásmódjának kiválasztása
Frissítésforrás hozzáadása
Alkalmazásmodulok frissítése
Proxykiszolgáló használata a frissítésekhez
Utolsó frissítés visszagörgetése
Fejlett vírusmentesítő technológia
Aktív fenyegetések vírusmentesítése munkaállomásokon
Az aktív fenyegetések vírusmentesítése a kiszolgálókon
Feldolgozatlan fenyegetések megszüntetése

Számítógépvédelem
Fájl védelem
A Fájl védelem engedélyezése és letiltása
A Fájl védelem automatikus szüneteltetése
A Fájl védelem összetevő által fertőzött fájl észlelésekor elvégzett művelet módosítása
A Fájl védelem összetevő védelmi hatókörének kialakítása
A vizsgálatmódok használata
Vizsgálati technológiák használata a Fájl védelem összetevő működése során
A fájlvizsgálat optimalizálása
Az összetett fájlok vizsgálata
Vizsgálatmód megváltoztatása
Tárolóvizsgálat
Behatolásmegelőző rendszer
A Behatolásmegelőző rendszer be- és kikapcsolása
Az alkalmazások megbízhatósági csoportjainak kezelése
Egy alkalmazás megbízhatósági csoportjának módosítása
A megbízhatósági csoport jogainak konfigurálása
A Kaspersky Endpoint Security előtt indított alkalmazások megbízhatósági csoportjának kiválasztása
Megbízhatósági csoport kiválasztása ismeretlen alkalmazásokhoz
Megbízhatósági csoport kiválasztása digitálisan aláírt alkalmazásokhoz
Alkalmazásjogok kezelése
Operációsrendszer-erőforrások és személyes adatok védelme
Nem használt alkalmazásokra vonatkozó adatok törlése
Behatolásmegelőző rendszer figyelése
A hang- és videórögzítéshez való hozzáférés védelme
BadUSB védelem
BadUSB védelem be- és kikapcsolása
Virtuális billentyűzet használata az USB-eszközök hitelesítésére
Vonalkódolvasó engedélyezése
AMSI védelem
Az AMSI védelem engedélyezése és letiltása
A fájlvizsgálat optimalizálása az AMSI védelemmel
Web védelem
A Web védelem engedélyezése és letiltása
A rosszindulatú webcím-észlelési módszerek konfigurálása
Adathalászat elleni védelem
Megbízható webcímek listájának létrehozása
Megbízható webcímek listájának exportálása és importálása
Levelezés védelem
A Levelezés védelem engedélyezése és letiltása
A fertőzött e-mail üzeneteken végrehajtandó művelet módosítása
A Levelezés védelem összetevő védelmi hatókörének kialakítása
Az e-mail üzenetekhez mellékelt összetett fájlok vizsgálata
E-mail-üzenetek mellékletének szűrése
Mellékletszűrő kiterjesztések exportálása és importálása
E-mailek vizsgálata a Microsoft Office Outlookban
E-mailek vizsgálata a Thunderbird, a MyOffice és az R7-Office alkalmazásban

Hálózati védelem
A Hálózati védelem engedélyezése és letiltása
Támadó számítógép blokkolása
A blokkolásból kizárt címek beállítása
Blokkolásból való kizárások listájának exportálása és importálása
A Hálózati védelem konfigurálása típus szerint
Tűzfal
A Tűzfal be- és kikapcsolása
A hálózati kapcsolat típusának módosítása
A hálózati csomagszabályok kezelése
Hálózati csomagszabály létrehozása
Hálózati csomagszabály be- és kikapcsolása
A Tűzfal műveletének módosítása hálózati csomagszabálynál
Hálózati csomagszabály prioritásának módosítása
Hálózati csomagszabályok exportálása és importálása
Hálózati csomagszabályok definiálása XML-ben
Az alkalmazások hálózati szabályainak kezelése
Alkalmazás hálózati szabályának létrehozása
Alkalmazás hálózati szabályának be- és kikapcsolása
A Tűzfal műveletének módosítása alkalmazás hálózati szabályánál
Alkalmazás hálózati szabálya prioritásának módosítása
Hálózatfigyelő
Biztonsági rések kihasználásának megelőzése
A Biztonsági rések kihasználásának megelőzése összetevő be- és kikapcsolása
Rendszerfolyamatok memóriavédelme
Viselkedésészlelés
Anti-Cryptor
Megosztott mappák külső titkosítás elleni védelmének be- és kikapcsolása
Nem megbízható számítógépek blokkolási időszakának konfigurálása
A védelem hatókörének szerkesztése
Megbízható számítógépek hozzáadása külső adattitkosításhoz
A megosztott mappák külső titkosítással szembeni védelméből származó kizárások listájának exportálása és importálása
Kármentesítő motor
Kaspersky Security Network
A Kaspersky Security Network használatának engedélyezése és letiltása
A Kaspersky Private Security Network korlátozásai
Felhő mód be- és kikapcsolása a védelmi összetevőknél
KSN Proxy beállítások
Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével
Titkosított kapcsolatok vizsgálata
Titkosított kapcsolatok vizsgálatának engedélyezése
Megbízható főtanúsítványok telepítése
Titkosított kapcsolatok vizsgálata nem megbízható tanúsítvánnyal
Kaspersky tanúsítvány hozzáadása a saját tanúsítványtárolóhoz
Titkosított kapcsolatok kizárása a vizsgálat alól
Adatok törlése

Számítógépvezérlés
Webfelügyelő
Webes erőforrás hozzáférési szabályainak megadása
Szűrés webes erőforrás címei szerint
Szűrés webes erőforrás tartalma szerint
A webes erőforrások hozzáférési szabályainak tesztelése
Web Control szabályok exportálása és importálása
A webfelügyelői szabályhoz tartozó webes erőforrás címeinek exportálása és importálása
A felhasználó internetes tevékenységének megfigyelése
A Webfelügyelő üzenetsablonjainak szerkesztése
Webes erőforrások címei maszkjainak használata
Webfelügyelő virtuális gépekhez
Változók a Web Control üzenetsablonjaiban
Eszközfelügyelő
A hozzáférési szabályokról
Az eszközökhöz való hozzáférés kezelése típus szerint
Az eszközökhöz való hozzáférés kezelése csatlakozási busz szerint
A felhasználók eszközökhöz való hozzáférési jogainak differenciálása
A mobileszközökhöz való hozzáférés kezelése
Bluetooth-eszközökhöz való hozzáférés kezelése
Nyomtatás szabályozása
Wi-Fi kapcsolatok szabályozása
Cserélhető meghajtók használatának figyelése
A gyorsítótárazás időtartamának módosítása
Megbízható eszközökkel végzett műveletek
Eszköz felvétele a megbízható listára az alkalmazás kezelőfelületén
Eszköz felvétele a megbízható listára a Kaspersky Security Centerben.
Megbízható eszközök listájának exportálása és importálása
Blokkolt eszközhöz való hozzáférés megszerzése
Online mode a hozzáférés megadásához
Offline mode a hozzáférés megadásához
Az Eszközfelügyelő üzenetsablonjainak szerkesztése
Anti-Bridging
Anti-Bridging engedélyezése
A csatlakozószabály állapotának módosítása
A csatlakozószabály prioritásának módosítása
Adaptív Anomáliafelügyelő
Az Adaptív Anomáliafelügyelő betanítása
Adaptív Anomáliafelügyeleti szabály engedélyezése és letiltása
Az Adaptív Anomáliafelügyeleti szabály kiváltásakor végrehajtott művelet módosítása
Kizárás létrehozása Adaptív Anomáliafelügyeleti szabályhoz
Kizárások exportálása és importálása az Adaptív Anomáliafelügyeleti szabályokhoz
Az Adaptív Anomáliafelügyeleti szabályok frissítéseinek alkalmazása
Adaptív Anomáliafelügyelő üzenetsablonok szerkesztése
Az Adaptív Anomáliafelügyelő műveleteinek figyelése

Alkalmazásfelügyelő
Az Alkalmazásfelügyelő funkciónak korlátozásai
A felhasználói számítógépeken telepített alkalmazásokra vonatkozó információk fogadása
A Blokkolt alkalmazások mód engedélyezése
Alapszámítógépen alapuló Alkalmazásfelügyelő
Alkalmazásfelügyeleti szabályok kezelése
Alkalmazásfelügyeleti szabályt kiváltó feltétel hozzáadása
Futtatható fájlok hozzáadása a Futtatható fájlok mappából az alkalmazáskategóriákba
Eseményhez kapcsolódó végrehajtható fájlok hozzáadása az alkalmazáskategóriához
Alkalmazásfelügyeleti szabály hozzáadása
Az Alkalmazásfelügyeleti szabályok állapotának módosítása a Kaspersky Security Center segítségével
Alkalmazásfelügyeleti szabályok exportálása és importálása
Az Alkalmazásfelügyelő összetevő működéséből eredő események megtekintése
A blokkolt alkalmazásokra vonatkozó jelentés megtekintése
Az Alkalmazásfelügyeleti szabályok tesztelése
Az Alkalmazásfelügyelő szabály tesztelés engedélyezése és letiltása
A teszt módban blokkolt alkalmazások jelentéseinek megtekintése
Az Alkalmazásfelügyelő összetevő tesztműködéséből eredő események megtekintése
Alkalmazástevékenység-figyelő
Fájlok vagy mappák névmaszkjainak létrehozási szabályai
Az Alkalmazásfelügyelő üzenetsablonjainak szerkesztése
Változók az Alkalmazásfelügyeleti üzenetsablonokban
A legjobb gyakorlat az engedélyezett alkalmazások listájának megvalósításához
Engedélyezési lista mód konfigurálása az alkalmazásokhoz
Engedélyezési lista mód tesztelése
Engedélyezési lista mód támogatása
Hálózati portok megfigyelése
Minden hálózati port figyelésének bekapcsolása
A figyelt hálózati portok listájának létrehozása
Azon alkalmazások listájának létrehozása, amelyeknél minden hálózati portot figyelni szeretne
Figyelt portok listájának exportálása és importálása
Naplóvizsgálat
Előre definiált szabályok konfigurálása
Egyéni szabályok hozzáadása
Rendszerintegritás-figyelő
A Rendszerintegritás-figyelő szabályairól
Valós idejű rendszerintegritás-figyelő
Igény szerinti rendszerintegritás-ellenőrzés
Rendszerintegritás-figyelői szabályok exportálása és importálása
A Rendszerintegritás-figyelői jelentések megtekintése
Rendszerintegritási állapot visszaállítása
Cloud Discovery
Megbízható zóna
Kizárás a vizsgálatból létrehozása
Kizárás létrehozása az észlelt objektumok típusa szerint
A megbízható alkalmazások listájának szerkesztése
Helyi megbízható zóna létrehozása

A megbízható zóna exportálása és importálása
Megbízható digitális aláírással rendelkező alkalmazások kezelése
Melléklet. Előre definiált vizsgálati kizárások és megbízható alkalmazások
SQL kiszolgáló
Microsoft Exchange-kiszolgáló
System Center Configuration Manager
Citrix
VMware
A Biztonsági mentés kezelése
A biztonsági mentésben lévő fájlok maximális tárolási idejének beállítása.
A biztonsági mentés maximális méretének megadása
Fájlok visszaállítása a Biztonsági mentésből
Fájlok biztonsági másolatainak törlése a Biztonsági mentésből
Értesítési szolgáltatás
Az eseménynapló beállításainak megadása
Az értesítések megjelenítésének és kézbesítésének beállítása
Az alkalmazás állapotával kapcsolatos figyelmeztetések értesítési területen történő megjelenítésének beállítása
Üzenetek a felhasználók és a rendszergazda között
A jelentések kezelése
Jelentések megtekintése
A jelentés maximális tárolási időtartamának beállítása
A jelentésfájlok maximális méretének beállítása
Jelentés mentése fájlba
Jelentések törlése
A Kaspersky Endpoint Security önvédelme
Az Önvédelem be- és kikapcsolása
Az AM-PPL támogatás engedélyezése és kikapcsolása
Az alkalmazásszolgáltatások külső felügyelettel szembeni védelme
A távoli adminisztrációs alkalmazások támogatása
Jelszóvédelem
Jelszóvédelem engedélyezése
Jogosultságok megadása egyéni felhasználóknak vagy csoportoknak
Ideiglenes jelszó használata a jogosultságok megadásához
Ideiglenes jelszó visszavonása
A Jelszóvédelem jogosultságok speciális szempontjai
A KLAdmin jelszó visszaállítása
Felügyeleti kiszolgálói kapcsolat védelme
Adattitkosítás
A titkosítási funkció korlátozásai
A titkosítási kulcs hosszának módosítása (AES56 / AES256)
Kaspersky lemeztitkosítás
Az SSD-meghajtó titkosításának speciális jellemzői
A Kaspersky lemeztitkosítás indítása
A titkosításból kizárt merevlemezek listájának létrehozása
A titkosításból kizárt merevlemezek listájának exportálása és importálása:
A Single Sign-On (SSO) technológia engedélyezése
A Hitelesítési ügynök fiókok kezelése

Token és okoskártya használata a Hitelesítési ügynökkel
Merevlemez visszafejtése
A hozzáférés visszaállítása Kaspersky lemeztitkosítási technológiával védett meghajtóhoz
Bejelentkezés a hitelesítési ügynöki szolgáltatásfiókkal
Az operációs rendszer frissítése
A titkosítás funkció hibáinak elhárításával kapcsolatos frissítés
A Hitelesítési ügynök felkutatása
Hitelesítési ügynök súgószövegeinek szerkesztése
A Hitelesítési ügynök működésének tesztelése után hátramaradt objektumok és adatok eltávolítása
BitLocker kezelés
BitLocker meghajtótitkosítás indítása
BitLocker által védett merevlemez visszafejtése
A hozzáférés visszaállítása BitLockerrel védett merevlemezhez
A BitLocker védelem szüneteltetése a szoftver frissítéséhez
Fájl szintű titkosítás a számítógép helyi meghajtóin
Fájlok titkosítása a számítógép helyi meghajtóin
A titkosított fájlok hozzáférési szabályainak kialakítása az alkalmazások számára
Adott alkalmazások által létrehozott és módosított fájlok titkosítása
Visszafejtési szabály előállítása
A számítógép helyi meghajtóin lévő fájlok visszafejtése
Titkosított csomagok létrehozása
Titkosított fájlok hozzáférésének helyreállítása
Titkosított adatokhoz való hozzáférés visszaállítása az operációs rendszer hibáját követően
A titkosított fájlokhoz való hozzáférés üzenetsablonjainak szerkesztése
Cserélhető meghajtók titkosítása
Cserélhető meghajtók titkosításának megkezdése
Titkosítási szabály megadása cserélhető meghajtóknál
Cserélhető meghajtók titkosítási szabályait tartalmazó lista exportálása és importálása
Hordozható mód a cserélhető meghajtókon lévő titkosított fájlok eléréséhez
Cserélhető meghajtók visszafejtése
Az adattitkosítási részletek megtekintése
A titkosítási állapot megtekintése
A titkosítási statisztikák megtekintése a Kaspersky Security Center irányítópanelein
A számítógép helyi meghajtóin lévő fájlok titkosítási hibáinak megtekintése
Az adattitkosítási jelentés megtekintése
Munkavégzés titkosított eszközökkel, ha nincs hozzájuk hozzáférés
Az adatok helyreállítása az FDERT visszaállító segédprogrammal
Operációs rendszer helyreállító lemezének létrehozása
Detection and Response-megoldások
MDR és EDR Optimum licencelése
Kompatibilitás harmadik féltől származó EDR-megoldásokkal
Kaspersky Endpoint Agent
A [KES+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra
Szabályzatok és feladatok áttelepítése a Kaspersky Endpoint Agent számára
Endpoint Detection and Response Agent (EDR Agent)
Az EDR Agent telepítése
Az EDR Agent integrálása az MDR megoldással

- Az EDR Agent integrálása a EDR (KATA) megoldással
- Az EDR Agent integrálása a NDR (KATA) megoldással
- EDR Agent integrálása az EDR Expert (on-premises) szolgáltatásba
- Kompatibilitás harmadik féltől származó EPP alkalmazásokkal

Managed Detection and Response

- A beépített ügynök integrációja az MDR megoldással
- KEA-KES migrációs útmutató az MDR számára

Endpoint Detection and Response

- A beépített ügynök integrációja az EDR Optimum / EDR Expert megoldással
- Biztonsági sérülési indikátorok vizsgálata (szabványos feladat)
- Kiterjesztett telemetria az IOC vizsgálathoz
- Fájl áthelyezése a Karanténba
- Fájl lekérése
- Fájl törlése
- Folyamat indítása
- Folyamat megszakítása
- Végrehajtás megelőzése
- Számítógép hálózatelkülönítése
- Cloud Sandbox
- KEA-KES migrációs útmutató az EDR Optimum számára

Kaspersky Sandbox

- A beépített ügynök integrációja a Kaspersky Sandbox megoldással
- Biztonsági sérülési indikátorok vizsgálata (önálló feladat)
- KEA-KES migrációs útmutató a Kaspersky Sandbox számára

Kaspersky Anti Targeted Attack Platform

- A beépített ügynök integrálása az EDR / NDR (KATA) megoldással
- Az EDR (KATA) telemetria konfigurálása
- EDR (KATA)-telemetriai kizárások
  - 1. példa Kizárt folyamatok
  - 2. példa Kizárt hálózati kommunikáció
  - 3. példa Kizárt fájlműveletek
  - 4. példa Kizárt beállításjegyzék-módosítások
- KATA Sandbox
  - A beépített ügynök integrációja a KATA Sandbox megoldással
  - A fenyegetésre adott válasz műveleteinek konfigurálása
- KEA-KES migrációs útmutató az EDR számára (KATA)

Endpoint Detection and Response Expert (on-premises)

- A beépített ügynök integrálása az EDR Expert (on-premises) megoldással
- Az EDR Expert (on-premises) telemetriabeállításainak konfigurálása
- Az EDR Expert (on-premises) telemetriai kizárásai
- Az EDR Expert (on-premises) eseményszűrőinek exportálása és importálása
- Különleges szempontok a rendszabályprofilok használatakor az EDR Expert (on-premises) és az EDR (KATA) integrációjának konfigurálásához

Endpoint Detection and Response Expert (cloud)

- A beépített ügynök integrálása az EDR Expert (cloud) megoldással
- Az EDR Expert (cloud) telemetriabeállításainak konfigurálása

Az EDR Expert (cloud) telemetriai kizárásai
Az EDR Expert (cloud) eseményszűrőinek exportálása és importálása
Karantén kezelése
A karantén maximális méretének konfigurálása
A karanténba helyezett fájlok adatainak küldése a Kaspersky Security Centernek
Fájlok visszaállítása a Karanténból
EDR műveletek figyelése
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
A Kaspersky Endpoint Security integrálása a KUMA-val
A KUMA-nak küldendő szűrési események
KUMA-eseményszűrők exportálása és importálása
Áttérés a KSWS rendszerről KES rendszerre – áttelepítési útmutató
A KSWS és a KES összetevőinek megfeleltetése
A KSWS és a KES beállításainak megfeleltetése
A KSWS-összetevők áttelepítése
A KSWS feladatok és házirendek áttelepítése
A KSWS megbízható zóna áttelepítése
A KSWS Alkalmazások indításvezérlése szabályainak áttelepítése
A KES telepítése a KSWS helyett
A [KSWS+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra
Győződjön meg arról, hogy a Kaspersky Security for Windows Server sikeresen eltávolításra került
A KES aktiválása egy KSWS-kulccsal
Speciális szempontok nagy terhelésű kiszolgálókon történő áttelepítéskor
Az alkalmazás kezelése egy kiszolgálón Server Core mode üzemmódban
A [KSWS+KEA] konfigurációról migrálás a [KES+beépített ügynök] konfigurációra
Light Agent üzemmód a virtuális gépek védelmére
Különleges szempontok a Light Agent üzemmódhoz
A virtuális gép előzetes konfigurálása
Kompatibilitás a Citrix App Layering technológiával
Kompatibilitás a Citrix Provisioning (Citrix Provisioning Services) technológiával
Kompatibilitás a Omnissa App Volumes technológiával
A Light Agent telepítése
A Light Agent csatlakoztatása az SVM-hez
SVM-felderítés
Az SVM kiválasztási algoritmus konfigurálása a Light Agenthez
A Light Agentek SVM-ekhez való kapcsolatainak elosztása (címkék)
A Light Agent és az SVM közötti kapcsolat védelme
A Light Agent aktiválása
A KSVLA Light Agentről KES Light Agentre való áttelepítés útmutatója
A KES Light Agent telepítése a KSVLA Light Agent helyett
A KSVLA Light Agent és a KES Light Agent összetevőinek megfeleltetése
A KSVLA Light Agent-feladatok és -házirendek áttelepítése
A [KSVLA Light Agent+KEA] konfiguráció áttelepítése a [KES Light Agent+beépített ügynök] konfigurációra
Az alkalmazás kezelése a parancssorból
Setup. Az alkalmazás telepítése
Setup /x. Az alkalmazás eltávolítása
msiexec /i. Az alkalmazás visszaállítása

AVP parancsok
- SCAN. Kártevő vizsgálata
- UPDATE. Adatbázisok és alkalmazás-szoftvermodulok frissítése
- ROLLBACK. Utolsó frissítés visszagörgetése
- TRACES. Nyomkövetés
- START. Profil indítása
- STOP. Profil leállítása
- STATUS. Profilállapot
- STATISTICS. Profilműveleti statisztikák
- RESTORE. Fájlok visszaállítása a Biztonsági mentésből
- EXPORT. Alkalmazásbeállítások exportálása
- IMPORT. Alkalmazásbeállítások importálása
- ADDKEY. Kulcsfájl alkalmazása
- LICENSE. Licencelés
- RENEW. Licenc vásárlása
- PBATESTRESET. A lemez ellenőrzési eredményeinek visszaállítása a lemez titkosítása előtt
- EXIT. Kilépés az alkalmazásból
- EXITPOLICY. Szabályzat letiltása
- STARTPOLICY. Szabályzat engedélyezése
- DISABLE. Védelem kikapcsolása
- SPYWARE. Spyware észlelés
- KSN. Váltás a KSN / KPSN között
- SERVERBINDINGDISABLE. A kiszolgálói kapcsolatvédelmem letiltása

KESCLI parancsok
- Scan. Kártevő vizsgálata
- GetScanState. Vizsgálat befejezési állapota
- GetLastScanTime. A vizsgálat befejezési időpontjának meghatározása
- GetThreats. Az észlelt fenyegetésekre vonatkozó adatok beszerzése
- UpdateDefinitions. Adatbázisok és alkalmazás-szoftvermodulok frissítése
- GetDefinitionState. Az adatbázisok legutóbbi frissítési dátumának és időpontjának meghatározása
- EnableRTP. Védelem engedélyezése
- GetRealTimeProtectionState. Fájl védelem állapota
- GetEncryptionState. Lemeztitkosítás állapota
- Version. Az alkalmazás verziójának azonosítása

Detection and Response felügyeleti parancsok
- SANDBOX. A Sandbox kezelése
- PREVENTION. A végrehajtás megakadályozásának kezelése
- ISOLATION. A hálózatelkülönítés kezelése
- RESTORE. Fájlok visszaállítása a Karanténból
- IOCSCAN. Biztonsági sérülési indikátorok (IOC) vizsgálata
- MDRLICENSE. MDR aktiválás
- EDRKATA. Integráció az EDR (KATA) megoldással
- KUMA. Integráció az KUMA-rel
- YARA. YARA-vizsgálat futtatása
- TELEMETRIAI SZŰRŐK. A KUMA-nak küldendő szűrési események

Light Agent felügyeleti parancsok
KSVLAINFO. A Light Agent üzemmód meghatározása
VIISINFO. A Light Agent és az Integrációs kiszolgáló közötti kapcsolat állapota
SVMINFO. A Light Agent és a Védelmi kiszolgáló közötti kapcsolat állapota
Hibakódok
Melléklet. Alkalmazásprofilok
Az alkalmazás kezelése a REST API-n keresztül
Az alkalmazás telepítése a REST API-val
Műveletek az API-val
Az alkalmazással kapcsolatos információforrások
Kapcsolatfelvétel a Terméktámogatással
Nyomkövetési fájlok tartalma és tárolása
Alkalmazás tevékenységének követése
Alkalmazás teljesítményének követése
Memóriakiíratás
Memóriakiíratási fájlok és nyomkövetési fájlok védelme
Operációs rendszer adatainak lekérése (Kaspersky Get System Info)
Korlátozások és figyelmeztetések
Szójegyzék
Adathalász webcímek adatbázisa
Adminisztrációs csoport
Aktív kulcs
Archívum
Cloud Discovery
Feladat
Fertőzhető fájl
Fertőzött fájl
Hitelesítési ügynök
Hordozható fájlkezelő
Integrációs kiszolgáló
IOC
IOC-fájl
Kártékony webcímek adatbázisa
Kerberos hitelesítés
Licenctanúsítvány
Light Agent
Maszk
Network Agent
OLE objektum
OpenIOC
SVM
Tanúsítvány kibocsátója
Téves riasztás
Trusted Platform Module
Védelem hatóköre
Vírusadatbázisok
Vírusmentesítés

Vizsgálat hatóköre
Webes erőforrás címének normalizált formája
Függelékek
1. melléklet Alkalmazásbeállítások
Fájl védelem
Web védelem
Levelezés védelem
Hálózati védelem
Tűzfal
BadUSB védelem
AMSI védelem
Biztonsági rések kihasználásának megelőzése
Viselkedésészlelés
Behatolásmegelőző rendszer
Kármentesítő motor
Kaspersky Security Network
Naplóvizsgálat
Anti-Cryptor
Webfelügyelő
Eszközfelügyelő
Alkalmazásfelügyelő
Adaptív Anomáliafelügyelő
Rendszerintegritás-figyelő
Végponti szenzor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Integráció az KUMA-rel
Teljes lemeztitkosítás
Fájl szintű titkosítás
Cserélhető meghajtók titkosítása
Sablonok (adattitkosítás)
Kizárások
Alkalmazásbeállítások
Jelentések és tároló
Hálózati beállítások
Felület
Beállítások kezelése
Adatbázisok és alkalmazás-szoftvermodulok frissítése
2. melléklet Alkalmazások megbízható csoportjai
3. melléklet Fájlkiterjesztések a cserélhető meghajtók gyors vizsgálatához
4. melléklet A Levelezés védelem mellékletszűrőhöz tartozó fájltípusok
5. melléklet A külső szolgáltatásokkal való interakció hálózati beállításai

6. melléklet Alkalmazás eseményei
Kritikus
Működési hiba
Figyelmeztet
Információs üzenet
7. melléklet Támogatott fájlkiterjesztések a végrehajtás megelőzéséhez
8. melléklet Támogatott szkript értelmezők a végrehajtás megelőzéséhez
9. melléklet IOC vizsgálat hatóköre a rendszerleíró adatbázisban (Registryltem)
10. melléklet IOC-fájl követelményei
Melléklet 11. Az EDR fenyegetésre adott válasz API-ja
Melléklet 12. Felhasználói fiókok az alkalmazásösszetevői szabályokban
Jogi információk
Adatok feletti rendelkezés
Az adatok feletti rendelkezés a Végfelhasználói licencszerződés szerint
Az adatok feletti rendelkezés a Kaspersky Security Network használatakor
Az adatok feletti rendelkezés a Detection and Response-megoldások használatakor
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integráció a Kaspersky Unified Monitoring and Analysis Platform (KUMA) megoldással
Az Európai Unió jogszabályainak való megfelelés (GDPR)
Védjegyekkel kapcsolatos megjegyzések
A harmadik féltől származó kódra vonatkozó információk

Kaspersky Endpoint Security for Windows súgó

Újdonságok

14.1-es frissítés

A Kaspersky Endpoint Security 14.1 for Windows az alábbi funkciókat és továbbfejlesztéseket vezeti be:

1. Megjelent a Windows Server 2025 operációs rendszer támogatása.

2. Az Endpoint Detection and Response Expert (on-premises) és a Kaspersky Endpoint Detection and Response Expert (cloud) esetében a telemetriai események szűrésére vonatkozó szabályok számának korlátozását megemeltük. A Kaspersky Endpoint Security mostantól összesen legfeljebb 10 000 inkluzív és exkluzív szűrőszabályt támogat.

3. Mostantól beállíthatja, hogy a feladatok csak a hét bizonyos napjain, meghatározott heti időközönként fussanak. Az ütemezés a Kaspersky Security Center 16.1 vagy újabb verziójában érhető el.

4. A *Kártevő-ellenőrzés* feladat esetében mostantól megadhat egy időintervallumot, amely alatt a feladat szünetel, például azért, hogy a megnövekedett terhelés idején minimálisra csökkentse a számítógép teljesítményére gyakorolt hatást.

5. A védett számítógépen a merevlemez-alrendszer teljesítményét az I/O-műveletek számának csökkentésével optimalizáltuk.

6. A Kaspersky Endpoint Security ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

14.0-s frissítés

A Kaspersky Endpoint Security 14.0 for Windows az alábbi funkciókat és továbbfejlesztéseket vezeti be:

1. Mostantól támogatottak az ARM-alapú számítógépek. Az alkalmazást normál módban vagy EDR Agent módban is telepítheti. Az alkalmazásnak azonban számos korlátja van (például az adattitkosítási technológiák közül csak a BitLocker támogatott).

2. A kiterjesztett szabályzatellenőrzés a Kaspersky Security Center Web Console 15.0-s vagy újabb verzióiban támogatott. Mostantól megtekintheti a szabályzat módosításait, és mentheti azokat egy fájlba. A *verzió* a felhasználó által mentett módosított paraméterek halmaza. A verziók lehetővé teszik a szabályzati paraméterek módosításainak összehasonlítását és visszaállítását.

3. A Kaspersky Endpoint Detection and Response felhasználói számára új telemetriai események állnak rendelkezésre. Ezek az új funkciók tovább növelik a Kaspersky EDR-megoldások fenyegetésészlelési képességeit.

4. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

12.12 frissítés

A Kaspersky Endpoint Security 12.12 for Windows az alábbi funkciókat és továbbfejlesztéseket vezeti be:

1. A megosztott mappák külső titkosítás elleni védelme, amely korábban a Viselkedéselemzés összetevő részét képezte, ma már külön összetevő: az Anti-Cryptor.

2. Bekerült a Kerberos protokoll támogatása az alkalmazás proxykiszolgálón internet-hozzáféréshez való hitelesítéséhez.

3. Most fájlkivonatot a megbízható alkalmazáshoz, és nem csak a teljes elérési útvonalhoz adhat meg.

4. További *IOC vizsgálat* feladatfunkciók az Endpoint Detection and Response (EDR) megoldások felhasználói számára érhetők el. A Visszamenőleges IOC vizsgálat funkció már elérhető. A *Visszamenőleges IOC vizsgálat* az *IOC vizsgálat* egyik módja, amelyben a Kaspersky Endpoint Security egy bizonyos időszak adatai alapján a sérülésekre utaló jelek után kutat. Ez az üzemmód a számítógép hálózati tevékenységére vonatkozó adatokban a sérülésekre utaló jelek észlelésére szolgál. A Kaspersky Endpoint Security elemzi az operációs rendszer naplóiban és a böngésző naplóiban található adatokat a számítógépen.

5. A Kaspersky Endpoint Detection and Response (EDR) felhasználói eltávolíthatják a karantén méretkorlátját. Erre a YARA vizsgálathoz lehet szükség, mert az alkalmazás nagy memóriakiíratási fájlokat tud menteni. Mostantól a teljes szabad lemezterületét használhatja a karanténhoz.

6. A HTTPS-tömörítés mostantól támogatott az események Kaspersky Unified Monitoring and Analysis Platformra (KUMA) való exportálásának optimalizálása érdekében. Ez segít csökkenteni a kimenő forgalmat.

7. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

12.11-es frissítés

A Kaspersky Endpoint Security 12.11 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Az alkalmazás a beállítások mentése előtt ellenőrzi a felügyeleti összetevők konfigurációját. Az ellenőrzést az Alkalmazásfelügyelő, az Eszközfelügyelő és a Rendszerintegritás-felügyelet összetevőkhöz adtuk hozzá. Az alkalmazás figyelmeztetést jelenít meg, ha a felügyeleti összetevő jelenlegi beállításai növelhetik a számítógép terhelését, vagy rendszerhibákat okozhatnak. Például, ha az Alkalmazásfelügyelő esetében olyan módot választott, amely az engedélyezetteken kívül minden alkalmazást blokkol, és nem adott hozzá egyetlen engedélyezési szabályt sem, az alkalmazás figyelmeztetést jelenít meg, mert az ilyen konfiguráció rendszerhibákat okozhat.

2. Támogatást kapott a KATA Sandboxnak történő automatikus fájlbeküldés felülvizsgálat céljából. A *KATA Sandbox* a Kaspersky Anti Targeted Attack Platform összetevője, amely az operációs rendszerek virtuális lemezképein futtat fájlokat. A Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (a Sandbox-kiszolgálók). A KATA Sandbox automatikus üzemmódú működéséhez a Kaspersky Anti Targeted Attack Platform 8.0 vagy újabb verzióját kell telepíteni.

3. Optimalizált EDR telemetriai küldés. Mostantól megadhatja a csomag maximális hosszát.

4. Továbbfejlesztett kapcsolatdiagnosztika a Kaspersky Security Networkkel. Kibővült a Kaspersky Security Network kapcsolódási hibáinak részletezése a lehetséges problémák megoldása érdekében.

5. Támogatást kapott a Kaspersky Unified Monitoring and Analysis Platform (KUMA) rendszernek küldendő eseménylisták konfigurálása. Mostantól a KUMA előre meghatározott eseménylistáin kívül manuálisan is hozzáadhat eseményeket a telemetriához, vagy kizárhatja az eseményeket az azonosítójuk alapján a Windows Eseménynaplóban.

6. Frissült a házirend kezelőfelülete a Web Console-on. A házirend részek elrendezése módosult az alapvető funkciók gyorsabb elérése érdekében.

7. Windows 11 25H2 támogatás.

8. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

12.10-es frissítés

A Kaspersky Endpoint Security 12.10 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. A BadUSB védelem összetevőhöz hozzáadottuk azt az opciót, hogy a vonalkód-olvasók engedélyezése a képernyőn megjelenő vonalkód beolvasásával is lehetséges legyen. Most már nem kell kódot beírnia a képernyőn megjelenő billentyűzet segítségével a vonalkód-olvasók hitelesítéséhez.

2. Az Endpoint Detection and Response (EDR) megoldások felhasználóinak a következő Kaspersky-funkciók és -fejlesztések állnak rendelkezésre:

   - Mostantól a riasztás részleteiben kezelheti a számítógép hálózatelkülönítését. Ezenkívül a riasztás részleteiben megadhatja a számítógép hálózatelkülönítésének időtartamát, és kivételeket is hozzáadhat.

   - Riasztási adatok új adatokkal történő kitöltése. Mostantól a riasztás részletei több információt tartalmaznak a fenyegetésről, beleértve azt is, hogy az alkalmazás hogyan viselkedik az EDR-fenyegetésekre reagálva.

   - Az IOC-fájlok feldolgozása javult. Mostantól megtekintheti és szerkesztheti az IOC-fájlok tartalmát a Kaspersky Security Center Web Console kezelőfelületén. Az IOC-fájl betöltése után az alkalmazás jelentést jelenít meg az IOC-feltételek alkalmazásáról.

   - Jobb reagálás az észlelt IOC-elemekre. Mostantól az *IOC vizsgálat* feladat által észlelt fájlokat közvetlenül az IOC észlelés eredményeiben, a feladat tulajdonságaiban helyezheti karanténba. A számítógépeket a feladat tulajdonságaiban is elkülönítheti a hálózattól.

   - Mostantól közvetlenül az *IOC vizsgálat* feladat tulajdonságaiban hozhat létre IOC-fájlokat a TXT fájlban generált fájlkivonatok, IP-címek vagy DNS-nevek listája alapján.

   - Kibővített vizsgálati hatókör az *IOC vizsgálat* feladathoz. Mostantól megadhat egy hatókört a beállításjegyzék IOC vizsgálatához (**Windows beállításjegyzék – Registryltem**). Az alkalmazás korábbi verzióiban csak egy előre megadott IOC-vizsgálati hatókört használhatott a beállításjegyzékben.

3. Új Jelszóvédelem engedély hozzáadva, *Beállítások exportálása*. Alapértelmezés szerint csak a KLAdmin felhasználó hozhat létre konfigurációs fájlt a Kaspersky Endpoint Security beállításaival az alkalmazás felületén. Ha hozzáférést szeretne adni más felhasználóknak, meg kell adnia számukra a megfelelő engedélyt.

4. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

12.9. frissítés

A Kaspersky Endpoint Security 12.9 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Új *ideiglenes jelszavakat kezelő* funkció került be az alkalmazásba. Az ideiglenes jelszó lehetővé teszi, hogy biztosítsa a hozzáférést a jelszóvédelemmel rendelkező Kaspersky Endpoint Securityhez egy különálló számítógép számára. Az ideiglenes jelszavak kezelése lehetővé teszi a jelszóelőzmények mentését (legfeljebb 30 nap), az ideiglenes jelszó állapotának figyelését (*Aktív*, *Lejárt*, *Visszavonva*), és az ideiglenes jelszavak visszavonását.

2. Bekerült a Webfelügyelői szabályok által tiltott webes erőforrásokhoz való kapcsolódás azonnali megszakításának lehetősége a házirend alkalmazása után. Az alkalmazás korábbi verzióiban a Webfelügyelő csak a tiltott webes erőforrásokra korlátozta az új kapcsolatokat.

3. A Kaspersky Anti Targeted Attack Platform felhasználói számára lehetőség nyílik a YARA-ellenőrzés helyi számítógépen történő futtatására. Ehhez le kell töltenie egy YARA-szabályokat tartalmazó fájlt, és ki kell adnia a parancsot a parancssorban.

4. Javítottuk az alkalmazás viselkedését, amikor a BitLocker olyan számítógépeken van engedélyezve, amelyeken a meghajtókat már védi a BitLocker harmadik féltől származó eszközökkel. A Kaspersky Endpoint Security elindítja a helyreállítási eljárást, hogy elküldje a helyreállítási kulcsot a Kaspersky Security Centerbe. Így a BitLocker felügyelete átkerül a Kaspersky Security Center konzolra.

5. A Kaspersky Detection and Response megoldások felhasználóinak elérhetővé vált egy új menüpont: **Response history**. Ez a szakasz a számítógépen végrehajtott fenyegetéselhárítási műveletekről tartalmaz információkat. Ilyen művelet lehet például a *Folyamat megszakítása* feladat futtatása vagy a számítógép elkülönítése a hálózattól. A reagálási előzmények csak a következő Kaspersky-megoldások felhasználóinak érhetőek el: MDR, EDR, KATA.

6. Már elérhető a Kaspersky Unified Monitoring and Analysis Platform felhasználói számára az EDR fenyegetésekre való reagálás műveleteinek támogatása. A fenyegetésekre adott válaszok során a KUMA olyan szkripteket futtat, amelyek megfelelő EDR feladatokat hoznak létre. Az EDR-feladatok végrehajtásához létre kell hoznia egy reagálási szabályt az egyéni szkripthez a KUMA-konzolon, és ki kell választania az eseményeket.

7. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

12.8 verziójú frissítés

A Kaspersky Endpoint Security 12.8 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Az alkalmazás mostantól támogatja a Light Agent üzemmódot a virtuális környezetek védelmére. Mostantól az alkalmazást Light Agentként telepítheti a Kaspersky Security for Virtualization Light Agent 6.2 megoldás részeként.

2. A kiszolgálókon lévő Docker-tárolók fájlműveleteinek elfogása mostantól támogatott. A *tároló* egy elszigetelt környezet, amelyben az alkalmazások az operációs rendszerrel való közvetlen interakció nélkül futhatnak. A Kaspersky Endpoint Security megvizsgálja a tárolókban lévő fájlokat, amelyekhez a felhasználó hozzáfér. Ha fenyegetést észlel, az alkalmazások blokkolják ezt a rosszindulatú tevékenységet, és megkísérlik a tárolóban lévő fájl vírusmentesítését. Ha a fájl nem vírusmentesíthető, az alkalmazás leállítja a tárolót.

3. Mostantól megadhat egy védelmi hatókört a megosztott mappák külső titkosítás elleni védelmére (Viselkedéselemzés összetevő). Mostantól megadhatja azokat a megosztott mappákat, amelyekben az alkalmazásnak figyelnie kell a fájltevékenységet. Fájlokat is kizárhat a védelem hatóköréből. Az alkalmazás korábbi verzióiban a Viselkedéselemzés összetevő minden megosztott mappában figyelte a fájltevékenységet.

4. Mostantól a telepítőcsomagban különböző összetevőkészleteket konfigurálhat a különböző operációs rendszerekhez. Ez azt jelenti, hogy ugyanazzal a telepítőcsomaggal telepítheti az alkalmazást munkaállomásokra és kiszolgálókra. A telepítőcsomag tulajdonságai automatikusan kizárják azokat az összetevőket, amelyek egy adott típusú operációs rendszerhez nem állnak rendelkezésre.

5. Az előre meghatározott vizsgálati kizárások és megbízható alkalmazások lehetőség hozzá lett adva. Az előre definiált vizsgálati kizárások és megbízható alkalmazások lehetővé teszik az alkalmazás megbízható zónájának gyors konfigurálását virtuális környezetben (Citrix, VMware). Az ilyen kizárások közé tartoznak például a VHD és VHDX típusú virtuálisgép-fájlok. A kizárások hozzáadhatók az alkalmazás telepítőcsomagjának létrehozásakor, házirend létrehozásakor vagy a Kaspersky Endpoint Security telepítésekor.

6. Az EDR telemetria mostantól tartalmazza az USB-re csatlakoztatott eszközökkel végzett műveletek eseményeit. Ezeket az eseményeket az EDR-telemetria kizárásaihoz is hozzáadhatja.

7. Új lehetőség az elavult TLS 1.0 protokollon keresztüli hálózati kapcsolatok blokkolására. A TLS 1.0 biztonsági szintje alacsony, ezért ajánlott ezt a protokollt letiltani, és az újabb TLS 1.2 vagy TLS 1.3 verziókat használni. Alapértelmezés szerint a Kaspersky Endpoint Security blokkolja a TLS 1.0 kapcsolatokat. Az alkalmazás verziójának frissítése után a TLS 1.0 protokollt használó külső szolgáltatások működése meghiúsulhat. A külső szolgáltatások működésével kapcsolatos problémák elkerülése végett engedélyezheti a TLS 1.0 protokoll használatát a csoportházirendben, mielőtt frissítené az alkalmazás verzióját.

8. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

12.7-es frissítés

A Kaspersky Endpoint Security 12.7 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Mostantól korlátozhatja a processzorerőforrás-felhasználást a *Kártevő vizsgálata* feladatoknál. Ehhez az alkalmazás beállításaiban adja meg az összes processzormag maximális terhelésének százalékos arányát, amelyet a számítógép vizsgálata során használhat.

2. Most már manuálisan is küldhet fájlokat vizsgálatra a KATA Sandboxba. A *KATA Sandbox* a Kaspersky Anti Targeted Attack Platform összetevője, amely az operációs rendszerek virtuális lemezképein futtat fájlokat. A Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (a Sandbox-kiszolgálók). Ha vizsgálatra szeretne elküldeni egy fájlt a KATA Sandboxnak, válassza ki a megfelelő parancsot a fájl helyi menüjében.

3. Mostantól beállíthatja az integrációt a vállalati helyi hálózatot védő *Kaspersky Network Detection and Response* megoldással. A Kaspersky Network Detection and Response (NDR) a Kaspersky Anti Targeted Attack Platform része. Az NDR-rel való interakciót normál üzemmódban és EDR Agent üzemmódban is beállíthatja.

4. A Levelezés védelem bővítmény a Microsoft Office Outlook levelezőprogram 2021-es verziójának támogatásával bővült. A kiterjesztés lehetővé teszi az üzenetek vizsgálatát a levelezőprogram szintjén a protokollszint helyett. Az üzeneteken kívül a kiterjesztés lehetővé teszi a Microsoft Exchange-tárhelyekről a MAPI-felületen keresztül kapott objektumok (például a Naptárban lévő objektumok) vizsgálatát is. Ez a vizsgálat a levelezőprogramban történik.

5. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

12.6-os frissítés

A Kaspersky Endpoint Security 12.6 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Bekerült a Kaspersky SIEM megoldással való integráció - *Kaspersky Unified Monitoring and Analysis Platform; KUMA* - új funkciója. Mostantól lehetőség van arra, hogy a Windows-eseménynaplókból eseményeket küldjön a KUMA-gyűjtőbe. Ez lehetővé teszi a KUMA számára, hogy Windows-eseményeket fogadjon (az eseményazonosítók korlátozott köre támogatott) minden olyan számítógépről, amelyen a Kaspersky Endpoint Security telepítve van, anélkül, hogy KUMA-ügynököket kellene telepíteni ezekre a számítógépekre.

2. Az új *Rendszerintegritás-figyelő* a Fájlintegritás-figyelő összetevőt váltja fel. A Rendszerintegritás-figyelő összetevő a Fájlintegritás-figyelő összes funkcióját tartalmazza, és lehetővé teszi a beállításjegyzék-változások és a külső eszközök csatlakoztatásának figyelését. A Rendszerintegritás-figyelő figyeli az operációs rendszerben bekövetkező olyan változásokat, amelyek a számítógépes biztonság sérülésére utalhatnak. Ilyen változások észlelésekor a Kaspersky Endpoint Security megfelelő eseményeket generál, és figyelmezteti a rendszergazdát. A Fájlintegritás-figyelő már nem része az alkalmazásnak. A Fájlintegritás-figyelő beállításai automatikusan átkerülnek a Rendszerintegritás-figyelőbe az alkalmazás frissítésekor. A Rendszerintegritás-figyelő megfelelő működésének biztosítása érdekében a Kaspersky Endpoint Security alkalmazást és az adminisztrációs bővítményt is frissíteni kell a 12.6-os verzióra.

3. A Kaspersky Security Center konzolon a számítógép tulajdonságaihoz hozzáadtuk a telepített beépített EDR Agent (KATA) állapotát. Ha van beépített EDR Agent (KATA) telepítve, az **Endpoint Sensor állapot** oszlopa jeleníti meg az összetevő aktuális állapotát (pl. *Fut*, *Leállítva*, *Nem támogatja a licenc* stb.).

4. Az előre meghatározott vizsgálati kizárások és megbízható alkalmazások lehetőség hozzá lett adva. Az előre meghatározott vizsgálati kizárások és a megbízható alkalmazások segítenek a megbízható zóna gyors konfigurálásában, amikor az alkalmazást SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és System Center Configuration Manageren használja. Az ilyen kizárások közé tartoznak például az MDF- és LDF-adatbázisfájlok. Kizárások adhatók hozzá új házirend létrehozásakor, egy meglévő házirend módosításakor, vagy a Kaspersky Endpoint Security telepítésekor.

5. A Kaspersky Endpoint Detection and Response Optimum riasztási adatainak megjelenítése a Kaspersky Endpoint Security adminisztrációs bővítményből egy különálló Kaspersky Endpoint Detection and Response adminisztrációs bővítménybe került át. Az EDR felügyeleti bővítmény egyetlen bővítmény a Windows, Mac és Linux operációs rendszereken futó ügynökökkel való munkavégzéshez. Mostantól az EDR Optimummal való munkavégzés során a Kaspersky Endpoint Security adminisztrációs bővítményre van szükség a fenyegetéselhárítási feladatok létrehozásához, valamint az EDR adminisztrációs bővítményre a riasztások részleteinek megtekintéséhez.

6. Windows 11 24H2 támogatás.

7. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

12.5 verziójú frissítés

A Kaspersky Endpoint Security 12.5 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Új lehetőség a telemetriakizárások konfigurálására. A *Telemetria* a védett számítógépen történt események listája. A telemetriai adatokat a Kaspersky Anti Targeted Attack Platform (EDR) a szervezet informatikai infrastruktúrájának felügyeletére és védelmére használja fel. A telemetriakizárások konfigurálása lehetővé teszi a számítógép teljesítményének növelését és az adatátvitel optimalizálását a telemetriagyűjtő kiszolgáló felé.

2. Javult az alkalmazás megbízható zónájának kezelőfelülete. A Kaspersky Endpoint Security mostantól elrejti a felhasználó elől a megbízható zóna objektumait, ha a rendszergazda megtiltotta a felhasználónak, hogy saját (helyi) vizsgálati kizárásokat és megbízható alkalmazásokat adjon hozzá. Ez megakadályozza, hogy egy behatoló illetéktelenül hozzáférjen a megbízható zónához, így növelve a számítógép biztonságának szintjét.

3. Új lehetőség a MyOffice Mail és az R7-Office Organizer levelezőprogramok forgalmának vizsgálatára. A Levelezés védelem összetevő mostantól nem csak az üzenetek mellékleteit vizsgálja letöltéskor, hanem az elküldött és fogadott üzeneteket is.

4. A webes erőforrások kategóriája kiegészült a *Generatív AI-eszközök* elemmel. Az új kategóriában található webhelyekhez való hozzáférést a Web Control segítségével konfigurálhatja.

5. Most már kiválaszthatja a hálózati csomagszabály helyét a Tűzfal listában. A hálózati csomagszabály listán belüli helye határozza meg annak prioritását. Az alkalmazás korábbi verzióiban új szabályt csak a lista végére lehetett hozzáadni, ezután manuálisan kellett mozgatnia a listán a fontossági sorrend megállapításához. Mostantól szabály hozzáadásakor kiválaszthatja, hogy a szabály a lista elejére, a végére vagy a kijelölt szabály mellé kerüljön-e.

6. A Kaspersky Endpoint Security összetevőinek szabályaiban mostantól nemcsak az Active Directoryból, hanem a Kaspersky Security Center felhasználói listájából is kiválaszthatja a felhasználókat. A helyi felhasználói fiókok adatait manuálisan is megadhatja. Ez a lehetőség a következő összetevők szabályaihoz került hozzáadásra: Alkalmazásfelügyelő, Eszközfelügyelő, Webfelügyelő, Adaptív Anomáliafelügyelő és Napló vizsgálata.

7. A hálózati támadásészlelési jelentés most már tartalmaz egy oszlopot a támadó számítógép MAC-címével (a Hálózati védelem összetevő). Mostantól láthatja a jelentésben az IP-címen kívül a támadó számítógép MAC-címét is. Ez hasznos az incidensek kivizsgálása során. A támadó számítógép MAC-címét tartalmazó jelentések a Kaspersky Security Center Linux konzol 15.1-es és újabb verzióin is elérhetők lesznek.

8. Növeltük a számítógép-védelmi követelmények szintjét. A magas védelmi szint mostantól megköveteli az alkalmazásszolgáltatások külső felügyelettel szembeni védelmének engedélyezését. Ellenőrizze a biztonsági szintjelzőt a szabályzati ablak felső részén. Közepes vagy alacsony biztonsági szint esetén a biztonsági szintjelző ajánlóablakában engedélyezheti az alkalmazásszolgáltatásoknak a külső felügyelettel szembeni védelmét.

9. Az objektumészlelés új eseményeinek támogatása, amikor az alkalmazás az Endpoint Detection and Response Agent (EDR Agent) konfigurációban fut. Ezeket az eseményeket a [KES+beépített ügynök] konfiguráció már támogatta.

10. A Kaspersky Endpoint Security for Windows ezen verziójának fejlesztésekor beépítettük a következő privát javítások módosításait: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

12.4-es frissítés

A Kaspersky Endpoint Security 12.4 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Új funkció a számítógép és a Kaspersky Security Center közötti kapcsolat védelmére. Az új *felügyeleti kiszolgálói kapcsolatvédelem* feladat lehetővé teszi jelszó beállítását egy megbízható kiszolgálóhoz való csatlakozáshoz. Ez azt jelenti, hogy a jelszó nélkül nem lehet újra csatlakoztatni a számítógépet és parancsokat futtatni egy másik kiszolgálóról.

2. A Jelszóvédelem összetevőhöz hozzáadták a lehetőséget, hogy a felhasználókat ne csak az Active Directoryból, hanem manuálisan is ki lehessen választani. Ez azt jelenti, hogy manuálisan megadhat egy felhasználónevet és jelszót, valamint hozzáférési jogokat rendelhet a Kaspersky Endpoint Security megoldáshoz ennél a fióknál. Így nem kell megosztania a KLAdmin jelszavát más felhasználókkal, és nem kell új Active Directory fiókokat létrehoznia az alkalmazáshoz való hozzáférés ellenőrzéséhez.

3. Windows 11 23H2 támogatás.

12.3 verziójú frissítés

A Kaspersky Endpoint Security 12.3 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Mostantól telepítheti az alkalmazást az Endpoint Detection and Response Agent konfigurációval. Ez a konfiguráció lehetővé teszi az alkalmazás telepítését a Kaspersky Detection and Response megoldásaihoz szükséges összetevőkkel: Kaspersky Managed Detection and Response és Kaspersky Anti Targeted Attack Platform (EDR). Az alkalmazást ebben a konfigurációban harmadik féltől származó megoldásokkal (például Dr.Web, Dallas Lock, ESET) együtt telepítheti. Ez lehetővé teszi harmadik féltől származó infrastruktúra-biztonsági eszközök használatát a Kaspersky Detection and Response mellett.

2. Továbbfejlesztettük a Kaspersky Endpoint Security működését Bluetooth-eszközökkel. Mostantól konfigurálhatja a kizárásokat, és korlátozhatja a hozzáférést az összes Bluetooth-eszközhöz, kivéve a beviteli eszközöket (vezeték nélküli billentyűzetek, egerek stb.).

3. Optimalizáltuk az Alkalmazásfelügyelő összetevő futtatható fájlok adatbázisával való működését. A Kaspersky Endpoint Security mostantól automatikusan eltávolítja a fájladatokat az adatbázisból, ha a fájlt törlik a számítógépről. Ez lehetővé teszi az adatbázis naprakészen tartását és a Kaspersky Security Center erőforrásainak kímélését.

4. Növeltük a számítógép-védelmi követelmények szintjét. A magas védelmi szint most megköveteli a Jelszóvédelem engedélyezését. Ellenőrizze a biztonsági szintjelzőt a szabályzati ablak felső részén. Közepes vagy alacsony biztonsági szint esetén a biztonsági szintjelző ajánlóablakában engedélyezheti a Jelszóvédelem funkciót.

5. HTTPS protokolltámogatás az alkalmazás Kaspersky Security Networkkel együttműködése céljából. Engedélyezze a HTTPS használatát a KSN proxykiszolgálói beállítások Felügyeleti kiszolgáló tulajdonságaiban.

12.2 verziójú frissítés

A Kaspersky Endpoint Security 12.2 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. A WPA3 protokoll támogatása hozzáadásra került a Wi-Fi hálózatokhoz való kapcsolódás szabályozása céljából (Eszközfelügyelő). Mostantól kiválaszthatja a WPA3 protokollt a megbízható Wi-Fi hálózati beállításokban, és megtagadhatja a hálózathoz való csatlakozást egy kevésbé biztonságos protokoll használatával.

2. Mostantól kiválaszthat egy protokollt és portokat a Hálózati védelem kizárásaihoz. Mostantól a megbízható eszközök IP-címének megadása mellett portot és protokollt is kiválaszthat. Ezzel kizárhatja az egyes adatfolyamokat, és megakadályozhatja a megbízható IP-címekről érkező hálózati támadásokat.

3. Helyi frissítésforrások eltérő sorrendje a helyi *Adatbázisok és alkalmazásmodulok frissítése feladatnál*, ha házirend vonatkozik a számítógépre. A Kaspersky Security Center kiszolgálója mostantól alapértelmezés szerint a Kaspersky-kiszolgálók helyett van használatban első frissítésforrásként. Ez segít az adatforgalom csökkentésében, amikor a felhasználó a helyi *Adatbázisok és alkalmazásmodulok frissítése* feladatot futtatja.

12.1 verziójú frissítés

A Kaspersky Endpoint Security 12.1 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Beépített ügynök a Kaspersky Anti Targeted Attack Platform megoldáshoz. A Kaspersky Endpoint Agent használatához már nincs szükség a EDR (KATA) megoldásra. A Kaspersky Endpoint Agent minden funkcióját a Kaspersky Endpoint Security végzi. A Kaspersky Endpoint Agent házirendjeinek áttelepítéséhez használja az áttelepítési varázslót. Az alkalmazás frissítése után a Kaspersky Endpoint Security átvált a beépített ügynök használatára, és eltávolítja a Kaspersky Endpoint Agent megoldást. A Kaspersky Endpoint Agent felkerült az inkompatibilis szoftverek listájára. A Kaspersky Endpoint Security beépített ügynökökkel rendelkezik az összes Detection and Response megoldáshoz, ezért a Kaspersky Endpoint Agent telepítése az ezen megoldásokkal való integrációhoz már nem szükséges.

2. Mostantól támogatott az Azure WVD-kompatibilitási mód. Ez a funkció biztosítja az Azure virtuális gép állapotának megfelelő megjelenítését a Kaspersky Anti Targeted Attack Platform konzolon. Az Azure WVD-kompatibilitási mód lehetővé teszi állandó egyedi érzékelőazonosító hozzárendelését ezekhez a virtuális gépekhez.

3. Mostantól konfigurálhatja a felhasználói hozzáférést a mobileszközökhöz az iTunes vagy hasonló alkalmazásokban. Vagyis például engedélyezheti, hogy a mobileszközt csak az iTunes-ban használják, és letilthatja a mobileszköz cserélhető meghajtóként való használatát. Az alkalmazás támogatja ezeket a szabályokat az Android Debug Bridge (ADB) alkalmazás esetében is.

4. A Kaspersky Security Center 11-es verziója többé nem támogatott. Frissítse a Kaspersky Endpoint Security alkalmazást a legújabb verzióra.

Javított problémák

Az alábbi táblázat felsorolja a Kaspersky Endpoint Security korábbi verzióiban feltárt és a jelenlegi verzióban kijavított összes hibát.

A 14.1-es verzióban javított problémák listája

Probléma azonosítója	A probléma leírása
10140523	A natív NVMe engedélyezése a Windows 11 rendszeren az alkalmazások instabil működéséhez vezethet.
9340076	Azokon az eszközökön, amelyeken az alkalmazás telepítve van és a Fájltitkosítás összetevő engedélyezve van, a Windows Intéző nem frissíti automatikusan a hálózati mappa tartalmát, ha azt egy másik eszközről módosítják.
9722863	Az Eszközfelügyelő jelentése nem tartalmazza az USB-token leválasztási eseményét.
10006481	A bejövő forgalmat megtagadó szabály alkalmazása után a külső szolgáltatásokkal fenntartott aktív TCP-kapcsolatok idő előtt megszakadhatnak az időtúllépés helytelen számítása miatt.
10140912	Az alkalmazás nem észleli a BHT1100B PDA eszközt.

Probléma azonosítója	A probléma leírása
10157563	Előfordulhat, hogy a Folder Redirection nem működik VDI munkaállomásokon újraindítás után.
10158494	Az Eszközfelügyelő naplózza a cserélhető eszköz többszöri csatlakoztatását és leválasztását anélkül, hogy az eszközt fizikailag újra csatlakoztatnák.

Gyakori kérdések

ÁLTALÁNOS

Milyen számítógépeken működik a Kaspersky Endpoint Security?

Mik változtak a legutóbbi verzió óta?

Melyik más Kaspersky alkalmazással tud a Kaspersky Endpoint Security működni?

Hogyan tudok spórolni a számítógépes erőforrásokkal a Kaspersky Endpoint Security használata során?

ÜZEMBEHELYEZÉS

Hogyan telepíthetem a Kaspersky Endpoint Security alkalmazást a szervezet összes számítógépére?

Milyen telepítési beállítások adhatók meg a parancssorban?

Hogyan tudom távolról eltávolítani a Kaspersky Endpoint Security alkalmazást?

FRISSÍTÉS

Milyen módszerek szolgálnak az adatbázisok frissítésére?

Mit tegyek, ha a probléma a frissítés után is fennáll?

Hogyan frissíthetek adatbázisokat a vállalati hálózaton kívül?

Használhatok proxykiszolgálót a frissítésekhez?

BIZTONSÁG

A Kaspersky Endpoint Security hogyan vizsgál e-maileket?

Hogyan zárhatok ki egy megbízható fájlt a vizsgálat alól?

Hogyan védhetem meg a számítógépem a pendrive-okról érkező vírusok ellen?

Hogyan futtathatom a rosszindulatú programok vizsgálatát úgy, hogy rejtve legyen a felhasználó elől?

Hogyan kapcsolom ki átmenetileg a Kaspersky Endpoint Security védelmet?

Hogyan állíthatok vissza egy fájlt, amit a Kaspersky Endpoint Security tévedésből törölt?

Hogyan akadályozhatom meg, hogy egy felhasználó törölje a Kaspersky Endpoint Security alkalmazást?

INTERNET

A Kaspersky Endpoint Security vizsgál titkosított kapcsolatokat (HTTPS)?

Hogyan engedélyezem a felhasználóknak, hogy csak megbízható Wi-Fi hálózatokhoz csatlakozzanak?

Hogyan blokkolhatok közösségi hálózatokat?

ALKALMAZÁSOK

Hogyan tudom meg, hogy melyik alkalmazások vannak telepítve a felhasználó számítógépére (leltár)?

Hogyan akadályozom meg, hogy fussanak a számítógépes játékok?

Hogyan hitelesíthetem, hogy az Alkalmazásfelügyelő megfelelően lett beállítva?

Hogyan adhatok hozzá alkalmazást a megbízható listához?

ESZKÖZÖK

Hogyan blokkolhatom a pendrive-ok használatát?

Hogyan adhatok hozzá eszközt a megbízható listához?

Lehetséges-e a blokkolt eszközhöz való hozzáférés megszerzése?

TITKOSÍTÁS

Milyen feltételek esetén nem lehetséges a titkosítás?

Hogyan használhatok jelszót arra, hogy korlátozzam egy archívum elérését?

Lehetséges okoskártyákat és tokeneket használni a titkosításra?

Hozzá lehet férni a titkosított adatokhoz, ha nincs kapcsolat a Kaspersky Security Centerrel?

Mit tegyek, ha a számítógépem operációs rendszere hibás, de az adat titkosítva marad?

TÁMOGATÁS

Hol van tárolva a jelentésfájl?

Hogyan hozhatok létre nyomkövetési fájlt?

Hogyan engedélyezhetem a kiíratást?

Kaspersky Endpoint Security for Windows

A Kaspersky Endpoint Security for Windows (továbbiakban Kaspersky Endpoint Security) átfogó számítógépvédelmet biztosít a már ismert és új fenyegetések, valamint a hálózati és adathalász támadások ellen.

Az alkalmazás nem használható olyan technológiai folyamatokban, amelyek automatizált vezérlőrendszereket tartalmaznak. Az ilyen rendszereken lévő eszközök védelméhez a Kaspersky Industrial CyberSecurity for Nodes alkalmazás használata javasolt.

Fenyegetésészlelő technológiák



Gépi tanulás

A Kaspersky Endpoint Security egy gépi tanuláson alapuló modellt használ. A modellt a Kaspersky szakértői fejlesztették ki. A későbbiekben a modell folyamatosan kapni fogja a KSN-től származó fenyegetési adatokat (modell tanítása).



Felhő alapú vizsgálat

A Kaspersky Endpoint Security fenyegetési adatokat kap a Kaspersky Security Networktől. A *Kaspersky Security Network (KSN)* felhőalapú szolgáltatások egy olyan infrastruktúrája, amely hozzáférést nyújt a Kaspersky online tudásbázisához, ahonnan információkat kaphat fájlok, webes erőforrások és szoftverek megbízhatóságáról.



Szakértői elemzés

A Kaspersky Endpoint Security a Kaspersky víruselemzői által hozzáadott fenyegetési adatokat használja. A víruselemzők értékelik az objektumokat, ha azok megbízhatósága nem határozható meg automatikusan.



Viselkedéselemzés

A Kaspersky Endpoint Security valós időben elemzi az objektumok tevékenységét.



Automatikus elemzés

A Kaspersky Endpoint Security adatokat kap az automatikus objektumelemző rendszertől. A rendszer feldolgozza a Kaspersky-nek küldött összes objektumot. A rendszer ezután meghatározza az objektum megbízhatóságát, és hozzáadja az adatokat a vírusadatbázisokhoz. Ha a rendszer nem tudja meghatározni az objektum megbízhatóságát, a rendszer lekéri a Kaspersky víruselemzőinek véleményét.



Sandbox

A Kaspersky Endpoint Security virtuális gépen dolgozza fel az objektumot. A Kaspersky Sandbox elemzi az objektum viselkedését, és dönt annak megbízhatóságáról. Ez a technológia csak akkor érhető el, ha Ön használja a Kaspersky Sandbox megoldást.



Cloud Sandbox

A Kaspersky Endpoint Security a Kaspersky által biztosított elszigetelt környezetben vizsgálja az objektumokat. A Cloud Sandbox technológia folyamatosan engedélyezve van és minden Kaspersky Security Network felhasználó számára elérhető, függetlenül attól, milyen típusú licencet használnak. Ha már telepítette az Endpoint Detection and Response megoldást, engedélyezhet egy külön számlálót a Cloud Sandbox által észlelt fenyegetésekhez.

Összetevők kiválasztása

Minden fenyegetéstípust egy külön összetevő kezel. Az összetevők függetlenül engedélyezhetők, letilthatók és a beállításaik konfigurálhatók.

Rész	Összetevő
Fenyegetések elleni alapvető védelem 	**Fájl védelem** A Fájl védelem összetevő lehetővé teszi a számítógép fájlrendszerében a fertőzések megelőzését. Alapértelmezés szerint a Fájl védelem összetevő állandóan a számítógép RAM-jában található, és valós időben vizsgálja az összes megnyitott, mentett és futtatott fájlt. Ez az összetevő megvizsgálja a számítógép összes meghajtóján lévő fájlokat, beleértve a csatlakoztatott meghajtókat is. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek. **Web védelem** A Web védelem összetevő megelőzi, hogy rosszindulatú fájlok legyenek letöltve az internetről, valamint blokkolja a rosszindulatú és az adathalász weboldalakat. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek. **Levelezés védelem** A „Levelezés védelem” összetevő a bejövő és kimenő e-mail üzenetek mellékleteiben vizsgálja a vírusok és egyéb fenyegetések jelenlétét. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek. A Levelezés védelem a bejövő és a kimenő üzeneteket is képes megvizsgálni. Az alkalmazás támogatja a POP3, SMTP, IMAP és NNTP protokollokat a következő levelezőprogramokban: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer A Mozilla Thunderbird, MyOffice Mail és R7-Office Organizer levelezőprogramok forgalmának vizsgálatához hozzá kell adnia a Kaspersky tanúsítványt a tanúsítványtárolóhoz, és ki kell választania a saját tanúsítványtárolót. A Levelezés védelem nem támogat más protokollokat és levelezőprogramokat. A Levelezés védelem nem mindig képes *protokollszintű* hozzáférést biztosítani az üzenetekhez (például a Microsoft Exchange megoldás használata esetén). Emiatt a Levelezés védelem tartalmaz egy bővítményt a Microsoft Office Outlookhoz. A bővítmény lehetővé teszi az üzenetek vizsgálatát a *levelezőprogram szintjén*. A Levelezés védelem bővítmény az Outlook 2010, 2013, 2016, 2019, 2021, 2024 és 365 32 bites és 64 bites verzióit támogatja. Az ARM-alapú számítógépeken a Levelezés védelem bővítmény az Outlook 2016, az Outlook 2021, az Outlook 2024 és az Outlook 365 for Arm64 32 bites és 64 bites verzióit támogatja. **Hálózati védelem** A *Hálózati védelem* összetevő (más néven Intrusion Detection System, IDS) figyeli a bejövő hálózati forgalmat a hálózati támadásokra jellemző tevékenységek szempontjából. Ha az alkalmazás hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában. Az alkalmazás-adatbázisok tartalmazzák a már ismert hálózati támadások típusainak és az elhárításuk módszereinek leírását. A Hálózati védelem összetevő által észlelhető hálózati támadások listája az alkalmazás adatbázisainak és alkalmazásmoduljainak frissítésekor frissül. **Tűzfal** A Tűzfal blokkolja a jogosulatlan kapcsolódási kísérleteket a számítógépen az interneten vagy a helyi hálózaton végzett munka során. A Tűzfal felügyeli a számítógépen futó alkalmazások hálózati tevékenységét is. Ez lehetővé teszi, hogy védje a vállalat helyi hálózatát a személyes adatok ellopásával és más támadásokkal szemben. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és előre definiált *hálózati szabályok*. segítségével biztosít védelmet a számítógépnek. **BadUSB védelem** A BadUSB védelem összetevő megakadályozza azt, hogy a billentyűzetet emuláló fertőzött USB eszközök a számítógéphez csatlakozzanak. **AMSI védelem** Az AMSI védelmi összetevő a Microsoft által az Antimalware Scan Interface számára nyújtott támogatás. Az *Antimalware Scan Interface (AMSI)* engedélyezi a harmadik féltől származó, AMSI támogatással rendelkező alkalmazásoknak, hogy objektumokat küldjenek (például PowerShell szkripteket) a Kaspersky Endpoint Security számára további vizsgálat érdekében, valamint azt, hogy vizsgálati eredményeket kapjanak ezen objektumokról.

Rész	Összetevő
Fenyegetések elleni fejlett védelem 	**Kaspersky Security Network** A *Kaspersky Security Network (KSN)* felhőalapú szolgáltatások egy olyan infrastruktúrája, amely hozzáférést nyújt a Kaspersky online tudásbázisához, ahonnan információkat kaphat fájlok, webes erőforrások és szoftverek megbízhatóságáról. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban reagál az új típusú fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken. Ha tagja a Kaspersky Security Networknek, a KSN szolgáltatások a Kaspersky Endpoint Security számára információkat nyújtanak a vizsgált webcímek megbízhatóságáról, valamint a vizsgált fájlok kategóriájáról és megbízhatóságáról. **Viselkedésészlelés** A Viselkedésészlelés összetevő a számítógépen futó alkalmazások műveleteiről fogad adatokat, és a teljesítmény növelése érdekében átadja ezeket az információkat a többi védelmem összetevőinek. A Viselkedésészlelés összetevő Viselkedésfolyam-aláírásokat (BSS) alkalmaz az alkalmazásokhoz. Ha egy alkalmazás aktivitása megegyezik egy viselkedésfolyam-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet. A Kaspersky Endpoint Security funkciói viselkedésfolyam-aláíráson alapulnak, és a számítógép számára proaktív védelmet nyújtanak. A Viselkedésészlelés összetevő emellett a hálózati portokat is figyeli az olyan alkalmazások folyamatait illetően, amelyek veszélyt jelenthetnek a számítógép biztonságára nézve. Az alkalmazás vírusadatbázisok segítségével szerez információt az ilyen folyamatokról. **Anti-Cryptor** Az Anti-Cryptor összetevő a megosztott mappákban végzett tevékenységeket elemzi. Ha ez a tevékenység megegyezik a külső titkosításra jellemző viselkedésfolyamat-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet. **Biztonsági rések kihasználásának megelőzése** A Biztonsági rések kihasználásának megelőzése összetevő észleli azon programkódokat, amik a számítógép sebezhetőségeinek segítségével kihasználják a rendszergazda jogait vagy rosszindulatú tevékenységeket hajtanak végre. Például, ezek a kihasználások puffertúlcsordulást eredményezhetnek. Ennek eléréséhez a kihasználás nagy mennyiségű adatot küld a sebezhető alkalmazásnak. Az adatok feldolgozásakor a sebezhető alkalmazás végrehajtja a rosszindulatú kódot. A támadás eredményeképp a kihasználás engedély nélkül indíthatja el a rosszindulatú program telepítését. Ha a Kaspersky Endpoint Security egy sebezhető alkalmazásból származó végrehajtható fájl futtatására irányuló olyan kísérletet észlel, amelyet nem a felhasználó végzett el, akkor blokkolja a fájl indítását vagy értesíti a felhasználót. A Biztonsági rések kihasználásának megelőzése összetevő emellett a hálózati portokat is figyeli az olyan alkalmazások folyamatai után, amelyek veszélyt jelenthetnek a számítógép biztonságára. Az alkalmazás vírusadatbázisok segítségével szerez információt az ilyen folyamatokról. **Behatolásmegelőző rendszer** A Behatolásmegelőző rendszer összetevő megelőzi, hogy az alkalmazások az operációs rendszerre esetleg veszélyes műveletbe kezdjenek, így felügyelve a hozzáférést az operációs rendszer erőforrásaihoz és a személyes adatokhoz. Az összetevő antivírus adatbázisok és a Kaspersky Security Network felhőszolgáltatás segítségével biztosít védelmet a számítógépnek. **Kármentesítő motor** A Kármentesítő motor összetevő révén a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben végrehajtott műveleteket visszagörgetni.

Rész	Összetevő
Biztonsági felügyelet 	**Alkalmazásfelügyelő** Az Alkalmazásfelügyelő kezeli az alkalmazások indítását a felhasználók számítógépén. Ez lehetővé teszi a vállalati biztonsági házirend bevezetését az alkalmazások használatára vonatkozóan. Az Alkalmazásfelügyelő emellett csökkenti a számítógép megfertőződésének kockázatát is azzal, hogy korlátozza a hozzáférést az alkalmazásokhoz. **Eszközfelügyelő** Az Eszközfelügyelő felügyeli az olyan eszközökhöz történő felhasználói elérést, amik csatlakoztatva vannak a számítógéphez (például merevlemezek, kamerák vagy Wi-Fi modulok). Ez lehetővé teszi, hogy megvédje számítógépét a fertőzésektől, ha ilyen eszközök vannak csatlakoztatva, valamint megelőzi az adatvesztést vagy -szivárgást. **Webfelügyelő** A Webfelügyelő kezeli a felhasználók hozzáférését a webes erőforrásokhoz. Ez csökkenti a forgalmat és a munkaidő nem megfelelő használatát. Ha a felhasználó a Webfelügyelő által korlátozott weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést vagy figyelmeztetést jelenít meg. **Adaptív Anomáliafelügyelő** Az Adaptív Anomáliafelügyelő összetevő megfigyeli és letiltja azokat a tevékenységeket, amelyek nem megszokottak a cég hálózatán található számítógépeken. Az Adaptív Anomáliafelügyelő egy szabálycsoport alapján követi nyomon a nem jellemző viselkedést (például a *Start of Microsoft PowerShell from office application* szabályt). A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján. Konfigurálhatja, hogy az Adaptív Anomáliafelügyelő miként kezelje az egyes szabályokat és engedélyezheti olyan PowerShell szkriptek végrehajtását, amelyek bizonyos feladatokat automatizálnak. A Kaspersky Endpoint Security az alkalmazás adatbázisával együtt frissíti a szabálycsoportokat. **Naplóvizsgálat** A Napló vizsgálata figyelemmel kíséri a védett környezetek integritását a Windows eseménynapló-elemzése alapján. Ha az alkalmazás szokatlan magatartást érzékel a rendszerben, jelzi a rendszergazdának, mert ez a magatartás kibertámadásra tett kísérlet jele is lehet. **Rendszerintegritás-figyelő** A Rendszerintegritás-figyelő figyeli az operációs rendszerben bekövetkező olyan változásokat, amelyek a számítógépes biztonság sérülésére utalhatnak. Ilyen változások észlelésekor a Kaspersky Endpoint Security megfelelő eseményeket generál, és figyelmezteti a rendszergazdát.
Feladatok 	**Kártevő vizsgálata** A Kaspersky Endpoint Security megvizsgálja a számítógépet vírusok és egyéb fenyegetések szempontjából. A Kártevő vizsgálata segít megelőzni a rosszindulatú programok terjedését, amiket például az alacsony biztonsági szint miatt nem észleltek a védelmi összetevők. **Adatbázisok és alkalmazásmodulok frissítése** A Kaspersky Endpoint Security letölti a frissített adatbázisokat és alkalmazásmodulokat. A frissítés révén a számítógép védelme fennmarad a legfrissebb vírusok és egyéb fenyegetések ellen. Az alkalmazás frissítésére alapértelmezés szerint automatikusan sor kerül, szükség esetén azonban az adatbázisokat és az alkalmazásmodulokat kézileg is frissítheti. **Utolsó frissítés visszagörgetése** A Kaspersky Endpoint Security visszagörgeti az adatbázisok és modulok legutóbbi frissítését. Ennek köszönhetően szükség esetén az adatbázisokat és az alkalmazásmodulokat vissza lehet görgetni korábbi verziójukra, például akkor, ha az új adatbázisverzió érvénytelen aláírást tartalmaz, ami miatt a Kaspersky Endpoint Security egy biztonságos alkalmazást blokkol. **Alkalmazás integritás-ellenőrzése** A Kaspersky Endpoint Security ellenőrzi, hogy az alkalmazás telepítési mappájában lévő alkalmazásmodulok nem sérültek vagy módosultak-e. Ha egy alkalmazásmodul digitális aláírása hibás, akkor az sérültnek minősül.
Adattitkosítás 	**Fájl szintű titkosítás** Az összetevő lehetővé teszi fájltitkosítási szabályok létrehozását. Kiválaszthatja az előre definiált mappákat a titkosításhoz, manuálisan kiválaszthat egy mappát, vagy kiterjesztés szerint választhat ki egyes fájlokat. **Teljes lemeztitkosítás** Az összetevő lehetővé teszi a merevlemez titkosítását a Kaspersky lemeztitkosítás vagy a BitLocker meghajtótitkosítás használatával. **Cserélhető meghajtók titkosítása** Az összetevő lehetővé teszi a cserélhető meghajtók adatainak védelmét. Használhat teljes lemeztitkosítást vagy fájlszintű titkosítást.

Rész	Összetevő
Detection and Response 	**Endpoint Detection and Response Optimum** Beépített ügynök a Kaspersky Endpoint Detection and Response Optimum megoldáshoz (a továbbiakban: „EDR Optimum"). A *Kaspersky Endpoint Detection and Response* megoldás a vállalat informatikai infrastruktúrájának védelmét biztosítja a fejlett számítógépes fenyegetések ellen. A megoldás ötvözi a fenyegetések különböző automatikus észlelését, és képes reagálni ezekre a fenyegetésekre, hogy ellensúlyozza a speciális támadásokat, beleértve az új biztonsági réseket, a zsarolóprogramokat, a fájlmentes támadásokat, valamint a legitim rendszereszközöket használó módszereket. A megoldással kapcsolatos további információkért lásd a Kaspersky Endpoint Detection and Response Optimum súgót. **Endpoint Detection and Response Expert** Beépített ügynök a Kaspersky Endpoint Detection and Response Expert megoldáshoz (a továbbiakban: „EDR Expert"). Az EDR Expert több fenyegetésfigyelési és reagálási funkciót kínál, mint az EDR Optimum. A megoldással kapcsolatos további információkért lásd a Kaspersky Endpoint Detection and Response Expert súgót. **Endpoint Detection and Response Expert (on-premises)** és **Network Detection and Response (KATA)** Beépített ügynökök a Kaspersky Anti Targeted Attack Platform megoldás részét képező Endpoint Detection and Response és Network Detection and Response összetevők kezeléséhez. A *Kaspersky Anti Targeted Attack Platform* egy megoldás, ami a kifinomult fenyegetések, például célzott támadások és speciális, állandó veszélyek (APT), valamint nagy kockázatú veszélyforrások időszerű észlelésére szolgál. A Kaspersky Anti Targeted Attack Platform három funkcionális egységet tartalmaz: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Az összes funkcionális egységet vagy az egyes funkcionális egységeket külön is megvásárolhatja. A megoldás részleteivel kapcsolatos információért lásd a Kaspersky Anti Targeted Attack Platform útmutatót. **Sandbox** Beépített ügynök a Sandboxhoz. *A Sandbox* összetevő észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (a Sandbox-kiszolgálók). A megoldás részleteivel kapcsolatos információkat a Kaspersky Sandbox súgóban és a Kaspersky Anti Targeted Attack Platform súgóban találja. **Managed Detection and Response** Beépített ügynök a Kaspersky Managed Detection and Response megoldás működésének támogatásához. A *Kaspersky Managed Detection and Response (MDR)* megoldás automatikusan észleli és elemzi az infrastruktúrában bekövetkező biztonsági incidenseket. Ehhez az MDR a végpontoktól és a gépi tanulásból kapott telemetriai adatokat használja. Az MDR incidensadatokat küld a Kaspersky szakértőinek. A szakértők ezután feldolgozhatják az incidenst, és például új bejegyzést adhatnak hozzá a vírusadatbázisokhoz. Alternatív megoldásként a szakértők javaslatokat tehetnek az incidens feldolgozására, és például javasolhatják a számítógép leválasztását a hálózatról. A megoldás működéséről részletes információt a Kaspersky Managed Detection and Response súgójában talál.

Az alkalmazási üzemmódjai: Standard, EDR Agent, Light Agent

A Kaspersky Endpoint Security for Windows számos Kaspersky-megoldás része. A megoldástól függően ki kell választania az alkalmazás módját.



Standard mód

Ez az alkalmazás fő és alapértelmezett módja. Az alkalmazást ebben a módban a Kaspersky EPP (Endpoint Protection Platform) megoldások részeként telepítheti. Például a Kaspersky Endpoint Security Standard módban a Kaspersky Endpoint Security for Business része. A Kaspersky Endpoint Security átfogó védelmet nyújt a munkaállomásoknak és a kiszolgálóknak a különféle fenyegetésekkel, hálózati támadásokkal és csalásokkal szemben. Normál módban beépített ügynökök is elérhetők a Kaspersky Detection and Response megoldásaival való integrációhoz, beleértve az EDR-t, az MDR-t, a KUMA-t és másokat.



EDR Agent

Ez a mód lehetővé teszi a Kaspersky Detection and Response megoldásainak és harmadik féltől származó EPP megoldásainak együttes telepítését. A Detection and Response megoldások közé tartozik a Kaspersky Managed Detection and Response (MDR) és a Kaspersky Anti Targeted Attack Platform (KATA). Az EDR Agent a Kaspersky SIEM megoldást és a Kaspersky Unified Monitoring and Analysis Platform (KUMA) megoldást is támogatja.

Ebben az üzemmódban nem érhetők el olyan szabványos védelmi összetevők, mint a Fájl védelem vagy a Web védelem. A számítógép szabványos védelméről a harmadik féltől származó EPP megoldás gondoskodik. Az EDR Agent folyamatosan figyeli az ezeken a számítógépeken futó folyamatokat, a nyitott hálózati kapcsolatokat és a módosítandó fájlokat, és együttműködik a Detection and Response megoldásokkal.



Light Agent

Ez a mód a virtuális környezetek védelmére szolgál. A Kaspersky Endpoint Security Light Agent üzemmódja a Kaspersky Hybrid Cloud Security megoldás része. A Light Agent védi a vendég operációs rendszerrel rendelkező virtuális gépeket munkaállomásokon és kiszolgálókon. Ugyanazok a védelmi és felügyeleti összetevők érhetők el ebben az üzemmódban, mint a Normál üzemmódban. A különbség az, hogy az objektumokat egy külön virtuális gépre telepített speciális megoldási összetevő, az SVM (Secure Virtual Machine) vizsgálja vírusok és egyéb rosszindulatú programok szempontjából. Így a Light Agent az SVM erőforrásait használja fel az infrastruktúra biztonságának biztosítására a virtuális gép erőforrásai helyett.

Forgalmazási készlet

A terjesztőkészlet a következő terjesztőcsomagokat tartalmazza:

- **AES256**

  Ez a disztribúciós csomag x86/x64 architektúrájú számítógépekre való telepítésre készült. Ez a terjesztőcsomag kriptográfiai eszközöket tartalmaz az AES (Advanced Encryption Standard) 256 bites hatásos kulcshosszúságú titkosítási algoritmus elvégzésére.

- **AES56**

  Ez a disztribúciós csomag x86/x64 architektúrájú számítógépekre való telepítésre készült. Ez a terjesztőcsomag kriptográfiai eszközöket tartalmaz az AES 56 bites hatásos kulcshosszúságú titkosítási algoritmus elvégzésére.

- **Arm64**

  Ez a terjesztőcsomag ARM-alapú számítógépekre való telepítésre szolgál. Ez a disztribúciós csomag nem kiszolgálókra való telepítésre készült.

Telepítés előtt győződjön meg arról, hogy a disztribúciós csomag megfelel a processzor architektúrájának. Ha a disztribúciós csomag nem egyezik a processzor architektúrájával, a telepítő hibával megszakítja a telepítést.

A disztribúciós csomag egy önkicsomagoló archívum EXE formátumban. A disztribúciós csomag tartalmának megtekintéséhez ki kell csomagolni az archívumot egy külön mappába. Minden terjesztőcsomag tartalmazza a következő fájlokat:

`kes_win.msi`	Kaspersky Endpoint Security terjesztőcsomag.
`setup_kes.exe`	Az alkalmazás telepítéséhez szükséges fájlok az igénybe vehető módszerek mindegyike esetén.
`kes_win.kud`	Fájl a telepítőcsomag létrehozásához a Kaspersky Endpoint Security számára.
`klcfginst.msi`	Telepítőcsomag az alkalmazás adminisztrációs bővítményéhez a Kaspersky Security Center Administration Console-ban.
`bases.cab`	Frissítse a telepítés során használt csomagfájlokat.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Fájlok az inkompatibilis szoftver eltávolításához.
`incompatible.txt`	A Kaspersky Endpoint Security termékkel való kompatibilitási problémákat okozó szoftverek listáját tartalmazó fájl. A Kaspersky nem garantálja a Kaspersky Endpoint Security kompatibilitását a listán szereplő szoftverekkel.
`ksn_<language ID>.txt`	A fájl, ahol elolvashatja a részvétel a Kaspersky Security Networkben feltételeit.
`license.txt`	A fájl, ahol átolvashatja a Végfelhasználói Licencszerződést és az Adatvédelmi szabályzatot.
`installer.ini`	A fájl, amely a terjesztőkészlet belső beállításait tartalmazza.
`kes.cab`	Fájlok az alkalmazás grafikus felületéhez.
`aes256.cab` / `aes56.cab`	Az AES kriptográfiai algoritmushoz tartozó fájlok (nem tartoznak az Arm64 terjesztőcsomaghoz).
`package.kcat`	Az alkalmazásterjesztő csomag aláírásait tartalmazó fájl. A digitális aláírás garantálja az alkalmazásterjesztő csomag hitelességét és sértetlenségét.

E beállítások értékeinek módosítása nem javasolt. Ha módosítani szeretné a telepítési lehetőségeket, használja a setup.ini fájlt.

Hardveres és szoftveres rendszerkövetelmények

Ez a cikk felsorolja azokat a szoftververziókat, amelyeken az alkalmazást tesztelték, és amelyek esetében garantált a megfelelő működés. Lehetséges, hogy az alkalmazás más szoftververziókkal is működik, de ezeket a konfigurációkat nem vetették alá teljes körű tesztelésnek, és nem szerepelnek a garantáltan támogatott verziók listáján.

A Kaspersky Endpoint Security megfelelő működéséhez a számítógépnek teljesítenie kell a következő követelményeket:

Az alkalmazás telepítéséhez rendszergazdai jogosultság szükséges a számítógépen.

Minimális általános követelmények

Minimális követelmények	Munkaállomás (x86/x64)	Kiszolgáló (x86/x64)	Arm
Tárhely	2 GB	2 GB	2 GB
CPU	1 GHz, SSE2 utasítások támogatása	1,4 GHz, SSE2 utasítások támogatása	1 GHz, Armv8.1 architektúra
RAM	Munkaállomás (x86): 1 GB Munkaállomás (x64): 2 GB	2 GB Megjegyzés: A kiszolgálónak 8 GB memóriára van szüksége az alkalmazás telepítéséhez a beépített ügynökkel, hogy integrálható legyen a Kaspersky Anti Targeted Attack Platformmal.	4 GB
Microsoft .NET keretrendszer	4 vagy újabb	4 vagy újabb	4.8 vagy újabb

Munkaállomások

Támogatott operációs rendszerek a munkaállomások esetében:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / több munkamenetes Enterprise
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

A Windows operációs rendszerek a 11 24H2 verziótól kezdve támogatják az UDP Receive Segment Coalescing Offload (URO) technológiát. A technológia alapértelmezés szerint engedélyezve van, ha a számítógépen kompatibilis hálózati kártya és illesztőprogramok vannak telepítve. Az URO letiltása a felhasználó számítógépén jelentősen csökkentheti az alkalmazás teljesítményét.

A Kaspersky Endpoint Security megfelelő működéséhez a Windows Security Center (wscsvc) szolgáltatásnak futnia kell a felhasználó számítógépén.

A Kaspersky Endpoint Security nem telepíthető Microsoft Windows 7 rendszerre az operációs rendszer következő frissítései nélkül: KB4490628 (2019. március 12.) és KB4474419 (2019. szeptember 23.). Részletes információkért tekintse meg a Terméktámogatási tudásbázist.

A Microsoft Windows 10 operációs rendszer támogatásának részleteiért lásd a Terméktámogatási Tudásbázist.

A Microsoft Windows 11 operációs rendszer támogatásának részleteiért lásd a Terméktámogatási Tudásbázist.

Kiszolgálók

A Kaspersky Endpoint Security támogatja az alkalmazás alapvető összetevőit a Windows operációs rendszert futtató számítógépeken kiszolgálók esetében. Használhatja a Kaspersky Endpoint Security for Windows szolgáltatást a Kaspersky Security for Windows Server helyett a cége kiszolgálóin és fürtjein (Cluster Mode). Az alkalmazás támogatja a következőt is: Server Core Mode (lásd: ismert problémák).

Támogatott operációs rendszerek a kiszolgálók esetében:

- Windows Small Business Server 2011 Essentials / Standard (64-bit)

  A Microsoft Small Business Server 2011 Standard (64 bites) csak akkor támogatott, ha a Service Pack 1 for Microsoft Windows Server 2008 R2 telepítve van.

- Windows MultiPoint Server 2011 (64-bit)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2016 Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2019 Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)

- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (beleértve a Server Core mode megoldást is)
- Windows Server 2025 Standard / Datacenter

A Kaspersky Endpoint Security nem telepíthető Microsoft Windows Server 2008 R2 rendszerre az operációs rendszer következő frissítései nélkül: KB4490628 (2019. március 12.) és KB4474419 (2019. szeptember 23.).

A Microsoft Windows Server 2016 és a Microsoft Windows Server 2019 operációs rendszerek támogatásának részleteiért lásd a Terméktámogatási tudásbázist.

A Microsoft Windows Server 2022 operációs rendszer támogatásának részleteiért lásd a Terméktámogatási Tudásbázist.

Nem támogatott operációs rendszerek a kiszolgálók esetében:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Virtuális platformok

Támogatott virtuális platformok az alkalmazások normál módú működéséhez:

- VMware Workstation Pro 26H1
- VMware ESXi 8.0 Update 3i
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

Az alkalmazás támogatja a Windows 11 Pro Arm64 rendszert futtató, Hyper-V használatával létrehozott virtuális gépeket.

Virtuális gépek a Light Agent telepítéséhez

A Kaspersky Endpoint Security telepítése Light Agent üzemmódban Arm-alapú virtuális gépekre nem támogatott.

A virtuális gépek BIOS-ának támogatnia kell az SMBIOS-specifikáció 2.1-es vagy újabb verzióját.

A következő csomagokat és segédprogramokat kell telepíteni a virtuális gépekre:

- Microsoft Hyper-V – Integration Services csomag használata esetén.
- VMware vSphere – VMware Tools csomag használata esetén.
- XenServer – XenTools csomag használata esetén.
- HUAWEI FusionSphere – HUAWEI Tools csomag használata esetén.
- KVM-alapú hipervizorok használata esetén – QEMU Guest Agent.

Az alkalmazás Light Agent módban történő futtatásához szükséges virtuális infrastrukturális követelményekért olvassa el a Kaspersky Security for Virtualization Light Agent súgóját.

Az alkalmazás megfelelő működéséhez legalább 100 Mbit/s sávszélességű virtualizált hálózati interfészt kell használnia.

Terminálkiszolgálók

Támogatott terminálkiszolgálói típusok:

- Microsoft Távoli asztali szolgáltatások Windows Server 2008 R2 SP1 rendszeren alapulva
- Microsoft Távoli asztali szolgáltatások Windows Server 2012 rendszeren alapulva
- Microsoft Távoli asztali szolgáltatások Windows Server 2012 R2 rendszeren alapulva
- Microsoft Távoli asztali szolgáltatások Windows Server 2016 rendszeren alapulva
- Microsoft Távoli asztali szolgáltatások Windows Server 2019 rendszeren alapulva
- Microsoft Távoli asztali szolgáltatások Windows Server 2022 rendszeren alapulva
- Microsoft Távoli asztali szolgáltatások Windows Server 2025 rendszeren alapulva
- Citrix RDSH a Citrix Virtual Apps and Desktops 7 2507 LTSR megoldásból

Kaspersky Security Center Támogatás

A Kaspersky Endpoint Security a Kaspersky Security Center alábbi verzióival támogatja az együttműködést:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2

Az operációs rendszer típusától függően elérhető alkalmazásfunkciók összehasonlítása.

A Kaspersky Endpoint Security elérhető funkciói az operációs rendszer típusától, a munkaállomástól és a szervertől függenek (lásd az alábbi táblázatot).

A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve a telepítőcsomagban különböző összetevőkészleteket konfigurálhat a különböző típusú operációs rendszerekhez. Ez azt jelenti, hogy ugyanazzal a telepítőcsomaggal telepítheti az alkalmazást munkaállomásokra és kiszolgálókra.

A Kaspersky Endpoint Security telepítése Light Agent üzemmódban Arm-alapú virtuális gépekre nem támogatott.

A Kaspersky Endpoint Security funkcióinak összehasonlítása

Funkció	Workstation	ARM-alapú munkaállomás	Kiszolgáló	Server Core mode
Fenyegetések elleni fejlett védelem				
Kaspersky Security Network	✓	✓	✓	✓
Viselkedésészlelés	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Biztonsági rések kihasználásának megelőzése	✓	✓	✓	✓

Funkció	Workstation	ARM-alapú munkaállomás	Kiszolgáló	Server Core mode
Behatolásmegelőző rendszer	✓	✓	–	–
Kármentesítő motor	✓	✓	✓	✓
Fenyegetések elleni alapvető védelem				
Fájl védelem	✓	✓	✓	✓
Web védelem	✓	✓	✓	–
Levelezés védelem	✓	✓	✓	–
Tűzfal	✓	✓	✓	✓
Hálózati védelem	✓	✓	✓	✓
BadUSB védelem	✓	✓	✓	–
AMSI védelem	✓	✓	✓	✓
Biztonsági felügyelet				
Naplóvizsgálat	–	–	✓	–
Alkalmazásfelügyelő	✓	✓	✓	✓
Eszközfelügyelő	✓	✓	✓	✓
Webfelügyelő	✓	✓	✓	–
Adaptív Anomáliafelügyelő	✓	✓	–	–
Rendszerintegritás-figyelő	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Adattitkosítás				
Kaspersky lemeztitkosítás	✓	–	–	–
BitLocker meghajtótitkosítás	✓	✓	✓	✓
Fájl szintű titkosítás	✓	–	–	–
Cserélhető meghajtók titkosítása	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	–	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
KUMA integráció	✓	✓	✓	✓

Az alkalmazásfunkciók összehasonlítása a kezelőeszközök alapján.

A Kaspersky Endpoint Security elérhető funkciói a kezelőeszközöktől függnek (lásd az alábbi táblázatot).

Az alkalmazást a Kaspersky Security Center következő konzoljai használatával kezelheti:

- Adminisztrációs konzol. A rendszergazda munkaállomásán telepített Microsoft Management Console (MMC) beépülő modul.

- Web Console. A Kaspersky Security Center összetevője, ami telepítve van az Adminisztrációs kiszolgálóra. A Web Console helyen bármilyen olyan számítógép böngészőjén dolgozhat, amely hozzáfér az Adminisztrációs kiszolgálóhoz.

Az alkalmazást a Kaspersky Security Center Cloud Console helyen is kezelheti. A *Kaspersky Security Center Cloud Console* a Kaspersky Security Center felhőalapú verziója. Ez azt jelenti, hogy az Adminisztrációs kiszolgáló és a Kaspersky Security Center egyéb összetevői a Kaspersky felhőalapú infrastruktúrájába vannak telepítve. Az alkalmazás Kaspersky Security Center Cloud Console-on keresztüli kezelésének részleteiről tájékozódjon a Kaspersky Security Center Cloud Console súgójában.

A Kaspersky Endpoint Security a Kaspersky Next Pro View megoldás része. A megoldás részeként működő alkalmazások elérhető funkcióiról a Kaspersky Next súgójában talál további információt.

A Kaspersky Endpoint Security funkcióinak összehasonlítása

Funkció	Kaspersky Security Center		Kaspersky Security Center
	Adminisztrációs konzol	Web Console	Cloud Console
Fenyegetések elleni fejlett védelem			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Viselkedésészlelés	✓	✓	✓
Anti-Cryptor			
Biztonsági rések kihasználásának megelőzése	✓	✓	✓
Behatolásmegelőző rendszer	✓	✓	✓
Kármentesítő motor	✓	✓	✓
Fenyegetések elleni alapvető védelem			
Fájl védelem	✓	✓	✓
Web védelem	✓	✓	✓
Levelezés védelem	✓	✓	✓
Tűzfal	✓	✓	✓
Hálózati védelem	✓	✓	✓
BadUSB védelem	✓	✓	✓
AMSI védelem	✓	✓	✓
Biztonsági felügyelet			
Naplóvizsgálat	✓	✓	✓
Alkalmazásfelügyelő	✓	✓	✓
Eszközfelügyelő	✓	✓	✓
Webfelügyelő	✓	✓	✓
Adaptív Anomáliafelügyelő	✓	✓	✓
Rendszerintegritás-figyelő	✓	✓	✓
Cloud Discovery	–	–	✓
Adattitkosítás			

Funkció	Kaspersky Security Center		Kaspersky Security Center
	Adminisztrációs konzol	Web Console	Cloud Console
Kaspersky lemeztitkosítás	✓	✓	–
BitLocker meghajtótitkosítás	✓	✓	✓
Fájl szintű titkosítás	✓	✓	–
Cserélhető meghajtók titkosítása	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
KUMA integráció	✓	✓	✓
Feladatok			
Kulcs hozzáadása	✓	✓	✓
Alkalmazásösszetevők módosítása	✓	✓	✓
Leltár	✓	✓	✓
Frissítés	✓	✓	✓
Frissítés visszaállítása	✓	✓	✓
Kártevő vizsgálata	✓	✓	✓
Alkalmazás integritás-ellenőrzése	✓	✓	–
Adatok törlése	✓	✓	✓
Hitelesítési ügynök fiókok kezelése (Kaspersky lemeztitkosítás)	✓	✓	–
IOC vizsgálat (EDR)	–	✓	✓
Fájl áthelyezése a karanténba (EDR)	–	✓	✓
Fájl lekérése (EDR)	–	✓	✓
Fájl törlése (EDR)	–	✓	✓
Folyamat indítása (EDR)	–	✓	✓
Folyamat leállítása (EDR)	–	✓	✓

Kompatibilitás más alkalmazásokkal

A Kaspersky Endpoint Security nem kompatibilis egyes Kaspersky-alkalmazásokkal, valamint egyes harmadik féltől származó alkalmazásokkal. Ezért a telepítés, az alkalmazás verziójának frissítése, és az alkalmazás összetevőinek módosítása előtt a Kaspersky Endpoint Security megvizsgálja a számítógépet, hogy nincs-e rajta ilyen alkalmazás.

Kompatibilitás harmadik féltől származó alkalmazásokkal

A Kaspersky Endpoint Security nem kompatibilis azokkal az alkalmazásokkal, amelyek harmadik felek végpontvédelmi rendszereinek (Endpoint Protection Platform, EPP) részét képezik. A Kaspersky Endpoint Security más alkalmazásokkal is okozhat kompatibilitási problémákat. A kompatibilitás megállapításához a Kaspersky Endpoint Security megvizsgálja a szoftverek Kaspersky által készített listáját. A lista az incompatible.txt fájlban található. Ezt a fájlt a terjesztőkészlet tartalmazza.

A Kaspersky nem garantálja a Kaspersky Endpoint Security kompatibilitását a listán szereplő szoftverekkel. Ha a listán szereplő alkalmazásokat észleli, a telepítő leállítja a Kaspersky Endpoint Security telepítését. A telepítő egyes alkalmazásokat automatikusan törölhet a listáról. Ha hajlandó figyelmen kívül hagyni a kockázatokat, és ugyanarra a számítógépre szeretné telepíteni a Kaspersky Endpoint Security alkalmazást, valamint a listából egy szoftvert, kihagyhatja a számítógép ellenőrzését (lásd az alábbi utasításokat).

TÖLTSE LE AZ INCOMPATIBLE.TXT FÁJLT

Kompatibilitás Kaspersky alkalmazásokkal

A Kaspersky Endpoint Security az alábbi Kaspersky alkalmazásokkal nem kompatibilis:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Az Endpoint Sensor a Kaspersky Anti Targeted Attack Platform és a Kaspersky Endpoint Detection and Response megoldások részeként.
- A Kaspersky Endpoint Agent a Kaspersky Detection and Response megoldásainak részeként.

  A Kaspersky a Kaspersky Endpoint Agent helyett a beépített Kaspersky Endpoint Security ügynökre állítja át az összes Detection and Response megoldást. A 12.1 verziótól kezdve az alkalmazás támogatja az összes Detection and Response megoldást.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.

- Kaspersky Security for Windows Server

  A Kaspersky Endpoint Security 12.0-tól kezdve áttérhet a Kaspersky Security for Windows Server termékről a Kaspersky Endpoint Security for Windows termékre, és ugyanazt a megoldást használhatja a munkaállomások és kiszolgálók védelmére.

- Kaspersky Embedded Systems Security.

Amennyiben a listában szereplő Kaspersky alkalmazások telepítve vannak a számítógépen, a Kaspersky Endpoint Security eltávolítja azokat. Kérjük, várja meg a folyamat végét a Kaspersky Endpoint Security telepítésének folytatása előtt.

A kompatibilitási problémákat okozó szoftverek ellenőrzésének kihagyása

Ha a Kaspersky Endpoint Security szoftvert észlel az incompatible.txt listában, az alkalmazás telepítése megszakad. A telepítés folytatásához el kell távolítania az alkalmazást. Ha azonban a harmadik féltől származó szoftverek szállítója a dokumentációjában jelezte, hogy szoftverük kompatibilis az Endpoint Protection Platform-zal (EPP), akkor telepítheti a Kaspersky Endpoint Security-t olyan számítógépre, amely az adott gyártótól származó alkalmazást tartalmazza. Például a Endpoint Detection and Response (EDR) megoldásszolgáltató kijelentheti, hogy kompatibilis harmadik félttől származó EPP rendszerekkel. Ebben az esetben a Kaspersky Endpoint Security telepítését a telepített szoftver ellenőrzése nélkül kell elindítania. Ehhez adja meg a következő paramétereket a telepítőnek:

- `SKIPPRODUCTCHECK=1` A telepített szoftverek ellenőrzésének letiltása. A kompatibilitási problémákat okozó szoftverek listája a terjesztési csomagban található incompatible.txt fájlban érhető el. Ha nincs megadva érték a paraméterhez, és a listán szereplő szoftver észlelhető, a Kaspersky Endpoint Security telepítése leáll.

- `SKIPPRODUCTUNINSTALL=1` Az incompatible.txt listán szereplő, észlelt szoftverek automatikus eltávolításának letiltása. Ha nincs megadva érték a paraméterhez, a Kaspersky Endpoint Security megpróbálja eltávolítani a kompatibilitási problémákat okozó szoftvert.

- `CLEANERSIGNCHECK=0` Az ellenőrzés által talált alkalmazások digitális aláírás-ellenőrzésének letiltása. Ha ez a paraméter nincs beállítva, a digitális aláírások ellenőrzése le van tiltva, amikor az alkalmazást a Kaspersky Security Centeren keresztül telepíti. Ha az alkalmazást helyileg telepíti, a digitális aláírás ellenőrzése alapértelmezés szerint engedélyezve van.

Az alkalmazás helyi telepítésekor a paramétereket a parancssorban adhatja át.

Ha a telepítés során kihagyta a kompatibilitási problémákat okozó szoftverek azonosítását, a Kaspersky Endpoint Security az alkalmazás összetevőinek megváltozásakor ismét elvégezheti ezt a keresést. A telepített szoftverek vizsgálatának kihagyásához konfigurálnia kell a *Alkalmazásösszetevők módosítása* feladatot.

Példa:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

A Kaspersky Endpoint Security távolról történő telepítéséhez a megfelelő paramétereket kell hozzáadnia a `kes_win.kud` telepítőcsomag-generáló fájlhoz a `[Setup]` alatt (lásd alább). A `kes_win.kud` fájlt a terjesztőkészlet tartalmazza.

kes_win.kud

```
[Setup]
UseWrapper=1
```

```
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Az alkalmazás telepítése és eltávolítása

A Kaspersky Endpoint Security több módon telepíthető a számítógépen:

- helyben, a Telepítővarázsló segítségével.
- helyben, a parancssorból.
- távolról, a Kaspersky Security Centeren keresztül.
- távolról, a Microsoft Windows csoportos rendszabálykezelő szerkesztőben (további információért keresse fel a Microsoft Terméktámogatás weboldalát).
- távolról, a Rendszerközpont-konfigurációs kezelővel.

Az alkalmazástelepítés beállításait több módot adhatja meg. Ha egyszerre több módszerrel adja meg a beállításokat, a Kaspersky Endpoint Security a legmagasabb prioritású beállítást alkalmazza. A Kaspersky Endpoint Security a következő prioritássorrendet használja:

1. A setup.ini fájlból kapott beállítások.
2. Az installer.ini fájlból kapott beállítások.
3. A parancssorból kapott beállítások.
4. A konfigurációs fájlból (install.cfg) kapott beállítások.

Javasoljuk, hogy a Kaspersky Endpoint Security telepítésének megkezdése előtt zárja be az összes futó alkalmazást (távoli telepítéskor is).

A Kaspersky Endpoint Security telepítésekor az operációs rendszer megjelenítheti a saját üzeneteit. A hálózati és internetkapcsolatok is megszakadhatnak az alkalmazás telepítésekor.

A Kaspersky Endpoint Security telepítésekor, frissítésekor vagy eltávolításakor hibák léphetnek fel. A hibák megoldásával kapcsolatos további információért tekintse meg a Terméktámogatási tudásbázist.

Üzembe helyezés a Kaspersky Security Centeren keresztül

A Kaspersky Endpoint Security számos módon üzembe helyezhető olyan számítógépeken, amik vállalati hálózaton vannak. Kiválaszthatja az üzembe helyezés legjobb módját az intézmény számára, vagy egyszerre kombinálhat több üzembehelyezési módot. Az alkalmazás telepítése előtt győződjön meg arról, hogy a Kaspersky Security Center Network Agent telepítve van a számítógépen. A *Network Agent* végzi el az Adminisztrációs szerver és az ügyfélszámítógép közötti interakciót.

A Kaspersky Security Center a következő főbb üzembehelyezési módszereket támogatja:

- Az alkalmazás telepítése a Védelmi Üzembehelyezési varázslóval.

  A Normál telepítési mód akkor megfelelő, ha elégedett a Kaspersky Endpoint Security alapértelmezett beállításaival, az intézményének pedig egyszerű infrastruktúrája van, ami nem igényel speciális beállításokat.

- Az alkalmazás telepítése a távoli telepítés feladattal.

  Univerzális telepítési mód, ami lehetővé teszi a Kaspersky Endpoint Security beállításainak konfigurálását és a távoli telepítési feladatok rugalmas kezelését. A Kaspersky Endpoint Security telepítése a következő lépésekből áll:

  1. Telepítőcsomag létrehozása.
  2. Távoli telepítés feladat létrehozása.

A Kaspersky Security Center támogat egyéb módokat is a Kaspersky Endpoint Security telepítésére is, például az operációs rendszer képén belül történő üzembe helyezést is. Az egyéb üzembe helyezési módokkal kapcsolatos tudnivalókért lásd a Kaspersky Security Center súgót.

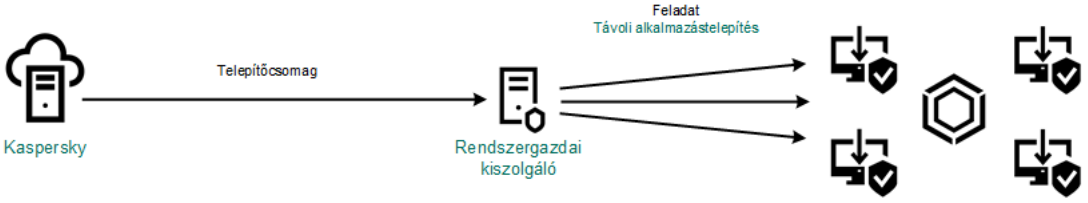
Az alkalmazás normál telepítése

A Kaspersky Security Center egy Távoli védelemtelepítési varázslót biztosít az alkalmazás telepítéséhez a vállalati számítógépeken. A Védelmi Üzembehelyezési varázsló a következő fő tevékenységeket tartalmazza:

1. A Kaspersky Endpoint Security telepítőcsomag kiválasztása.

   A *telepítőcsomag* fájlok egy csoportját jelenti, amik a Kaspersky alkalmazás távoli, Kaspersky Security Center-en keresztül történő telepítésére lettek létrehozva. A telepítőcsomag az alkalmazás telepítéséhez szükséges számos beállítást tartalmaz, a telepítés után ezeket egyből futtatja. A telepítőcsomag az alkalmazás forgalmazási készletben található, .kpd és .kud kiterjesztésű fájlok használatával lett létrehozva. A Kaspersky Endpoint Security telepítőcsomag a Windows támogatott verziói, valamint a processzor-architektúrák esetében is használatos.

2. A Kaspersky Security Center felügyeleti kiszolgáló *Install application remotely* feladatának létrehozása.



Kaspersky Endpoint Security végrehajtás

A Távoli védelemtelepítési varázsló futtatásának menete az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Advanced** → **Remote installation** lehetőséget.
3. Kattintson a **Deploy installation package on managed devices (workstations)** hivatkozásra.

Ez elindítja a Védelmi Üzembehelyezési varázslót. Kövesse a varázsló utasításait.

A 139-es és 445-ös TCP portokat és a 137-es és 138-as UDP portokat ügyfélszámítógépen kell megnyitni.

1. lépés. A telepítőcsomag kiválasztása

Válassza ki a Kaspersky Endpoint Security telepítőcsomagot a listából. Ha a listában nem szerepel a Kaspersky Endpoint Security telepítőcsomagja, létrehozhatja azt a varázslóban.

A installation package settings a Kaspersky Security Centerben adhatja meg. Például kiválaszthatja az alkalmazás összetevőket, amik telepítve lesznek a számítógépre.

A rendszer a hálózati ügynököt is telepíti a Kaspersky Endpoint Security telepítésekor. A *Network Agent* végzi el az Adminisztrációs szerver és az ügyfélszámítógép közötti interakciót. Ha a Hálózati ügynök már telepítve van a számítógépre, akkor nem kell újra telepíteni.

2. lépés. A telepítőcsomag forrásának kiválasztása

Válassza ki a **Deploy Kaspersky Security Center package** forrást.

3. lépés Eszközök kiválasztása a telepítéshez

Válassza ki a számítógépeket a Kaspersky Endpoint Security telepítéséhez. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. A Hálózati ügynök nincs telepítve a hozzá nem rendelt eszközökön. Ebben az esetben a feladat bizonyos eszközökhöz lesz hozzárendelve. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés A távoli telepítési feladat beállításainak megadása

Konfigurálja a következő további alkalmazásbeállításokat:

- **Force installation package download**. Válassza ki az alkalmazás telepítésének módszerét:

  - **Using Network Agent**. A hálózati ügynök felel a Kaspersky Endpoint Security telepítőcsomagjának az ügyfélszámítógépekre való eljuttatásáért. Ha a Hálózati ügynök összetevő nincs telepítve, a feladat hibával ér véget. Ebben az esetben adja hozzá a Hálózati ügynök telepítőcsomagot a *Install application remotely* feladathoz, és engedélyezze a fájlkézbesítést az operációs rendszer erőforrásain keresztül. Ezután a Hálózati ügynök telepítésre kerül az operációs rendszer erőforrásainak használatával. Ezután a Kaspersky Endpoint Security lesz telepítve a Hálózati ügynök eszközeivel.

  - **Using operating system resources through distribution points**. A telepítőcsomag az operációs rendszer erőforrásai használatával, a elosztói pontokon keresztül lesz elküldve a számítógépekre. Ezt az opciót akkor választhatja, ha legalább egy elosztói pont van a hálózatban. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Súgót.

  - **Using operating system resources through Administration Server**. A fájlok az operációs rendszer erőforrásaival továbbítva lesznek az ügyfél számítógépekre az Adminisztrációs kiszolgálón keresztül. Ezt az opciót akkor választhatja, ha nincs Hálózati ügynök telepítve az ügyfél számítógépen, és az ügyfél számítógép ugyanazon hálózaton van, mint az Adminisztrációs kiszolgáló.

- **Behavior for devices managed through other Administration Servers**. Válassza ki a Kaspersky Endpoint Security telepítésének módját. Ha a hálózaton több mint egy Adminisztrációs kiszolgáló van telepítve, akkor ezek az Adminisztrációs kiszolgálók láthatják ugyanazon ügyfélszámítógépeket. Ez okozhatja például, hogy egy alkalmazást távolról, többször kell telepíteni ugyanazon ügyfél számítógépeken különböző Adminisztrációs kiszolgálókon keresztül, valamint egyéb hibák is felléphetnek.

- **Do not re-install application if it is already installed**. Törölje ezt a jelölőnégyzetet, ha például az alkalmazás egy korábbi verzióját akarja telepíteni.

- **Assign Network Agent installation in Active Directory group policies**. A Hálózati ügynök telepítése kézzel az Active Directory erőforrásainak segítségével. A Hálózati ügynök telepítéséhez tartomány adminisztrációs jogosultsággal kell futtatni a távoli telepítés feladatot.

5. lépés Licenckulcs kiválasztása

Adjon hozzá az alkalmazás aktiválására szolgáló kulcsot a telepítőcsomaghoz. Ez a lépés nem kötelező. Ha az Adminisztrációs kiszolgálónak van terjesztő funkcióval rendelkező kulcsa, akkor a kulcs később automatikusan hozzá lesz adva. Az alkalmazást később is aktiválhatja a *Add key* feladat segítségével.

6. lépés Az operációs rendszer újraindítására vonatkozó beállítás megadása

Adja meg, hogy a rendszer milyen műveletet hajtson végre, ha a számítógép újraindítása szükségessé válik. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.

7. lépés A nem kompatibilis alkalmazások eltávolítása az alkalmazás telepítése előtt

Gondosan tekintse végig az inkompatibilis alkalmazások listáját, majd engedélyezze ezek eltávolítását. Ha a számítógépre inkompatibilis alkalmazások vannak telepítve, a Kaspersky Endpoint Security telepítése hibával ér véget.

8. lépés. Fiók kiválasztása az eszközök eléréshez

Válassza ki az operációs rendszer eszközeinek segítségével a Hálózati ügynök telepítéséhez használt fiókot. Ebben az esetben rendszergazda jogosultságok szükségesek a számítógép eléréséhez. Több fiókot is hozzáadhat. Ha a fióknak nincs elegendő jogosultsága, a telepítő varázsló a következő fiókot fogja használni. Ha a Hálózati ügynök használatával telepíti a Kaspersky Endpoint Security alkalmazást, akkor nem kell fiókot választania.

9. lépés A telepítés elindítása

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

A Távoli védelemtelepítési varázsló elindításának menete a Web Console-ban és a Cloud Console-ban

A Web Console fő ablakában válassza az **Discovery & deployment** → **Deployment & assignment** → **Protection deployment wizard** lehetőséget.

Ez elindítja a Védelmi Üzembehelyezési varázslót. Kövesse a varázsló utasításait.

A 139-es és 445-ös TCP portokat és a 137-es és 138-as UDP portokat ügyfélszámítógépen kell megnyitni.

1. lépés. A telepítőcsomag kiválasztása

Válassza ki a Kaspersky Endpoint Security telepítőcsomagot a listából. Ha a listában nem szerepel a Kaspersky Endpoint Security telepítőcsomagja, létrehozhatja azt a varázslóban. A telepítőcsomag létrehozásához nem kell megkeresnie a terjesztőcsomagot, és nem kell elmentenie a számítógépes memóriába. A Kaspersky Security Center alkalmazásban megtekintheti a Kaspersky kiszolgálókon található terjesztőcsomagok listáját, a rendszer pedig automatikusan létrehozza a telepítőcsomagot. A Kaspersky frissíti a listát, miután az alkalmazások új verziója érhető el.

A installation package settings a Kaspersky Security Centerben adhatja meg. Például kiválaszthatja az alkalmazás összetevőket, amik telepítve lesznek a számítógépre.

2. lépés Licenckulcs kiválasztása

Adjon hozzá az alkalmazás aktiválására szolgáló kulcsot a telepítőcsomaghoz. Ez a lépés nem kötelező. Ha az Adminisztrációs kiszolgálónak van terjesztő funkcióval rendelkező kulcsa, akkor a kulcs később automatikusan hozzá lesz adva. Az alkalmazást később is aktiválhatja a *Add key* feladat segítségével.

3. lépés Hálózati ügynök kiválasztása

Válassza ki a Kaspersky Endpoint Security alkalmazással együtt telepítendő Hálózati ügynök verzióját. A *Network Agent* végzi el az Adminisztrációs szerver és az ügyfélszámítógép közötti interakciót. Ha a Hálózati ügynök már telepítve van a számítógépre, akkor nem kell újra telepíteni.

4. lépés Eszközök kiválasztása a telepítéshez

Válassza ki a számítógépeket a Kaspersky Endpoint Security telepítéséhez. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. A Hálózati ügynök nincs telepítve a hozzá nem rendelt eszközökön. Ebben az esetben a feladat bizonyos eszközökhöz lesz hozzárendelve. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

5. lépés. Speciális beállítások megadása

Konfigurálja a következő további alkalmazásbeállításokat:

- **Force installation package download**. Válassza ki az alkalmazás telepítésének módszerét:
  - **Using Network Agent**. A hálózati ügynök felel a Kaspersky Endpoint Security telepítőcsomagjának az ügyfélszámítógépekre való eljuttatásáért. Ha a Hálózati ügynök összetevő nincs telepítve, a feladat hibával ér véget. Ebben az esetben adja hozzá a Hálózati ügynök telepítőcsomagot a *Install application remotely* feladathoz, és engedélyezze a fájlkézbesítést az operációs rendszer erőforrásain keresztül. Ezután a Hálózati ügynök telepítésre kerül az operációs rendszer erőforrásainak használatával. Ezután a Kaspersky Endpoint Security lesz telepítve a Hálózati ügynök eszközeivel.
  - **Using operating system resources through distribution points**. A telepítőcsomag az operációs rendszer erőforrásai használatával, a elosztói pontokon keresztül lesz elküldve a számítógépekre. Ezt az opciót akkor választhatja, ha legalább egy elosztói pont van a hálózatban. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Súgót.
  - **Using operating system resources through Administration Server**. A fájlok az operációs rendszer erőforrásaival továbbítva lesznek az ügyfél számítógépekre az Adminisztrációs kiszolgálón keresztül. Ezt az opciót akkor választhatja, ha nincs Hálózati ügynök telepítve az ügyfél számítógépen, és az ügyfél számítógép ugyanazon hálózaton van, mint az Adminisztrációs kiszolgáló.
- **Do not re-install application if it is already installed**. Törölje ezt a jelölőnégyzetet, ha például az alkalmazás egy korábbi verzióját akarja telepíteni.
- **Assign package installation in Active Directory group policies**. A Kaspersky Endpoint Security a Hálózati Ügynökkel vagy kézileg, az Active Directory segítségével van telepítve. A Hálózati ügynök telepítéséhez tartomány adminisztrációs jogosultsággal kell futtatni a távoli telepítés feladatot.

6. lépés Az operációs rendszer újraindítására vonatkozó beállítás megadása

Adja meg, hogy a rendszer milyen műveletet hajtson végre, ha a számítógép újraindítása szükségessé válik. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.

7. lépés A nem kompatibilis alkalmazások eltávolítása az alkalmazás telepítése előtt

Gondosan tekintse végig az inkompatibilis alkalmazások listáját, majd engedélyezze ezek eltávolítását. Ha a számítógépre inkompatibilis alkalmazások vannak telepítve, a Kaspersky Endpoint Security telepítése hibával ér véget.

8. lépés. Hozzárendelés egy adminisztrációs csoporthoz

Válassza ki azt az adminisztrációs csoportot, amelybe áthelyezi a számítógépeket a Hálózati ügynök telepítését követően. A számítógépeket át kell helyezni adminisztrációs csoportba ahhoz, hogy alkalmazni lehessen rendszabályokat és csoportfeladatokat. Ha egy számítógép már tagja adminisztrációs csoportnak, a számítógépet nem lehet áthelyezni. Ha nem választ ki adminisztrációs csoportot, a számítógép az **Unassigned devices** csoportjához lesz hozzáadva.

9. lépés. Fiók kiválasztása az eszközök eléréshez

Válassza ki az operációs rendszer eszközeinek segítségével a Hálózati ügynök telepítéséhez használt fiókot. Ebben az esetben rendszergazda jogosultságok szükségesek a számítógép eléréséhez. Több fiókot is hozzáadhat. Ha a fióknak nincs elegendő jogosultsága, a telepítő varázsló a következő fiókot fogja használni. Ha a Hálózati ügynök használatával telepíti a Kaspersky Endpoint Security alkalmazást, akkor nem kell fiókot választania.

10. lépés. A telepítés megkezdése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Telepítőcsomag létrehozása

A *telepítőcsomag* fájlok egy csoportját jelenti, amik a Kaspersky alkalmazás távoli, Kaspersky Security Center-en keresztül történő telepítésére lettek létrehozva. A telepítőcsomag az alkalmazás telepítéséhez szükséges számos beállítást tartalmaz, a telepítés után ezeket egyből futtatja. A telepítőcsomag az alkalmazás forgalmazási készletben található, .kpd és .kud kiterjesztésű fájlok használatával lett létrehozva. A Kaspersky Endpoint Security telepítőcsomag a Windows támogatott verziói, valamint a processzor-architektúrák esetében is használatos.

Telepítőcsomag létrehozásának menete az Adminisztrációs Konzolon (MMC)

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Advanced** → **Remote installation** → **Installation packages** mappát.

   Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.

2. Kattintson az **Create installation package** gombra.

Elindul az Új csomag varázsló. Kövesse a varázsló utasításait.

1. lépés. A telepítőcsomag típusának kiválasztása

Válassza a **Create an installation package for a Kaspersky application** lehetőséget.

2. lépés A telepítőcsomag nevének megadása

Adja meg a telepítőcsomag nevét, például *Kaspersky Endpoint Security for Windows 14.1*.

3. lépés A terjesztőcsomag kiválasztása telepítéshez

Kattintson a **Tallózás** gombra, és válassza ki a `kes_win.kud` fájlt a terjesztőkészletben.

Szükség esetén frissítse a telepítőcsomagban elérhető víruskeresési adatbázist a **Copy updates from repository to installation package** négyzet bejelölésével.

4. lépés Végfelhasználói licencszerződés és Adatvédelmi szabályzat

Olvassa el és fogadja el a Végfelhasználói licencszerződést és az Adatvédelmi szabályzat kitételeit.

A rendszer létrehozza a telepítőcsomagot, és hozzáadja a Kaspersky Security Centerhez. A telepítőcsomag használatával telepítheti a Kaspersky Endpoint Security alkalmazást vállalati hálózati számítógépekre, valamint frissítheti az alkalmazás verzióját.

A telepítőcsomag beállításaiban kiválaszthatja az alkalmazásösszetevőket a különböző operációs rendszertípusokhoz. Ez azt jelenti, hogy a telepítőcsomag két összetevőkészletet tartalmaz: egyet a munkaállomásokhoz és egyet a kiszolgálókhoz. A telepítőcsomag telepítése előtt a telepítőprogram felismeri az operációs rendszer típusát, és csak azokat az alkalmazásösszetevőket telepíti, amelyeket az adott operációs rendszer típusához választott ki. Ily módon ugyanazt a telepítőcsomagot használhatja a munkaállomásokhoz és a kiszolgálókhoz.

A telepítőcsomag az Adminisztrációs kiszolgáló tárhelyének antivírus adatbázisait tartalmazza. Frissítheti a telepítőcsomagban lévő adatbázisokat, hogy csökkentse a forgalomhasználatot, miután a Kaspersky Endpoint Security telepítése után frissíti az adatbázisokat.

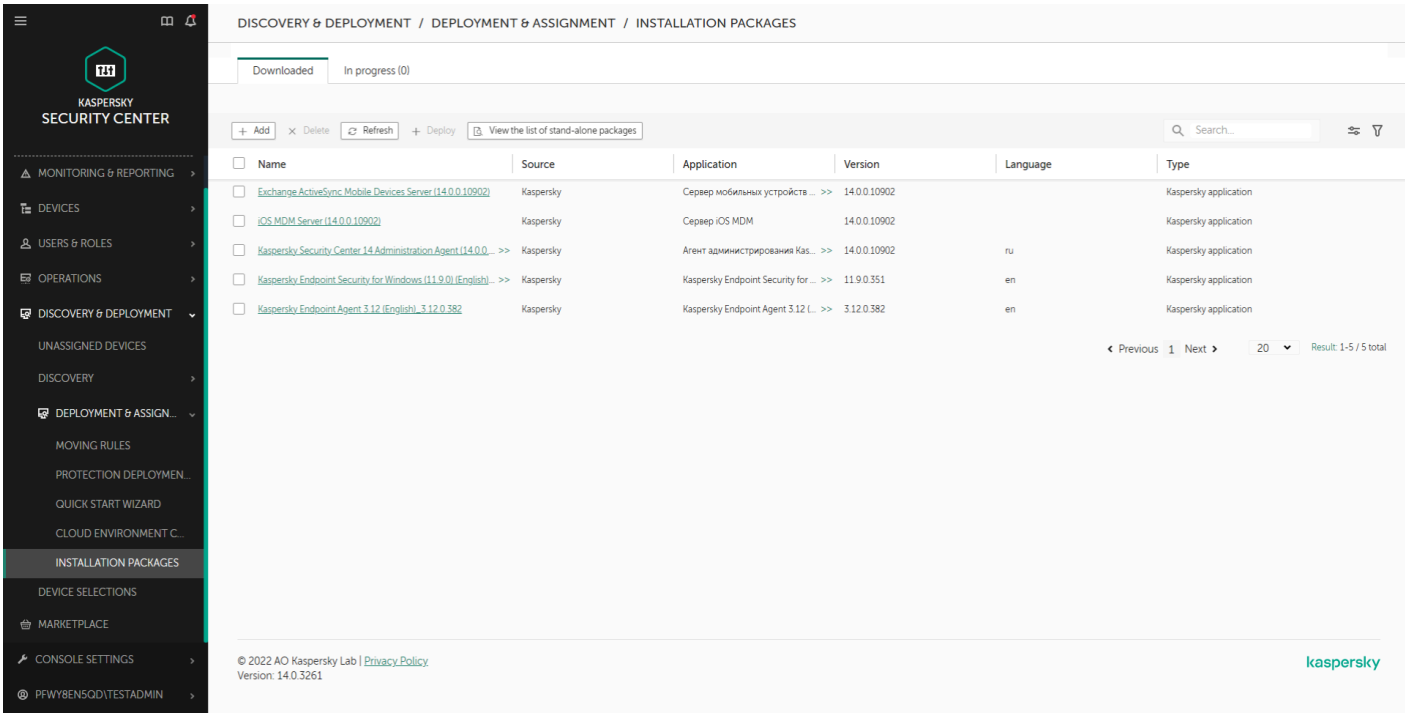
Telepítőcsomag létrehozásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza az **Discovery & deployment** → **Deployment & assignment** → **Installation packages** lehetőséget.

   Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.

2. Kattintson az **Add** gombra.

Elindul az Új csomag varázsló. Kövesse a varázsló utasításait.



A telepítőcsomagok listája

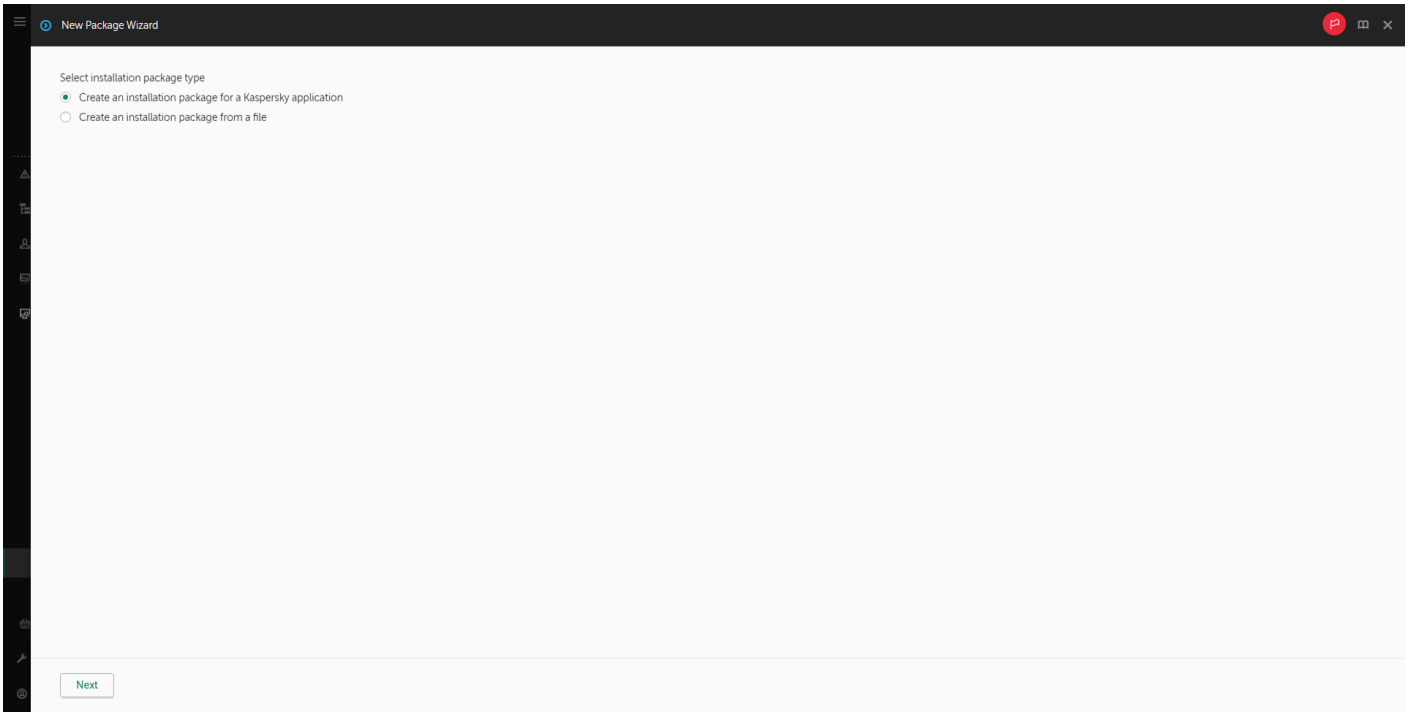
1. lépés. A telepítőcsomag típusának kiválasztása

Válassza a **Create an installation package for a Kaspersky application** lehetőséget.

A Varázsló létrehoz egy telepítőcsomagot a Kaspersky szervereken lévő terjesztőcsomagból. A lista automatikusan frissül, amint az alkalmazások új verziója elérhető. Ajánlott ezt az opciót választani a Kaspersky Endpoint Security telepítéséhez.

Létrehozhat telepítőcsomagot fájlból is.

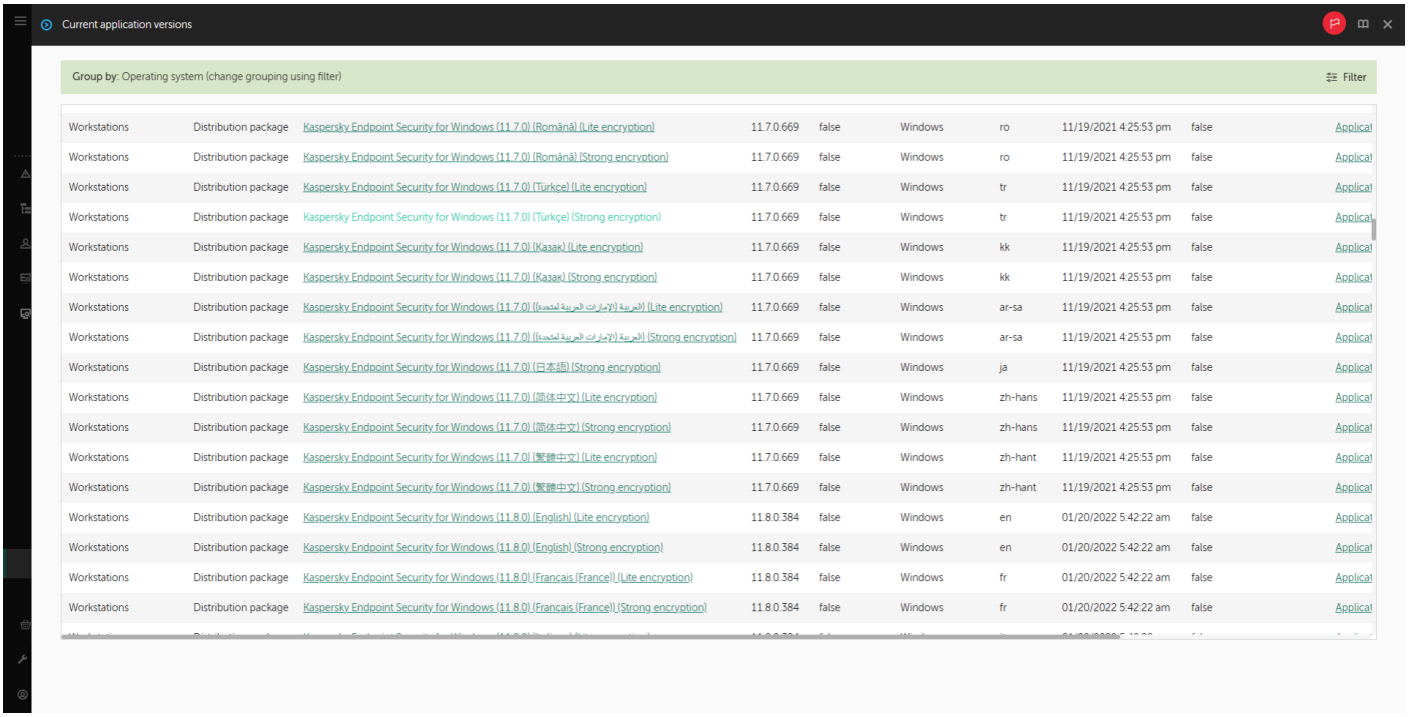
A Kaspersky Endpoint Security telepítőcsomagjának fájlból történő létrehozása kizárólag a Kaspersky Security Center Web Console-on érhető el.



A telepítőcsomagok típusai

2. lépés. A telepítőcsomagok megadása

Válassza ki a Kaspersky Endpoint Security for Windows telepítőcsomagot. Elindul a telepítőcsomag létrehozásának folyamata. A telepítőcsomag létrehozása közben el kell fogadnia a Végfelhasználói licencszerződés és az Adatvédelmi szabályzat feltételeit.

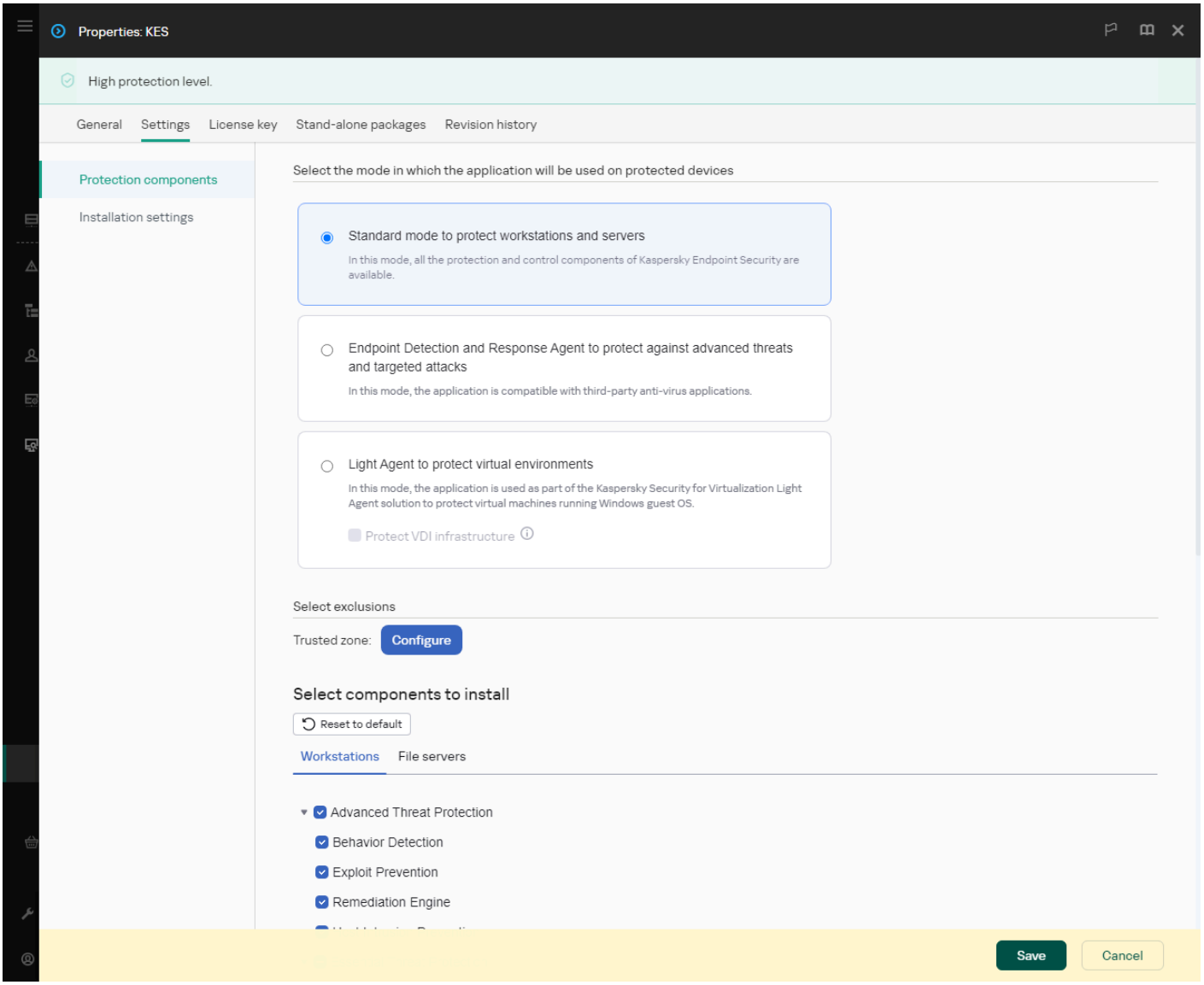


A Kaspersky-kiszolgálókon található telepítőcsomagok listája

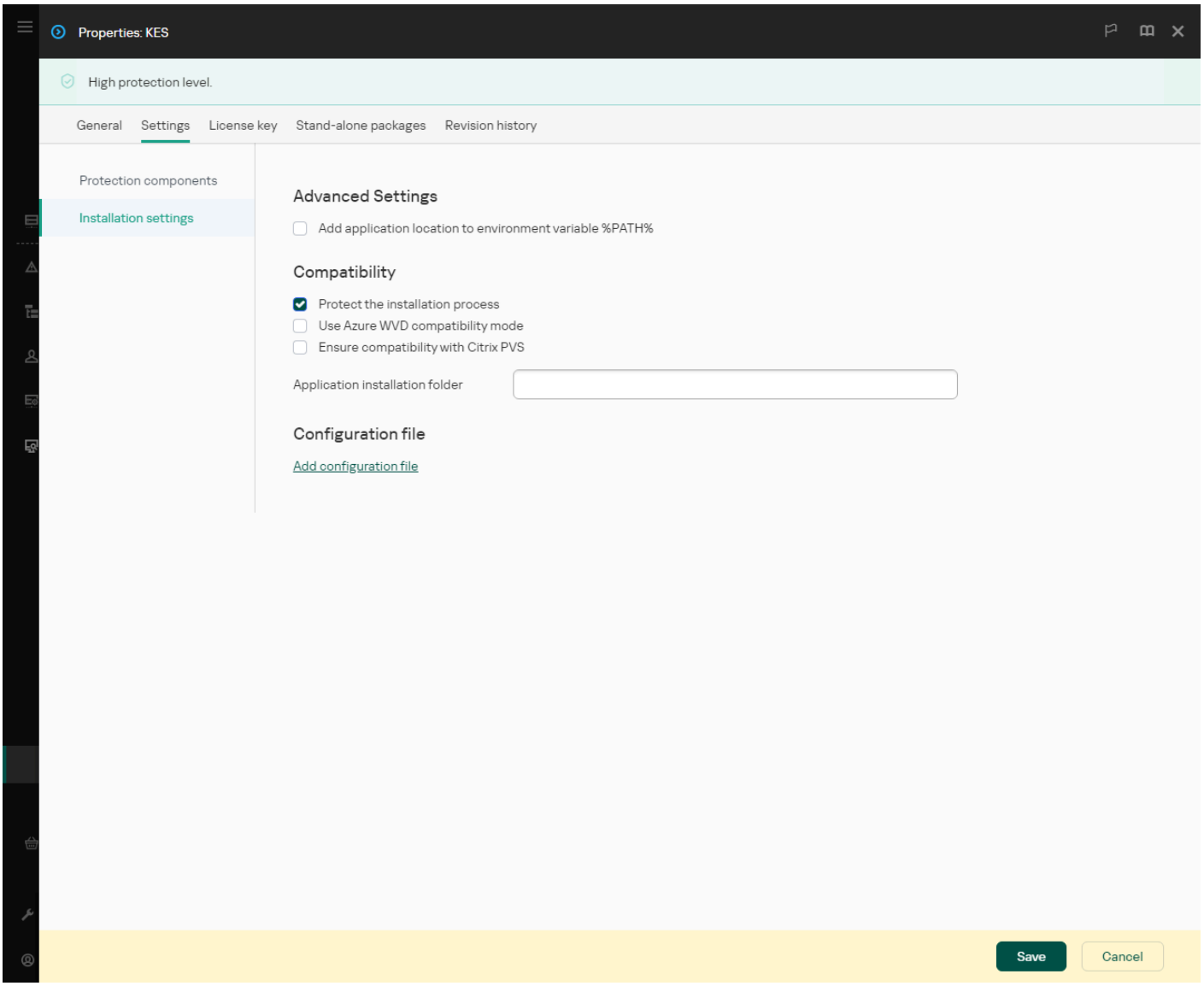
A rendszer létrehozza a telepítőcsomagot, és hozzáadja a Kaspersky Security Centerhez. A telepítőcsomag használatával telepítheti a Kaspersky Endpoint Security alkalmazást vállalati hálózati számítógépekre, valamint frissítheti az alkalmazás verzióját.

A telepítőcsomag beállításaiban kiválaszthatja az alkalmazásösszetevőket a különböző operációs rendszertípusokhoz. Ez azt jelenti, hogy a telepítőcsomag két összetevőkészletet tartalmaz: egyet a munkaállomásokhoz és egyet a kiszolgálókhoz. A telepítőcsomag telepítése előtt a telepítőprogram felismeri az operációs rendszer típusát, és csak azokat az alkalmazásösszetevőket telepíti, amelyeket az adott operációs rendszer típusához választott ki. Ily módon ugyanazt a telepítőcsomagot használhatja a munkaállomásokhoz és a kiszolgálókhoz.

A telepítőcsomag az Adminisztrációs kiszolgáló tárhelyének antivírus adatbázisait tartalmazza. Frissítheti a telepítőcsomagban lévő adatbázisokat, hogy csökkentse a forgalomhasználatot, miután a Kaspersky Endpoint Security telepítése után frissíti az adatbázisokat.



A telepítőcsomagban található összetevők



A telepítőcsomag telepítési beállításai

Telepítőcsomag beállítások

Rész	Leírás
Védelmi összetevők	**Standard mód**. Az alapértelmezett konfiguráció. Ez a konfiguráció lehetővé teszi az alkalmazás összes összetevőjének használatát, beleértve a Detection and Response megoldásokat támogató összetevőket is. Ez a konfiguráció a számítógép átfogó védelmére szolgál számos fenyegetés, hálózati támadás és csalás ellen. **Endpoint Detection and Response Agent**. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal. **Light Agent a virtuális környezetek védelme céljából**. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **VDI infrastruktúra védelme** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.
Kizárások	A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazást Light Agent üzemmódban is telepítheti a virtuális környezetek védelme céljából. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben. A megbízható zónát később a házirend tulajdonságaiban is beállíthatja: vizsgálati kizárások és megbízható alkalmazások.

Rész	Leírás
Válassza ki a telepítendő összetevőket	Ebben a részben kiválaszthatja az alkalmazás összetevőket, amik elérhetőek lesznek. Ön később módosíthatja az alkalmazásösszetevők készletét a *Change application components* feladattal. A munkaállomásokhoz és a kiszolgálókhoz külön összetevőkészleteket hozhat létre. A telepítőcsomag telepítése előtt a telepítőprogram felismeri az operációs rendszer típusát, és csak azokat az alkalmazásösszetevőket telepíti, amelyeket az adott operációs rendszer típusához választott ki. Ily módon ugyanazt a telepítőcsomagot használhatja a munkaállomásokhoz és a kiszolgálókhoz. Az elérhető összetevők készlete az alkalmazás konfigurációjától függ: **Standard mód** A BadUSB védelem összetevő, a Detection and Response összetevő és az adattitkosítási összetevők alapértelmezetten nincsenek telepítve. Ezek az összetevők a telepítőcsomag beállításaiban adhatók hozzá. **Endpoint Detection and Response Agent** Ebben a konfigurációban csak a Kaspersky Detection and Response megoldásainak beépített ügynökei érhetők el. **Light Agent a virtuális környezetek védelme céljából** Ebben a konfigurációban az adattitkosítási összetevők és az Adaptív Anomáliafelügyelő kivételével szinte az összes olyan alkalmazásösszetevő használható, amely a **Normál üzemmódú** konfigurációban is elérhető.
License key	Ezen a részen aktiválhatja az alkalmazást. Az alkalmazás aktiválásához ki kell választania egy licenckulcsot. Mielőtt ezt megtenné, hozzá kell adnia a kulcsot a felügyeleti kiszolgálóhoz. A Kaspersky Security Center felügyeleti kiszolgálójához történő kulcshozzáadáshoz lásd a Kaspersky Security Center Súgót.
Incompatible applications	Gondosan tekintse végig az inkompatibilis alkalmazások listáját, majd engedélyezze ezek eltávolítását. Ha a számítógépre inkompatibilis alkalmazások vannak telepítve, a Kaspersky Endpoint Security telepítése hibával ér véget.
Installation settings	**Adja hozzá az avp.com fájl elérési útját a %PATH% rendszerváltozóhoz**. A parancssori felület kényelmes használata érdekében hozzáadhatja a telepítés elérési útvonalát a %PATH% változóhoz. **Protect the installation process**. A telepítési védelembe tartozik a terjesztőcsomagok rosszindulatú alkalmazásokkal való kicserélése elleni védelem, a Kaspersky Endpoint Security telepítési mappái elérésének blokkolása, valamint az alkalmazáskulcsokat tartalmazó beállításjegyzék-rész elérésének blokkolása. Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni. **A Citrix PVS kompatibilitás biztosítása**. Engedélyezheti a Citrix Provisioning Services támogatását, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre telepítse. **Használja az Azure WVD-kompatibilitási módot**. Ez a funkció biztosítja az Azure virtuális gép állapotának megfelelő megjelenítését a Kaspersky Anti Targeted Attack Platform konzolon. A számítógép teljesítményének figyelése céljából a Kaspersky Endpoint Security telemetriai adatokat küld a KATA-kiszolgálóknak. A telemetria tartalmazza a számítógép azonosítóját (Sensor ID). Az Azure WVD-kompatibilitási mód lehetővé teszi állandó egyedi (Sensor ID) hozzárendelését ezekhez a virtuális gépekhez. Ha a kompatibilitási mód ki van kapcsolva, az Azure-beli virtuális gépek működése miatt az (Sensor ID). a számítógép újraindítása után megváltozhat. Ez azt eredményezheti, hogy a virtuális gépek duplikátumai jelennek meg a konzolon. **Application installation folder**. Megváltoztathatja a Kaspersky Endpoint Security telepítési útvonalát egy ügyfélszámítógépen. Alapértelmezés szerint az alkalmazás telepítési mappája a `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`. **Configuration file**. Az alkalmazás telepítése előre megadott beállításokkal. Ehhez fel kell töltenie egy fájlt, ami megszabja a Kaspersky Endpoint Security beállításait. Létrehozhat egy konfigurációs fájlt az alkalmazás helyi felületén.

Az adatbázisok frissítése a telepítőcsomagban

A telepítőcsomag az Adminisztrációs kiszolgáló tárhelyének antivírus adatbázisait tartalmazza, amelyek naprakészek a telepítőcsomag létrehozásakor. A telepítőcsomag létrehozásakor frissítheti az antivírus adatbázisokat a telepítőcsomagban. Ezzel csökkentheti az adatfogyasztást, ha a Kaspersky Endpoint Security telepítése után frissíti az antivírus adatbázisokat.

Az Adminisztrációs kiszolgáló tárhelyének antivírus adatbázisainak frissítéséhez használja az Adminisztrációs kiszolgáló *Download updates to the Administration Server repository* feladatát. Az Adminisztrációs kiszolgáló tárhelyén lévő vírusadatbázisok frissítéséről szóló további információért lásd a Kaspersky Security Center Súgót.

Csak az Adminisztrációs Konzol és a Kaspersky Security Center Web Console helyen frissítheti a telepítőcsomagok adatbázisait. Nem lehet frissíteni a telepítőcsomag adatbázisait a Kaspersky Security Center Cloud Console helyen.

A telepítőcsomagban tárolt antivírus adatbázisok frissítésének menete az Adminisztrációs Konzolon keresztül (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki a konzolfán az **Advanced** → **Remote installation** → **Installation packages** mappát.

   Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.
3. Nyissa meg a telepítőcsomag tulajdonságait.
4. Az **General** részen kattintson az **Update databases** lehetőségre.

Ennek eredményeképpen a telepítőcsomag antivírus adatbázisai frissülnek az Adminisztrációs kiszolgáló tárhelyén. A bases.cab részét képező `bases.cab` fájlt felülírja a `bases` mappa. A frissítőcsomag fájljai a mappában lesznek.

A telepítőcsomagban tárolt antivírus adatbázisok frissítésének menete a Web Console-on keresztül

1. A Web Console fő ablakában válassza az **Discovery & deployment** → **Deployment & assignment** → **Installation packages** lehetőséget.

   Ez megnyitja a Webfelügyelőre letöltött telepítőcsomagok listáját.
2. Kattintson annak a Kaspersky Endpoint Security telepítőcsomagnak a nevére, amiben frissíteni kívánja az antivírus adatbázisokat.

   Megnyílik a telepítőcsomag tulajdonságainak ablaka.
3. A **General information** lapon kattintson az **Update databases** hivatkozásra.

Ennek eredményeképpen a telepítőcsomag antivírus adatbázisai frissülnek az Adminisztrációs kiszolgáló tárhelyén. A bases.cab részét képező `bases.cab` fájlt felülírja a `bases` mappa. A frissítőcsomag fájljai a mappában lesznek.

Távoli telepítés feladat létrehozása

Az *Install application remotely* feladat a Kaspersky Endpoint Security távoli telepítésére szolgál. Az *Install application remotely* feladat lehetővé teszi az alkalmazás telepítőcsomagjának távoli telepítését a szervezet összes számítógépére. A telepítőcsomag távoli telepítése előtt lehetősége van frissíteni a antivírus adatbázisokat a csomagon belül, valamint kijelölni az elérhető alkalmazásösszetevőket a telepítőcsomag tulajdonságai között.

Távoli telepítési feladat létrehozása az Adminisztrációs Konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.
3. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza az **Kaspersky Security Center Administration Server → Install application remotely** lehetőséget.

2. lépés. A telepítőcsomag kiválasztása

Válassza ki a Kaspersky Endpoint Security telepítőcsomagot a listából. Ha a listában nem szerepel a Kaspersky Endpoint Security telepítőcsomagja, létrehozhatja azt a varázslóban.

A installation package settings a Kaspersky Security Centerben adhatja meg. Például kiválaszthatja az alkalmazás összetevőket, amik telepítve lesznek a számítógépre.

A rendszer a hálózati ügynököt is telepíti a Kaspersky Endpoint Security telepítésekor. A *Network Agent* végzi el az Adminisztrációs szerver és az ügyfélszámítógép közötti interakciót. Ha a Hálózati ügynök már telepítve van a számítógépre, akkor nem kell újra telepíteni.

3. lépés Egyebek

Válassza ki a Hálózati ügynök telepítőcsomagot. A Hálózati ügynök kiválasztott verziója, ami telepítve lesz a Kaspersky Endpoint Security mellett.

4. lépés Beállítások

Konfigurálja a következő további alkalmazásbeállításokat:

- **Force installation package download**. Válassza ki az alkalmazás telepítésének módszerét:
  - **Using Network Agent**. A hálózati ügynök felel a Kaspersky Endpoint Security telepítőcsomagjának az ügyfélszámítógépekre való eljuttatásáért. Ha a Hálózati ügynök összetevő nincs telepítve, a feladat hibával ér véget. Ebben az esetben adja hozzá a Hálózati ügynök telepítőcsomagot a *Install application remotely* feladathoz, és engedélyezze a fájlkézbesítést az operációs rendszer erőforrásain keresztül. Ezután a Hálózati ügynök telepítésre kerül az operációs rendszer erőforrásainak használatával. Ezután a Kaspersky Endpoint Security lesz telepítve a Hálózati ügynök eszközeivel.
  - **Using operating system resources through distribution points**. A telepítőcsomag az operációs rendszer erőforrásai használatával, a elosztói pontokon keresztül lesz elküldve a számítógépekre. Ezt az opciót akkor választhatja, ha legalább egy elosztói pont van a hálózatban. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Súgót.
  - **Using operating system resources through Administration Server**. A fájlok az operációs rendszer erőforrásaival továbbítva lesznek az ügyfél számítógépekre az Adminisztrációs kiszolgálón keresztül. Ezt az opciót akkor választhatja, ha nincs Hálózati ügynök telepítve az ügyfél számítógépen, és az ügyfél számítógép ugyanazon hálózaton van, mint az Adminisztrációs kiszolgáló.

- **Behavior for devices managed through other Administration Servers**. Válassza ki a Kaspersky Endpoint Security telepítésének módját. Ha a hálózaton több mint egy Adminisztrációs kiszolgáló van telepítve, akkor ezek az Adminisztrációs kiszolgálók láthatják ugyanazon ügyfélszámítógépeket. Ez okozhatja például, hogy egy alkalmazást távolról, többször kell telepíteni ugyanazon ügyfél számítógépeken különböző Adminisztrációs kiszolgálókon keresztül, valamint egyéb hibák is felléphetnek.

- **Do not re-install application if it is already installed**. Törölje ezt a jelölőnégyzetet, ha például az alkalmazás egy korábbi verzióját akarja telepíteni.

5. lépés Az operációs rendszer újraindítására vonatkozó beállítás megadása

Adja meg, hogy a rendszer milyen műveletet hajtson végre, ha a számítógép újraindítása szükségessé válik. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.

6. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki a számítógépeket a Kaspersky Endpoint Security telepítéséhez. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.

- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. A Hálózati ügynök nincs telepítve a hozzá nem rendelt eszközökön. Ebben az esetben a feladat bizonyos eszközökhöz lesz hozzárendelve. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.

- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

7. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válassza ki az operációs rendszer eszközeinek segítségével a Hálózati ügynök telepítéséhez használt fiókot. Ebben az esetben rendszergazda jogosultságok szükségesek a számítógép eléréséhez. Több fiókot is hozzáadhat. Ha a fióknak nincs elegendő jogosultsága, a telepítő varázsló a következő fiókot fogja használni. Ha a Hálózati ügynök használatával telepíti a Kaspersky Endpoint Security alkalmazást, akkor nem kell fiókot választania.

8. lépés Feladatindítási ütemezés konfigurálása

Állítson be ütemezést egy adott feladat elindításához, például kézi indítást vagy a számítógép tétlen időszakára esőt.

9. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *Kaspersky Endpoint Security for Windows 14.1 telepítése*.

10. lépés. A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Az alkalmazás csendes módban lesz telepítve. A telepítés után az ikon lesz hozzáadva a felhasználó számítógépének értesítési területéhez. Az ikon a következőképpen néz ki: , így győződjön meg arról, hogy aktiválta az alkalmazást.

Távoli telepítési feladat létrehozásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. A **Application** legördülő listából válassza ki az **Kaspersky Security Center** lehetőséget.
2. A **Task type** legördülő listából válassza ki az **Install application remotely** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *A Kaspersky Endpoint Security telepítése kezelőkhöz*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

2. lépés. Számítógépek kiválasztása a telepítéshez

Ennél a lépésnél a kiválasztott feladathatókör alapján válassza ki a számítógépeket, amikre telepíti a Kaspersky Endpoint Security alkalmazást.

3. lépés. A telepítőcsomag megadása

Ennél a lépésnél konfigurálja a telepítőcsomagot:

1. Válassza ki a Kaspersky Endpoint Security for Windows (14.1) telepítőcsomagot.

2. Válassza ki a Hálózati ügynök telepítőcsomagot.

   A Hálózati ügynök kiválasztott verziója, ami telepítve lesz a Kaspersky Endpoint Security mellett. A *Network Agent* végzi el az Adminisztrációs szerver és az ügyfélszámítógép közötti interakciót. Ha a Hálózati ügynök már telepítve van a számítógépre, akkor nem kell újra telepíteni.

3. A **Force installation package download** blokkban válassza ki az alkalmazás telepítésének módját:

   - **Using Network Agent**. A hálózati ügynök felel a Kaspersky Endpoint Security telepítőcsomagjának az ügyfélszámítógépekre való eljuttatásáért. Ha a Hálózati ügynök összetevő nincs telepítve, a feladat hibával ér véget. Ebben az esetben adja hozzá a Hálózati ügynök telepítőcsomagot a *Install application remotely* feladathoz, és engedélyezze a fájlkézbesítést az operációs rendszer erőforrásain keresztül. Ezután a Hálózati ügynök telepítésre kerül az operációs rendszer erőforrásainak használatával. Ezután a Kaspersky Endpoint Security lesz telepítve a Hálózati ügynök eszközeivel.

   - **Using operating system resources through distribution points**. A telepítőcsomag az operációs rendszer erőforrásai használatával, a elosztói pontokon keresztül lesz elküldve a számítógépekre. Ezt az opciót akkor választhatja, ha legalább egy elosztói pont van a hálózatban. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Súgót.

   - **Using operating system resources through Administration Server**. A fájlok az operációs rendszer erőforrásaival továbbítva lesznek az ügyfél számítógépekre az Adminisztrációs kiszolgálón keresztül. Ezt az opciót akkor választhatja, ha nincs Hálózati ügynök telepítve az ügyfél számítógépen, és az ügyfél számítógép ugyanazon hálózaton van, mint az Adminisztrációs kiszolgáló.

4. Az **Maximum number of concurrent downloads** mezőben állítson be egy korlátot az Adminisztrációs kiszolgálóra küldhető telepítőcsomag-letöltési kérelmekhez. A kérelmek számának korlátja segít megelőzni a hálózat túlterhelését.

5. A **Maximum number of installation attempts** mezőben állítsa be az alkalmazás-telepítési kísérletek számának korlátértékét. Ha a Kaspersky Endpoint Security telepítése hibával ér véget, a feladat automatikusan elindítja újra a telepítést.

6. Ha szükséges, törölje a jelölést a **Do not re-install application if it is already installed** jelölőnégyzetből. Például engedélyezi az alkalmazás egyik előző verziójának telepítését.

7. Ha szükséges, törölje a jelölést a **Verify operating system type before downloading** jelölőnégyzetből. Ezzel megelőzheti az alkalmazás terjesztőcsomag letöltését, ha a számítógép operációs rendszere nem felel meg a szoftverkövetelményeknek. Ha biztos benne, hogy a számítógépe operációs rendszere megfelel a szoftverkövetelményeknek, akkor kihagyhatja ezt a hitelesítést.

8. Ha szükséges, tegyen jelölést a **Assign package installation in Active Directory group policies** jelölőnégyzetbe. A Kaspersky Endpoint Security a Hálózati Ügynökkel vagy kézileg, az Active Directory segítségével van telepítve. A Hálózati ügynök telepítéséhez tartomány adminisztrációs jogosultsággal kell futtatni a távoli telepítés feladatot.

9. Ha szükséges, tegyen jelölést a **Prompt users to close running applications** jelölőnégyzetbe. A Kaspersky Endpoint Security telepítése számítógépes erőforrásokat használ fel. A felhasználó kényelme érdekében az Alkalmazás telepítési varázsló figyelmezteti, hogy zárja be a futó alkalmazásokat, mielőtt elindítja a telepítést. Ezzel megelőzheti, hogy más alkalmazások működése megzavarja a telepítést, valamint megakadályozza a számítógép meghibásodását.

10. A **Behavior for devices managed through other Administration Servers** blokkban válassza ki a Kaspersky Endpoint Security telepítésének módját. Ha a hálózaton több mint egy Adminisztrációs kiszolgáló van telepítve, akkor ezek az Adminisztrációs kiszolgálók láthatják ugyanazon ügyfélszámítógépeket. Ez okozhatja például, hogy egy alkalmazást távolról, többször kell telepíteni ugyanazon ügyfél számítógépeken különböző Adminisztrációs kiszolgálókon keresztül, valamint egyéb hibák is felléphetnek.

4. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válassza ki az operációs rendszer eszközeinek segítségével a Hálózati ügynök telepítéséhez használt fiókot. Ebben az esetben rendszergazda jogosultságok szükségesek a számítógép eléréséhez. Több fiókot is hozzáadhat. Ha a fióknak nincs elegendő jogosultsága, a telepítő varázsló a következő fiókot fogja használni. Ha a Hálózati ügynök használatával telepíti a Kaspersky Endpoint Security alkalmazást, akkor nem kell fiókot választania.

5. lépés A feladat létrehozásának befejezése

Fejezze be a varázslót a **Finish** gombra való kattintással. Egy új feladat jelenik meg a feladatok listájában. A feladat futtatásához jelölje be a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra. Az alkalmazás csendes módban lesz telepítve. A telepítés után az ikon lesz hozzáadva a felhasználó számítógépének értesítési területéhez. Az ikon a következőképp néz ki: , így győződjön meg arról, hogy aktiválta az alkalmazást.

Az alkalmazás telepítése helyben, a Varázsló segítségével

A Telepítővarázsló alkalmazás felülete az alkalmazás telepítési lépéseinek megfelelő ablakok sorozatából áll. Ellenőrizze, hogy a felhasználói fiók, amellyel a Telepítővarázslót futtatja, rendszergazdai csoportban van-e.

Az alkalmazás telepítése, illetve korábbi verziójának frissítése a Telepítővarázsló segítségével:

1. Másolja a terjesztőkészlet mappáját a felhasználó számítógépére.

2. Futtassa a setup_kes.exe fájlt.

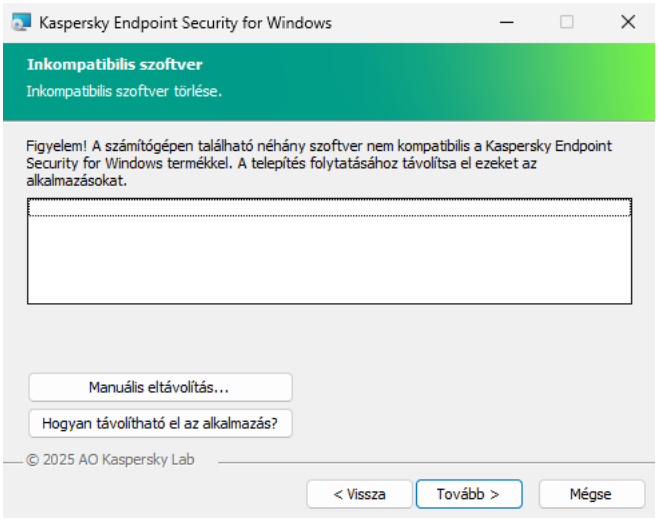
   A Telepítővarázsló elindul.

Felkészülés a telepítésre

A Kaspersky Endpoint Security számítógépen való telepítését, illetve az alkalmazás korábbi verziójának frissítését megelőzően az alábbi feltételeket ellenőrzi a rendszer:

- Van-e telepítve olyan szoftver, amelynek kompatibilitási problémái lehetnek a Kaspersky Endpoint Security-vel (a szoftverek listája a disztribúciós készletben található incompatible.txt fájlban érhető el).
- Teljesülnek-e a hardver- és szoftverkövetelmények.
- A Microsoft .NET Framework jelenléte.
- A felhasználó jogosult-e a szoftvertermék telepítésére.

Ha a fenti feltételek közül bármelyik nem teljesül, a képernyőn ezt jelző értesítés jelenik meg. Például egy értesítés az inkompatibilis szoftverről (lásd az alábbi ábrát).



Inkompatibilis szoftverek eltávolítása

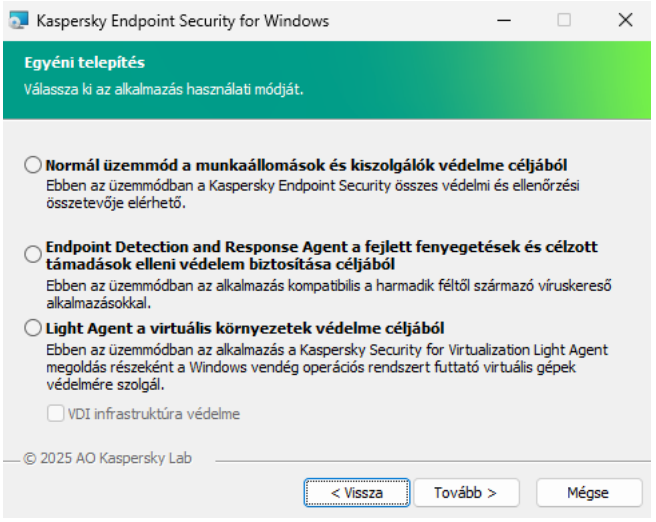
Ha a számítógép teljesíti a felsorolt követelményeket, a Telepítővarázsló megkeresi azokat a Kaspersky alkalmazásokat, amelyek ütközésekhez vezethetnek, ha az alkalmazás telepítésével egy időben futnak. Ha ilyen alkalmazást talál, a telepítő felkéri, hogy távolítsa el kézileg.

Ha az észlelt alkalmazások között megtalálhatók a Kaspersky Endpoint Security korábbi verziói, akkor minden áttelepíthető adat a Kaspersky Endpoint Security 14.1 for Windows telepítése során megőrzésre és felhasználásra kerül (köztük az aktiválási adatok és az alkalmazás beállításai), és az alkalmazás korábbi verziója automatikusan törlődik. Ez az alábbi alkalmazásverziókra vonatkozik:

- Kaspersky Endpoint Security 12.1 for Windows (12.1.0.506 számú build)
- Kaspersky Endpoint Security 12.2 for Windows (12.2.0.462 számú build)
- Kaspersky Endpoint Security 12.3 for Windows (12.3.0.493 számú build)
- Kaspersky Endpoint Security 12.4 for Windows (12.4.0.467 számú build)
- Kaspersky Endpoint Security 12.5 for Windows (12.5.0.539 számú build)
- Kaspersky Endpoint Security 12.6 for Windows (12.6.0.438 számú build)

- Kaspersky Endpoint Security 12.7 for Windows (12.7.0.533 számú build)
- Kaspersky Endpoint Security 12.8 for Windows (12.8.0.505 számú build)
- Kaspersky Endpoint Security 12.9 for Windows (12.9.0.384 számú build)
- Kaspersky Endpoint Security 12.10 for Windows (12.10.0.466 számú build)
- Kaspersky Endpoint Security 12.11 for Windows (12.11.0.637 számú build)
- Kaspersky Endpoint Security 12.12 for Windows (12.12.0.522 számú build)
- Kaspersky Endpoint Security 14.0 for Windows (14.0.0.504 számú build)

A Kaspersky Endpoint Security konfigurációja



Az alkalmazás konfigurációjának kiválasztása

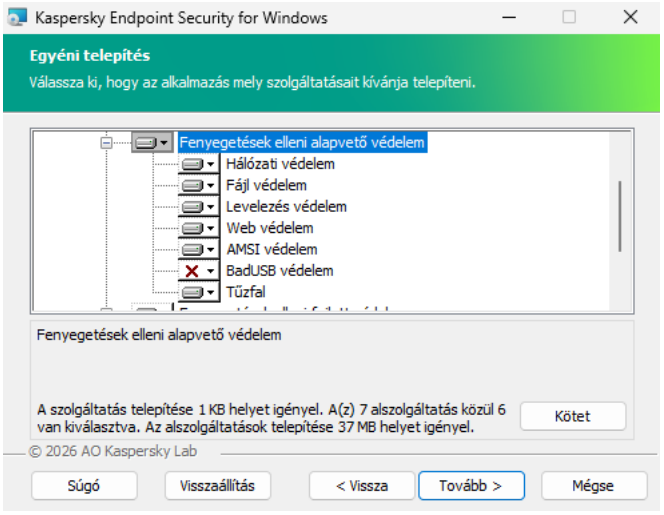
Standard mód. Az alapértelmezett konfiguráció. Ez a konfiguráció lehetővé teszi az alkalmazás összes összetevőjének használatát, beleértve a Detection and Response megoldásokat támogató összetevőket is. Ez a konfiguráció a számítógép átfogó védelmére szolgál számos fenyegetés, hálózati támadás és csalás ellen.

Endpoint Detection and Response Agent. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.

Light Agent a virtuális környezetek védelme céljából. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **VDI infrastruktúra védelme** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.

Kaspersky Endpoint Security összetevők

A telepítés során kiválaszthatja a Kaspersky Endpoint Security telepíteni kívánt összetevőit (lásd az alábbi ábrát). A Fájl védelem egy kötelezően telepítendő összetevő. Telepítését nem lehet törölni.



Alkalmazásösszetevők kiválasztása a telepítéshez

Alapértelmezés szerint az alábbi összetevők kivételével az összes alkalmazásösszetevő telepítése ki van választva:

- BadUSB védelem.
- Adattitkosítási összetevők.
- Detection and Response összetevők.

Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket. Ehhez futtatnia kell a Telepítővarázslót, és ki kell választania az elérhető összetevőket.

Ha telepítenie kell a Detection and Response összetevőket, a Kaspersky Endpoint Security a következő konfigurációkat támogatja:

- Csak Endpoint Detection and Response Optimum
- Csak Endpoint Detection and Response Expert (cloud)
- Csak Endpoint Detection and Response Expert (on-premises)
- Csak Network Detection and Response (KATA)
- Csak Sandbox
- Endpoint Detection and Response Optimum és Sandbox
- Endpoint Detection and Response Expert (cloud) és Sandbox
- Endpoint Detection and Response Expert (on-premises) és Sandbox

- Network Detection and Response (KATA) és Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) és Managed Detection and Response

A Kaspersky Endpoint Security az alkalmazás telepítése előtt ellenőrzi az összetevők kiválasztását. Ha a Detection and Response összetevők kiválasztott konfigurációja nem támogatott, a Kaspersky Endpoint Security nem telepíthető.

Az alkalmazás telepítési mappájának kiválasztása

Megváltoztathatja a Kaspersky Endpoint Security telepítési útvonalát egy ügyfélszámítógépen. Alapértelmezés szerint az alkalmazás telepítési mappája a `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`.

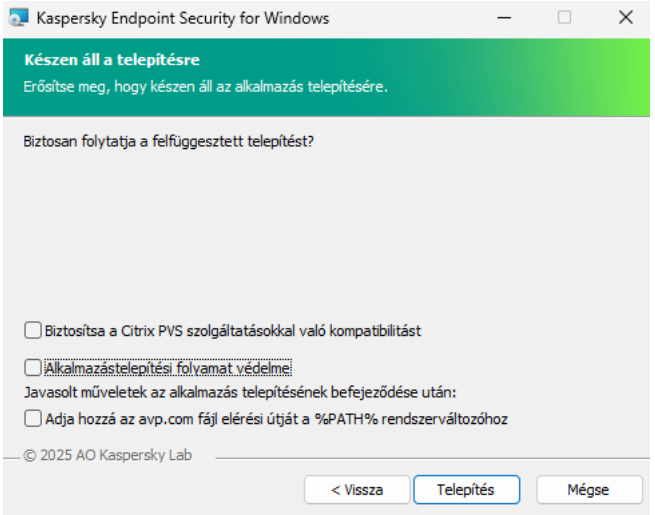
A megbízható zóna konfigurálása

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon.

A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazást Light Agent üzemmódban is telepítheti a virtuális környezetek védelme céljából. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben.

A megbízható zónát később a házirend tulajdonságaiban is beállíthatja: vizsgálati kizárások és megbízható alkalmazások.

Speciális beállítások



Alkalmazás telepítési beállításai

Alkalmazástelepítési folyamat védelme. A telepítési védelembe tartozik a terjesztőcsomagok rosszindulatú alkalmazásokkal való kicserélése elleni védelem, a Kaspersky Endpoint Security telepítési mappái elérésének blokkolása, valamint az alkalmazáskulcsokat tartalmazó beállításjegyzék-rész elérésének blokkolása. Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni.

A Citrix PVS kompatibilitás biztosítása. Engedélyezheti a Citrix Provisioning Services támogatását, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre telepítse.

Adja hozzá az avp.com fájl elérési útját a %PATH% rendszerváltozóhoz. A parancssori felület kényelmes használata érdekében hozzáadhatja a telepítés elérési útvonalát a %PATH% változóhoz.

Az alkalmazás távoli telepítése a Rendszerközpont beállításkezelő segítségével

Ezek az utasítások a System Center Configuration Manager 2012 R2-re vonatkoznak.

Alkalmazás távoli telepítése a Rendszerközpont beállításkezelő segítségével:

1. Nyissa meg a Konfigurációkezelő konzolt.
2. A konzol jobb oldalán lévő **Application management** részben válassza ki a **Csomagok** lehetőséget.
3. A vezérlőpulton lévő konzol felső részén kattintson a **Create package** gombra.
   Ezzel elindul az *Új csomag és alkalmazás varázsló*.
4. Az Új csomag és alkalmazás varázslóban:
   a. A **Csomag** részben:
      - A **Név** mezőbe írja be a telepítőcsomag nevét.
      - Adja meg a **Forrásmappa** mezőben a Kaspersky Endpoint Security terjesztőcsomagját tartalmazó mappa elérési útját.
   b. Az **Alkalmazás típusa** részben válassza ki a **Standard program** lehetőséget.
   c. A **Standard program** részben:
      - Írja be a **Név** mezőbe a telepítőcsomag egyedi nevét (például az alkalmazás nevét a verzióval együtt).
      - Adja meg a **Parancssor** mezőben a Kaspersky Endpoint Security parancssori telepítési beállításait.
      - Kattintson a **Tallózás** gombra az alkalmazás végrehajtható fájlja elérési útjának megadásához.
      - Győződjön meg arról, hogy a **Futtatás módja** listán ki van választva a **Futtatás rendszergazdai jogosultságokkal** elem.

d. A **Követelmények** részben:

- Jelölje be az **Először egy másik program futtatása** jelölőnégyzetet, ha a Kaspersky Endpoint Security telepítése előtt egy másik alkalmazást szeretne elindítani.

  Válassza ki az alkalmazást az **Alkalmazás** legördülő listán, vagy adja meg az alkalmazás végrehajtható fájljának elérési útját a **Tallózás** gombra kattintva.

- Válassza ki az **Ez a program csak a megadott platformokon futtatható** lehetőséget a **Platformkövetelmények** részben, ha azt szeretné, hogy az alkalmazást csak a meg adott operációs rendszereken lehessen telepíteni.

  Jelölje be a lenti listán a jelölőnégyzeteket azokkal az operációs rendszerekkel szemben, amelyeken a Kaspersky Endpoint Security telepíthető lesz.

Ez a lépés nem kötelező.

e. Ellenőrizze az **Összegzés** részben a beállítások összes megadott értékét, majd kattintson a **Tovább** gombra.

A létrehozott telepítőcsomag felbukkan a rendelkezésre álló telepítőcsomagok listáján a **Csomagok** részben.

5. A telepítőcsomag helyi menüjében válassza ki az **Üzembehelyezés** elemet.

   Ezzel elindul az *Üzembehelyezési varázsló*.

6. Az Üzembehelyezési varázslóban:

   a. Az **Általános** részben:

   - Adja meg a **Szoftver** mezőben a telepítőcsomag egyedi nevét, vagy válassza ki a telepítőcsomagot a listáról a **Tallózás** gombra kattintva.

   - Adja meg a **Gyűjtemény** mezőben azon számítógépek gyűjteményét, amelyeken az alkalmazás telepítése megtörténik, vagy válassza ki a gyűjteményt a **Tallózás** gombra kattintva.

   b. Adjon meg a **Tartalmaz** részben terjesztési pontokat (részletesebb információ a Rendszerközpont beállításkezelő súgódokumentációjában található).

   c. Szükség esetén adja meg az Üzembehelyezési varázslóban a többi beállítás értékeit. Ezek a beállítások a Kaspersky Endpoint Security távoli telepítése esetén nem kötelezők.

   d. Ellenőrizze az **Összegzés** részben a beállítások összes megadott értékét, majd kattintson a **Tovább** gombra.

   Az Üzembehelyezési varázsló befejeződését követően a Kaspersky Endpoint Security távoli telepítéséhez egy feladat jön létre.

A setup.ini fájl telepítései beállításainak leírása

A setup.ini fájlt a rendszer az alkalmazás parancssori telepítésekor, illetve a Microsoft Windows Group Policy Editorának használatakor használja. Ahhoz, hogy alkalmazza a beállításokat a setup.ini fájlból, helyezze ezt a fájlt a Kaspersky Endpoint Security terjesztőcsomagot tartalmazó mappába.

A setup.ini fájlt csak akkor használja, ha az alkalmazást csendes módban telepíti.

Nem adhat hozzá elérési utat a install.cfg konfigurációs fájlhoz a setup.ini fájlban. Az alkalmazás továbbá figyelmen kívül hagyja az install.cfg konfigurációs fájlt, ha az a Kaspersky Endpoint Security telepítőcsomaggal azonos mappában található. A(z) install.cfg konfigurációs fájlból származó beállítások alkalmazásához, meg kell adnia a fájl elérési útját a következő alkalmazástelepítési parancsban: `CONFIGPATH=<path to the configuration file>`.

TÖLTSE LE A SETUP.INI FÁJLT

A setup.ini fájl a következő részekből áll:

- `[Setup]` – az alkalmazástelepítés általános beállításai.
- `[Components]` – a Standard módban telepítendő alkalmazásösszetevők kiválasztása. Ha egyik összetevő sincs megadva, akkor az operációs rendszeren rendelkezésre álló összes összetevő telepítésére sor kerül. A Fájl védelem egy kötelező összetevő, és az ebben a részben megadott beállításoktól függetlenül sor kerül telepítésére a számítógépen.
- `[Tasks]` – a Kaspersky Endpoint Security feladatainak listájára felvenni kívánt feladatok kiválasztása. Ha nincs megadva egy feladat sem, az összes feladat felkerül a Kaspersky Endpoint Security feladatainak listájára.

A `1` érték alternatívái a `yes`, `on`, `enable`, `enabled` és `true` értékek. A `0` érték alternatívái a `no`, `off`, `disable`, `disabled` és `false` értékek.

A setup.ini fájl beállításai

Rész	Paraméter	Leírás
`[Setup]`	`InstallDir`	Az alkalmazás telepítési mappájának elérési útja.
	`ActivationCode`	Kaspersky Endpoint Security aktiváló kód.
	`Eula`	A Végfelhasználói licencszerződés feltételeinek elfogadása. A Licencszerződés szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. A Végfelhasználói licencszerződés feltételeit az alkalmazás telepítéséhez, illetve verziójának frissítéséhez kötelező elfogadni.

Rész	Paraméter	Leírás
	`PrivacyPolicy`	Az Adatvédelmi szabályzat elfogadása. Az Adatvédelmi szabályzat szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. Az alkalmazás telepítéséhez, vagy a verziója frissítéséhez el kell fogadnia az Adatvédelmi szabályzatot.
	`KSN`	A Kaspersky Security Network (KSN) való részvétel elfogadása vagy elutasítása. Ha nincs megadott érték a paraméterhez, a Kaspersky Endpoint Security kérni fogja, hogy erősítse meg a KSN-ben való részvételének hozzájárulását vagy elutasítását, amikor a Kaspersky Endpoint Security először elindul. Választható értékek: • `1` – a KSN-ben való részvétel elfogadása. • `0` – a KSN-ben való részvétel elutasítása (alapértelmezett érték). A Kaspersky Endpoint Security terjesztőcsomag a with Kaspersky Security Networkkel való használatra van optimalizálva. Ha úgy döntött, hogy nem vesz részt a Kaspersky Security Networkben, a telepítés befejezését követően azonnal frissítenie kell a Kaspersky Endpoint Security rendszert.
	`CLEANERSIGNCHECK`	Az incompatible.txt listán szereplő, észlelt szoftverfájlok digitális aláírásának ellenőrzése. A szoftver eltávolításához a Kaspersky Endpoint Security futtatja a szoftvertelepítő fájlt. Ha a telepítőfájl nem rendelkezik digitális aláírással, a Kaspersky Endpoint Security nem tekinti a fájlt megbízhatónak, és leállítja a szoftver eltávolítását, hogy elkerülje a potenciálisan rosszindulatú kód futtatását. Ha az alkalmazás nem tudja ellenőrizni az észlelt szoftverfájl digitális aláírását, a Kaspersky Endpoint Security telepítése hibával leáll. Az alapértelmezett érték a szoftvertelepítési módtól függően eltérő: • `0` azt jelenti, hogy a digitális aláírás ellenőrzése le van tiltva (alapértelmezett érték, ha a Kaspersky Security Centeren keresztül telepíti). • `1` azt jelenti, hogy a digitális aláírás ellenőrzése engedélyezve van (alapértelmezett érték, ha az alkalmazást helyileg telepíti).
	`Login`	Állítsa be a felhasználónevet a Kaspersky Endpoint Security funkcióinak és beállításainak eléréséhez (a Jelszóvédelem összetevő). A felhasználónevet a `Password` és a `PasswordArea` paraméterekkel együtt kell megadni. Alapértelmezetten a KLAdmin felhasználónév van használva.
	`Password`	A Kaspersky Endpoint Security funkcióihoz és beállításaihoz való hozzáférés jelszavának megadása (a jelszót a `Login` és a `PasswordArea` paraméterekkel együtt kell megadni). Ha a `Login` paraméternél jelszót megadott, de felhasználónevet nem, alapértelmezés szerint a rendszer a KLAdmin felhasználónevet használja.
	`PasswordArea`	A Kaspersky Endpoint Security-hez való hozzáférési jelszó hatókörének megadása. Ha a felhasználó megpróbál végrehajtani egy olyan tevékenységet, ami beletartozik ebbe a hatókörbe, a Kaspersky Endpoint Security kérni fogja a felhasználó fiókjának bejelentkezési adatait (`Login` és `Password` paraméterek). Használja a `;` karaktert több érték megadásához. Választható értékek: • `SET` – az alkalmazásbeállítások módosítása. • `EXIT` – kilépés az alkalmazásból. • `DISPROTECT` – védelem összetevőinek letiltása és a vizsgálati feladatok leállítása. • `DISPOLICY` – a Kaspersky Security Center rendszabályának letiltása. • `UNINST` – az alkalmazás eltávolítása a számítógépről. • `DISCTRL` – a felügyeleti összetevők kikapcsolása. • `REMOVELIC` – a kulcs eltávolítása. • `REPORTS` – a jelentések megtekintése. • `EXPORT` – alkalmazásbeállítások exportálása. Például: `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Az alkalmazástelepítés védelmi mechanizmusának engedélyezése és letiltása. Választható értékek: • `1` – az alkalmazástelepítés védelmi mechanizmusa engedélyezve van (alapértelmezett érték). • `0` – az alkalmazástelepítés védelmi mechanizmusa nincs engedélyezve. A telepítési védelembe tartozik a terjesztőcsomagok rosszindulatú alkalmazásokkal való kicserélése elleni védelem, a Kaspersky Endpoint Security telepítési mappái elérésének blokkolása, valamint az alkalmazáskulcsokat tartalmazó beállításjegyzék-rész elérésének blokkolása. Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni.

Rész	Paraméter	Leírás
	PROTECTOSSERVICES	Az operációs rendszer szolgáltatásainak védelme. Az operációs rendszer szolgáltatásainak védelme megakadályozza, hogy harmadik féltől származó alkalmazások beavatkozzanak az operációs rendszer szolgáltatásainak működésébe. Ilyen szolgáltatások közé tartozik például az alkalmazás automatikus indítási szolgáltatása. • Az `1` azt jelenti, hogy az operációs rendszer szolgáltatásainak védelme engedélyezve van (alapértelmezett érték). • A `0` azt jelenti, hogy az operációs rendszer szolgáltatásainak védelme le van tiltva.
	EnableAzureSupport	Az Azure WVD-kompatibilitási mód engedélyezése vagy letiltása. Választható értékek: • `1` – az Azure WVD-kompatibilitási mód engedélyezve van. • `0` – az Azure WVD-kompatibilitási mód le van tiltva (alapértelmezett érték). Ez a funkció biztosítja az Azure virtuális gép állapotának megfelelő megjelenítését a Kaspersky Anti Targeted Attack Platform konzolon. A számítógép teljesítményének figyelése céljából a Kaspersky Endpoint Security telemetriai adatokat küld a KATA-kiszolgálóknak. A telemetria tartalmazza a számítógép azonosítóját (Sensor ID). Az Azure WVD-kompatibilitási mód lehetővé teszi állandó egyedi (Sensor ID) hozzárendelését ezekhez a virtuális gépekhez. Ha a kompatibilitási mód ki van kapcsolva, az Azure-beli virtuális gépek működése miatt az (Sensor ID). a számítógép újraindítása után megváltozhat. Ez azt eredményezheti, hogy a virtuális gépek duplikátumai jelennek meg a konzolon.
	Reboot	A számítógép automatikus újraindítása, ha szükséges az alkalmazás telepítése vagy frissítése után. Ha nincs érték megadva ehhez a paraméterhez, blokkolva lesz a számítógép automatikus újraindítása. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.
	AddEnvironment	Kiegészíti a %PATH% rendszerváltozót a Kaspersky Endpoint Security telepítési mappájában lévő végrehajtható fájlok elérési útjával. Választható értékek: • `1` – a %PATH% rendszerváltozó kiegészül a Kaspersky Endpoint Security telepítési mappájában lévő végrehajtható fájlok elérési útjával. • `0` – a %PATH% rendszerváltozó nem egészül ki a Kaspersky Endpoint Security telepítési mappájában lévő végrehajtható fájlok elérési útjával.
	AMPPL	Engedélyezi vagy kikapcsolja a Kaspersky Endpoint Security folyamatok védelmét az AM-PPL technológiával (Antimalware Protected Process Light). Az AM-PPL technológia részleteiért lásd a Microsoft weboldalt. Az AM-PPL technológia a Windows 10 1703-as (RS2) vagy újabb verziói, valamint a Windows Server 2019 operációs rendszerek számára érhető el. Választható értékek: • `1` – a Kaspersky Endpoint Security folyamatok AM-PPL technológiával történő védelme engedélyezve van. • `0` – a Kaspersky Endpoint Security folyamatok AM-PPL technológiával történő védelme ki van kapcsolva.
	UPGRADEMODE	Alkalmazásfrissítési mód: • A `Seamless` azt jelenti, hogy az alkalmazás frissítése a számítógép újraindításával történik (alapértelmezett érték). • A `Force` azt jelenti, hogy az alkalmazást újraindítás nélkül frissítjük. Az alkalmazást a 11.10.0 verzióval kezdődően újraindítás nélkül frissítheti. Az alkalmazás korábbi verziójának frissítéséhez újra kell indítania a számítógépet. A javításokat a 11.11.0 verzióval kezdődően újraindítás nélkül is telepítheti. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Tehát az alkalmazás frissítési módja az alkalmazás beállításaiban lesz megadva. Ezt a paramétert az alkalmazás beállításaiban vagy a házirendben módosíthatja. A már telepített alkalmazás frissítésekor a setup.ini fájlban megadott paraméter prioritása magasabb, mint az alkalmazásbeállításokban vagy a parancssorban megadott paraméter. Például ha a `Force` frissítési mód van megadva a setup.ini fájlban, és a `Seamless` mód van megadva az alkalmazásbeállításokban, a frissítés újraindítás nélkül fog települni (`Force`). Ha a setup.ini fájlt használja, ahol az `UPGRADEMODE` paraméter nincs megadva, a telepítő alapértelmezett értéket fog használni (`Seamless`), és a számítógép újraindításával telepíti a frissítést.
	SetupReg	Engedélyezi a beállításkulcsok írását a setup.reg fájlból a beállításjegyzékbe. `SetupReg: setup.reg` paraméter értéke.

Rész	Paraméter	Leírás
	`EnableTraces`	Az alkalmazások nyomkövetésének engedélyezése vagy kikapcsolása. Indulása után a Kaspersky Endpoint Security elmenti a nyomkövetési fájlokat a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappába. Választható értékek: • `1` – a nyomkövetés engedélyezve van. • `0` – a nyomkövetés ki van kapcsolva (alapértelmezett érték).
	`TracesLevel`	A nyomkövetések részleteinek szintje. Választható értékek: • `100` (kritikus). Csak a súlyos hibákról szóló üzenetek. • `200` (magas). Minden hibáról szóló üzenet, köztük a súlyos hibáké. • `300` (diagnosztika). Üzenetek a hibákról, valamint a figyelmeztetésekről. • `400` (fontos). Minden hibaüzenet, figyelmeztetés és további információ. • `500` (normális). Üzenetek a hibákról és figyelmeztetésekről, valamint részletes információ az alkalmazás normál módban történő működéséről (alapértelmezett). • `600` (alacsony). Minden üzenet.
	`RESTAPI`	Alkalmazás kezelése a REST API felületen keresztül. Ahhoz, hogy az alkalmazást kezelni tudja a REST API felületen keresztül, meg kell adnia a felhasználónevet (`RESTAPI_User` paraméter). Választható értékek: • `1` – a REST API felületen keresztül történő kezelés engedélyezve van. • `0` – a REST API felületen keresztül történő kezelés blokkolva van (alapértelmezett érték). Ahhoz, hogy a REST API felületen keresztül tudjon alkalmazásokat kezelni, engedélyezni kell az adminisztrációs rendszerek használatával történő kezelést. Ehhez állítsa be az `AdminKitConnector=1` paramétert. Ha a REST API felületen keresztül kezeli az alkalmazást, akkor nem lehet az alkalmazást a Kaspersky adminisztrációs rendszereinek használatával kezelni.
	`RESTAPI_User`	Az alkalmazás REST API felületen keresztül történő kezeléséhez használt Windows tartományfiók felhasználóneve. A REST API felületen keresztül történő alkalmazáskezelés csak ennek a felhasználónak lehetséges. Adja meg a felhasználónevet a következő formátumban: `<DOMAIN>\<UserName>` (például `RESTAPI_User=COMPANY\Administrator`). A REST API-val történő munkálatokhoz csak egy felhasználót választhat ki. Egy felhasználónév megadása szükséges ahhoz, hogy az alkalmazást a REST API felületen keresztül kezelhesse.
	`RESTAPI_Port`	Az alkalmazás REST API felületen keresztül történő kezeléséhez használt port. A 6782 az alapértelmezett port. Győződjön meg arról, hogy a port szabad.
	`RESTAPI_Certificate`	Tanúsítvány a kérések azonosítására (pl. `RESTAPI_Certificate=C:\cert.pem`). A Kaspersky Endpoint Security és a REST kliens közötti biztonságos interakció megköveteli a kérésazonosítás konfigurálását. Ehhez telepítenie kell egy tanúsítványt, majd alá kell írnia az egyes kérések adattartalmát.
	`StandaloneMode`	Az alkalmazás telepítése Endpoint Detection and Response Agent (EDR Agent) módban. Az *Endpoint Detection and Response Agent* egy olyan alkalmazás, amely a vállalat informatikai infrastruktúrájában az egyes munkaállomásokra és kiszolgálókra telepítve támogatja a Kaspersky Managed Detection and Response és Kaspersky Anti Targeted Attack Platform megoldásokat. Az EDR Agent kompatibilis harmadik féltől származó EPP alkalmazásokkal. Ez lehetővé teszi harmadik féltől származó infrastruktúra-biztonsági eszközök használatát a Kaspersky Detection and Response mellett. Az EDR Agent telepítéséhez a `[Components]` részen válassza ki a `StandaloneKATA`, a `StandaloneNDR` vagy a `StandaloneMDR` összetevőket. Az EDR Agent nem támogatja az alkalmazás más összetevőit. Választható értékek: • `1` az alkalmazás EDR Agent módban történő telepítéséhez. • `0` az alkalmazás Standard módban történő telepítéséhez (alapértelmezett).
	`KSVLAMode`	Az alkalmazás telepítése Light Agent üzemmódban. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Választható értékek: • `1` az alkalmazás Light Agent módban történő telepítéséhez. • `0` az alkalmazás Standard módban történő telepítéséhez (alapértelmezett).

Rész	Paraméter	Leírás
	`InstallOnVDI`	A VDI védelmi mód engedélyezése az alkalmazás Light Agent üzemmódban történő telepítésekor (`KSVLAMode=1`). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját. Választható értékek: • `1` a VDI védelmi mód engedélyezéséhez. • `0` a VDI védelmi mód letiltásához (alapértelmezett).
	`KESExclusions`	Előre definiált vizsgálati kizárások és megbízható alkalmazások hozzáadása az alkalmazás kiszolgálón történő telepítésekor. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Például az SQL-kiszolgálók előre definiált vizsgálati kizárásai közé tartoznak az MDF és LDF adatbázisfájlok. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. Választható értékek: • Az `1` engedélyezi az előre definiált vizsgálati kizárásokat és a megbízható alkalmazásokat. • A `0` letiltja az előre definiált vizsgálati kizárásokat és a megbízható alkalmazásokat (alapértelmezett).
	`LAExclusions`	Előre definiált vizsgálati kizárások és megbízható alkalmazások hozzáadása az alkalmazás virtuális gépre történő telepítésekor (Light Agent üzemmód). Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben. Választható értékek: • Az `1` engedélyezi az előre definiált vizsgálati kizárásokat és a megbízható alkalmazásokat. • A `0` letiltja az előre definiált vizsgálati kizárásokat és a megbízható alkalmazásokat (alapértelmezett).
	`EnableUniqueSensorID`	Egyedi számítógép-azonosító (Sensor ID) létrehozása az alkalmazás telepítése vagy frissítése során. A Sensor ID a Kaspersky Anti Targeted Attack Platform megoldásban azon számítógépek azonosítására szolgál, amelyek telemetriai adatokat küldenek a kiszolgálónak. A Sensor ID létrehozásakor az alkalmazás olyan algoritmust használ, amely figyelembe veszi a számítógép konfigurációját, például az alaplap sorozatszámát. Egyes esetekben, például amikor az alkalmazást virtuális környezetben használja, a Sensor ID duplikálódhat. Emiatt a Kaspersky Anti Targeted Attack Platform nem tudja azonosítani azt a számítógépet, amelyről a telemetriai adatokat küldték. Egyedi Sensor ID létrehozásához be kell állítania a `EnableUniqueSensorID=1` paramétert. Emiatt az alkalmazás egy másik algoritmust használ majd a Sensor ID létrehozásához, amely a számítógépre vonatkozó egyéb adatokat is figyelembe vesz. Ez egyedi Sensor ID-t biztosít. Alapértelmezés szerint a paraméter nincs beállítva. Az alkalmazás a következő esetekben örökli a Sensor ID-t: • az alkalmazás verziójának frissítése; • a [KES+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra. Az alkalmazás javításának részeként a telepítő megkísérli örökölni az Sensor ID értékét. Ha az Sensor ID nem állítható vissza, az alkalmazás új Sensor ID jön létre.
	`CitrixCompatibility`	A Citrix Provisioning Services támogatásának engedélyezése, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre lehessen telepíteni.
`[Components]`	`ALL`	Az összes összetevő telepítése. Az `1` paraméterérték megadása esetén minden összetevő telepítésére sor kerül, függetlenül az egyedi összetevők telepítési beállításaitól. A Detection and Response megoldások támogatottsága miatt az Endpoint Detection and Response Optimum és a Sandbox összetevők telepítve vannak a számítógépre. A Endpoint Detection and Response Expert (cloud) összetevő nem kompatibilis ezzel a konfigurációval.
	`MailThreatProtection`	Levelezés védelem.
	`WebThreatProtection`	Web védelem.
	`AMSI`	AMSI védelem.
	`HostIntrusionPrevention`	Behatolásmegelőző rendszer.
	`BehaviorDetection`	Viselkedésészlelés.

Rész	Paraméter	Leírás
	`ExploitPrevention`	Biztonsági rések kihasználásának megelőzése.
	`RemediationEngine`	Kármentesítő motor.
	`Firewall`	Tűzfal.
	`NetworkThreatProtection`	Hálózati védelem.
	`WebControl`	Webfelügyelő.
	`DeviceControl`	Eszközfelügyelő.
	`ApplicationControl`	Alkalmazásfelügyelő.
	`AdaptiveAnomaliesControl`	Adaptív Anomáliafelügyelő.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Naplóvizsgálat
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	Fájl védelem.
	`SystemIntegrityMonitor`	Rendszerintegritás-figyelő.
	`FileEncryption`	Fájlszintű titkosítás könyvtárak.
	`DiskEncryption`	Teljes lemeztitkosítás rész.
	`MSBitLocker`	BitLocker titkosításkezelő könyvtárak.
	`BadUSBAttackPrevention`	BadUSB védelem.
	`EDR`	Endpoint Detection and Response Optimum Az összetevő nem kompatibilis a Endpoint Detection and Response Expert (cloud) (`EDRCloud`) és az Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) összetevőkkel.
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Az összetevő nem kompatibilis az Endpoint Detection and Response Optimum (`EDR`) és az Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) összetevőkkel.
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Az összetevő nem kompatibilis a Endpoint Detection and Response Expert (cloud) (`EDRCloud`) és az Endpoint Detection and Response Optimum (`EDR`) összetevőkkel.
	`SB`	Kaspersky Sandbox vagy KATA Sandbox. A *Kaspersky Sandbox* a Kaspersky önálló Detection and Response megoldása. A *KATA Sandbox* a Kaspersky Anti Targeted Attack Platform megoldás egyik összetevője.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Az összetevő nem kompatibilis a Endpoint Detection and Response Expert (cloud) (`EDRCloud`) és az Endpoint Detection and Response Optimum (`EDR`) összetevőkkel.

Rész	Paraméter	Leírás
	`AdminKitConnector`	Alkalmazáskezelés adminisztrációs rendszerek használatával. Adminisztrációs rendszerek, többek között a Kaspersky Security Center. A Kaspersky adminisztrációs rendszerek mellett harmadik féltől származó megoldásokat is használhat. A Kaspersky Endpoint Security API-t biztosít ebből a célból. Választható értékek: • `1` – az adminisztrációs rendszerekkel történő alkalmazáskezelés engedélyezve van (alapértelmezett érték). • `0` – az alkalmazáskezelés csak a helyi felületen keresztül van engedélyezve.
	`KUMAIntegration`	Integráció az KUMA-rel.
	`StandaloneKATA`	Az alkalmazás telepítése Endpoint Detection and Response Agent (EDR Agent) üzemmódban a Kaspersky Anti Targeted Attack Platform (EDR) integrálásához.
	`StandaloneMDR`	Az alkalmazás telepítése az Endpoint Detection and Response Agent (EDR Agent) üzemmódban a Kaspersky Managed Detection and Response rendszerrel való integrációhoz.
	`StandaloneNDR`	Az alkalmazás telepítése Endpoint Detection and Response Agent (EDR Agent) üzemmódban a Kaspersky Anti Targeted Attack Platform (NDR) integrálásához.
	`StandaloneSiemTelemetry`	Az alkalmazás telepítése az Endpoint Detection and Response Agent (EDR Agent) üzemmódban a KUMA rendszerrel való integrációhoz.
`[Tasks]`	`ScanMyComputer`	Teljes vizsgálat feladat. Választható értékek: • `1` – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • `0` – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.
	`ScanCritical`	Kritikus területek vizsgálata feladat. Választható értékek: • `1` – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • `0` – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.
	`Updater`	Frissítési feladat. Választható értékek: • `1` – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • `0` – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.

Alkalmazásösszetevők módosítása

Az alkalmazás telepítése során ki kell választania az összetevőket, amik elérhetők lesznek. A következő módszerekkel módosíthatja az alkalmazásösszetevőket:

- Helyben, a Telepítővarázsló segítségével.

  Az alkalmazásösszetevők módosítása a Windows operációs rendszer normál módszerével történik, tehát a Vezérlőpanelen keresztül. Futtassa az Alkalmazásbeállítási varázslót, és válassza a rendelkezésre álló alkalmazásösszetevők megváltoztatásának lehetőségét. Kövesse a képernyőn lévő utasításokat.

  > Ez a módszer nem érhető el, ha az alkalmazást a Kaspersky Security Centeren keresztül telepítette. Az alkalmazás összetevőinek kiválasztását a Vezérlőpulton csak az alkalmazás helyi telepítése után módosíthatja.

- Távolról a Kaspersky Security Centeren keresztül.

  Az *Change application components* feladat segítségével módosíthatja a Kaspersky Endpoint Security összetevőit, miután az alkalmazás telepítve lett.

Az alkalmazásösszetevők módosításakor vegye figyelembe a következő szempontokat:

- A Windows Servert futtató számítógépeken nem tudja telepíteni a Kaspersky Endpoint Security összes összetevőjét (például az Adaptív Anomálisfelügyelő összetevő nem érhető el).
- A számítógépe merevlemezeit a Teljes lemeztitkosítás (FDE) védi, nem távolíthatja el a Teljes lemeztitkosítás összetevőt. A Teljes lemeztitkosítás eltávolításához fejtse vissza a számítógép összes merevlemezét.
- Ha a számítógépen találhatók titkosított fájlok (FLE), vagy a felhasználó titkosított cserélhető meghajtókat használ (FDE vagy FLE), akkor nem lehet hozzáférni a fájlokhoz és a cserélhető meghajtókhoz az Adattitkosító összetevők eltávolítása után. A fájlokhoz és a cserélhető meghajtókhoz az Adattitkosítás összetevők újratelepítésével férhet hozzá.
- Ha az alkalmazás Light Agent üzemmódban van telepítve egy VDI infrastruktúrában, a beállított összetevők módosítása nem támogatott.

Alkalmazásösszetevők hozzáadásának és eltávolításának menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Összetevők kiválasztása a telepítéshez** elemet.

2. lépés Feladatbeállítások az alkalmazásösszetevők módosításához

Válassza ki az alkalmazás konfigurációját:

- **Normál mód a gazdagépek védelmére**. Az alapértelmezett konfiguráció. Ez a konfiguráció lehetővé teszi az alkalmazás összes összetevőjének használatát, beleértve a Detection and Response megoldásokat támogató összetevőket is. Ez a konfiguráció a számítógép átfogó védelmére szolgál számos fenyegetés, hálózati támadás és csalás ellen.

- **Endpoint Detection and Response Agent a speciális fenyegetések és a célzott támadások elleni védelemhez**. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.

  Amikor az EDR Agent alkalmazáskonfigurációját módosítja, hogy működjön az MDR-rel, győződjön meg arról, hogy a telemetria fogadásáért felelős összetevők engedélyezve vannak.

- **Light Agent a virtuális környezetek védelme céljából**. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **VDI infrastruktúra védelme** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.

Válassza ki, hogy mely alkalmazásösszetevők lesznek elérhetők a felhasználó számítógépén.

3. lépés: Speciális beállítások

Konfigurálhatja a feladat speciális beállításait (lásd az alábbi táblázatot).

4. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

5. lépés Feladatindítási ütemezés konfigurálása

Állítson be ütemezést egy adott feladat elindításához, például kézi indítást vagy a számítógép tétlen időszakára esőt.

6. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például: *Az Alkalmazásfelügyelő összetevő hozzáadása*.

7. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Alkalmazásösszetevő hozzáadásának, illetve eltávolításának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.
2. A **Task type** legördülő listából válassza ki az **Change application components** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *Alkalmazásfelügyelő-összetevő hozzáadása*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. Választhat például külön adminisztrációs csoportot, vagy létrehozhat egy válogatást.

3. lépés A feladat létrehozásának befejezése

Tegyen jelölést az **Open task details when creation is complete** jelölőnégyzetbe, és zárja be a varázslót.

A feladat tulajdonságainál válassza az **Application settings** lapot. Ezután válassza ki az alkalmazás konfigurációját:

- **Standard mode to protect workstations and servers**. Az alapértelmezett konfiguráció. Ez a konfiguráció lehetővé teszi az alkalmazás összes összetevőjének használatát, beleértve a Detection and Response megoldásokat támogató összetevőket is. Ez a konfiguráció a számítógép átfogó védelmére szolgál számos fenyegetés, hálózati támadás és csalás ellen.

- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.

  Amikor az EDR Agent alkalmazáskonfigurációját módosítja, hogy működjön az MDR-rel, győződjön meg arról, hogy a telemetria fogadásáért felelős összetevők engedélyezve vannak.

- **Light Agent to protect virtual environments**. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **Protect VDI infrastructure** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.

Válassza ki, hogy mely alkalmazásösszetevők lesznek elérhetők a felhasználó számítógépén. Konfigurálhatja a feladat speciális beállításait (lásd az alábbi táblázatot).

Ennek eredményeképpen a Kaspersky Endpoint Security összetevőkészlet csendes módban megváltozik a felhasználói számítógépen. Az elérhető összetevők beállításai megjelennek az alkalmazás helyi felületén. Az alkalmazásban nem található összetevők ki lesznek kapcsolva, a beállításaik nem lesznek elérhetőek.

A Kaspersky Endpoint Security telepítésekor, frissítésekor vagy eltávolításakor hibák léphetnek fel. A hibák megoldásával kapcsolatos további információért tekintse meg a Terméktámogatási tudásbázist.

A feladat speciális beállításai

Paraméter	Leírás
Feladatbeállítások	**Ellenőrizze, hogy nincsenek-e nem kompatibilis, harmadik féltől származó alkalmazásai**. Alapértelmezés szerint a Kaspersky Endpoint Security ellenőrzi a telepített alkalmazások kompatibilitását. A kompatibilitási problémákat okozó szoftverek listája a(z) incompatible.txt fájlban érhető el. A fájlt a terjesztőkészlet tartalmazza. Ha a telepített szoftverek vizsgálata engedélyezve van, a listán szereplő alkalmazás észlelésekor a Kaspersky Endpoint Security leállítja a feladatot. Letilthatja a telepített szoftverek vizsgálatát, ha a harmadik féltől származó szoftver gyártói dokumentációja azt állítja, hogy a szoftver kompatibilis a következővel: Endpoint Protection Platform (EPP). **Harmadik féltől származó, nem kompatibilis alkalmazások eltávolítása**. A(z) incompatible.txt fájlban felsorolt alkalmazások automatikus eltávolítása az összetevőkészlet módosítása előtt. Ha ez a funkció engedélyezve van, a Kaspersky Endpoint Security a feladat folytatása érdekében megkísérli eltávolítani a kompatibilitási problémákat okozó alkalmazásokat. **Használja az Azure WVD-kompatibilitási módot**. Ez a funkció biztosítja az Azure virtuális gép állapotának megfelelő megjelenítését a Kaspersky Anti Targeted Attack Platform konzolon. A számítógép teljesítményének figyelése céljából a Kaspersky Endpoint Security telemetriai adatokat küld a KATA-kiszolgálóknak. A telemetria tartalmazza a számítógép azonosítóját (Sensor ID). Az Azure WVD-kompatibilitási mód lehetővé teszi állandó egyedi (Sensor ID) hozzárendelését ezekhez a virtuális gépekhez. Ha a kompatibilitási mód ki van kapcsolva, az Azure-beli virtuális gépek működése miatt az (Sensor ID). a számítógép újraindítása után megváltozhat. Ez azt eredményezheti, hogy a virtuális gépek duplikátumai jelennek meg a konzolon.

Paraméter	Leírás
Kizárások	A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazást Light Agent üzemmódban is telepítheti a virtuális környezetek védelme céljából. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben. A megbízható zónát később a házirend tulajdonságaiban is beállíthatja: vizsgálati kizárások és megbízható alkalmazások.
Külön üzemmód / Kombinált üzemmód	A munkaállomásokhoz és a kiszolgálókhoz külön összetevőkészleteket hozhat létre – **Külön üzemmód**. A telepítőcsomag telepítése előtt a telepítőprogram felismeri az operációs rendszer típusát, és csak azokat az alkalmazásösszetevőket telepíti, amelyeket az adott operációs rendszer típusához választott ki. Ily módon ugyanazt a telepítőcsomagot használhatja a munkaállomásokhoz és a kiszolgálókhoz. A **kombinált üzemmód** a munkaállomások és a kiszolgálók összetevőinek közös listáját kínálja. Az egyes összetevők elérhetősége az operációs rendszer típusától függ. Javasoljuk, hogy ebben az üzemmódban külön telepítőcsomagot hozzon létre a munkaállomásokhoz és külön telepítőcsomagot a kiszolgálókhoz. A telepítőcsomag összetevőinek általános listája csak Normál üzemmódban konfigurálható.
Jelszó használata az alkalmazás összetevőkészletének módosításához	A rendszergazdák általában engedélyezik a Jelszóvédelmet, hogy korlátozzák a Kaspersky Endpoint Security-hez való hozzáférést. Vagyis az alkalmazásösszetevők kiválasztásának módosításához meg kell adnia annak a felhasználónak a hitelesítő adatait, aki rendelkezik az **Alkalmazás eltávolítása/módosítása/visszaállítása** engedéllyel. Használhatja például a KL Admin fiókot.
Jelszó használata a Kaspersky Endpoint Agent és a Kaspersky Security for Windows Server eltávolításához	A rendszergazdák általában engedélyezik a Jelszóvédelmet ezen feladatok beállításainál, hogy korlátozzák a Kaspersky Endpoint Agent (KEA) és a Kaspersky Security for Windows Server (KSWS) megoldásokahoz való hozzáférést. Ez azt jelenti, hogy ha a [KES+KEA] konfigurációról a [KES+beépített ügynök] megoldásra tér át, vagy ha a KSWS-ről a KES-re megoldásra tér át, meg kell adnia egy jelszót az alkalmazások eltávolításához.

Az alkalmazás korábbi verziójának frissítése

Amikor az alkalmazás korábbi verzióját egy újabb verzióra frissíti, vegye figyelembe a következőt:

- A Kaspersky Endpoint Security új verziója honosításának meg kell egyeznie az alkalmazás telepített verziójának honosításával. Ha az alkalmazások honosításai nem egyeznek meg, az alkalmazás frissítése hibaüzenettel fejeződik be.
- Ajánlott kilépni minden aktívan futó alkalmazásból, mielőtt megkezdi a frissítést.
- A frissítés előtt a Kaspersky Endpoint Security blokkolni fogja a Teljes lemeztitkosítás funkciót. Ha a Teljes lemeztitkosítás zárolása nem sikerült, a frissítés telepítése nem indul el. Az alkalmazás frissítése után a Teljes lemeztitkosítás funkció ismét helyreáll.

A Kaspersky Endpoint Security az alkalmazás következő verziófrissítéseit támogatja:

- Kaspersky Endpoint Security 12.1 for Windows (12.1.0.506 számú build)
- Kaspersky Endpoint Security 12.2 for Windows (12.2.0.462 számú build)
- Kaspersky Endpoint Security 12.3 for Windows (12.3.0.493 számú build)
- Kaspersky Endpoint Security 12.4 for Windows (12.4.0.467 számú build)
- Kaspersky Endpoint Security 12.5 for Windows (12.5.0.539 számú build)
- Kaspersky Endpoint Security 12.6 for Windows (12.6.0.438 számú build)

- Kaspersky Endpoint Security 12.7 for Windows (12.7.0.533 számú build)
- Kaspersky Endpoint Security 12.8 for Windows (12.8.0.505 számú build)
- Kaspersky Endpoint Security 12.9 for Windows (12.9.0.384 számú build)
- Kaspersky Endpoint Security 12.10 for Windows (12.10.0.466 számú build)
- Kaspersky Endpoint Security 12.11 for Windows (12.11.0.637 számú build)
- Kaspersky Endpoint Security 12.12 for Windows (12.12.0.522 számú build)
- Kaspersky Endpoint Security 14.0 for Windows (14.0.0.504 számú build)

A Kaspersky Endpoint Security telepítésekor, frissítésekor vagy eltávolításakor hibák léphetnek fel. A hibák megoldásával kapcsolatos további információért tekintse meg a Terméktámogatási tudásbázist.

Alkalmazásfrissítési módszerek

A Kaspersky Endpoint Security több módon frissíthető a számítógépen:

- A Kaspersky frissítési szolgáltatás (Seamless Update – SMU) használatával.
- helyben, a Telepítővarázsló segítségével.
- helyben, a parancssorból.
- távolról, a Kaspersky Security Centeren keresztül.
- távolról, a Microsoft Windows csoportos rendszabálykezelő szerkesztőben (további információért keresse fel a Microsoft Terméktámogatás weboldalát).
- távolról, a Rendszerközpont-konfigurációs kezelővel.

Ha a vállalati hálózatra telepített alkalmazás az alapértelmezetteken felüli összetevőket tartalmaz, akkor az Adminisztrációs konzolon (MMC) keresztül történő alkalmazásfrissítés eltér a Web Console-on és a Cloud Console-on keresztül történő alkalmazásfrissítéstől. Amikor frissíti a Kaspersky Endpoint Security alkalmazást, vegye figyelembe a következőt:

- Kaspersky Security Center Web Console vagy Kaspersky Security Center Cloud Console.

  Ha Ön létrehozott egy telepítőcsomagot az alkalmazás új verziójának az alapértelmezett összetevőkkel, akkor az összetevők listája nem változik a felhasználó számítógépén. A Kaspersky Endpoint Security alapértelmezett összetevőkkel való használatához nyissa meg a telepítőcsomag tulajdonságait, változtassa meg az összetevők listáját, állítsa vissza az eredeti összetevőket, majd mentse el a változtatásokat.

- Kaspersky Security Center Adminisztrációs Konzol.

  A frissítés után az alkalmazásösszetevők listája egyezni fog a telepítőcsomag összetevőinek listájával. Azaz, ha az alkalmazás új verziója az összetevők alapértelmezett listájával rendelkezik, akkor például a BadUSB védelem el lesz távolítva a számítógépről, mivel ez az összetevő nem tartozik bele az alapértelmezett listába. Az alkalmazás használatának a frissítés előtti összetevőivel való folytatásához válassza ki a szükséges összetevőket a telepítőcsomag beállításaiban.

Az alkalmazás frissítése újraindítás nélkül

Mivel az alkalmazás frissítéséhez nem kell újraindítani a rendszert, a kiszolgáló megszakítás nélkül működhet az alkalmazás verziójának frissítésekor.

Az alkalmazás újraindítás nélküli frissítése a következő korlátozásokkal jár:

- Az alkalmazást a 11.10.0 verzióval kezdődően újraindítás nélkül frissítheti. Az alkalmazás korábbi verziójának frissítéséhez újra kell indítania a számítógépet.
- A javításokat a 11.11.0 verzióval kezdődően újraindítás nélkül telepítheti. Az alkalmazás korábbi verzióihoz tartozó javítások telepítéséhez szükség lehet a számítógép újraindítására.
- Az alkalmazás újraindítás nélküli frissítése nem érhető el azokon a számítógépeken, amelyeken engedélyezve van az adattitkosítás (Kaspersky-titkosítás (FDE), BitLocker, Fájlszintű titkosítás (FLE)). Az alkalmazás frissítéséhez az engedélyezett adattitkosítással rendelkező számítógépeken a rendszert újra kell indítani.
- Az alkalmazás nem frissíthető virtuális gépen újraindítás nélkül. Az alkalmazás virtuális gépen való frissítéséhez újra kell indítania a virtuális gépet.

Az alkalmazás frissítése, a javítás telepítése, az alkalmazás összetevőinek módosítása vagy a visszaállítás után a Kaspersky Endpoint Security újraindul, hogy elkezdhesse használni az új verziót. A Kaspersky Endpoint Security újraindítása akár egy percig is eltarthat. Eközben a számítógép védelmi szintje csökken. Az alkalmazás újraindítása után a számítógép védelmi szintje visszaáll.

Az alkalmazás frissítési módjának kiválasztása az Adminisztrációs konzolban (MMC)

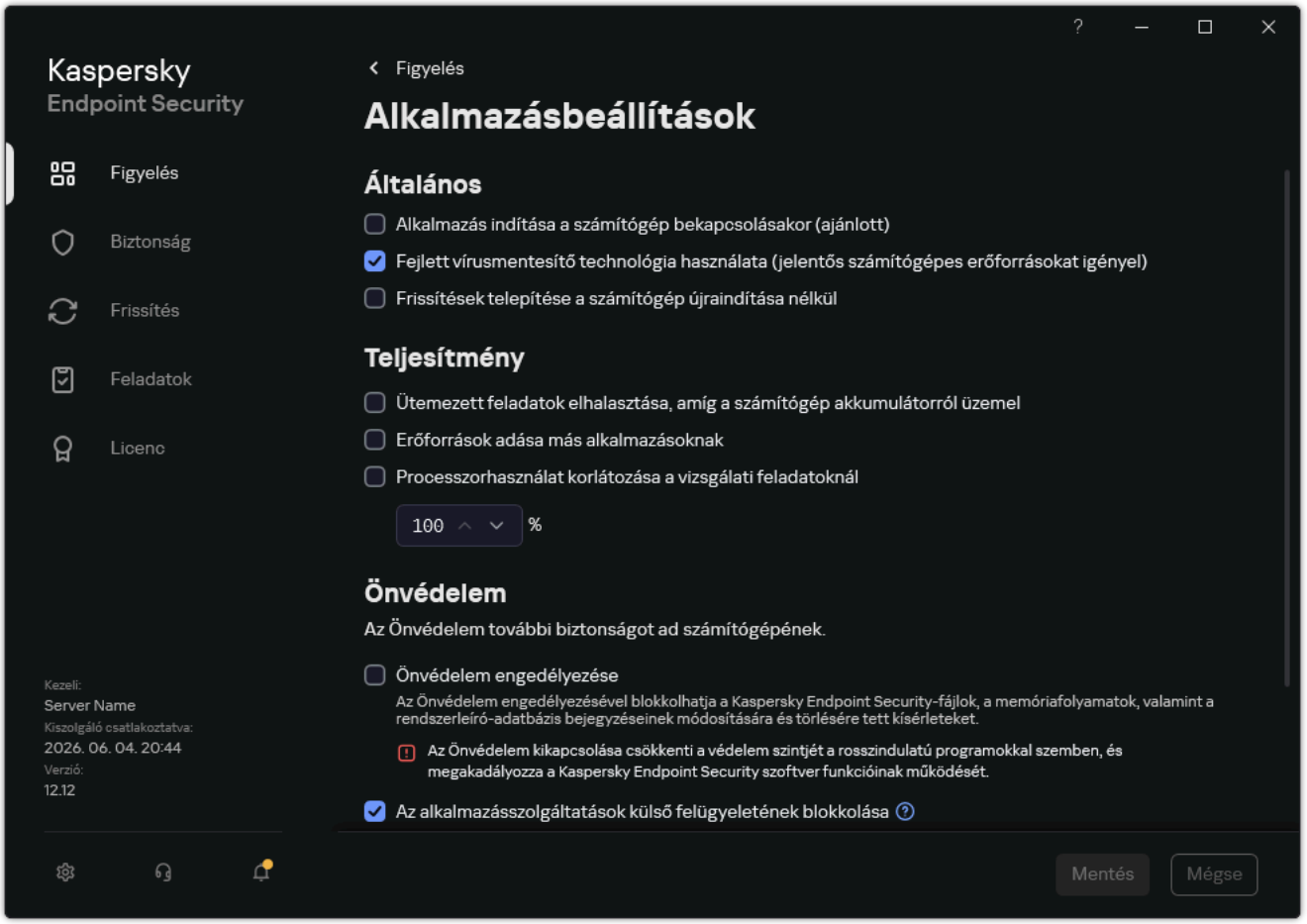
1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **User Interaction** elemet.
5. Az **Application update settings** részen jelölje be a **Install application updates without restart** négyzetet vagy törölje a négyzet jelölését az alkalmazásfrissítési mód konfigurálásához.
6. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. A **Speciális beállítások** részen jelölje be az **Alkalmazásfrissítések telepítése újraindítás nélkül** jelölőnégyzetet az alkalmazásfrissítési mód konfigurálásához, vagy törölje a bejelölést.
5. Mentse el a módosításokat.

Az alkalmazás frissítési módjának kiválasztása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. Az **Általános** részen jelölje be a **Frissítések telepítése a számítógép újraindítása nélkül** jelölőnégyzetet az alkalmazásfrissítési mód konfigurálásához, vagy törölje a bejelölést.
4. Mentse el a módosításokat.

Az alkalmazás újraindítás nélküli frissítésének folyamata után a Kaspersky Endpoint Security új verziója telepítve lesz a számítógépen. Az alkalmazás korábbi verziója automatikusan törlődik.

Nem kezdeményezhet alkalmazásfrissítést az előző frissítés teljes befejezése előtt.

A Kaspersky Endpoint Security frissítési állapotát a Kaspersky Security Center konzol Kaspersky alkalmazásverziói jelentésével ellenőrizheti.

Az alkalmazás SMU-frissítése

Ahhoz, hogy az alkalmazást a Kaspersky frissítési szolgáltatásával frissítse (Seamless Update; SMU), nem kell futtatnia a telepítőt, ellentétben az egyéb frissítési módszerekkel. A Kaspersky Endpoint Security az alkalmazás új verzióját, valamint a víruskereső adatbázisokat ugyanabból a forrásból kapja meg.

Az SMU-frissítések lehetővé teszik az alkalmazás legújabb verzióra való frissítését a vállalata összes számítógépén. Az SMU-frissítések alkalmazása előtt javasoljuk, hogy tesztelje az alkalmazás új verzióját néhány számítógépen. Ehhez manuálisan kell frissítenie az alkalmazást ezeken a számítógépeken (például helyileg a Telepítővarázsló segítségével). Az SMU frissítése során nem választhat ki egyes számítógépeket.

Az alkalmazás frissítési ütemezését a Kaspersky munkatársai határozzák meg. Annak érdekében, hogy az alkalmazás új verziója zökkenőmentesen fusson, a Kaspersky lépésről lépésre teszi elérhetővé a frissítéseket. Ez azt jelenti, hogy az SMU-frissítést az új verzió megjelenése után akár két hónappal később is megkaphatja.

Az alkalmazás SMU-frissítését az *Adatbázisok és alkalmazásmodulok frissítése* feladattal tudja kezelni. Ahhoz, hogy az alkalmazás új verziója ugyanabban a csomagban szerepeljen, mint a vírusirtó adatbázisok, engedélyeznie kell az *alkalmazásmodulok* frissítését az *Adatbázisok és alkalmazásmodulok frissítése* feladatbeállításokban. Az *Adatbázisok és alkalmazásmodulok frissítése* feladatbeállításokban engedélyezheti az alkalmazás újraindítás nélküli frissítését is.

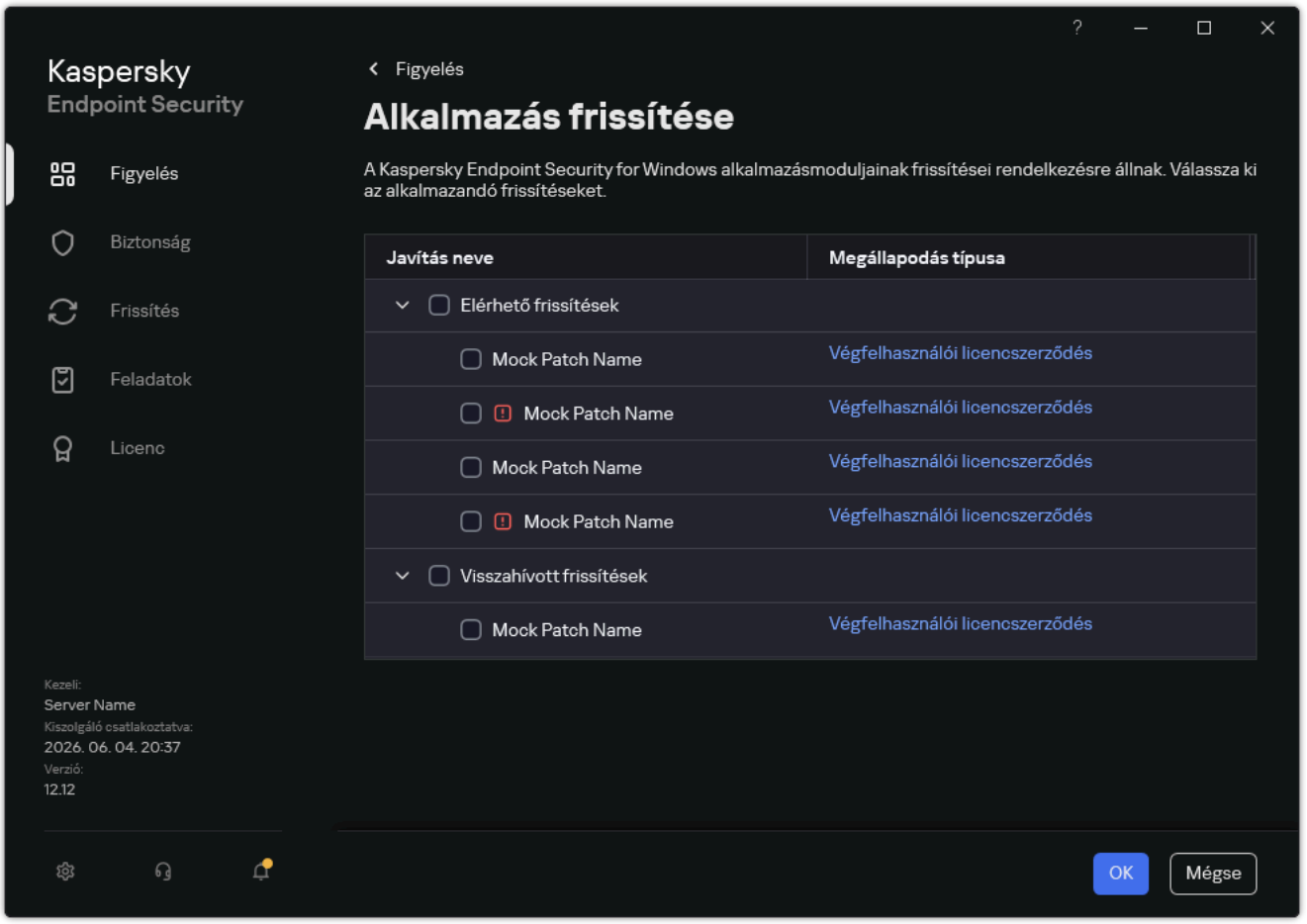
Az alkalmazás SMU-frissítésének lépései

1. **Az alkalmazás új verziójának megjelenése után a Kaspersky forgalmazza a frissítést.**
2. **A felhasználó jóváhagyja az alkalmazás frissítését.**

   Ha a számítógép csatlakozik a Kaspersky Security Centerhez, a frissítés elérhető a Kaspersky Security Centerben, a(z) **Update of Kaspersky databases and application modules** szakaszban. A frissítések jóváhagyásával kapcsolatos további részletekért lásd a Kaspersky Security Center súgóját.

   Ha a számítógép nem csatlakozik a Kaspersky Security Centerhez, a frissítés az alkalmazás kezelőfelületének értesítési részében érhető el: . A frissítés jóváhagyásához válassza ki az alkalmazás egy verzióját, és fogadja el a szerződési feltételeket (lásd az alábbi ábrát).
3. **A Kaspersky Endpoint Security futtatja a *Adatbázisok és alkalmazásmodulok frissítése* feladatot a beállított ütemezésnek megfelelően.**

Ennek eredményeként a Kaspersky Endpoint Security „csendes” módban frissíti az alkalmazást.



Elérhető alkalmazásfrissítések

Az alkalmazás eltávolítása

A Kaspersky Endpoint Security eltávolításával a számítógép és a felhasználói adatok a fenyegetésekkel szemben védelem nélkül maradnak.

A Kaspersky Endpoint Security telepítésekor, frissítésekor vagy eltávolításakor hibák léphetnek fel. A hibák megoldásával kapcsolatos további információért tekintse meg a Terméktámogatási tudásbázist.

Az alkalmazás távoli eltávolítása a Kaspersky Security Center segítségével

Távolról is eltávolíthatja az alkalmazást az *Uninstall application remotely* feladattal. A feladat elvégzése után a Kaspersky Endpoint Security letölti az alkalmazás eltávolító segédprogramját a felhasználó számítógépére. Az alkalmazás eltávolítása után a segédprogram automatikusan el lesz távolítva.

Az alkalmazás eltávolításának menete az Adminisztrációs Konzolon (MMC) keresztül

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.
   Megnyílik a feladatok listája.
3. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza a **Kaspersky Security Center Administration Server → Advanced → Uninstall application remotely** lehetőséget.

2. lépés Az eltávolítani kívánt alkalmazás kiválasztása

Válassza a **Uninstall application supported by Kaspersky Security Center** lehetőséget.

3. lépés Feladatbeállítások az alkalmazás eltávolításához

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)**.

4. lépés Az eltávolító segédprogram beállításai

Konfigurálja a következő további alkalmazásbeállításokat:

- **Force download of the uninstallation utility**. Válassza ki a segédprogram küldésének módját:
  - **Using Network Agent**. Ha nem volt Hálózati ügynök telepítve a számítógépére, akkor először a Hálózati ügynök lesz telepítve az operációs rendszer eszközeinek használatával. Ezután a Kaspersky Endpoint Security el lesz távolítva a Hálózati ügynök eszközeivel.
  - **Using operating system resources through Administration Server**. A segédprogram az operációs rendszer erőforrásaival továbbítva lesznek az ügyfél számítógépekre az Adminisztrációs kiszolgálón keresztül. Ezt az opciót akkor választhatja, ha nincs Hálózati ügynök telepítve az ügyfél számítógépen, és az ügyfél számítógép ugyanazon hálózaton van, mint az Adminisztrációs kiszolgáló.
  - **Using operating system resources through distribution points**. A segédprogram az operációs rendszer erőforrásai használatával, a elosztói pontokon keresztül lesznek elküldve a számítógépekre. Ezt az opciót akkor választhatja, ha legalább egy elosztói pont van a hálózatban. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Súgót.
- **Verify operating system type before downloading**. Ha szükséges, törölje a jelölést ebből a jelölőnégyzetből. Ezzel megelőzheti az eltávolítási segédprogram letöltését, ha a számítógép operációs rendszere nem felel meg a szoftverkövetelményeknek. Ha biztos benne, hogy a számítógépe operációs rendszere megfelel a szoftverkövetelményeknek, akkor kihagyhatja ezt a hitelesítést.

Ha az alkalmazáseltávolítási művelet jelszóval védett, tegye a következőket:

1. Tegyen jelölést a **Use uninstallation password** jelölőnégyzetbe.
2. Kattintson az **Edit** gombra.
3. Adja meg a KLAdmin fiók jelszavát.

5. lépés Az operációs rendszer újraindítására vonatkozó beállítás megadása

Az alkalmazás eltávolítását követően a rendszert újra kell indítani. Válassza ki a számítógép újraindítása érdekében végrehajtandó műveletet.

6. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

7. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válassza ki az operációs rendszer eszközeinek segítségével a Hálózati ügynök telepítéséhez használt fiókot. Ebben az esetben rendszergazda jogosultságok szükségesek a számítógép eléréséhez. Több fiókot is hozzáadhat. Ha a fióknak nincs elegendő jogosultsága, a telepítő varázsló a következő fiókot fogja használni. Ha a Hálózati ügynök használatával eltávolítja a Kaspersky Endpoint Security alkalmazást, akkor nem kell fiókot választania.

8. lépés Feladatindítási ütemezés konfigurálása

Állítson be ütemezést egy adott feladat elindításához, például kézi indítást vagy a számítógép tétlen időszakára esőt.

9. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *Kaspersky Endpoint Security 14.1 eltávolítása*.

10. lépés. A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Az alkalmazás csendes módban lesz eltávolítva.

Az alkalmazás eltávolításának menete a Web Console-on, illetve a Cloud Console-on keresztül

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. A **Application** legördülő listából válassza ki az **Kaspersky Security Center** lehetőséget.
2. A **Task type** legördülő listából válassza ki az **Uninstall application remotely** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például *A Kaspersky Endpoint Security eltávolítása a terméktámogatási számítógépekről*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. Választhat például külön adminisztrációs csoportot, vagy létrehozhat egy válogatást.

3. lépés. Alkalmazáseltávolítási beállítások megadása

Ennél a lépésnél adja meg az alkalmazás eltávolítási beállításait:

1. Válassza ki az **Uninstall managed application** típust.
2. Válassza a **Kaspersky Endpoint Security for Windows** lehetőséget.

3. **Force download of the uninstallation utility**. Válassza ki a segédprogram küldésének módját:

   - **Using Network Agent**. Ha nem volt Hálózati ügynök telepítve a számítógépére, akkor először a Hálózati ügynök lesz telepítve az operációs rendszer eszközeinek használatával. Ezután a Kaspersky Endpoint Security el lesz távolítva a Hálózati ügynök eszközeivel.

   - **Using operating system resources through Administration Server**. A segédprogram az operációs rendszer erőforrásaival továbbítva lesznek az ügyfél számítógépekre az Adminisztrációs kiszolgálón keresztül. Ezt az opciót akkor választhatja, ha nincs Hálózati ügynök telepítve az ügyfél számítógépen, és az ügyfél számítógép ugyanazon hálózaton van, mint az Adminisztrációs kiszolgáló.

   - **Using operating system resources through distribution points**. A segédprogram az operációs rendszer erőforrásai használatával, a elosztói pontokon keresztül lesznek elküldve a számítógépekre. Ezt az opciót akkor választhatja, ha legalább egy elosztói pont van a hálózatban. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Súgót.

4. A **Maximum number of concurrent downloads** mezőben adja meg kérelmek maximális számát, amit az Adminisztrációs kiszolgálóra küld az alkalmazás eltávolító segédprogramjának letöltésére. A kérelmek számának korlátja segít megelőzni a hálózat túlterhelését.

5. A **Maximum number of uninstallation attempts** mezőben állítsa be az alkalmazás-eltávolítási kísérletek számának korlátértékét. Ha a Kaspersky Endpoint Security telepítése hibával ér véget, a feladat automatikusan elindítja újra az eltávolítást.

6. Ha szükséges, törölje a jelölést a **Verify operating system type before downloading** jelölőnégyzetből. Ezzel megelőzheti az eltávolítási segédprogram letöltését, ha a számítógép operációs rendszere nem felel meg a szoftverkövetelményeknek. Ha biztos benne, hogy a számítógépe operációs rendszere megfelel a szoftverkövetelményeknek, akkor kihagyhatja ezt a hitelesítést.

4. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válassza ki az operációs rendszer eszközeinek segítségével a Hálózati ügynök telepítéséhez használt fiókot. Ebben az esetben rendszergazda jogosultságok szükségesek a számítógép eléréséhez. Több fiókot is hozzáadhat. Ha a fióknak nincs elegendő jogosultsága, a telepítő varázsló a következő fiókot fogja használni. Ha a Hálózati ügynök használatával eltávolítja a Kaspersky Endpoint Security alkalmazást, akkor nem kell fiókot választania.

5. lépés A feladat létrehozásának befejezése

Fejezze be a varázslót a **Finish** gombra való kattintással. Egy új feladat jelenik meg a feladatok listájában.

A feladat futtatásához jelölje be a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra. Az alkalmazás csendes módban lesz eltávolítva. Az eltávolítás után a Kaspersky Endpoint Security kéri a számítógép újraindítását.

Ha az alkalmazás eltávolítása jelszóval védett, akkor adja meg a KLAdmin fiók jelszavát az *Uninstall application remotely* feladat tulajdonságaiban. Jelszó nélkül a feladat nem lesz végrehajtva.

Ahhoz, hogy használja a KLAdmin fiók jelszavát az Uninstall application remotely feladatban:

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Security Center **Uninstall application remotely** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Tegyen jelölést a **Use uninstallation password** jelölőnégyzetbe.

5. Adja meg a KLAdmin fiók jelszavát.

6. Mentse el a módosításokat.

Az eltávolítás befejezéséhez indítsa újra a számítógépet. Ehhez a Hálózati ügynök megjelenít egy felugró ablakot.

Az alkalmazás távoli eltávolítása az Active Directory segítségével

Távolról is eltávolíthatja az alkalmazást az Microsoft Windows csoportházirendet használva. Az alkalmazás eltávolításához meg kell nyitnia a Csoportházirend-kezelő konzolt (gpmc.msc) és használnia kell a Csoportházirend szerkesztőt az alkalmazás-eltávolítás feladat létrehozásához (további részletekért keresse fel a Microsoft Terméktámogatás honlapot).

Ha az alkalmazáseltávolítási művelet jelszóval védett, a következőket kell tennie:

1. BAT fájl létrehozása a következő tartalommal:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   A `<GUID>` az alkalmazás egyedi azonosítója. Az alkalmazás GUID-ját a Terméktámogatás tudásbázisában vagy a következő parancs segítségével lehet megkeresni:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Példa

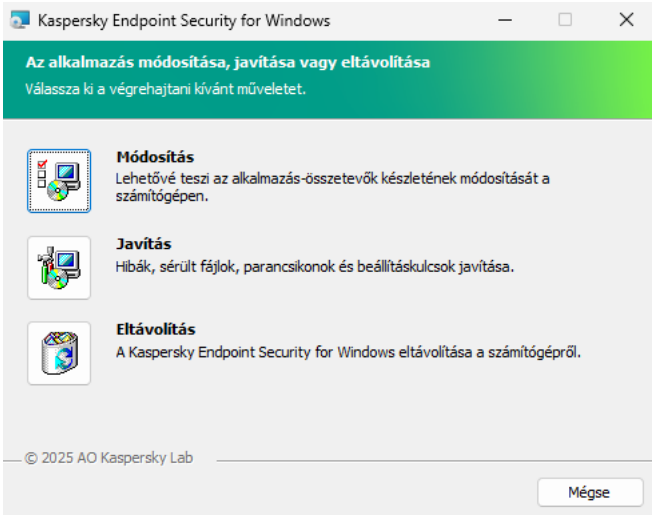
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Új Microsoft Windows létrehozása számítógépek részére a Csoportházirend kezelése konzolban (gpmc.msc).

3. Az új házirend segítségével futtassa a létrehozott BAT fájlt a számítógépeken.

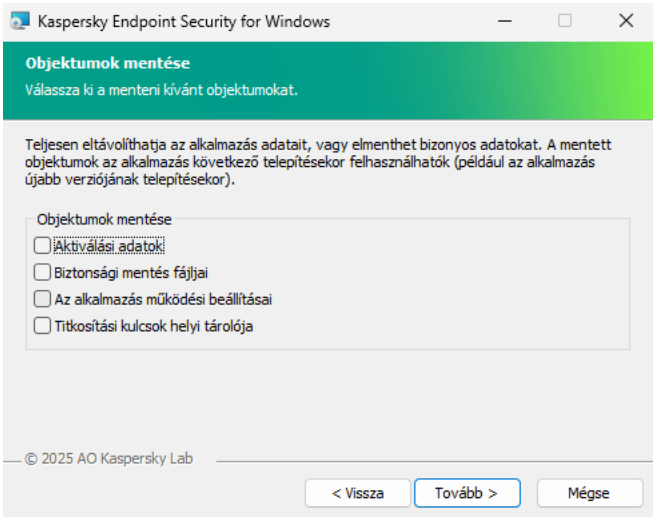
Az alkalmazás helyi eltávolítása

Az alkalmazást helyileg is törölheti a telepítővarázsló segítségével. A Kaspersky Endpoint Security eltávolítása a Windows operációs rendszer normál módszerével történik, tehát a Vezérlőpanelen keresztül. A Telepítővarázsló elindul. Kövesse a képernyőn lévő utasításokat.



Az alkalmazáseltávolítási művelet kiválasztása

Megadhatja, hogy az alkalmazás által használt melyik adatokat szeretné elmenteni a jövőbeli használatra, az alkalmazás következő telepítésekor (például, ha az alkalmazás újabb verziójára frissít). Ha nem ad meg adatokat, a rendszer teljesen eltávolítja az alkalmazást (lásd a lenti ábrát).



Adatok mentése eltávolítás után

Az alábbi adatokat mentheti:

- **Aktiválási adatok**, melyek segítségével nem kell újra aktiválnia az alkalmazást. A Kaspersky Endpoint Security automatikusan hozzáad egy licenckulcsot, ha a licenc nem járt le a telepítés előtt.
- **Biztonsági mentés fájljai** – az alkalmazás által vizsgált, és a Karanténba helyezett fájlok.

> Az alkalmazás eltávolítása után mentett, a Biztonsági mentés fájljai csak az alkalmazásnak ugyanazon verziójából érhetők el, mint amelyet mentésükhöz használt.

Ha az alkalmazás eltávolítása után Biztonsági mentésbe helyezett objektumokat használni szeretné, akkor az alkalmazás eltávolítása előtt vissza kell állítani ezeket az objektumokat. A Kaspersky szakértői azonban nem javasolják a Biztonsági mentés objektumainak visszaállítását, mivel ez kárt tehet a számítógépben.

- **Az alkalmazás működési beállításai** – az alkalmazás beállításainak megadásakor kiválasztott értékei.
- **Titkosítási kulcsok helyi tárolója** – az alkalmazás eltávolítása előtt titkosított fájlokhoz és meghajtókhoz hozzáférést nyújtó adatok. A titkosított fájlok és meghajtók eléréséhez válassza ki az adattitkosítás funkciót, ha újratelepíti a Kaspersky Endpoint Security alkalmazást. Nincs szükség további műveletre a korábban titkosított fájlok és meghajtók eléréséhez.

A Kaspersky Endpoint Security az adatokat a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappába menti.

Az alkalmazást a parancssor használatával is törölheti helyileg.

Az alkalmazás licencelése

Ez a szakasz tájékoztatást nyújt a Kaspersky Endpoint Security licencelésével kapcsolatos általános fogalmakról.

A végfelhasználói licencszerződésről

A *Végfelhasználói licencszerződés* egy kötelező erejű megállapodás Ön és az AO Kaspersky Lab között, amely meghatározza az alkalmazás használatának feltételeit.

Javasoljuk, hogy az alkalmazás használata előtt figyelmesen olvassa el a Végfelhasználói licencszerződés feltételeit.

A Licencszerződés feltételeit az alábbi módokon tekintheti meg:

- A Kaspersky Endpoint Security interaktív módban történő telepítésekor.
- A license.txt fájlt elolvasva. Ez a dokumentum beletartozik az alkalmazás terjesztőkészletébe, valamint az alkalmazás telepítési mappájába is: `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

A Végfelhasználói licencszerződés elfogadásának alkalmazástelepítéskor történő megerősítésével kijelenti, hogy elfogadja a Végfelhasználói licencszerződés feltételeit. Ha nem fogadja el a végfelhasználói licencszerződés feltételeit, meg kell szakítania az alkalmazás telepítését.

A licenc

A *licenc* az alkalmazás időben korlátozott használati joga, amelyet a felhasználó a Végfelhasználói licencszerződés alapján kap.

A licenc feljogosítja Önt az alkalmazásnak a végfelhasználói licencszerződés feltételei alapján történő használatára és a terméktámogatás igénybevételére. Az elérhető funkciók listája és az alkalmazás használatának időtartama az alkalmazás aktiválásához használt licenc típusától függ.

Az alábbi licencek biztosítottak:

- *Próbaverzió* – ingyenes licenc, amely az alkalmazás kipróbálását szolgálja.

  A próbalicenc általában rövid ideig érvényes. A próbalicenc lejárata után a Kaspersky Endpoint Security minden funkciója letiltásra kerül. Az alkalmazás további használatához meg kell vásárolni egy kereskedelmi licencet.

  Mindössze egyszer aktiválhatja az alkalmazást próbalicenccel. Az alkalmazás nem aktiválható próbalicenccel, miután már aktiválták kereskedelmi licenccel.

- *Kereskedelmi* – fizetős licenc, melyet a Kaspersky Endpoint Security vásárlásakor kap.

  A kereskedelmi licenc alapján rendelkezésre álló alkalmazásfunkciók köre a kiválasztott terméktől függ. A kiválasztott termék a Licenctanúsítványon van feltüntetve. A rendelkezésre álló termékekre vonatkozó információ a Kaspersky webhelyén található.

Ha a kereskedelmi licenc lejár, az alkalmazás legfontosabb funkciói letiltásra kerülnek. Az alkalmazás további használatához meg kell újítania a kereskedelmi licencét. Ha nem kívánja megújítani a licencét, akkor el kell távolítania az alkalmazást a számítógépéről.

A licenctanúsítványról

A *licenctanúsítvány* egy, a felhasználó részére a kulcsfájllal vagy aktiváló kóddal együtt átadott dokumentum.

A licenctanúsítvány az alábbi licencadatokat tartalmazza:

- Licencazonosító vagy rendelési szám.
- A licencet kapó felhasználó adatai.
- A licenc segítségével aktiválható alkalmazás adatai.
- A licencelt egységek számára vonatkozó korlátozás (például az, hogy a licenc alapján hány eszközön lehet az alkalmazást használni).
- Licencidőszak kezdési dátuma.
- Licenc lejárati dátuma vagy licencidőszak.
- Licenctípus.

Az előfizetés

Az *előfizetés a Kaspersky Endpoint Security alkalmazásra* egy adott paraméterekkel (például az előfizetés lejárati dátuma, védett eszközök száma) rendelkező alkalmazás megrendelése. Kaspersky Endpoint Security-előfizetés a szolgáltatótól rendelhető (például az internetszolgáltatótól). Az előfizetés megújítható kézileg és automatikusan, illetve le is mondható. Az előfizetését a szolgáltató webhelyén kezelheti.

Az előfizetés lehet korlátozott (például egy éves) vagy korlátlan (lejárati dátum nélküli). Ha a Kaspersky Endpoint Security működését a korlátozott előfizetési időszak lejárta után is szeretné fenntartani, meg kell újítania az előfizetést. A korlátlan előfizetés megújítása automatikus, ha a forgalmazó szolgáltatásainak előre fizetése idejében történik.

Ha egy korlátozott előfizetés lejár, egy türelmi időszak következik, mely alatt az alkalmazás működni fog. Az ilyen türelmi időszakok elérhetőségét és időtartamát a szolgáltató szabja meg.

A Kaspersky Endpoint Security előfizetéses használatához alkalmaznia kell a szolgáltatótól kapott aktiváló kódot. Az aktiváló kód alkalmazását követően a rendszer hozzáadja az aktív kulcsot. Az aktív kulcs határozza meg az alkalmazás előfizetés alapján történő használatának licencét. Az előfizetéses alkalmazást nem lehet kulcsfájl segítségével aktiválni. A szolgáltató csak aktiváló kódot tud biztosítani. Nem lehet tartalék kulcsot hozzáadni előfizetés keretében.

Előfordulhat, hogy az előfizetés alapján vásárolt aktiváló kódok a Kaspersky Endpoint Security korábbi verzióinak aktiválásához nem használhatók.

Tudnivalók a licenckulcsról

A *licenckulcs* olyan bitsorozat, amelynek segítségével aktiválhatja, majd használhatja az alkalmazást a Végfelhasználói licencszerződés feltételeinek megfelelően.

Az előfizetés részeként felvett kulcshoz nem jár licenctanúsítvány.

Az alkalmazáshoz licenckulcsot adhat hozzá egy kulcsfájl használatával vagy egy aktiváló kód megadásával.

A kulcsot a végfelhasználói licencszerződés feltételeinek megsértése esetén a Kaspersky blokkolhatja. Ha a kulcs blokkolva van, az alkalmazás további használatához másik kulcsra van szükség.

Kétféle kulcs létezik: aktív és tartalék.

Az *aktív kulcs* az a kulcs, amelyet az alkalmazás jelenleg használ. A próbaverziós vagy kereskedelmi licenckulcs megadható aktív kulcsként. Az alkalmazásban csak egy aktív kulcs lehet.

A *tartalék kulcs* lehetővé teszi a felhasználó számára az alkalmazás használatát, de jelenleg nincs használatban. Az aktív kulcs lejáratakor a rendszer automatikusan aktivál egy tartalék kulcsot. Tartalék kulcsot csak abban az esetben lehet hozzáadni, ha van elérhető aktív kulcs.

Próbaverziós licenckulcsot csak aktív kulcsként lehet megadni. Tartalék kulcsként történő megadása nem lehetséges. A próbaverziós licenckulcs nem válthatja fel kereskedelmi licenc aktív kulcsát.

Ha egy kulcs van hozzáadva a tiltott kulcsok listájához, az alkalmazás aktiválásához használt licenc által meghatározott alkalmazásfunkciók nyolc napig állnak rendelkezésre. Az alkalmazás értesíti a felhasználót, hogy a kulcs felkerült a tiltott kulcsok listájára. Nyolc nap elteltével az alkalmazás funkciói közül azok maradnak elérhetők, amelyek a licenc lejárta után hozzáférhetők maradnak. A védelmi és felügyeleti összetevőket használhatja, és a licenc lejárta előtt telepített alkalmazás-adatbázisokkal vizsgálatot végezhet. Az alkalmazás továbbra is titkosítja az olyan fájlokat, amelyek módosultak, és a titkosításuk a licenc lejárta előtt történt, azonban új fájlokat nem titkosít. A Kaspersky Security Network reputációs szolgáltatás nem vehető igénybe.

Az aktiváló kód

Az *aktiválási kód* egy egyedi karaktersorozat, amely 20 alfanumerikus karakterből áll. Ön egy aktiváló kód megadásával adhat hozzá licenckulcsot, amely aktiválja a Kaspersky Endpoint Security alkalmazást. Az aktiváló kódot a Kaspersky Endpoint Security megvásárlásakor megadott e-mail-címre kapja.

Az alkalmazás aktiváló kóddal történő aktiválásához internethozzáférés szükséges, hogy a Kaspersky aktiválási kiszolgálóihoz kapcsolódhasson.

Amikor az alkalmazás aktiválását az aktiváló kóddal hajtja végre, azzal hozzáadja az aktív kulcsot. A tartalék kulcsot csak aktiváló kóddal lehet hozzáadni, kulcsfájl segítségével nem.

Ha az alkalmazás aktiválását követően elveszti az aktiváló kódot, a kódot visszaállíthatja. Az aktiváló kód például Kaspersky CompanyAccount fiók regisztrálásakor szükséges. Ha az aktiváló kód az alkalmazás aktiválása után elveszett, forduljon ahhoz a Kaspersky-partnerhez, ahol a licencet vásárolta.

A kulcsfájl

A *kulcsfájl* egy .key kiterjesztésű fájl, melyet Ön a Kaspersky vállalattól kap. A kulcsfájl célja az alkalmazást aktiváló licenckulcs megadása.

A kulcsfájlt arra az e-mail-címre kapja, amelyet a Kaspersky Endpoint Security megvásárlásakor vagy a Kaspersky Endpoint Security próbaverziójának megrendelésekor megadott.

Az alkalmazás kulcsfájllal történő aktiválásához nem szükséges a Kaspersky aktiválási kiszolgálóihoz kapcsolódnia.

A kulcsfájlt visszaállíthatja, ha véletlenül törlődik. Kulcsfájlra például Kaspersky CompanyAccount fiók regisztrálásához lehet szüksége.

Kulcsfájl visszaállításához tegye az alábbiak valamelyikét:

- Lépjen kapcsolatba a licenc eladójával.
- Kulcsfájl beszerzése a Kaspersky webhelyen a meglévő aktiváló kód alapján.
- Kulcsfájl beszerzése egy másik felügyeleti kiszolgálóról.

Amikor az alkalmazás aktiválását a kulcsfájllal hajtja végre, azzal hozzáadja az aktív kulcsot. Tartalék kulcsot csak kulcsfájllal lehet hozzáadni, aktiváló kód segítségével nem.

Alkalmazások funkcionalitásának összehasonlítása a munkaállomási licenctípustól függően

A munkaállomásokon elérhető Kaspersky Endpoint Security funkciói a licenctípustól függenek (lásd az alábbi táblázatot).

Lásd még az alkalmazásfunkciók összehasonlítását a kiszolgálók esetében

Az alkalmazás funkcióinak összehasonlítását a Kaspersky Next licenc típusától függően a Kaspersky Next Súgóban találja.

A Kaspersky Endpoint Security funkcióinak összehasonlítása

Funkció	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Fenyegetések elleni fejlett védelem								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Viselkedészlelés	✓	✓	✓	✓	✓	✓	✓	✓

Funkció	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Biztonsági rések kihasználásának megelőzése	✓	✓	✓	✓	✓	✓	✓	✓
Behatolásmegelőző rendszer	✓	✓	✓	✓	✓	✓	✓	✓
Kármentesítő motor	✓	✓	✓	✓	✓	✓	✓	✓
Fenyegetések elleni alapvető védelem								
Fájl védelem	✓	✓	✓	✓	✓	✓	✓	✓
Web védelem	✓	✓	✓	✓	✓	✓	✓	✓
Levelezés védelem	✓	✓	✓	✓	✓	✓	✓	✓
Tűzfal	✓	✓	✓	✓	✓	✓	✓	✓
Hálózati védelem	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB védelem	✓	✓	✓	✓	✓	✓	✓	✓
AMSI védelem	✓	✓	✓	✓	✓	✓	✓	✓
Biztonsági felügyelet								
Naplóvizsgálat	–	–	–	–	–	–	–	–
Alkalmazásfelügyelő	✓	✓	✓	✓	✓	✓	✓	✓
Eszközfelügyelő	✓	✓	✓	✓	✓	✓	✓	✓
Webfelügyelő	✓	✓	✓	✓	✓	✓	✓	✓
Adaptív Anomáliafelügyelő	–	✓	✓	✓	✓	✓	–	✓
Rendszerintegritás-figyelő	–	–	–	–	–	–	–	–
Adattitkosítás								
Kaspersky lemeztitkosítás	–	✓	✓	✓	✓	✓	–	✓
BitLocker meghajtótitkosítás	–	✓	✓	✓	✓	✓	–	✓
Fájl szintű titkosítás	–	✓	✓	✓	✓	✓	–	✓
Cserélhető meghajtók titkosítása	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(A Kaspersky Sandbox-licencet külön kell megvásárolni)*	✓	✓	✓	✓	✓	✓	✓	✓

Funkció	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Integráció az KUMA-rel *(a KUMA integráció licencét külön kell megvásárolni)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent üzemmód *(az alkalmazás aktiválásához licenckulcsot kell hozzáadnia ahhoz az SVM-hez, amelyhez a Light Agent csatlakozik)*	–	–	–	–	–	–	✓	✓

Alkalmazások funkcionalitásának összehasonlítása a kiszolgálói licenctípustól függően

A kiszolgálókon elérhető Kaspersky Endpoint Security funkciói a licenctípustól függenek (lásd az alábbi táblázatot).

Lásd még az alkalmazásfunkciók összehasonlítását a munkaállomások esetében

Az alkalmazás funkcióinak összehasonlítását a Kaspersky Next licenc típusától függően a Kaspersky Next Súgóban találja.

A Kaspersky Endpoint Security funkcióinak összehasonlítása

Funkció	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Fenyegetések elleni fejlett védelem								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Viselkedésészlelés	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Biztonsági rések kihasználásának megelőzése	✓	✓	✓	✓	✓	✓	✓	✓
Behatolásmegelőző rendszer	–	–	–	–	–	–	–	–
Kármentesítő motor	✓	✓	✓	✓	✓	✓	✓	✓
Fenyegetések elleni alapvető védelem								
Fájl védelem	✓	✓	✓	✓	✓	✓	✓	✓
Web védelem	–	✓	✓	✓	✓	✓	✓	✓
Levelezés védelem	–	✓	✓	✓	✓	✓	✓	✓

Funkció	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Tűzfal	✓	✓	✓	✓	✓	✓	✓	✓
Hálózati védelem	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB védelem	✓	✓	✓	✓	✓	✓	✓	✓
AMSI védelem	✓	✓	✓	✓	✓	✓	✓	✓
Biztonsági felügyelet								
Naplóvizsgálat	–	–	–	–	–	–	–	✓
Alkalmazásfelügyelő	–	✓	✓	✓	✓	✓	–	✓
Eszközfelügyelő	–	✓	✓	✓	✓	✓	✓	✓
Webfelügyelő	–	✓	✓	✓	✓	✓	✓	✓
Adaptív Anomáliafelügyelő	–	–	–	–	–	–	–	–
Rendszerintegritás-figyelő	–	–	–	–	–	–	–	✓
Adattitkosítás								
Kaspersky lemeztitkosítás	–	–	–	–	–	–	–	–
BitLocker meghajtótitkosítás	–	✓	✓	✓	✓	✓	–	✓
Fájl szintű titkosítás	–	–	–	–	–	–	–	–
Cserélhető meghajtók titkosítása	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(A Kaspersky Sandbox-licencet külön kell megvásárolni)*	✓	✓	✓	✓	✓	✓	✓	✓
Integráció az KUMA-rel *(a KUMA integráció licencét külön kell megvásárolni)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent üzemmód *(az alkalmazás aktiválásához licenckulcsot kell hozzáadnia ahhoz az SVM-hez, amelyhez a Light Agent csatlakozik)*	–	–	–	–	–	–	✓	✓

Alkalmazás aktiválása

Az *Aktiválás* annak a licencnek az aktiválását jelenti, amellyel lejártáig az alkalmazás teljesen funkcionális verzióját használhatja. Az alkalmazás aktiválása során meg kell adni egy licenckulcsot.

Az alkalmazást az alábbi módokon aktiválhatja:

- Helyileg az alkalmazás felületéről, az Aktiváló Varázsló segítségével. Így az aktív és a tartalék kulcsot is megadhatja.
- A Kaspersky Security Center szoftvercsomag távoli használata.
  - A *Kulcs hozzáadása* feladat használata.

    Ezzel a módszerrel hozzáadhat egy kulcsot egy megadott számítógéphez vagy számítógépekhez, amik az adminisztrációs csoport tagjai. Így az aktív és a tartalék kulcsot is megadhatja.
  - A számítógépekkel történő kulcsmegosztással, ami a Kaspersky Security Center felügyeleti kiszolgálóján van.

    Ezzel a módszerrel automatikusan hozzáadhat egy kulcsot a számítógépekhez, amik más csatlakozva vannak a Kaspersky Security Center-hez, valamint új számítógépekhez is. A módszer használatával először hozzá kell adnia a kulcsot a Kaspersky Security Center felügyeleti kiszolgálóhoz. A Kaspersky Security Center felügyeleti kiszolgálójához történő kulcshozzáadáshoz lásd a Kaspersky Security Center Súgót.

    > Elsőként az előfizetés alapján vásárolt aktiváló kód terjesztésére kerül sor.

  - A kulcs Kaspersky Endpoint Security telepítőcsomaghoz való hozzáadásával.

    Ez a módszer lehetővé teszi a kulcs hozzáadását a telepítőcsomag tulajdonságaihoz a Kaspersky Endpoint Security üzembe helyezése során. Az alkalmazás a telepítés után automatikusan aktiválódik.
- A parancssor használatával.

> Az alkalmazás aktiváló kóddal történő aktiválása eltarthat egy ideig (a távoli, illetve a nem interaktív telepítés során) a Kaspersky aktiválási kiszolgálói közti terheléselosztás miatt. Ha az alkalmazást azonnal aktiválni szeretné, megszakíthatja a folyamatban lévő aktiválási eljárást, és elkezdheti az aktiválást az Aktiválási varázslóval.

> Ha a Kaspersky Endpoint Security alkalmazást Light Agent üzemmódban használja a virtuális környezetek védelmére, nem kell külön aktiválnia az alkalmazást.

Alkalmazás aktiválása

Az alkalmazás aktiválásának menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Kulcs hozzáadása** elemet.

2. lépés Kulcs hozzáadása

Adjon meg aktiválási kódot, vagy jelöljön ki egy kulcsfájlt.

Ha további részletekre kíváncsi arra vonatkozóan, hogy miként adhat kulcsokat a Kaspersky Security Center tárolójához, olvassa el a Kaspersky Security Center súgóját.

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés Feladatindítási ütemezés konfigurálása

Állítson be ütemezést egy adott feladat elindításához, például kézi indítást vagy a számítógép tétlen időszakára esőt.

5. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *Kaspersky Endpoint Security for Windows aktiválása*.

6. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Ennek eredményeképpen a rendszer csendes módban aktiválja a Kaspersky Endpoint Security alkalmazást minden felhasználói számítógépen.

Az alkalmazás aktiválásának menete a Web Console-ban, illetve a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.
2. A **Task type** legördülő listából válassza ki az **Add key** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például: *A Kaspersky Endpoint Security for Windows aktiválása*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört. Lépjen a következő lépésre.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. Lépés Licenc kiválasztása

Válassza ki a licencet, amivel aktiválni szeretné az alkalmazást. Lépjen a következő lépésre.

Hozzáadhat kulcsokat a Webfelügyelőhöz (**Operations** → **Licensing**).

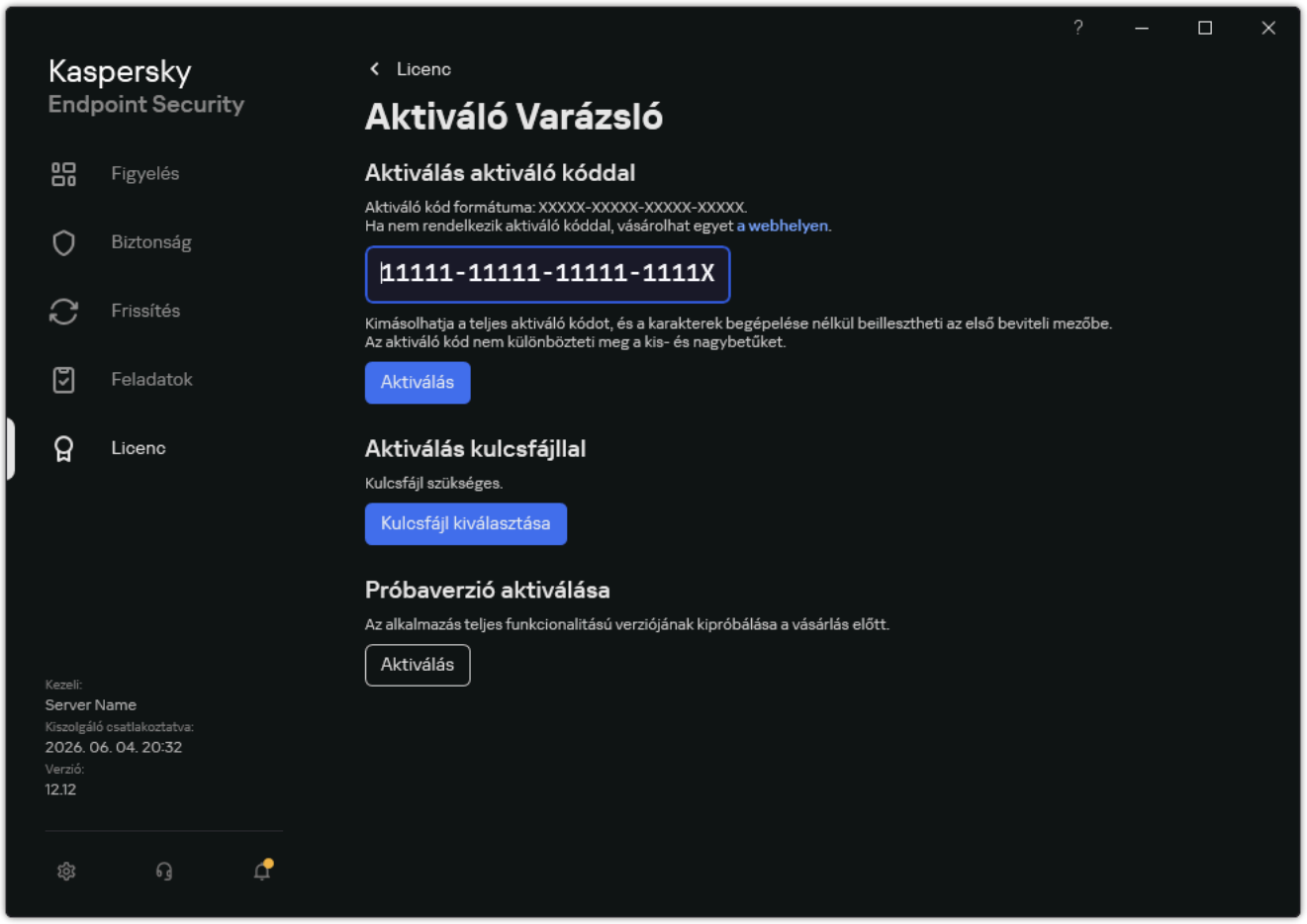
4. lépés A feladat létrehozásának befejezése

Fejezze be a varázslót a **Finish** gombra való kattintással. Egy új feladat jelenik meg a feladatok listájában. A feladat futtatásához jelölje be a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra. Ennek eredményeképpen a rendszer csendes módban aktiválja a Kaspersky Endpoint Security alkalmazást minden felhasználói számítógépen.

Az alkalmazás aktiválása az alkalmazás felületén

1. Nyissa meg a fő alkalmazásablakban a **Licenc** részt.
2. Kattintson **Az alkalmazás aktiválása új licenc használatával** elemre.

Elindul az Alkalmazás aktiválása varázsló. Kövesse az Aktiválási varázsló utasításait.



Alkalmazás aktiválása

A *Kulcs hozzáadása* feladat tulajdonságaiban megadhat egy tartalék kulcsot a számítógéphez. A *tartalék kulcs* akkor lép érvénybe, amikor az aktív kulcs érvényessége lejár. A rendelkezésre álló tartalék kulcs segítségével elkerülheti, hogy az alkalmazás funkciói csak korlátozottan legyenek elérhetők a licenc lejárata esetén.

Licenckulcs automatikus hozzáadása az Adminisztrációs Konzolon keresztül (MMC)

1. Az Adminisztrációs Konzolon nyissa meg a **Kaspersky Licenses** mappát.

   Megnyílik a licencek listája.

2. Nyissa meg a licenckulcs tulajdonságait.

3. A **General** részben jelölje be az **Automatically distribute license key to managed devices** jelölőnégyzetet.

4. Mentse el a módosításokat.

   Ennek eredményeképp a kulcs automatikusan meg lesz osztva a megfelelő számítógépekkel. Egy kulcs akár aktív, akár tartalék kulcsként történő automatikus megosztása esetén a számítógépek számára vonatkozóan (a kulcs tulajdonságaiban megadott) licencelési korlát van érvényben. A licencelés korlátjának elérése esetén a kulcs megosztása automatikusan leáll. A kulccsal ellátott számítógépek számát és más adatokat megtekinthet a kulcstulajdonságai között, az **Devices** területen.

Licenckulcs számítógépekhez való automatikus hozzáadásának menete a Web Console-on, illetve a Cloud Console-on keresztül

1. A Web Console fő ablakában válassza az **Operations** → **Licensing** → **Licenses** lehetőséget.

   Megnyílik a licencek listája.

2. Nyissa meg a licenckulcs tulajdonságait.

3. A **General** lapon engedélyezze a **Automatically distribute license key to managed devices** kapcsolót.

4. Mentse el a módosításokat.

Ennek eredményeképp a kulcs automatikusan meg lesz osztva a megfelelő számítógépekkel. Egy kulcs akár aktív, akár tartalék kulcsként történő automatikus megosztása esetén a számítógépek számára vonatkozóan (a kulcs tulajdonságaiban megadott) licencelési korlát van érvényben. A licencelés korlátjának elérése esetén a kulcs megosztása automatikusan leáll. A kulcstulajdonságokban megtekintheti a számítógépeket, amikhez a kulcs hozzá lett adva, valamint egyéb adatokat is, ha az **Devices** fülre lép.

Ha az alkalmazást *aktiváló kóddal* aktiválja, internet-hozzáférésre van szükség a Kaspersky aktiváló kiszolgálóihoz való csatlakozáshoz. Ha az alkalmazást *kulcsfájl* segítségével aktiválja, nincs szükség internet-hozzáférésre. Ha a számítógépek internet-hozzáférés nélküli, elszigetelt hálózati szegmensben vannak, az alkalmazás kóddal történő aktiválásához engedélyeznie kell a Kaspersky Security Center Felügyeleti kiszolgáló proxykiszolgálói használatát. Ez azt jelenti, hogy az alkalmazás az internet-hozzáféréssel rendelkező felügyeleti kiszolgálón keresztül férhet hozzá az aktiváló kiszolgálókhoz.

A felügyeleti kiszolgáló proxykiszolgálói használatának engedélyezése az alkalmazás aktiválásához a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.

4. Jelölje be **A Kaspersky Security Center használata proxykiszolgálóként az aktiváláshoz** jelölőnégyzetet.

5. Mentse el a módosításokat.

A felügyeleti kiszolgáló proxykiszolgálói használatának engedélyezése az alkalmazás aktiválásához a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **KSC Integration** elemet.

5. Tegyen jelölést a **Use Kaspersky Security Center as proxy server for activation** jelölőnégyzetbe.

6. Mentse el a módosításokat.

Ha nem tudja aktiválni az alkalmazást egy *aktiváló kóddal*, megpróbálhat szerezni egy *kulcsfájlt* a Kaspersky megoldás segítségével, és megkísérelheti újból aktiválni az alkalmazást egy másik módszerrel.

Licenchasználat figyelése

A licencek használatát a következő módokon figyelheti meg:

- Tekintse meg a *Report on usage of license keys* elemet a szervezet felépítése tekintetében (**Monitoring** → **Reports**).
- A számítógép állapotának megtekintésével az **Managed devices** →**Devices** fülön. Ha az alkalmazás nincs aktiválva, a számítógép állapota ⚠ *Az alkalmazás nincs aktiválva* lesz.
- Tekintse meg a licencadatokat a számítógép tulajdonságaiban.
- Kulcstulajdonságok megtekintése (**Operations** → **Licensing**).

Az alkalmazás Kaspersky Security Center Cloud Console részeként történő aktiválásának jellemzői

A Kaspersky Security Center Cloud Console alkalmazáshoz jár egy próbaverzió. A *próbaverzió* a Kaspersky Security Center Cloud Console egy speciális verziója, ami ismerteti a felhasználót az alkalmazás funkcióival. A verzióval 30 napon át végezhet műveleteket a munkafelületen. Minden kezelt alkalmazás automatikusan fut a Kaspersky Security Center Cloud Console próbalicence alatt, köztük a Kaspersky Endpoint Security is. Azonban nem fogja tudni aktiválni a Kaspersky Endpoint Security alkalmazást a saját próbalicence alatt, miután a Kaspersky Security Center Cloud Console próbalicence lejár. A Kaspersky Security Center licencéről szóló részletes információért kérjük, olvassa el a következőt: Kaspersky Security Center Cloud Console Help.

A Kaspersky Security Center Cloud Console próbalicence nem teszi lehetővé, hogy egymás után váltson kereskedelmi verzióra. 30 nappal a próbaidőszak lejárta után a munkafelület összes tartalma törlődik.

Licenckulcs eltávolítása

A licenckulcs eltávolításához egy speciális feladatot kell futtatnia a számítógépeken. Eltávolíthat egy licenckulcsot, például a licencegységek átrendezéséhez. Ezenkívül a licenc lejártakor a Kaspersky Endpoint Security értesíti Önt. Ha olyan licenckulcsot adott hozzá, amely rövid időre szól az alkalmazás kipróbálása céljából (például: EDR Optimum kiegészítő), akkor eltávolíthatja ezt a licenckulcsot, hogy eltűnjenek az értesítések, és javítsa a számítógép állapotát.

A *Kulcs eltávolítása* feladat lehetővé teszi a licenckulcsok eltávolítását a számítógépről. Eltávolíthat aktív licenckulcsokat és tartalék licenckulcsokat. A Kaspersky Endpoint Security aktiválási licenckulcsán kívül a Kaspersky Detection and Response megoldások (például EDR Optimum kiegészítő) egyes licenckulcsait is eltávolíthatja.

Licenckulcs eltávolítása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Kulcs eltávolítása** elemet.

2. lépés Licenc kiválasztása

Válassza ki a törölni kívánt licenckulcsot. Kiválaszthat egy licenckulcsot a Kaspersky Security Center kulcstárolójából, vagy választhat egy kulcsfájlt.

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés Feladatindítási ütemezés konfigurálása

Állítson be ütemezést egy adott feladat elindításához, például kézi indítást vagy a számítógép tétlen időszakára esőt.

5. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *A bétakulcs eltávolítása*.

6. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Licenckulcs eltávolítása a Web Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.
2. A **Task type** legördülő listából válassza ki az **Remove key** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *A bétakulcs eltávolítása*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört. Lépjen a következő lépésre.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. Lépés Licenc kiválasztása

Válassza ki a törölni kívánt licenckulcsot. Kiválaszthat egy licenckulcsot a Kaspersky Security Center kulcstárolójából, vagy választhat egy kulcsfájlt. Lépjen a következő lépésre.

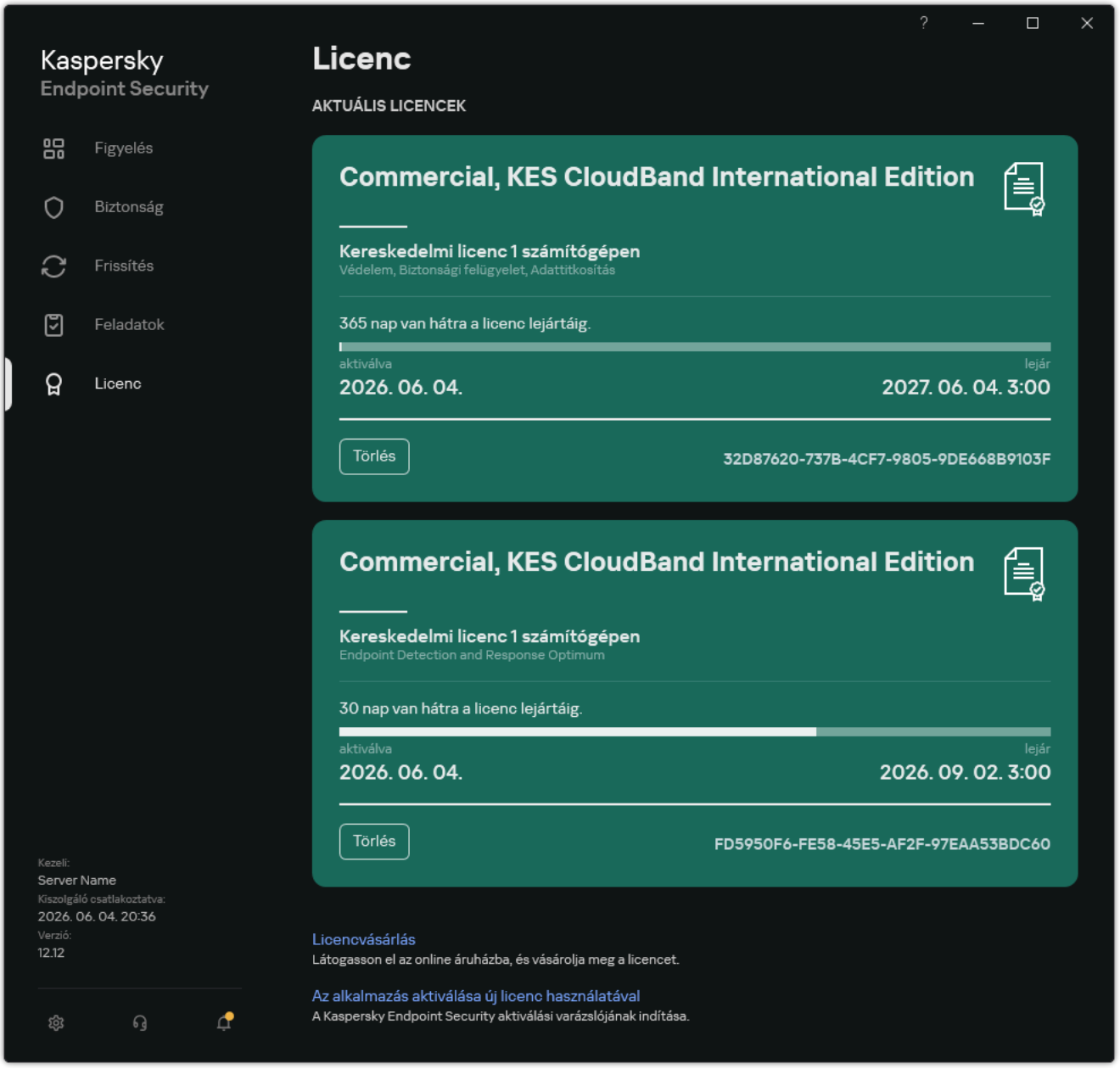
4. lépés A feladat létrehozásának befejezése

Fejezze be a varázslót a **Finish** gombra való kattintással. Egy új feladat jelenik meg a feladatok listájában. A feladat futtatásához jelölje be a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra.

Licenckulcs eltávolítása az alkalmazás felületén

1. Nyissa meg a fő alkalmazásablakban a **Licenc** részt.

2. Válassza ki a törölni kívánt kulcsot, és kattintson a **Törlés** gombra.



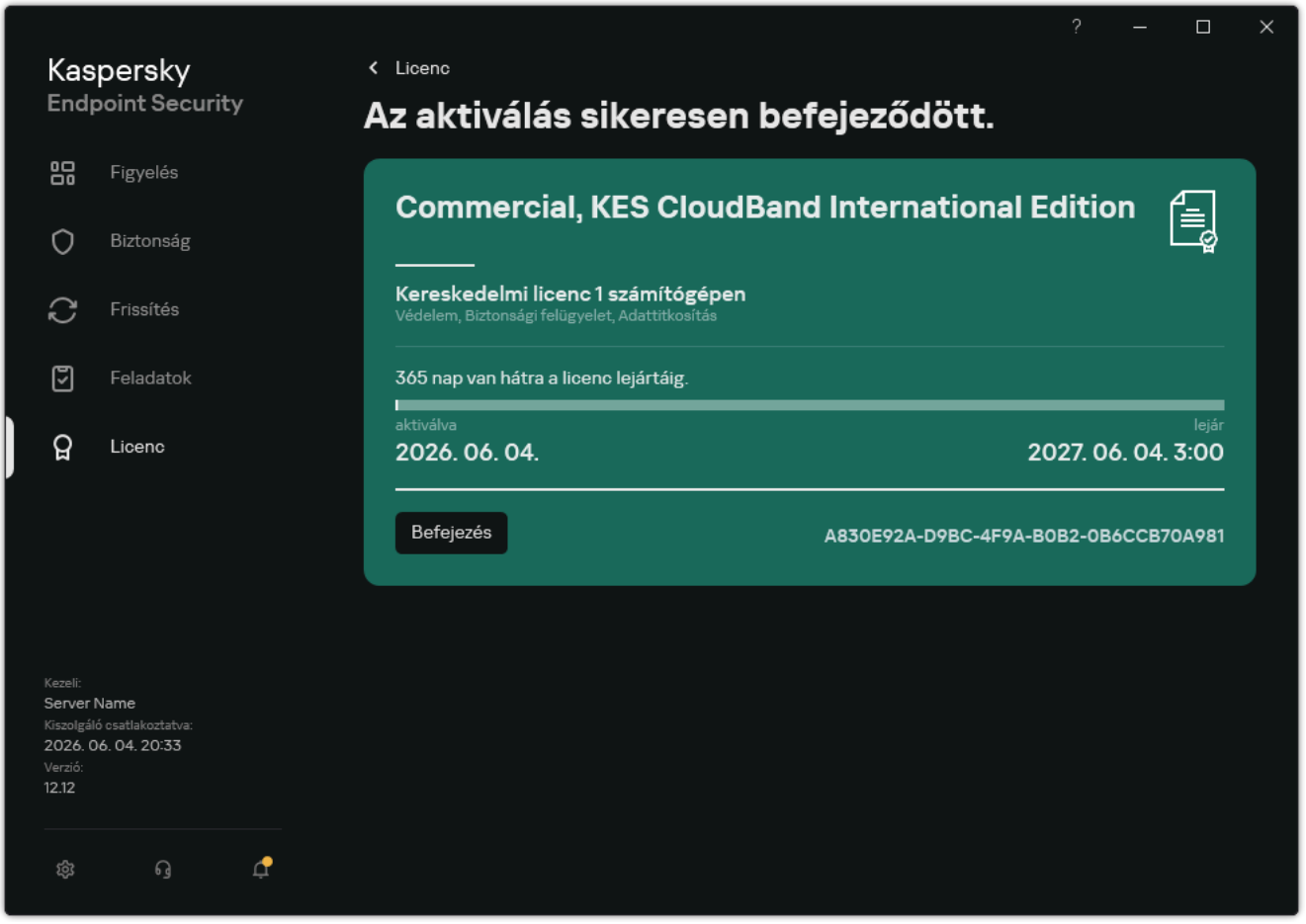
Licenckezelés ablak

Azt is megteheti, hogy egy licenckulcsot a parancssorban távolít el.

A licencadatok megtekintése

Információk megtekintése a licencről:

Nyissa meg a fő alkalmazásablakban a **Licenc** részt (lásd az alábbi ábrát).



Licenckezelés ablak

A szakaszban az alábbi részletek láthatók:

- *Kulcs állapota*. Számos kulcs tárolható a számítógépen. Kétféle kulcs létezik: aktív és tartalék. Az alkalmazásban csak egy aktív kulcs lehet. Tartalék kulcs csak akkor válhat aktívvá, ha az aktív kulcs lejárt, vagy ha a kulcsot korábban törölték a **Törlés** gombra kattintva.
- *Alkalmazásnév*. A megvásárolt Kaspersky alkalmazás teljes neve.
- *Licenctípus*. A következő típusú licencek érhetőek el: próbaverzió és kereskedelmi.
- *Funkció*. A licence alatt elérhető alkalmazásfunkciók. A funkciók közé tartozhat a Védelem, a Biztonsági felügyelet, az Adattitkosítás és egyebek. Az elérhető funkciók listája a Licenctanúsítványban is megtalálható.

- *További információk a licencről*. A licencidőszak kezdő és záró dátuma (csak az aktív kulcs esetében), a licencidőszak hátralévő időtartama.

  A licenc lejárati dátuma az operációs rendszerben konfigurált időzóna alapján jelenik meg.

- *Kulcs*. A kulcs egy egyedi alfanumerikus sorozat, ami az aktiváló kódból vagy a kulcsfájlból van létrehozva.

A Licencelés ablakban az alábbiak egyikét is megteheti:

- **Licencvásárlás/Licenc megújítása**. Megnyitja a Kaspersky online üzletének weboldalát, ahol vásárolhat vagy megújíthat egy licencet. Ehhez adja meg a vállalati információit, majd fizessen a rendelésért.

- **Az alkalmazás aktiválása új licenc használatával**. Elindítja az Alkalmazás aktiválása varázslót. Ebben a Varázslóban hozzáadhat egy kulcsot az aktiváló kód vagy a kulcsfájl használatával. Az alkalmazás aktiválási varázslója egy aktív kulcs és egy tartalék kulcs hozzáadását teszi lehetővé.

Licenc vásárlása

Az alkalmazás telepítését követően licencet vásárolhat. Licenc vásárlásakor kap egy aktiváló kódot vagy egy kulcsfájlt, amellyel aktiválhatja az alkalmazást.

Licenc vásárlása:

1. Nyissa meg a fő alkalmazásablakban a **Licenc** részt.

2. Végezze el az alábbiak egyikét:

   - Ha nem adott meg kulcsot, vagy próbalicenchez való kulcsot adott meg, kattintson a **Licencvásárlás** gombra.

   - Ha kereskedelmi licenchez való kulcsot adott meg, kattintson a **Licenc megújítása** gombra.

   Megnyílik egy ablak, melyben a Kaspersky internetes áruházának webhelye látható, ahol licencet vásárolhat.

Előfizetés megújítása

Ha alkalmazást előfizetés alapján használja, a Kaspersky Endpoint Security az előfizetés lejártáig automatikusan adott időközönként kapcsolatba lép az aktiválási kiszolgálóval.

Ha alkalmazást korlátlan előfizetés alapján használja, a Kaspersky Endpoint Security a háttérben automatikusan ellenőrzi, hogy az aktiválási kiszolgálón vannak-e megújított kulcsok. Ha az aktiválási kiszolgálón egy kulcs áll rendelkezésre, az alkalmazás a korábbi kulcsot lecseréli rá. Ily módon a Kaspersky Endpoint Security korlátlan előfizetése a felhasználó közbenjárása nélkül megújításra kerül.

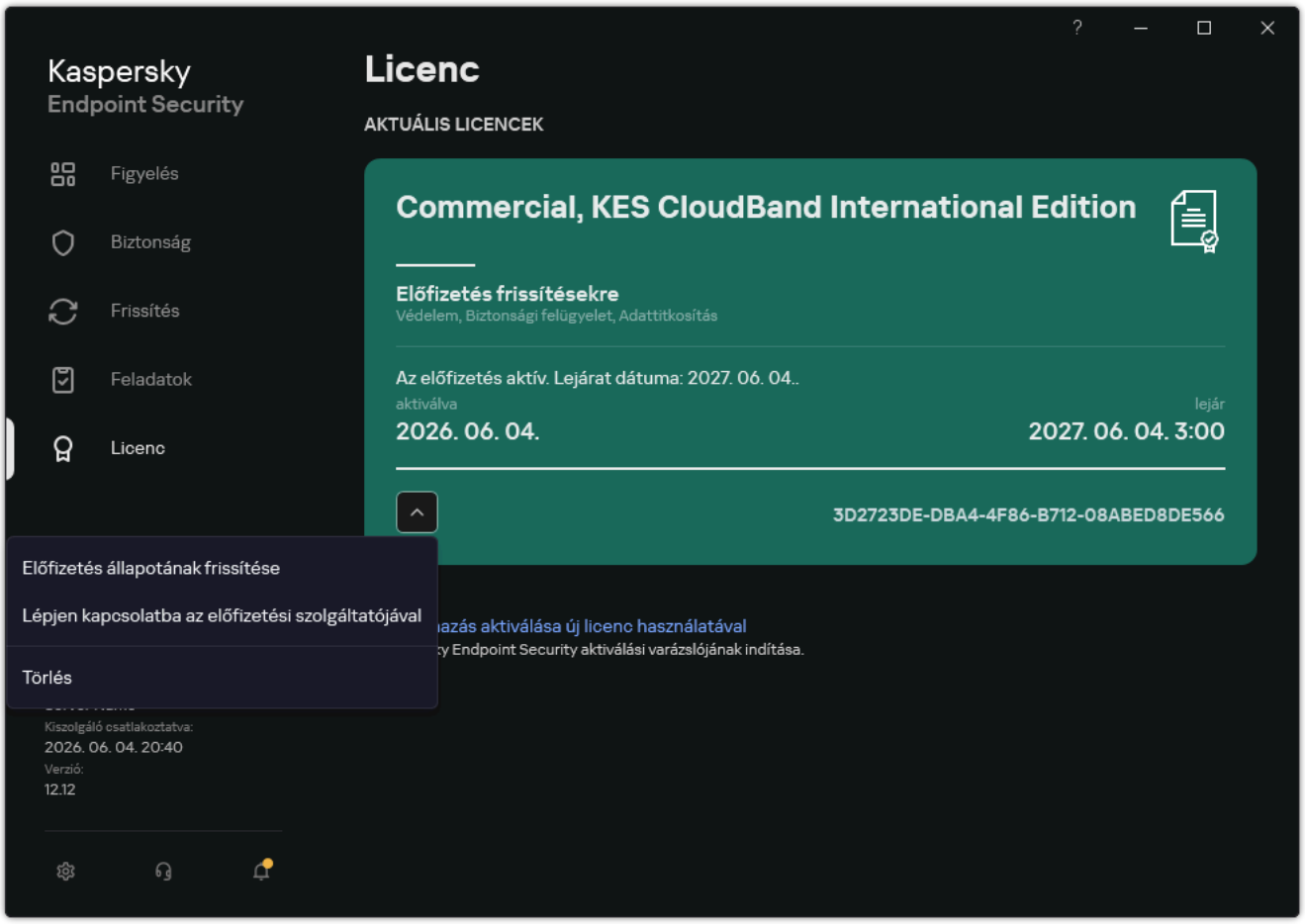
Ha az alkalmazást korlátozott előfizetés alapján használja, akkor az előfizetés (vagy az előfizetés türelmi időszaka) lejártának napján a Kaspersky Endpoint Security értesíti, és felhagy az előfizetés automatikus meghosszabbítási kísérletével. Ilyenkor a Kaspersky Endpoint Security ugyanúgy viselkedik, mint amikor az alkalmazás kereskedelmi licence jár le: az alkalmazás frissítések nélkül működik, a Kaspersky Security Network pedig nem használható.

Az előfizetést automatikusan megújíthatja a szolgáltató webhelyén.

A szolgáltató webhelyének felkeresése az alkalmazás felületéről:

1. Nyissa meg a fő alkalmazásablakban a **Licenc** részt.
2. Kattintson a **Lépjen kapcsolatba az előfizetési szolgáltatójával** elemre.

Az előfizetés állapotát manuálisan is frissítheti. Erre akkor lehet szükség, ha az előfizetést a türelmi időszak után hosszabbította meg, és az alkalmazás nem frissítette automatikusan az előfizetés állapotát.



Előfizetés megújítása

Első lépések

A Kaspersky Endpoint Security telepítése után a következő felületekkel kezelheti az alkalmazást:

- Helyi alkalmazásfelület.
- Kaspersky Security Center Adminisztrációs Konzol.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Adminisztrációs Konzolt

A Kaspersky Security Center segítségével távolról telepítheti és eltávolíthatja, illetve elindíthatja és leállíthatja a Kaspersky Endpoint Security alkalmazást, megadhatja az alkalmazás beállításait, módosíthatja a rendelkezésre álló alkalmazásösszetevők körét, kulcsokat adhat meg, valamint frissítési és vizsgálati feladatokat indíthat el és állíthat le.

Az alkalmazás a Kaspersky Security Centeren keresztül a Kaspersky Endpoint Security Adminisztrációs bővítmény segítségével kezelhető.

A Kaspersky Security Center alkalmazáskezeléséről szóló további részletekért lásd a Kaspersky Security Center súgót.

Kaspersky Security Center Web Console és Kaspersky Security Center Cloud Console

A Kaspersky Security Center Web Console (továbbiakban „*Web Console*") a fő feladatok központi elvégzésére szánt webes alkalmazás, ami kezeli és karbantartja a szervezet hálózatának biztonsági rendszerét. A Webfelügyelő egy olyan Kaspersky Security Center összetevő, ami felhasználói felületet biztosít. A Kaspersky Security Center Web Console-ról szóló részletes információkért kérjük, olvassa el a következőt: Kaspersky Security Center Súgó.

A Kaspersky Security Center Cloud Console (a továbbiakban „*Cloud Console*") egy felhőalapú megoldás, ami védi és kezeli egy vállalat hálózatát. A Kaspersky Security Center Cloud Console-ról szóló részletes információkért kérjük, lásd a Kaspersky Security Center Cloud Console Súgót.

A Web Console és a Cloud Console segítségével a következőket teheti:

- Megfigyelheti az intézmény biztonsági rendszerének állapotát.
- Telepítheti a Kaspersky alkalmazásokat az eszközén a hálózatán belül.
- Kezelheti a telepített alkalmazásokat.
- A biztonsági rendszer állapotának jelentéseinek megtekintése.

A Kaspersky Endpoint Security Web Console, Cloud Console és a Kaspersky Security Center Adminisztrációs konzol helyen keresztül történő kezelésével különböző kezelési lehetőségek érhetőek el. Az elérhető összetevők és feladatok a különböző Konzoloktól függően eltérőek lehetnek.

Tudnivalók a Kaspersky Endpoint Security for Windows adminisztrációs bővítményről

A Kaspersky Endpoint Security for Windows adminisztrációs bővítmény lehetővé teszi a Kaspersky Endpoint Security és a Kaspersky Security Center közötti interakciót. Az Adminisztrációs bővítménnyel kezelheti a Kaspersky Endpoint Security alkalmazást, a következők használatával: rendszabályok, feladatok és helyi alkalmazásbeállítások. A Kaspersky Security Center Web Console alkalmazással történő interakciót a webes bővítmény biztosítja.

Az Adminisztrációs bővítmény verziója az ügyfélszámítógépen telepített Kaspersky Endpoint Security alkalmazás verziójától eltérhet. Ha az Adminisztrációs bővítmény telepített verziója kevesebb funkciót kínál, mint a Kaspersky Endpoint Security telepített verziója, akkor a hiányzó funkciók beállításait az adminisztrációs bővítmény nem szabályozza. Ezeket a beállításokat a felhasználó a Kaspersky Endpoint Security helyi felületén adhatja meg.

A webes bővítmény alapértelmezetten nincs telepítve a Kaspersky Security Center Web Console. A webes beépülő modult olyan számítógépen kell telepíteni, amelyen telepítve van a Kaspersky Security Center Web Console. A webes bővítmény funkciója minden rendszergazdának elérhető, akik hozzáférnek a Webfelügyelőhöz egy böngészőben. Megtekintheti a telepített webes bővítmények listáját a Web Console felületén (**Console settings** → **Web plug-ins**). A webes bővítmények kompatibilitásáról és a Webfelügyelőről szóló további információkért lásd a Kaspersky Security Center Súgót.

Ha a Kaspersky Endpoint Security terméket a Kaspersky Endpoint Detection and Response Optimum megoldás részeként használja, telepítenie kell a Kaspersky Endpoint Detection and Response adminisztrációs bővítményt. Szükség van a adminisztrációs bővítményre a riasztás részleteinek megjelenítéséhez. Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Így a fenyegetéselhárítási feladatok létrehozásához szükség van a Kaspersky Endpoint Security adminisztrációs bővítményre, a riasztások részleteinek megtekintéséhez pedig az EDR adminisztrációs bővítményre.

A webes bővítmény telepítése

A következőképp telepítheti a webes bővítményt:

- A webes bővítmény telepítése a Kaspersky Security Center Web Console Kezdeti beállító varázslójával.

  A Web Console automatikusan figyelmezteti, hogy futtassa a Kezdeti beállító varázslót, ha először csatlakoztatja a Web Console-t az Adminisztrációs kiszolgálóhoz. A Web Console felületén is futtathatja a Kezdeti beállító varázslót (**Discovery & deployment** → **Deployment & assignment** → **Quick start wizard**). A Kezdeti beállító varázsló ellenőrzi, hogy a telepített webes bővítmények naprakészek, majd letölti a szükséges frissítéseket. A Kaspersky Security Center Web Console Kezdeti beállító varázslójáról szóló további információkért lásd a Kaspersky Security Center Súgót.

- A webes bővítmény telepítése a Web Console-ban elérhető terjesztőcsomagok listájából.

  A webes bővítmény telepítéséhez válassza ki a Kaspersky Endpoint Security webes bővítmény terjesztőcsomagját a Web Console felületén (**Console settings** → **Web plug-ins**). Az elérhető terjesztőcsomagok listája automatikusan frissül, miután a Kaspersky alkalmazás új verziója érhető el.

- Töltse le egy külső forrásból a terjesztőcsomagot a Webfelügyelőre

  A webes bővítmény telepítéséhez adja meg a Kaspersky Endpoint Security webes bővítmény terjesztőcsomagjának ZIP-archívumát a Web Console felületén (**Console settings** → **Web plug-ins**). A webes bővítmény terjesztőcsomagja például a Kaspersky webhelyéről tölthető le.

A Kaspersky Endpoint Security 12.11 for Windows verziótól megváltozott a webes beépülő modul telepítési eljárása. A terjesztőcsomag mostantól két webes bővítményt tartalmaz: *Kaspersky Endpoint Security for Windows 14.1.0* és *Unified Protection and Management Plug-in*. Ez a Kaspersky-alkalmazások egyetlen egységesített webes beépülő moduljára való átállásnak köszönhető. Az egyesített webes beépülő modul egyetlen házirend létrehozását teszi lehetővé több Kaspersky-alkalmazás (például a Kaspersky Endpoint Security for Windows, macOS és Linux) kezeléséhez. Az egyesített webes beépülő modulra való átállás több kiadáson keresztül valósulhat meg. Az átállás befejezése után a terjesztőcsomag csak a *Unified Protection and Management Plug-in* modult fogja tartalmazni.

Az Adminisztrációs bővítmény frissítése

A Kaspersky Endpoint Security for Windows Adminisztrációs bővítmény frissítéséhez töltse le a bővítmény legfrissebb verzióját (beletartozik a terjesztő készletbe), majd futtassa a bővítményt a telepítő varázslóban.

Ha a webes bővítmény új verziója érhető el, a Webfelügyelő megjeleníti a *Frissítések érhetők el a felhasznált bővítményekhez* értesítést. A Webfelügyelő értesítéseiből frissítheti a webes bővítmény verzióját. A Webfelügyelő felületéről manuálisan is kereshet új webesbővítmény-frissítéseket (**Console settings** → **Web plug-ins**). A webes bővítmény előző verziója a frissítés során automatikusan el lesz távolítva.

> Ha a webes bővítmény frissül, a meglévő elemeket (például a szabályzatokat vagy a feladatokat) elmenti a rendszer. Az elemek új beállításai, amelyek a Kaspersky Endpoint Security új funkcióit teljesítik, a meglévő elemekben fognak megjelenni, és alapértelmezett értékük lesz.

A következőképp frissítheti a webes bővítményt:

- Frissítse online módban a webes bővítményt a webes bővítmények listáján.

  A webes bővítmény frissítéséhez válassza ki a Kaspersky Endpoint Security webes bővítmény terjesztőcsomagját a Web Console felületén (**Console settings** → **Web plug-ins**). A Webfelügyelő megkeresi az elérhető frissítéseket a Kaspersky kiszolgálókon, és letölti a szükségeseket.

- Frissítse fájlból a webes bővítményt.

  A webes bővítmény frissítéséhez válassza ki a Kaspersky Endpoint Security webes bővítmény terjesztőcsomagjának ZIP-archívumát a Web Console felületén (**Console settings** → **Web plug-ins**). A webes bővítmény terjesztőcsomagja például a Kaspersky webhelyéről tölthető le. A Kaspersky Endpoint Security webes bővítményt csak újabb verzióra tudja frissíteni. A webes bővítmény nem frissíthető korábbi verzióra.

Ha bármely elem megnyílik (úgy mint szabályzat vagy feladat), a webes bővítmény ellenőrzi a kompatibilitási információt. Ha a webes bővítmény verziója megegyezik vagy későbbi, mint a kompatibilitási információban megadott verzió, akkor az adott elem beállításai módosíthatók. Ellenkező esetben a webes bővítmény segítségével a kiválasztott elem beállításait nem lehet módosítani. Javasoljuk, hogy frissítse a webes bővítményt.

Az adminisztrációs bővítmény különböző verzióival való munkavégzés különleges szempontjai

A Kaspersky Endpoint Security alkalmazást csak akkor felügyelheti a Kaspersky Security Center segítségével, ha olyan adminisztrációs bővítménnyel rendelkezik, amelynek a verziója megegyezik a Kaspersky Endpoint Security és az adminisztrációs bővítmény kompatibilitására megadott verziószámmal vagy újabb annál. Az adminisztrációs bővítmény szükséges minimális verziószáma a forgalmazási készlet installer.ini fájljában megtalálható.

Az Adminisztrációs bővítmény minden összetevő (például szabályzat vagy feladat) megnyitása esetén ellenőrzi a kompatibilitására vonatkozó információit. Ha az Adminisztrációs bővítmény verziója megegyezik vagy későbbi, mint a kompatibilitásra vonatkozó információkban megadott verzió, akkor az adott összetevő beállításai módosíthatók. Ellenkező esetben az Adminisztrációs bővítmény segítségével a kiválasztott összetevő beállításait nem lehet módosítani. Javasoljuk, hogy frissítse az adminisztrációs bővítményt.

Ha a Kaspersky Endpoint Security adminisztrációs bővítmény az Adminisztrációs konzolban van telepítve, akkor az adminisztrációs bővítmény új verziójának telepítésekor vegye figyelembe a következőket:

- A Kaspersky Endpoint Security adminisztrációs bővítmény korábbi verziója el lesz távolítva.
- A Kaspersky Endpoint Security adminisztrációs bővítmény új verziója támogatja a Kaspersky Endpoint Security for Windows előző verziójának felhasználói számítógépeken történő felügyeletét.
- Az adminisztrációs bővítmény új verzióját használhatja arra, hogy megváltoztassa az adminisztrációs bővítmény korábbi verziójában létrehozott szabályzatok, feladatok és egyéb elemek beállításait.
- Az új beállításoknál az adminisztrációs bővítmény új verziója az alapértelmezett értékeket osztja ki a rendszabályok, rendszabályprofilok és feladatok első mentésekor.

  Az adminisztrációs bővítmény frissítése után javasolt ellenőrizni és elmenteni a szabályzatok és rendszabályprofilok új beállításait. Ha nem tesz így, a felhasználói számítógépeken a Kaspersky Endpoint Security beállításainak új csoportjai felveszik az alapértelmezett értéket, és szerkeszthetőek lesznek (a tulajdonság). Javasolt ellenőrizni a beállításokat, kezdve a rendszabályokkal és a rendszabályprofilokkal, mivel ezek a legfontosabbak. Továbbá javasolt olyan felhasználói fiókot használni, ami hozzáfér a Kaspersky Security Center összes működési területéhez.

  Az alkalmazás új tulajdonságainak megtekintéséhez lásd a Kibocsátási megjegyzést vagy az alkalmazássúgót.

- Ha az adminisztrációs bővítmény új verziójának csoportbeállításaihoz új paraméter lett hozzáadva, a csoportbeállítás / tulajdonsága korábban meghatározott állapota nem változik meg.

Különleges szempontok a külső szolgáltatásokkal való interakcióhoz használt titkosított protokollok használatakor

A Kaspersky Endpoint Security és a Kaspersky Security Center titkosított kommunikációs csatornát használ TLS-sel (Transport Layer Security) a Kaspersky külső szolgáltatásaival való együttműködéshez. A Kaspersky Endpoint Security külső szolgáltatásokat használ a következő funkciókhoz:

- adatbázisok és alkalmazás-szoftvermodulok frissítése;
- az alkalmazás aktiválása aktiváló kóddal (aktiválás 2.0);
- a Kaspersky Security Network használata.

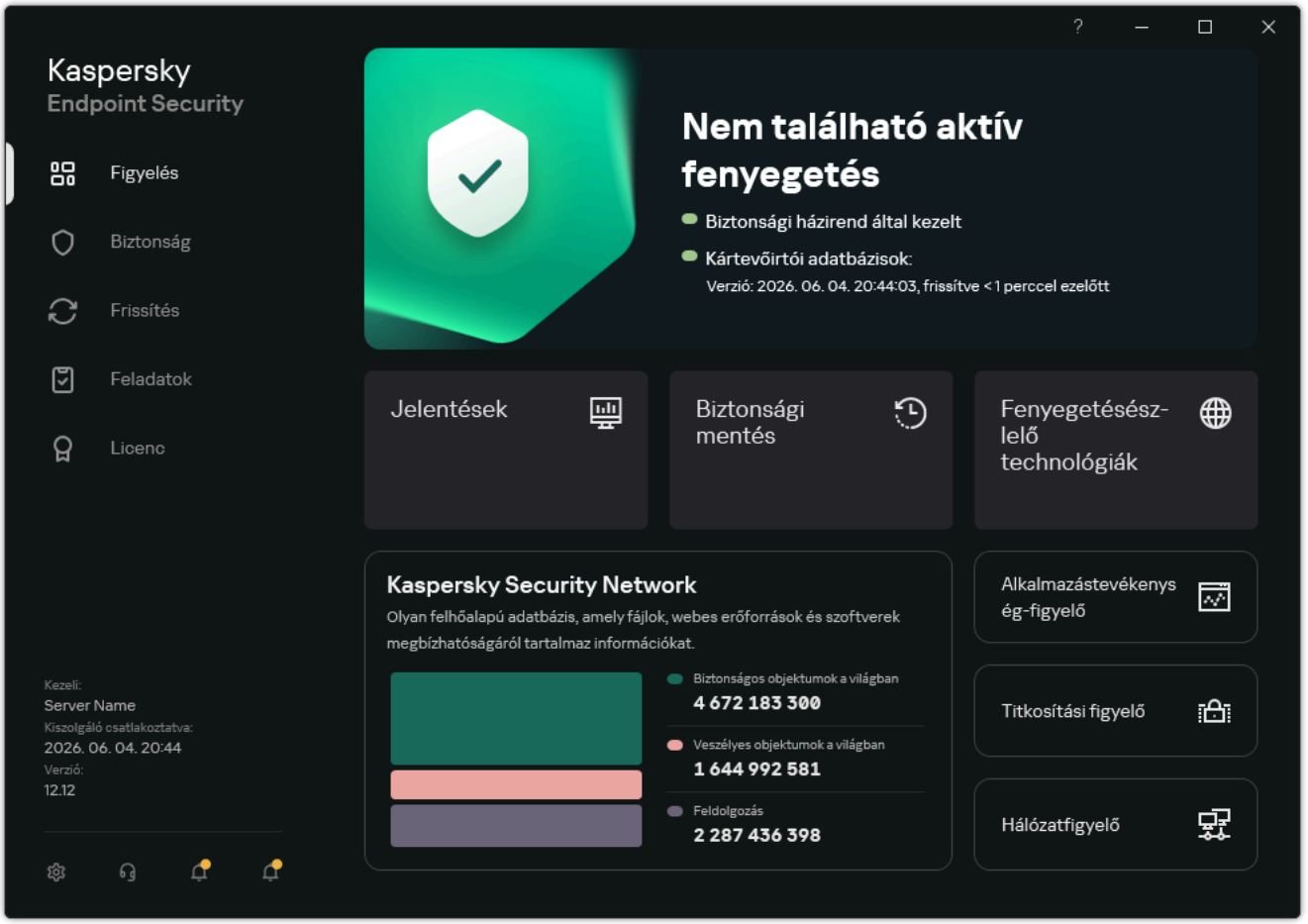
A TLS használata a következő funkciókkal növeli az alkalmazás biztonságát:

- Titkosítás. Az üzenetek tartalma bizalmas, és azok külső felhasználókkal nincsenek megosztva.
- Integritás. Az üzenet címzettje biztos lehet abban, hogy az üzenet tartalma nem módosult azóta, hogy az üzenetet a feladó továbbította.
- Hitelesítés. A címzett biztos lehet abban, hogy a kommunikáció csak megbízható Kaspersky kiszolgálóval jön létre.

A Kaspersky Endpoint Security nyilvános kulcsú tanúsítványokat használ a kiszolgáló hitelesítéséhez. A tanúsítványokkal való munkához Public Key Infrastructure (PKI) szükséges. A tanúsító hatóság a PKI része. A Kaspersky saját tanúsító hatóságát használja, mert a Kaspersky szolgáltatások inkább technikai jellegűek és nem nyilvánosak. Ebben az esetben, azaz a Thawte, a VeriSign, a GlobalTrust és mások gyökértanúsítványainak visszavonásakor a Kaspersky PKI megszakítás nélkül működik.

Az MITM-mel (a HTTPS protokoll elemzését támogató szoftveres és hardveres eszközök) rendelkező környezeteket a Kaspersky Endpoint Security nem tartja biztonságosnak. A Kaspersky szolgáltatásokkal való együttműködés során hibák léphetnek fel. Például hibák lehetnek az Self-Signed Certificate funkció használatával kapcsolatban. Ezek a hibák azért fordulhatnak elő, mert a környezetből származó HTTPS-ellenőrző eszköz nem ismeri fel a Kaspersky PKI-t. E problémák kijavításához konfigurálnia kell a külső szolgáltatásokkal való interakció kizárásait.

Az alkalmazás felülete



Fő alkalmazásablak

Figyelés	• **Jelentések**. Az alkalmazás, egyes összetevők és feladatok működése során bekövetkezett események megtekintése. • **Biztonsági mentés**. Tekintse meg az alkalmazás által törölt fertőzött fájlok mentett példányainak listáját. • **Fenyegetésészlelő technológiák**. Információk megtekintése a fenyegetésészlelő technológiákról és az ezen technológiák által észlelt fenyegetések számáról. • **Kaspersky Security Network**. A Kaspersky Endpoint Security és a Kaspersky Security Network közötti kapcsolat és a globális KSN statisztika állapota. A *Kaspersky Security Network (KSN)* felhőalapú szolgáltatások egy olyan infrastruktúrája, amely hozzáférést nyújt a Kaspersky online tudásbázisához, ahonnan információkat kaphat fájlok, webes erőforrások és szoftverek megbízhatóságáról. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban reagál az új típusú fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken. Ha tagja a Kaspersky Security Networknek, a KSN szolgáltatások a Kaspersky Endpoint Security számára információkat nyújtanak a vizsgált webcímek megbízhatóságáról, valamint a vizsgált fájlok kategóriájáról és megbízhatóságáról. • **Alkalmazástevékenység-figyelő**. Információk megtekintése a telepített alkalmazások működéséről. Az Alkalmazástevékenység-figyelő az alkalmazással kapcsolatos fájl-, beállításjegyzék-, illetve operációsrendszer-eseményeket követi nyomon. • **Hálózatfigyelő**. Információk megtekintése valós időben a számítógép hálózati tevékenységéről. • **Titkosítási figyelő**. Valós időben figyeli a lemez titkosítási vagy visszafejtési folyamatát. A Titkosítási figyelő akkor érhető el, ha a Kaspersky lemeztitkosítás vagy a BitLocker meghajtótitkosítás összetevő telepítve van.
Biztonság	A telepített összetevők működési állapota. Továbbá folytathatja az összetevők konfigurálását vagy a jelentések megtekintését.
Frissítés	A Kaspersky Endpoint Security frissítési feladatainak kezelése. Frissítheti a vírusadatbázisokat és az alkalmazásmodulokat, és visszagörgetheti a legutolsó frissítést. A rendszergazda elrejtheti a szakaszt a felhasználó elől, vagy korlátozhatja a feladatkezelést.
Feladatok	A Kaspersky Endpoint Security vizsgálati feladatainak kezelése. Futtathatja a rosszindulatú programok vizsgálatát és az alkalmazás integritás-ellenőrzését. A rendszergazda elrejtheti a feladatokat egy felhasználó elől, vagy korlátozhatja a feladatok kezelését.
Licenc	Az alkalmazás licencelése. Vásárolhat licencet, aktiválhatja az alkalmazást vagy megújíthatja az előfizetést. Megtekintheti a jelenlegi licenccel kapcsolatos információkat.
⚙	Alkalmazásbeállítások konfigurálása. A rendszergazda megtilthatja a Kaspersky Security Center beállításainak módosításait.

	Információ az alkalmazásról: a Kaspersky Endpoint Security jelenlegi verziója, az adatbázis kiadási dátuma, a kulcs és egyéb információk. Továbbléphet a Kaspersky információs erőforrásokra, melyek hasznos információkat, javaslatokat és válaszokat is tartalmaznak az alkalmazás megvásárlásával, telepítésével és használatával kapcsolatos gyakori kérdésekre.
	A titkosított fájlokhoz és eszközökhöz való hozzáférésre vonatkozó információkat tartalmazó üzenetek.

Alkalmazásikon a tálca értesítési területén

Közvetlenül a Kaspersky Endpoint Security telepítése után a Microsoft Windows tálca értesítési területén megjelenik az alkalmazás ikonja.

Ha az alkalmazás ikonja a tálca értesítési területén el van rejtve, akkor a rendszergazda letiltotta az alkalmazás felületének megjelenítését a házirendben.

Az ikon az alábbiakra szolgál:

- Jelzi az alkalmazások tevékenységét.
- Az alkalmazás helyi menüjének és főablakának gyors elérésére szolgál.

A alkalmazásikon-állapotok vannak biztosítva az alkalmazás műveleti információinak megjelenítéséhez:

- A ikon az alkalmazás kritikusan fontos védelmi összetevőinek engedélyezett állapotát jelzi. A Kaspersky Endpoint Security egy figyelmeztetést jelenít meg, ha a felhasználónak műveletet kell végrehajtania, például újra kell indítania a számítógépet az alkalmazás frissítése után.
- A ikon azt jelzi, hogy az alkalmazás kritikusan fontos védelmi összetevői le vannak tiltva vagy hibásan működnek. A védelmi összetevők hibásan működhetnek, például akkor, ha a licenc lejárt, vagy alkalmazáshiba történt. A Kaspersky Endpoint Security egy figyelmeztetést jelenít meg, benne a számítógépes védelem problémájának leírásával.

Az alkalmazásikon helyi menüje az alábbi elemeket tartalmazza:

- **Kaspersky Endpoint Security for Windows**. Megnyitja az alkalmazás főablakát. Ebben az ablakban beállíthatja az alkalmazásösszetevők és a feladatok működését, és megtekintheti a feldolgozott fájlok és az észlelt fenyegetések statisztikáját.
- **Védelem felfüggesztése** / **Védelem folytatása**. Szünetelteti a védelmi és felügyeleti összetevők műveleteit, amik nincsenek zárolva a () rendszabályban. Mielőtt elvégezné ezt a műveletet, javasolt kikapcsolni a Kaspersky Security Center rendszabályt.

  A védelmi és felügyeleti összetevők szüneteltetése előtt az alkalmazás kéri a jelszót a Kaspersky Endpoint Security eléréséhez (fiókjelszó vagy átmeneti jelszó). Ezután kiválaszthatja a szünet idejét: megadott ideig, újraindításig, felhasználói utasításig.

  Ez a helyi menüelem akkor érhető el, ha a Jelszóvédelem engedélyezve van. A védelmi és felügyeleti összetevők működésének folytatásához kattintson a **Védelem folytatása** lehetőségre az alkalmazás helyi menüjében.

  Ha szünetelteti a védelmi és felügyeleti összetevők működését, az nem lesz hatással a frissítési és a kártevővizsgálati feladatok teljesítményére. Az alkalmazás folytatja a Kaspersky Security Network használatát.

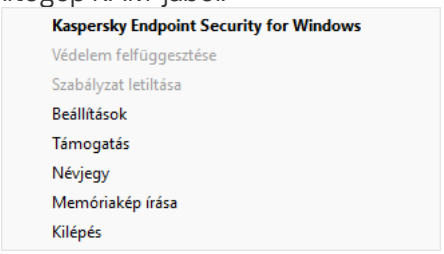
- **Szabályzat letiltása** / **Szabályzat engedélyezése**. A Kaspersky Security Center szabályzat letiltása a számítógépen. Minden Kaspersky Endpoint Security beállítás elérhető a konfiguráció számára, köztük azok is, amelyeken zárt lakat van a szabályzatban (). Ha a rendszabály le van tiltva, az alkalmazás kéri a Kaspersky Endpoint Security eléréséhez szükséges jelszót (fiókjelszót vagy ideiglenes jelszót). Ez a helyi menüelem akkor érhető el, ha a Jelszóvédelem engedélyezve van. A rendszabály engedélyezéséhez válassza a **Szabályzat engedélyezése** lehetőséget az alkalmazás helyi menüjéből.

- **Beállítások**. Megnyitja az alkalmazásbeállítások ablakát.

- **Támogatás**. Ez megnyitja a Kaspersky Terméktámogatással való kapcsolatfelvételhez szükséges információkat tartalmazó ablakot.

- **Névjegy**. Ez az elem az alkalmazás adatait tartalmaz tájékoztató ablakot nyitja meg.

- **Kilépés**. Ezzel az elemmel kiléphet a Kaspersky Endpoint Security alkalmazásból. Erre a helyi menüelemre kattintva az alkalmazás törlődik a számítógép RAM-jából.



Az alkalmazás ikonjának helyi menüje

Egyszerűsített alkalmazásfelület

Ha az egyszerűsített alkalmazásfelület megjelenítése beállítással rendelkező Kaspersky Security Center rendszabály egy olyan ügyfélszámítógépen van alkalmazva, melyre fel van telepítve a Kaspersky Endpoint Security, a főablak nem elérhető az ügyfélszámítógépen. Nyissa meg jobb kattintással a Kaspersky Endpoint Security ikon helyi menüjét (lásd az alábbi ábrát), mely a következő elemeket tartalmazza:

- **Szabályzat letiltása** / **Szabályzat engedélyezése**. A Kaspersky Security Center szabályzat letiltása a számítógépen. Minden Kaspersky Endpoint Security beállítás elérhető a konfiguráció számára, köztük azok is, amelyeken zárt lakat van a szabályzatban (). Ha a rendszabály le van tiltva, az alkalmazás kéri a Kaspersky Endpoint Security eléréséhez szükséges jelszót (fiókjelszót vagy ideiglenes jelszót). Ez a helyi menüelem akkor érhető el, ha a Jelszóvédelem engedélyezve van. A rendszabály engedélyezéséhez válassza a **Szabályzat engedélyezése** lehetőséget az alkalmazás helyi menüjéből.

- **Feladatok**. A következő elemeket tartalmazó legördülő lista:

  - **Alkalmazás integritás-ellenőrzése**.

  - **Adatbázisok visszaállítása az előző verzióra**.

  - **Teljes vizsgálat**.

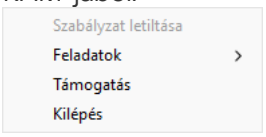
  - **Egyéni vizsgálat**.

  - **Kritikus területek vizsgálata**.

  - **Frissítés**.

- **Támogatás**. Ez megnyitja a Kaspersky Terméktámogatással való kapcsolatfelvételhez szükséges információkat tartalmazó ablakot.

- **Kilépés**. Ezzel az elemmel kiléphet a Kaspersky Endpoint Security alkalmazásból. Erre a helyi menüelemre kattintva az alkalmazás törlődik a számítógép RAM-jából.



Az alkalmazásikon helyi menüje az egyszerűsített felület megjelenítése esetén

Az alkalmazás felülete megjelenítésének beállítása

A felhasználónak konfigurálhatja az alkalmazásfelület megjelenítési módját. A felhasználó a következő módokon keresztül léphet kapcsolatba az alkalmazással:

- **Egyszerűsített felület megjelenítése**. Az ügyfélszámítógépen a fő alkalmazásablak nem érhető el, csak a Windows értesítési sávon lévő ikon érhető el. Az ikon helyi menüjében a felhasználó korlátozott számú műveletet hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security csak azokat az értesítéseket jeleníti meg az alkalmazás ikonja felett, amelyek felhasználói beavatkozást igényelnek.

- **Felhasználói felület megjelenítése**. Ügyfélszámítógépeken a Kaspersky Endpoint Security fő ablaka és a Windows értesítési területén lévő ikon érhető el. Az ikon helyi menüjében a felhasználó műveleteteket hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security értesítéseket is megjelenít az alkalmazásikon felett.

- **Ne jelenítse meg a felhasználói felületet**. Az ügyfélszámítógépen nincs jelen a Kaspersky Endpoint Security működésének. A Windows értesítési sávon lévő ikon és az értesítések nem érhetők el.

Hogyan konfigurálhatja az alkalmazásfelület megjelenítési módját az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.

4. Az **Interaction with user** részben konfigurálja az alkalmazásfelület megjelenésének módját:

   - **Felhasználói felület megjelenítése**. Ügyfélszámítógépeken a Kaspersky Endpoint Security fő ablaka és a Windows értesítési területén lévő ikon érhető el. Az ikon helyi menüjében a felhasználó műveleteteket hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security értesítéseket is megjelenít az alkalmazásikon felett. Szükség esetén engedélyezheti az **Alkalmazástevékenység-figyelő elrejtése** funkciót, hogy elrejtse az alkalmazástevékenységgel kapcsolatos adatokat a számítógépen, ezáltal korlátozva a felhasználók hozzáférését az Alkalmazástevékenység-figyelő eszközhöz.

   - **Egyszerűsített felület megjelenítése**. Az ügyfélszámítógépen a fő alkalmazásablak nem érhető el, csak a Windows értesítési sávon lévő ikon érhető el. Az ikon helyi menüjében a felhasználó korlátozott számú műveletet hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security csak azokat az értesítéseket jeleníti meg az alkalmazás ikonja felett, amelyek felhasználói beavatkozást igényelnek.

   - **Ne jelenítse meg a felhasználói felületet**. Az ügyfélszámítógépen nincs jelen a Kaspersky Endpoint Security működésének. A Windows értesítési sávon lévő ikon és az értesítések nem érhetők el.

5. Mentse el a módosításokat.

Az alkalmazásfelület megjelenítési módja konfigurálásának menete a Web Console-ban, illetve a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **User Interaction** elemet.

5. A(z) **Visibility for users** részben konfigurálhatja az alkalmazásfelület megjelenésének módját:

   - **Display user interface**. Ha ez a funkció ki van kapcsolva, a kliensszámítógépen semmilyen jel nem utal a Kaspersky Endpoint Security működésére. A Windows értesítési sávon lévő ikon és az értesítések nem érhetők el.

   - **Simplified**. Az ügyfélszámítógépen a fő alkalmazásablak nem érhető el, csak a Windows értesítési sávon lévő ikon érhető el. Az ikon helyi menüjében a felhasználó korlátozott számú műveletet hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security csak azokat az értesítéseket jeleníti meg az alkalmazás ikonja felett, amelyek felhasználói beavatkozást igényelnek.

   - **Full**. Ügyfélszámítógépeken a Kaspersky Endpoint Security fő ablaka és a Windows értesítési területén lévő ikon érhető el. Az ikon helyi menüjében a felhasználó műveleteteket hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security értesítéseket is megjelenít az alkalmazásikon felett.

   - **Hide Application Activity Monitor section**. Ha el szeretné rejteni az alkalmazástevékenység adatait a felhasználó számítógépén, korlátozhatja a felhasználók hozzáférését az Alkalmazástevékenység-figyelő eszközhöz.

6. Mentse el a módosításokat.

Az alkalmazás használatra való előkészítése

Miután telepíti az alkalmazást az ügyfélszámítógépekre, ahhoz, hogy a Kaspersky Endpoint Security a Kaspersky Security Center Web Console-tol dolgozhasson, a következő tevékenységeket kell végrehajtania:

- Hozzon létre és adjon meg egy rendszabályt.

  Rendszabályok segítségével ugyanazokat a Kaspersky Endpoint Security beállításokat alkalmazhatja egy adminisztrációs csoport összes ügyfélszámítógépére. A Kaspersky Security Center kezdeti beállító varázslója automatikusan létrehoz egy rendszabályt a Kaspersky Endpoint Security számára.

- Hozza létre az *Adatbázisok és alkalmazásmodulok frissítése* és a *Rosszindulatú programok vizsgálata* feladatokat.

  Az *Adatbázisok és alkalmazásmodulok frissítése* feladat ahhoz szükséges, hogy a számítógép védelme naprakész legyen. A feladat végrehajtásakor a Kaspersky Endpoint Security frissíti az antivírus adatbázisokat és az alkalmazásmodulokat. Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

  A *Kártevő vizsgálata* feladatra szükség van ahhoz, hogy időben észlelje a vírusokat és más rosszindulatú programokat. Kézileg kell létrehoznia a *Kártevő vizsgálata* feladatot.

  A Rosszindulatú programok vizsgálata feladat létrehozásának menete az Adminisztrációs konzolban (MMC)

  1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

     Megnyílik a feladatok listája.

  2. Kattintson az **New task** gombra.

  Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Kártevő-ellenőrzés** elemet.

2. lépés: Vizsgálat hatóköre

Hozzon létre egy objektumlistát, amit a Kaspersky Endpoint Security a vizsgálati feladat végrehajtása során megvizsgál.

3. lépés: Kaspersky Endpoint Security művelet

Fenyegetés észlelése esetén végrehajtott művelet kiválasztása:

- **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

- **Vírusmentesítés, értesítés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.

- **Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.

- **Fejlett vírusmentesítés futtatása azonnal**. Ha be van jelölve a jelölőnégyzet, a Kaspersky Endpoint Security a vizsgálat során Fejlett vírusmentesítő technológiát használ az aktív fenyegetések megszüntetésére.

  A *fejlett vírusmentesítő technológia* célja az operációs rendszer megtisztítása az olyan rosszindulatú alkalmazásoktól, amelyek már elindították folyamataikat a RAM-ban, és amelyek megakadályozzák, hogy a Kaspersky Endpoint Security más módszerekkel távolítsa el őket. Ennek eredményeképpen a fenyegetés semlegesítésre kerül. A Fejlett vírusmentesítés közben ajánlott tartózkodni az új folyamatok indításától, illetve az operációs rendszer beállításjegyzékének szerkesztésétől. A fejlett vírusmentesítő technológia az operációs rendszer jelentős erőforrásait vesz igénybe, amitől a többi alkalmazás lelassulhat. A fejlett vírusmentesítés elvégzését követően a Kaspersky Endpoint Security anélkül újraindítja a számítógépet, hogy ehhez a felhasználó megerősítését kérné.

- **Run only when the computer is idle**. A feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították. Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.

4. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.

- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.

- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

5. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válasszon fiókot a *Kártevő vizsgálata* feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot. Ha a vizsgálat hatókörébe hálózati meghajtók vagy egyéb, korlátozott hozzáférésű objektumok tartoznak, válasszon az elegendő hozzáférési joggal rendelkező felhasználói fiókot.

6. lépés Feladatindítási ütemezés konfigurálása

Adjon meg ütemtervet a feladat indításához, például kézileg vagy azután, hogy az antivírus adatbázisok letöltődtek a könyvtárba.

7. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például: *Napi teljes vizsgálat*.

8. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Ennek eredményeképpen a Kártevő vizsgálata feladat végre lesz hajtva a felhasználói számítógépeken, a megadott ütemterv alapján.

A Rosszindulatú programok vizsgálata feladat létrehozásának menete a Web Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Malware Scan** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *Heti vizsgálat*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. A feladat ütemtervének megadásához menjen a feladatok tulajdonságaiba.

   Ajánlott ütemezni a feladat futtatását legalább heti egy alkalomra.

8. Válassza ki a feladat melletti jelölőnégyzetet.

9. Kattintson az **Start** gombra.

   Megfigyelheti a feladat állapotát, valamint az eszközök számát, ahol a feladat sikeresen vagy hibásan lett végrehajtva.

Ennek eredményeképpen a Kártevő vizsgálata feladat végre lesz hajtva a felhasználói számítógépeken, a megadott ütemterv alapján.

- A Kaspersky Endpoint Security teljesítményének optimalizálása.

A rendszabályok kezelése

A *rendszabály* azon alkalmazásbeállítások gyűjteménye, amelyek egy adminisztrációs csoport számára vannak megszabva. Több rendszabályt is beállíthat egy alkalmazásnak, különböző értékekkel. Az alkalmazások különböző beállítások alatt futhatnak különböző adminisztrációs csoportoknál. Minden adminisztrációs csoportnak megvan a maga rendszabálya az alkalmazáshoz.

Minden házirend-beállítás rendelkezik a ("lakat") attribútummal. Az attribútum állapota határozza meg, hogy a beállítás átadásra kerül-e az adminisztrációs csoport felügyelt eszközeinek:

- Ha a „lakat” nyitva van ( ), a beállítás értéke nem kerül átadásra a felügyelt eszközöknek. A beállítás az alkalmazás helyi felületén lesz módosítható. Az ilyen beállításokra *feloldott* néven hivatkozunk.

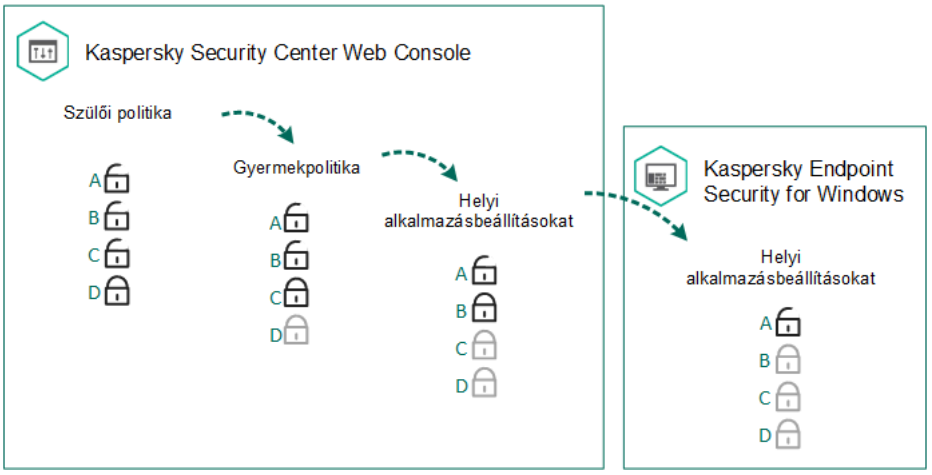
- Ha a „lakat” zárva van ( ), a beállítás értéke átadásra kerül és alkalmazásra kerül a felügyelt eszközökön. Az ilyen beállításokra *zárolt* néven hivatkozunk. A blokkolt beállítások nem módosíthatók az alkalmazás helyi felületén.

A rendszabály beállításai a *szinkronizáció* alatt el lesznek küldve az ügyfélszámítógépekre a Hálózati ügynök által. Alapértelmezetten az Adminisztrációs kiszolgáló szinkronizációt hajt végre rögtön azután, hogy megváltoztak a rendszabály beállításai. Az UDP-port 15000 szinkronizációs célokra van használva az ügyfélszámítógépen. Az Adminisztrációs kiszolgáló alapértelmezés szerint 15 percenként hajt végre szinkronizációt. Ha a következő szinkronizáció sikertelen a rendszabály beállításainak megváltoztatása után, akkor a szinkronizáció a beállított ütemterv szerint lesz végrehajtva.

A beállítások öröklődése

A rendszabályok, például az adminisztrációs csoportok hierarchiával rendelkeznek. A *Gyermekrendszabály* egy rendszabály a beágyazott hierarchiaszintekhez, vagyis egy rendszabály a beágyazott adminisztrációs csoportokhoz és a másodlagos adminisztrációs kiszolgálókhoz.

Alapértelmezés szerint a gyermek rendszabályok öröklik a szülő rendszabályok beállításait. Ha a szülőházirendben a beállítás rendelkezik a (zárt „lakat") attribútummal, a gyermek házirendekben és a helyi alkalmazásbeállításokban a beállítás értéke a szülőházirendnek megfelelően felül lesz írva, és a beállítás zárolásra kerül. Szükség esetén letilthatja a beállítások öröklődését a szülőházirendből. A házon kívüli rendszabályok nincsenek hatással más rendszabályokra az adminisztrációs csoportok hierarchiáján keresztül.



A beállítások öröklődése

A rendszabályok beállításainak hozzáférési jogosultságai (olvasás, írás, végrehajtás) minden olyan felhasználóhoz meg van adva, aki hozzáfér a Kaspersky Security Center felügyeleti kiszolgálóhoz, és külön-külön a Kaspersky Endpoint Security egyes funkcionális hatóköreinél. A házirend-beállításokhoz való hozzáférés jogainak konfigurálásához nyissa meg a Kaspersky Security Center felügyeleti kiszolgáló tulajdonságok ablakának **Security** szakaszát (alapértelmezés szerint ez a szakasz a konzolfelületen el van rejtve).

Szabályzati módosítások

A Kaspersky Security Center nyomon követi a szabályzati módosításokat, és verziókat hoz létre. A *verzió* a felhasználó által mentett módosított paraméterek halmaza. A verziók lehetővé teszik a szabályzati paraméterek módosításainak összehasonlítását és visszaállítását. A módosított paraméterek készletén kívül a verzió tartalmazza a módosítást végző felhasználóra vonatkozó információkat, valamint az időpontot, az IP-címet, a felhasználó megjegyzését és más lényeges adatokat.

A verziónapló megtekintéséhez nyissa meg a szabályzat tulajdonságait, és lépjen a következő szakaszra: **Revision history**. A verziók kezelésével kapcsolatos további részletekért olvassa el a Kaspersky Security Center súgóját.

Rendszabály létrehozása

Házirend létrehozásakor a varázsló a kiválasztott üzemmódhoz tartozó beállításokat javasolja. A Light Agent üzemmódhoz például hozzá kell adnia egy Védelmi kiszolgálót (SVM). Ha az alkalmazást SQL-kiszolgáló védelmére használja, előre definiált vizsgálati kizárásokat kell hozzáadnia, hogy a kiszolgáló működését ne zavarja. A varázsló az üzemmód kiválasztása után a megfelelő házirend-beállításokat javasolja. Ezeket a beállításokat ezután a házirend tulajdonságaiban szerkesztheti.

Rendszabály létrehozásának menete az Adminisztrációs Konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Policies** lapot.
4. Kattintson az **New policy** gombra.

   Elindul a Rendszabályvarázsló.
5. Kövesse a Rendszabályvarázsló utasításait.

1. lépés: A csoportházirend létrehozására szolgáló alkalmazás kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** alkalmazást.

2. lépés: A csoportházirend elnevezése

Adjon meg egy nevet a csoportházirendnek, például *Az iroda házirendje*.

A Házirend varázsló segítségével új házirendeket is létrehozhat a meglévő házirendek alapján. Ehhez a csoportházirend nevének megadásakor jelölje be a **Use policy settings for an earlier version of the application** jelölőnégyzetet. A varázsló lehetővé teszi a Kaspersky Endpoint Security (KES) házirend létrehozását egy másik megoldás, például a Kaspersky Security for Windows Server (KSWS) vagy a Kaspersky Security for Virtualization Light Agent for Windows házirendje alapján is

3. lépés. Részvétel a Kaspersky Security Networkben

Olvassa el és fogadja el a Kaspersky Security Network (KSN) nyilatkozatának feltételeit.

4. lépés: Az alkalmazás használati módjának kiválasztása számítógépeken

A Kaspersky Endpoint Security rendeltetési helyétől függően a következő alkalmazásmódokhoz konfigurálhat szabályzatot:

- Normál mód a gazdagépek védelmére

Ebben a módban kiválaszthatja, hogyan szeretné konfigurálni a szabályzatot:

- **Szabályzat létrehozása alapértelmezett beállításokkal**. Az alapértelmezett beállítások tekinthetők optimálisnak. A Kaspersky szakértői ezeket a beállításokat ajánlják. Az alapértelmezett beállítások biztosítják az ajánlott védelmi szintet és az optimális erőforrás-felhasználást.

- **Szabályzati beállítások módosítása a varázslóban**. Ez a módszer lehetővé teszi a szabályzati beállítások lépésről lépésre történő kezelését egy varázsló segítségével. A szabályzati beállításokat egy konfigurációs fájl segítségével is kezelheti (lásd a következő lépést).

- Az Endpoint Detection and Response Agent a speciális fenyegetések és a célzott támadások elleni védelemhez.

  Az *Endpoint Detection and Response Agent* egy olyan alkalmazás, amely a vállalat informatikai infrastruktúrájában az egyes munkaállomásokra és kiszolgálókra telepítve támogatja a Kaspersky Detection and Response megoldásait. A következő lépésben ki kell választania az EDR Agent integrációjának megoldását.

- Light Agent a virtuális környezetek védelme céljából.

  Az alkalmazás Light Agent üzemmódban való használatához konfigurálnia kell a kapcsolatot egy SVM virtuális géppel. Ezekre a beállításokra van szükség ahhoz, hogy az alkalmazás Light Agent üzemmódban működjön.

A Kaspersky Endpoint Security közös házirendet biztosít minden alkalmazási módhoz és operációs rendszer típushoz. Ez azt jelenti, hogy a házirend a beállítások teljes körére kiterjed. Előfordulhat azonban, hogy az alkalmazás figyelmen kívül hagy néhány házirend-beállítást, mert a Kaspersky Endpoint Security olyan üzemmódban van telepítve, amelyben bizonyos funkciók nem érhetők el. Ha például az alkalmazást Endpoint Detection and Response Agent módban használja, csak a Kaspersky Detection and Response megoldásokkal való integrációra és a KUMA-val való integrációra vonatkozó beállítások érhetők el.

Javasoljuk, hogy a különböző üzemmódokhoz és operációsrendszer-típusokhoz különböző házirendeket használjon.

5. lépés Importálási beállítások

Ez a lépés akkor érhető el, ha a szabályzat manuális konfigurációját választotta a 4. lépésben.

A Kaspersky Endpoint Security beállításai alapján szabályzatot hozhat létre egy CFG konfigurációs fájlból. Alkalmazás konfigurációs fájljának importálásakor nem minden szabályzati beállítás érhető el a varázsló számára. Például hiányoznak a szabályzati profilok az alkalmazás beállításaiból. Ha az összes beállítást és profilt át szeretné vinni a szabályzatba, importálhat egy másik szabályzatot egy KLP-fájlból.

Konfigurációs fájlok importálásakor a Kaspersky Endpoint Security nem továbbítja a kriptokonténer jelszavait. Ha a kiszolgálókhoz való csatlakozáskor kétirányú hitelesítést használ, akkor a kriptokonténer jelszavait újra meg kell adnia.

6–10. lépés. Szabályzati beállításainak konfigurálása

Ez a lépés akkor érhető el, ha a szabályzat manuális konfigurációját választotta a 4. lépésben.

Kövesse a szabályzati beállítások kezelésének lépéseit.

11. lépés. A megbízható zóna konfigurálása

Konfigurálja a megbízható zónát. Előre definiált vizsgálati kizárásokat és megbízható alkalmazásokat adhat hozzá. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. Az előre definiált vizsgálati kizárások és a megbízható alkalmazások szintén segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Light Agent üzemmódban Citrix és VMware virtuális környezetekben.

12. lépés. A szabályzat állapotának kiválasztása

- **Active**. A következő szinkronizáció után a rendszabály aktív rendszabályként lesz használva a számítógépen.

  Az aktív rendszabály beállításai az ügyfélszámítógépekre vannak mentve a szinkronizáció alatt. Nem tud egyszerre több rendszabályt alkalmazni egy számítógépen, ezért egy csoportban csak egy rendszabály lehet aktív.

- **Inactive**. Biztonsági mentési rendszabály. Szükség esetén az inaktív rendszabály átváltható aktív állapotra.

  Korlátlan számú inaktív rendszabályt hozhat létre. Az inaktív rendszabály nincs hatással a hálózatban a számítógépen lévő alkalmazásbeállításokra. Az inaktív rendszabályok vészhelyzetek esetére készültek, például vírustámadásra. Ha a flash meghajtókon keresztül érkezik támadás, akkor aktiválhat egy rendszabályt, ami blokkolja a flash meghajtókhoz való hozzáférést. Ebben az esetben az aktív rendszabály inaktív lesz.

- **Out-of-office**. A rendszabály akkor lesz aktív, ha a számítógép elhagyja a szervezet hálózatának területét.

Fejezze be a varázslót.

Rendszabály létrehozásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson az **Add** gombra.

   Elindul a Rendszabályvarázsló.
3. Válassza ki a Kaspersky Endpoint Security lehetőséget, majd kattintson a **Next** lehetőségre.
4. Kérjük, olvassa el és fogadja el a Kaspersky Security Network (KSN) nyilatkozatának feltételeit, majd kattintson a **Next** lehetőségre.

5. Válassza ki az alkalmazás üzemmódját:

   - Standard mode to protect workstations and servers
   - Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks.

     Ha ezt az üzemmódot választja, házirendet hozhat létre a számítógép és a Kaspersky Detection and Response megoldásainak integrálására. A varázsló a Kaspersky Managed Detection and Response, majd a Kaspersky Anti Targeted Attack Platform (EDR) integrációjának konfigurálását kéri.
   - Light Agent to protect virtual environments.

     Ha ezt az üzemmódot választja, a következő lépésben konfigurálnia kell a kapcsolatot a védelmi kiszolgálóval (SVM). Ezekre a beállításokra van szükség ahhoz, hogy az alkalmazás Light Agent üzemmódban működjön.

   A Kaspersky Endpoint Security közös házirendet biztosít minden alkalmazási módhoz és operációs rendszer típushoz. Ez azt jelenti, hogy a házirend a beállítások teljes körére kiterjed. Előfordulhat azonban, hogy az alkalmazás figyelmen kívül hagy néhány házirend-beállítást, mert a Kaspersky Endpoint Security olyan üzemmódban van telepítve, amelyben bizonyos funkciók nem érhetők el. Ha például az alkalmazást Endpoint Detection and Response Agent módban használja, csak a Kaspersky Detection and Response megoldásokkal való integrációra és a KUMA-val való integrációra vonatkozó beállítások érhetők el.

   > Javasoljuk, hogy a különböző üzemmódokhoz és operációsrendszer-típusokhoz különböző házirendeket használjon.

6. Konfigurálja a megbízható zónát. Előre definiált vizsgálati kizárásokat és megbízható alkalmazásokat adhat hozzá. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. Az előre definiált vizsgálati kizárások és a megbízható alkalmazások szintén segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Light Agent üzemmódban Citrix és VMware virtuális környezetekben.

7. Az **General** fülön a következő műveleteket végezheti el:

   - A rendszabály nevének megváltoztatása.
   - A rendszabály állapotának kiválasztása:

     - **Active**. A következő szinkronizáció után a rendszabály aktív rendszabályként lesz használva a számítógépen.

       Az aktív rendszabály beállításai az ügyfélszámítógépekre vannak mentve a szinkronizáció alatt. Nem tud egyszerre több rendszabályt alkalmazni egy számítógépen, ezért egy csoportban csak egy rendszabály lehet aktív.
     - **Inactive**. Biztonsági mentési rendszabály. Szükség esetén az inaktív rendszabály átváltható aktív állapotra.

       Korlátlan számú inaktív rendszabályt hozhat létre. Az inaktív rendszabály nincs hatással a hálózatban a számítógépen lévő alkalmazásbeállításokra. Az inaktív rendszabályok vészhelyzetek esetére készültek, például vírustámadásra. Ha a flash meghajtókon keresztül érkezik támadás, akkor aktiválhat egy rendszabályt, ami blokkolja a flash meghajtókhoz való hozzáférést. Ebben az esetben az aktív rendszabály inaktív lesz.
     - **Out-of-office**. A rendszabály akkor lesz aktív, ha a számítógép elhagyja a szervezet hálózatának területét.

- A beállítás öröklésének megváltoztatása:

  - **Inherit settings from parent policy**. Ha ez a kapcsológomb be van kapcsolva, a rendszabály beállítások értéke a legfelsőbb szintű rendszabálytól lesz örökölve. A rendszabály beállítások nem szerkeszthetők, ha a be van állítva a szülőrendszabályhoz.

  - **Force inheritance of settings in child policies**. Ha a kapcsoló be van kapcsolva, a rendszabály-beállítások értékeit megkapják a gyermekrendszabályok. A gyermekrendszabály tulajdonságai között a **Inherit settings from parent policy** kapcsológomb automatikusan bekapcsolt helyzetben van, kikapcsolására pedig nincs mód. A gyermekrendszabály-beállításokat örökli a szülőrendszabály, kivéve a jelzéssel ellátott beállításokat. A gyermekrendszabály beállítások nem szerkeszthetők, ha a be van állítva a szülőrendszabályhoz.

8. Az **Application settings** fülön beállíthatja a Kaspersky Endpoint Security rendszabály beállításait.

9. Fejezze be a varázslót.

Ennek eredményeképpen a Kaspersky Endpoint Security beállításai a következő szinkronizáció során be lesznek állítva az ügyfél számítógépeken. Lehetősége van megtekinteni a számítógépen alkalmazott rendszabályra vonatkozó információt (például a házirend nevét) a Kaspersky Endpoint Security kezelőfelületén, ha a főképernyő gombjára kattint. Ehhez a Hálózati ügynök rendszabályának beállításaiban engedélyeznie kell a bővített rendszabályadatok fogadását. A Hálózati ügynök rendszabály további részleteiről a Kaspersky Security Center súgójából tájékozódhat.

Szabályzat exportálása és importálása

A Kaspersky Endpoint Security lehetővé teszi a szabályzat beállításainak és profiljainak KLP-fájlba történő exportálását. Ezt követően a szabályzat exportálási/importálási funkciójával biztonsági mentéseket készíthet, házirendeket migrálhat egy másik kiszolgálóra, vagy például házirendeket migrálhat a Kaspersky Security Center Windows rendszerről a Kaspersky Security Center Linux rendszerre. A szabályzatok kezelésével kapcsolatos részletekért olvassa el a Kaspersky Security Center súgóját.

Szabályzat exportálása és importálása az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.

3. Válassza ki a munkaterületen a **Policies** lapot.

4. Szabályzat exportálása:

   a. Kattintson az exportálni kívánt szabályzatra.

   b. Kattintson a **Export policy to file** gombra az ablak jobb oldali részén.

   c. A megnyíló ablakban adja meg a KLP-fájl nevét, amelybe exportálni szeretné a szabályzatot, és válassza ki a fájl mentésére szolgáló mappát.

   d. Mentse a fájlt.

5. Szabályzat importálása:

   a. Kattintson az **Import policy from file** gombra.

   b. A megnyíló ablakban válassza ki azt a KLP-szabályzatfájlt, amelyet importálni szeretne.

   c. Nyissa meg a fájlt.

   Ez egy új szabályzatot ad hozzá *Inactive policy* állapottal.

Szabályzat exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Szabályzat exportálása:

   a. Jelölje be az exportálni kívánt szabályzat melletti jelölőnégyzetet.

   b. Kattintson az **Export** gombra.

   c. A megnyíló ablakban adja meg a KLP-fájl nevét, amelybe exportálni szeretné a szabályzatot, és válassza ki a fájl mentésére szolgáló mappát.

   d. Mentse a fájlt.

3. Szabályzat importálása:

   a. Kattintson az **Import** gombra.

   b. Válassza ki az importálni kívánt KLP-szabályzatfájlt.

   c. A szabályzat sikeres feldolgozása után válassza ki azt az adminisztrációs csoportot, amelyre alkalmazni szeretné a szabályzatot.

   d. Kattintson a **Complete** gombra a szabályzat importálásának befejezéséhez.

   Ez egy új szabályzatot ad hozzá *Inactive* állapottal.

Biztonságiszint-jelző

A biztonsági szintjelző a rendszabályok tulajdonságai ablak felső részén jelenik meg. A jelzés a következő értékek egyikével rendelkezhet:

- **Magas védelmi szint**. A jelzés felveszi ezt az értéket és zöldre változik, ha a következő kategóriák minden összetevője engedélyezve van:
  - **Kritikus**. Ez a kategória a következő összetevőket foglalja magába:
    - Fájl védelem.
    - Viselkedésészlelés.
    - Biztonsági rések kihasználásának megelőzése.

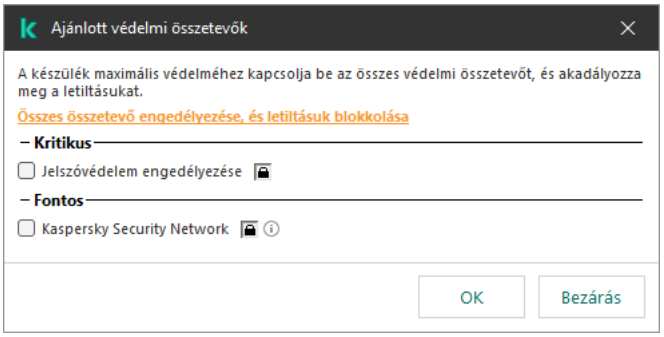
- Kármentesítő motor.
- Az alkalmazásszolgáltatások külső felügyelettel szembeni védelme.

- **Fontos**. Ez a kategória a következő összetevőket foglalja magába:
  - Kaspersky Security Network.
  - Web védelem.
  - Levelezés védelem.
  - Behatolásmegelőző rendszer.
  - Jelszóvédelem.

- **Közepes védelmi szint**. A jelzés felveszi ezt az értéket és sárgává változik, ha a fontos összetevők egyike ki van kapcsolva.
- **Alacsony védelmi szint**. A jelzés felveszi ezt az értéket és pirossá változik a következő esetekben:
  - Egy vagy több kritikus összetevő ki van kapcsolva.
  - Két vagy több fontos összetevő ki van kapcsolva.

Ha a mutató **Közepes védelmi szint** vagy **Alacsony védelmi szint** értékkel rendelkezik, a mutató jobb oldalán megjelenik egy hivatkozás, amely az **Ajánlott védelmi összetevők** ablakot nyitja meg. Ebben az ablakban engedélyezheti az ajánlott védelmi összetevők bármelyikét.

Az alkalmazás frissítése után a védelmi szint jelzője alacsonyabb védelmi szintet jelezhet, mint a frissítés előtt. Ez azért történik, mert az alkalmazás újabb verziója olyan új összetevőket vagy funkciókat tartalmaz, amelyek fontosak a számítógép biztonsága szempontjából. Az alkalmazás frissítése után kezelnie kell az új beállításokat, hogy a védelmi szint magas maradjon.



A házirend biztonsági szintjelzője

Feladatkezelés

A Kaspersky Endpoint Security Kaspersky Security Centeren keresztül történő adminisztrációjához az alábbi típusú feladatokat hozhatja létre:

- Egyedi ügyfélszámítógéphez beállított helyi feladatok.
- Adminisztrációs csoportokba tartozó ügyfélszámítógépekhez beállított csoportos feladatok.
- Feladatok a kiválasztott számítógépeknek.

Bármennyi csoportos feladatot létrehozhat a kiválasztott számítógépekhez vagy a helyi feladatokhoz. Az adminisztrációs csoportokkal és a kiválasztott számítógépekkel való dolgozással kapcsolatos tudnivalókért lásd a Kaspersky Security Center Súgót.

A Kaspersky Endpoint Security az alábbi feladatokat támogatja:

- **Kártevő vizsgálata**. A Kaspersky Endpoint Security megvizsgálja a számítógép feladatbeállításokban megadott területein a vírusok és egyéb fenyegetések jelenlétét. A *Kártevő vizsgálata* feladatra szükség van a Kaspersky Endpoint Security működéséhez, így létrejön a Kezdeti beállító varázsló futtatásakor. Ajánlott ütemezni a feladat futtatását legalább heti egy alkalomra.
- **Kulcs hozzáadása**. A Kaspersky Endpoint Security kulcsot – ideértve a további kulcsot is – ad meg alkalmazások aktiválásához. A feladat futtatása előtt győződjön meg róla, hogy a számítógépek száma, amikhez a feladat végre volt hajtva, ne lépje túl a licenc által megengedettet.
- **Change application components**. A Kaspersky Endpoint Security a feladat beállításaiban megadott összetevőlista alapján összetevőket telepít vagy távolít el az ügyfélszámítógépeken. A Fájl védelem összetevő nem távolítható el. A Kaspersky Endpoint Security összetevők optimális készlete segít megőrizni a számítógép erőforrásait.
- **Leltár**. A Kaspersky Endpoint Security adatokat fogad a számítógépeken tárolt összes alkalmazás futtatható fájljairól. A *Leltár* feladatot az Alkalmazásfelügyelő összetevő hajtja végre. Ha az Alkalmazásfelügyelő összetevő nincs telepítve, a feladat hibával ér véget.
- **Adatbázisok és alkalmazásmodulok frissítése**. A Kaspersky Endpoint Security frissíti az adatbázisokat és alkalmazásmodulokat. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat a Kaspersky Endpoint Security működése érdekében szükséges, a Kezdeti beállító varázsló során van létrehozva. Javasolt olyan ütemtervet megadni, ami naponta legalább egyszer futtatja a feladatot.
- **Adatok törlése**. A Kaspersky Endpoint Security azonnal törli a fájlokat és a mappákat a felhasználó számítógépéről, vagy ha régóta nincs kapcsolat a Kaspersky Security Centerrel.
- **Frissítés visszaállítása**. A Kaspersky Endpoint Security visszagörgeti az adatbázisok és alkalmazásmodulok legutóbbi frissítését. Ez például akkor lehet szükséges, ha az új adatbázisok helytelen adatokat tartalmaznak, amik miatt a Kaspersky Endpoint Security blokkolhat egy biztonságos alkalmazást.
- **Alkalmazás integritás-ellenőrzése**. A Kaspersky Endpoint Security elemzi az alkalmazásfájlokat, ellenőrzi a fájlok fertőzöttségét és módosítását, hitelesíti az alkalmazásfájlok digitális aláírását.
- **Hitelesítési ügynök fiókok kezelése**. A Kaspersky Endpoint Security konfigurálja a Hitelesítési ügynök-fiók beállításait. Hitelesítési ügynökre van szükség a titkosított meghajtókkal történő munkavégzéshez. Az operációs rendszer betöltése előtt a felhasználónak el kell végeznie a hitelesítést az ügynökkel.

Ha az alkalmazás a Kaspersky Endpoint Detection and Response megoldás részeként működik, akkor további feladatokat futtathat felderítési válaszműveletként (responses). Például távolról is leállíthat folyamatokat a *Folyamat megszakítása* feladattal.

A feladatok csak akkor futnak a számítógépen, ha a Kaspersky Endpoint Security fut.

Feladat létrehozása

Távoli telepítési feladat létrehozásának menete az Adminisztrációs Konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában a **Tasks** mappát.
3. Kattintson az **New task** gombra.
   Elindul a Feladatvarázsló.
4. Kövesse a Feladatvarázsló utasításait.

Feladat létrehozásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.
   Megnyílik a feladatok listája.
2. Kattintson az **Add** gombra.
   Elindul a Feladatvarázsló.
3. Adja meg a feladatok beállításait:
   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.
   b. A **Task type** legördülő listában válassza ki a feladatot, amit a felhasználói számítógépeken akar futtatni.
   c. A **Task name** mezőben adjon meg egy rövid leírást.
   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.
4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.
5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.
6. Fejezze be a varázslót.

Egy új feladat jelenik meg a feladatok listájában. A feladatoknak alapértelmezett beállításai lesznek. A feladat beállításainak megadásához menjen a feladatok tulajdonságaiba. A feladat futtatásához be kell jelölnie a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra. A feladat indítása után szüneteltetheti a feladatot, később pedig folytathatja.

A feladatok listájában megfigyelheti a feladat eredményeit, amibe beletartozik a feladat állapota és a számítógép feladatainak teljesítményéről szóló statisztika. Létrehozhat eseményeket a feladatok teljesítésének megfigyelése érdekében (**Monitoring** → **Event selections**). Az eseményválasztás további részleteiért lásd a Kaspersky Security Center súgót. A feladat végrehajtásának eredményei a Windows eseménynaplóba is mentésre kerülnek helyileg, valamint a Kaspersky Endpoint Security jelentésekbe is.

Feladat hozzáférésének kezelése

A Kaspersky Endpoint Security feladatok hozzáférési jogosultságai (olvasás, írás, végrehajtás) minden olyan felhasználó esetében definiálva van a Kaspersky Endpoint Security funkcionális területeihez való hozzáférés beállításain keresztül, aki hozzáfér a Kaspersky Security Center felügyeleti kiszolgálóhoz. A Kaspersky Endpoint Security funkcionális területeihez való hozzáférés beállításához lépjen a Kaspersky Security Center felügyeleti kiszolgáló tulajdonságok ablakában **Security** részhez. A Kaspersky Security Center feladatkezeléséről szóló további részletekért lásd a Kaspersky Security Center Súgó útmutatót.

A felhasználóknak rendszabállyal adhat hozzáférési jogot a feladatokhoz (*feladatkezelési mód*). Például elrejthet csoportfeladatokat a Kaspersky Endpoint Security felületen.

A feladatkezelési mód konfigurálásának menete a Kaspersky Endpoint Security felületen, az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakban válassza a **Helyi feladatok** → **Feladatkezelés** részt.
4. Feladatkezelési mód beállítása (lásd az alábbi ábrát).
5. Mentse el a módosításokat.

A feladatkezelési mód konfigurálásának menete a Kaspersky Endpoint Security felületen, a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **User Interaction** elemet.
5. A **Permitted actions** területen konfigurálhatja a feladatkezelési módot (lásd az alábbi ábrát).
6. Mentse el a módosításokat.

Paraméter	Leírás
Access to local tasks	Ha a jelölőnégyzet be van jelölve, a helyi feladatok megjelennek a Kaspersky Endpoint Security helyi felületén. Ha nincsenek további irányelvi korlátozások, a felhasználó beállíthat és futtathat feladatokat. A feladat futási ütemezésének konfigurálása azonban továbbra sem érhető el a felhasználó számára. A felhasználó csak manuálisan futtathat feladatokat. Ha a jelölőnégyzet nincs bejelölve, a helyi feladatok felhasználása leáll. Ebben a módban a helyi feladatok nem futnak az ütemezésnek megfelelően. Feladatok nem indíthatók el és nem állíthatók be a Kaspersky Endpoint Security helyi felületén, illetve a parancssorban végzett munka során sem. A felhasználó ilyenkor is el tudja végezni egy fájl vagy mappa vizsgálatát, ha az adott fájl vagy mappa helyi menüjében kiválasztja a **Vírusok keresése** lehetőséget. A vizsgálati feladat az egyéni vizsgálati feladatok alapértelmezett értékeivel indul el.
View group tasks	Ha a jelölőnégyzet be van jelölve, a csoportfeladatok megjelennek a Kaspersky Endpoint Security helyi felületén. A felhasználó az alkalmazás felületén tekintheti meg a feladatok teljes listáját. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security egy üres feladatlistát jelenít meg.
Manage group tasks	Ha a jelölőnégyzet be van jelölve, a felhasználó elindíthat és leállíthat a Kaspersky Security Center konzolon megadott csoportfeladatokat. A felhasználók az alkalmazás felületén vagy az egyszerűsített alkalmazásfelületen indíthatnak el vagy állíthatnak le feladatokat. A jelölőnégyzet törlése után a Kaspersky Endpoint Security automatikusan elindítja az ütemezett feladatot vagy a rendszergazda manuálisan elindítja a feladatokat a Kaspersky Security Center konzolon.

Helyi alkalmazásbeállítások megadása.

A Kaspersky Security Centerben megadhatja a Kaspersky Endpoint Security beállításait egy bizonyos számítógépen. Ezek a *helyi alkalmazásbeállítások*. Bizonyos beállításokat nem lehet szerkeszteni. Ezek a beállítások zárolva vannak a rendszabály tulajdonságokban.

A helyi alkalmazásbeállítások konfigurálásának menete az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Devices** lapot.
4. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.
5. Válassza ki a számítógép tulajdonságainak ablakában a **Applications** részt.
6. A számítógépre telepített Kaspersky alkalmazások listájában válassza a **Kaspersky Endpoint Security for Windows (14.1)** lehetőséget, és kattintson rá duplán az alkalmazás tulajdonságainak megnyitásához.
7. Konfigurálja az **Általános beállítások** részen a Kaspersky Endpoint Security és a Jelentések és tároló beállításait.

   Az alkalmazás tulajdonságai ablak többi része a Kaspersky Security Center szabványos része. E részek ismertetése a Kaspersky Security Center Súgó található.

   > Ha egy alkalmazásra olyan rendszabály érvényes, amely tiltja adott beállítások megváltoztatását, akkor ezek nem szerkeszthetők az alkalmazás beállításainak **Általános beállítások** részben történő megadása során.

8. Mentse el a módosításokat.

A helyi alkalmazásbeállítások konfigurálásának menete a Web Console-ban, illetve a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.

   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.

   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Adja meg a helyi alkalmazásbeállításokat.
7. Mentse el a módosításokat.

A helyi alkalmazásbeállítások megegyeznek a rendszabálybeállításokkal, kivéve a titkosítási beállításokkal.

A Kaspersky Endpoint Security elindítása és leállítása

Miután telepíti a Kaspersky Endpoint Security alkalmazást a felhasználó számítógépére, az alkalmazás automatikusan elindul. Alapértelmezés szerint a Kaspersky Endpoint Security elindul az operációs rendszer elindítása után. Nincs mód arra, hogy az alkalmazás automatikus indítását konfigurálja az operációs rendszer beállításai között.

A Kaspersky Endpoint Security antivírus adatbázisainak letöltése az operációs rendszer elindulását követően a számítógép képességeitől függően akár két percig is eltarthat. Eközben a számítógép védelmi szintje csökken. Az antivírus adatbázisok letöltése a Kaspersky Endpoint Security már betöltött operációs rendszeren történő elindítása esetén nem csökkenti a számítógép védelmének szintjét.

A Kaspersky Endpoint Security elindításának konfigurálási menete az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. Használja **Az alkalmazás indítása a számítógép bekapcsolásával egy időben (ajánlott)** jelölőnégyzetet az alkalmazás indításának beállításához.
5. Mentse el a módosításokat.

A Kaspersky Endpoint Security elindításának konfigurálási menete a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **User Interaction** elemet.

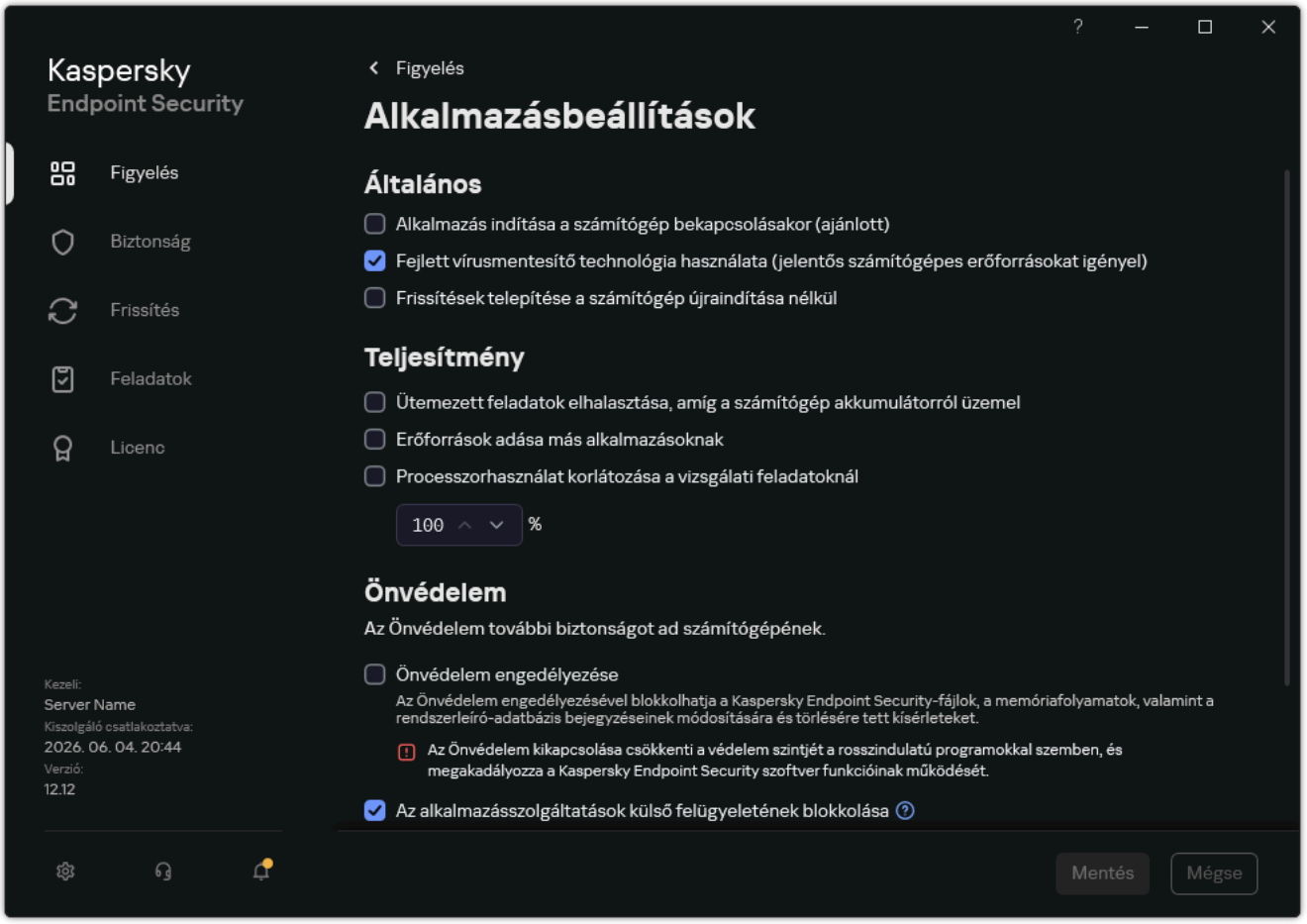
5. A(z) **Start Kaspersky Endpoint Security on computer startup (recommended)** jelölőnégyzettel konfigurálhatja az alkalmazás indítását.

6. Mentse el a módosításokat.

A Kaspersky Endpoint Security elindításának konfigurálási menete az alkalmazásfelületben

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. Használja **Az alkalmazás indítása a számítógép bekapcsolásával egy időben (ajánlott)** jelölőnégyzetet az alkalmazás indításának beállításához.

4. Mentse el a módosításokat.

A Kaspersky szakértői nem javasolják a Kaspersky Endpoint Security kézi leállítását, mivel ezzel a számítógépet és személyes adatait különféle fenyegetéseknek teszi ki. Szükség esetén tetszés szerinti időtartamra szüneteltetheti a számítógép védelmét az alkalmazás leállítása nélkül.

A **Protection status** widgettel megfigyelheti az alkalmazásállapotot.

A Kaspersky Endpoint Security elindításának vagy leállításának menete az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Devices** lapot.
4. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.
5. Válassza ki a számítógép tulajdonságainak ablakában a **Applications** részt.
6. A számítógépre telepített Kaspersky alkalmazások listájában válassza a **Kaspersky Endpoint Security for Windows (14.1)** lehetőséget, és kattintson rá duplán az alkalmazás tulajdonságainak megnyitásához.
7. Végezze el az alábbiak egyikét:
   - Az alkalmazás elindításához kattintson a  gombra a Kaspersky alkalmazások listájának jobb oldalán:
   - Az alkalmazás leállításához kattintson a  gombra a Kaspersky alkalmazások listájának jobb oldalán:

A Kaspersky Endpoint Security elindításának vagy leállításának módja a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Kattintson a számítógép nevére, ahol el akarja indítani vagy le szeretné állítani a Kaspersky Endpoint Security alkalmazást.

   Megnyílik a számítógép tulajdonságainak ablaka.
3. Válassza ki az **Applications** lapot.
4. Jelölje be a **Kaspersky Endpoint Security for Windows** elemmel szemközti jelölőnégyzetet.
5. Kattintson az **Indítás** vagy **Leállítás** gombra.

A Kaspersky Endpoint Security alkalmazás elindítása vagy leállítása a parancssorból

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Nyissa meg azt a mappát, ahol a klpsm.exe futtatható fájl található.
3. Ahhoz, hogy elindítsa az alkalmazást a parancssorból, adja meg a következőt: `klpsm.exe start_avp_service`.
4. Ahhoz, hogy leállítsa az alkalmazást a parancssorból, adja meg a következőt: `klpsm.exe stop_avp_service`.

Ahhoz, hogy leállítsa az alkalmazást a parancssorból, be kell kapcsolnia a rendszerszolgáltatások külső kezelését.



Az alkalmazás indítása és leállítása a parancssorból

A számítógép védelmének és felügyeletének szüneteltetése és folytatása

A számítógép védelmének és felügyeletének szüneteltetése azt jelenti, hogy a Kaspersky Endpoint Security minden védelmi és felügyeleti összetevője bizonyos időre kikapcsol.

Az alkalmazás állapota a tálca értesítési területén elhelyezkedő alkalmazásikon segítségével jelenik meg.

- A ikon azt jeleni, hogy a számítógép védelme és felügyelete szünetel.
- A ikon azt jeleni, hogy a számítógép védelme és felügyelete engedélyezve van.

A számítógép védelmének és felügyeletének szüneteltetése és újraindítása a vizsgálati és frissítési feladatokra nincsenek hatással.

Ha a számítógép védelmének és felügyeletének felfüggesztése, illetve újraindítása idején hálózati kapcsolatok létesülnek, értesítés jelenik meg ezen kapcsolatok megszakításáról.

A számítógép védelmének és felügyeletének szüneteltetése és folytatása:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.
2. A helyi menüjében válassza a **Védelem felfüggesztése** elemet (lásd az alábbi ábrát).

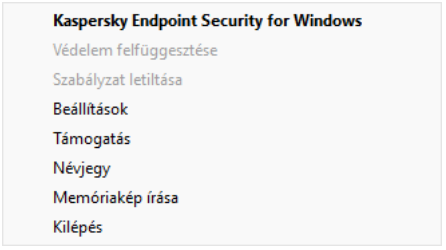
   Ez a helyi menüelem akkor érhető el, ha a Jelszóvédelem engedélyezve van.

3. Válassza ki az alábbi lehetőségek egyikét:

   - **Felfüggesztés <megadott időre>** – a számítógép védelme és felügyelete a lenti legördülő listán megadott idő elteltével folytatódik.
   - **Felfüggesztés az alkalmazás újraindításáig** – A számítógép védelme és felügyelete azt követően folytatódik, hogy Ön újraindítja az alkalmazást, vagy újraindítja az operációs rendszert. A lehetőség használatához engedélyezni kell az alkalmazás automatikus indítását.
   - **Felfüggesztés** – a számítógép védelme és felügyelete akkor folytatódik, amikor Ön a visszakapcsolás mellett dönt.

4. Kattintson a **Védelem felfüggesztése** gombra.

A Kaspersky Endpoint Security szünetelteti a védelmi és felügyeleti összetevők műveleteit, amik nincsenek zárolva a (🔓) rendszabályban. Mielőtt elvégezné ezt a műveletet, javasolt kikapcsolni a Kaspersky Security Center rendszabályt.



Az alkalmazás ikonjának helyi menüje

A számítógép védelmének és felügyeletének folytatása:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.
2. A helyi menüben válassza a **Védelem folytatása** elemet.

A számítógép védelmét és felügyeletét attól függetlenül bármikor folytathatja, hogy korábban milyen szüneteltetési lehetőséget választott ki.

Konfigurációs fájl létrehozása és használata

A Kaspersky Endpoint Security beállításokat tartalmazó konfigurációs fájl révén az alábbi feladatokat lehet elvégezni:

- A Kaspersky Endpoint Security helyi telepítésének elvégzése a parancssorban előre megadott beállításokkal.
- A Kaspersky Endpoint Security távoli telepítésének elvégzése a Kaspersky Security Centeren keresztül előre megadott beállításokkal.
- Alkalmazásbeállítások átvitele szabályzatba.
- A Kaspersky Endpoint Security beállításainak áttelepítése egyik számítógépről a másikra (lásd az alábbi útmutatót).

Konfigurációs fájl exportálása

Konfigurációs fájl létrehozása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Beállítások kezelése** lehetőséget.
3. Kattintson az **Export** gombra.
4. A megnyíló ablakban adja meg a konfigurációs fájl mentésének elérési útját, és adja meg a nevét.

   Ahhoz, hogy a konfigurációs fájlt a Kaspersky Endpoint Security helyi, illetve távoli telepítéséhez használhassa, az install.cfg nevet kell adnia.

5. Ha szükséges, adjon meg egy jelszót az alkalmazás konfigurációjának fájlba való exportálásához.

   A konfigurációs fájl mentéséhez engedélyezni kell a jelszavas védelmet. A felhasználónak rendelkeznie kell a **Beállítások exportálása** engedéllyel.

6. Mentse a fájlt.

Ennek eredményeként az alkalmazás létrehoz egy konfigurációs fájlt. A konfigurációs fájl felhasználói fiókadatokat tartalmazhat, ezért a Kaspersky Endpoint Security titkosítja a fájlt. A konfigurációs fájl nem szerkeszthető. A konfigurációs fájl bármilyen módosítására irányuló kísérlet esetén a fájl megsérül.

Konfigurációs fájl importálása

A konfigurációs fájlok tartalmazhatják az alkalmazáshoz hozzáadott felhasználói fiókok adatait. Ha a fájlt ugyanarra a számítógépre importálja, ahol a fájlt létrehozta, a Kaspersky Endpoint Security importálja a felhasználói fiókok jelszavát. Ha a fájlt egy másik számítógépről importálja, akkor a jelszavakat manuálisan kell megadnia.

Konfigurációs fájlok importálásakor a Kaspersky Endpoint Security nem továbbítja a kriptokonténer jelszavait. Ha a kiszolgálókhoz való csatlakozáskor kétirányú hitelesítést használ, akkor a kriptokonténer jelszavait újra meg kell adnia.

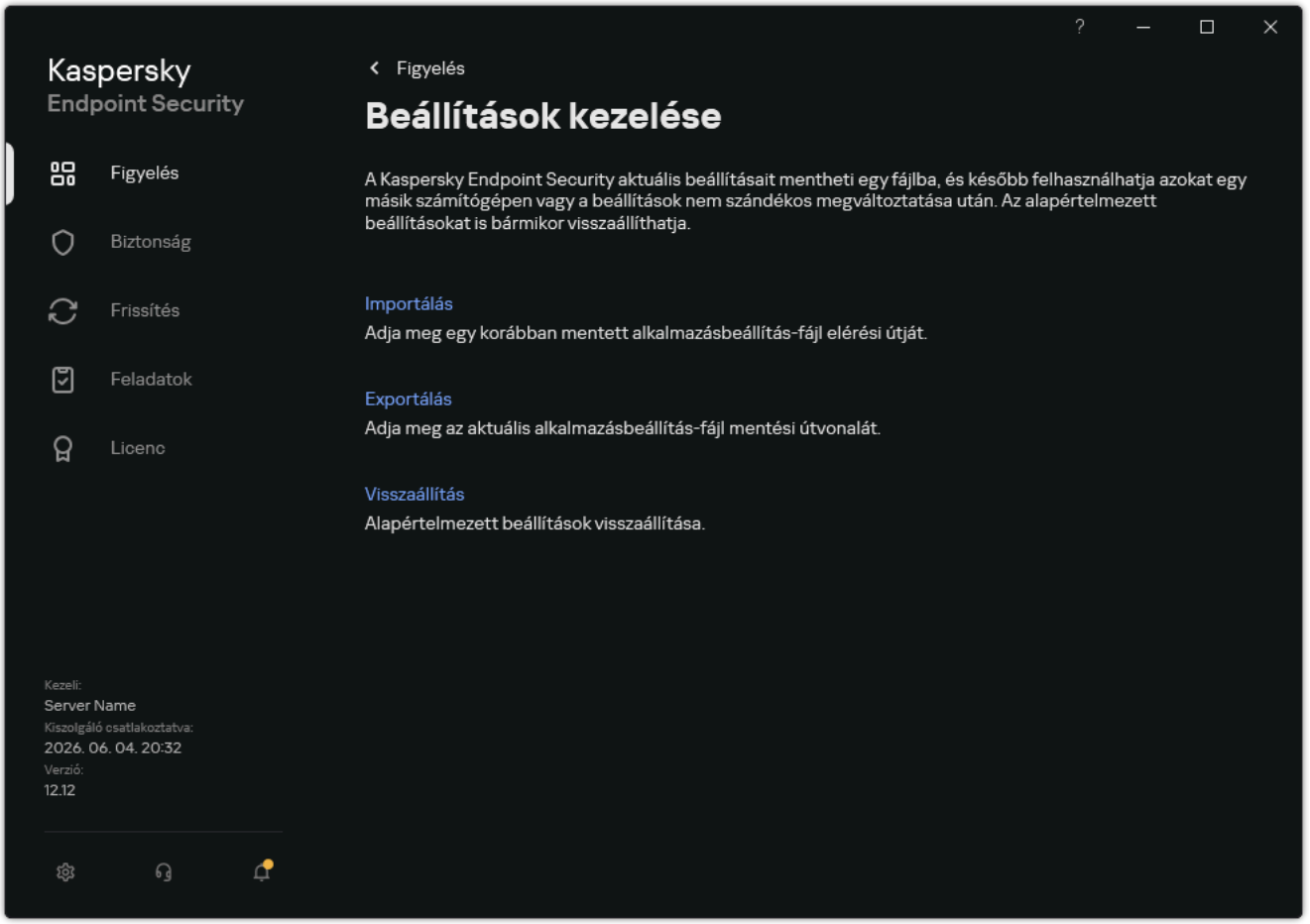
A Kaspersky Endpoint Security beállításainak importálása konfigurációs fájlból:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Beállítások kezelése** lehetőséget.
3. Kattintson az **Import** gombra.

4. A megnyíló ablakban adja be a konfigurációs fájl elérési útját.

5. Nyissa meg a fájlt.

A Kaspersky Endpoint Security összes beállítási értéke a kiválasztott konfigurációs fájl alapján kerül beállításra.



Az alkalmazás beállításainak szerkesztése

Az alapértelmezett alkalmazásbeállítások visszaállítása

Az Kaspersky által ajánlott alkalmazás beállításokat bármikor visszaállíthatja. A beállítások visszaállítása után minden védelmi összetevőnél az **Ajánlott** biztonsági szint lesz beállítva.

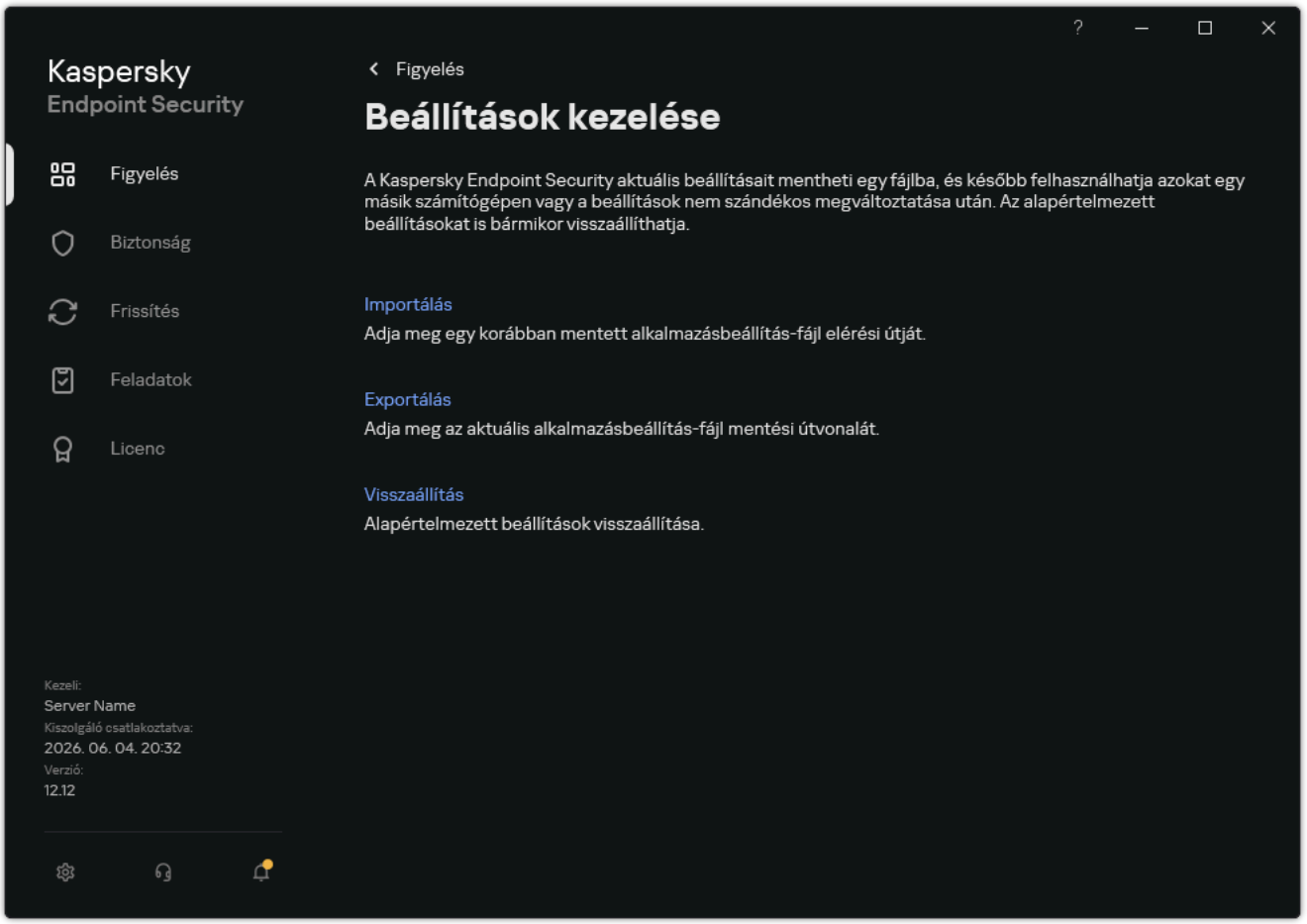
Az alapértelmezett alkalmazásbeállítások visszaállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Beállítások kezelése** lehetőséget.

3. Kattintson a **Visszaállítás** gombra.

4. Mentse el a módosításokat.



Az alkalmazás beállításainak szerkesztése

A Kaspersky Endpoint Security teljesítménye és kompatibilitása más alkalmazásokkal

A Kaspersky Endpoint Security teljesítménye a számítógépnek ártani képes észlelhető objektumtípusok számát, valamint az energiafogyasztást és a számítógépes erőforrások használatát jelöli.

Az észlelhető objektumok típusának kiválasztása

A Kaspersky Endpoint Security lehetővé teszi a számítógép védelmének finomhangolását, és az alkalmazás által működés közben észlelt objektumtípusok kiválasztását. A Kaspersky Endpoint Security az operációs rendszerben mindig vizsgálja a vírusok, férgek és trójaiak jelenlétét. Az ilyen típusú objektumok vizsgálatát nem lehet kikapcsolni. Az ilyen rosszindulatú programok jelentős károkat okozhatnak a számítógépen. A számítógép biztonságának fokozása érdekében az észlelhető objektumtípusok skáláját kibővítheti az olyan jogszerű szoftverek figyelésének bekapcsolása révén, amelyekkel a bűnözők kárt tehetnek a számítógépben, illetve a személyes adatokban.

Az energiatakarékos mód használata

Az alkalmazások energiafogyasztása jelentős kérdés a hordozható számítógépeknél. A Kaspersky Endpoint Security ütemezett feladatainak erőforrásigénye rendszerint jelentős. Ha a számítógép akkumulátorról működik, az energiatakarékos mód segítségével takarékosabban bánhat az energiával.

Energiatakarékos módban az alábbi ütemezett vizsgálatok automatikusan elhalasztódnak:

- Teljes vizsgálat feladat;
- Kritikus területek vizsgálata feladat;
- Egyéni vizsgálat feladat;
- Integritás-ellenőrzés feladat.

Az energiatakarékos mód bekapcsolt állapotától függetlenül a Kaspersky Endpoint Security felfüggeszti a titkosítási feladatokat, ha egy hordozható számítógép akkumulátoros tápellátásra vált. Az alkalmazás akkor folytatja a titkosítási feladatokat, ha a hordozható számítógép visszavált hálózati tápellátásra.

A számítógép erőforrásainak átadása más alkalmazásoknak

A számítógép erőforrásainak felhasználása a számítógép átvizsgálása során növelheti a processzor és a merevlemez alrendszereinek terhelését. A CPU és a merevlemez alrendszerek több alkalmazás egyidejű működése által okozott fokozott terhelése problémájának megoldása érdekében a Kaspersky Endpoint Security képes erőforrásokat átengedni a többi alkalmazásnak.

A fejlett vírusmentesítő technológia használata

A mai rosszindulatú alkalmazások a legalacsonyabb szinteken juthatnak be az operációs rendszerekbe, ezáltal a törlésük gyakorlatilag lehetetlen. Miután az operációs rendszerben rosszindulatú tevékenységet észlelt, a Kaspersky Endpoint Security kiterjedt vírusmentesítési eljárást végez, amely különleges fejlett vírusmentesítő technológiát alkalmaz. A *fejlett vírusmentesítő technológia* célja az operációs rendszer megtisztítása az olyan rosszindulatú alkalmazásoktól, amelyek már elindították folyamataikat a RAM-ban, és amelyek megakadályozzák, hogy a Kaspersky Endpoint Security más módszerekkel távolítsa el őket. Ennek eredményeképpen a fenyegetés semlegesítésre kerül. A Fejlett vírusmentesítés közben ajánlott tartózkodni az új folyamatok indításától, illetve az operációs rendszer beállításjegyzékének szerkesztésétől. A fejlett vírusmentesítő technológia az operációs rendszer jelentős erőforrásait vesz igénybe, amitől a többi alkalmazás lelassulhat.

Miután a Fejlett vírusmentesítési folyamat futása munkaállomásokra való Microsoft Windows rendszert futtató számítógépen véget ért, a Kaspersky Endpoint Security engedélyt kér a felhasználótól a számítógép újraindítására. A rendszer újraindítása során a Kaspersky Endpoint Security törli a rosszindulatú programok fájljait, és elindít a számítógépen egy kisebbfajta teljes vizsgálatot.

Az újraindítási párbeszédpanel használata nem lehetséges a kiszolgálókra szánt Microsoft Windows rendszert futtató számítógépeken a Kaspersky Endpoint Security tulajdonságai miatt. A fájlkiszolgáló nem tervezett újraindítása különféle problémákat okozhat, ami a fájlkiszolgáló adatainak átmeneti elérhetetlenségével vagy a nem mentett adatok elvesztésével járhat. Javasoljuk, hogy a fájlkiszolgálókat szigorúan az ütemezés szerint indítsa újra. Emiatt a Fejlett vírusmentesítési technológia alapértelmezés szerint ki van kapcsolva fájlkiszolgálókon.

Ha egy fájlkiszolgálón aktív fertőzés észlelhető, az alkalmazás eseményt továbbít a Kaspersky Security Center részére, és tájékoztatást küld arról, hogy Fejlett vírusmentesítés szükséges. Kiszolgáló aktív fertőzésének megszüntetéséhez engedélyezze a kiszolgálókhoz készült Fejlett vírusmentesítés technológiát, és indítson *Kártevő vizsgálata* csoportos feladatot a kiszolgáló felhasználóinak megfelelő időpontban.

Az energiatakarékos mód be- és kikapcsolása

Az *energiatakarékos mód* egy olyan funkció, amely csökkenti a laptop erőforrásainak terhelését és meghosszabbítja az akkumulátor élettartamát anélkül, hogy jelentősen veszélyeztetné a biztonsági szintet. Energiatakarékos módban az alkalmazás korlátozza az ütemezett feladatok indítását. Ily módon az energiatakarékos mód egyensúlyt teremt a biztonsági szint és a laptop akkumulátorának élettartama között.

Ha az energiatakarékos mód be van kapcsolva, a számítógép pedig akkumulátorról működik, az alábbi feladatok akkor sem futnak, ha be vannak ütemezve:

- *Teljes vizsgálat*.
- *Kritikus területek vizsgálata*.
- *Egyéni vizsgálat*.
- *Alkalmazás integritás-ellenőrzése*.
- *IOC vizsgálat*.
- *Adatbázisok és alkalmazásmodulok frissítése* (csak javítások)

Az alkalmazás csak akkor hagyja ki az ütemezett adatbázis-frissítéseket, ha a laptop akkumulátorról működik, és az akkumulátor töltöttségi szintje 30% alatt van. Minden más esetben a Kaspersky Endpoint Security az ütemterv szerint frissíti az adatbázisokat, függetlenül attól, hogy a laptop csatlakoztatva van-e a hálózathoz vagy akkumulátorról működik, illetve hogy az alkalmazás energiatakarékos módban van-e.

Az energiatakarékos mód engedélyezése vagy letiltása az Administration Console-on (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
5. A **Teljesítmény** részben használja az **Ütemezett feladatok elhalasztása, amíg a számítógép akkumulátorról üzemel** jelölőnégyzetet az energiatakarékos mód engedélyezéséhez vagy letiltásához.
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

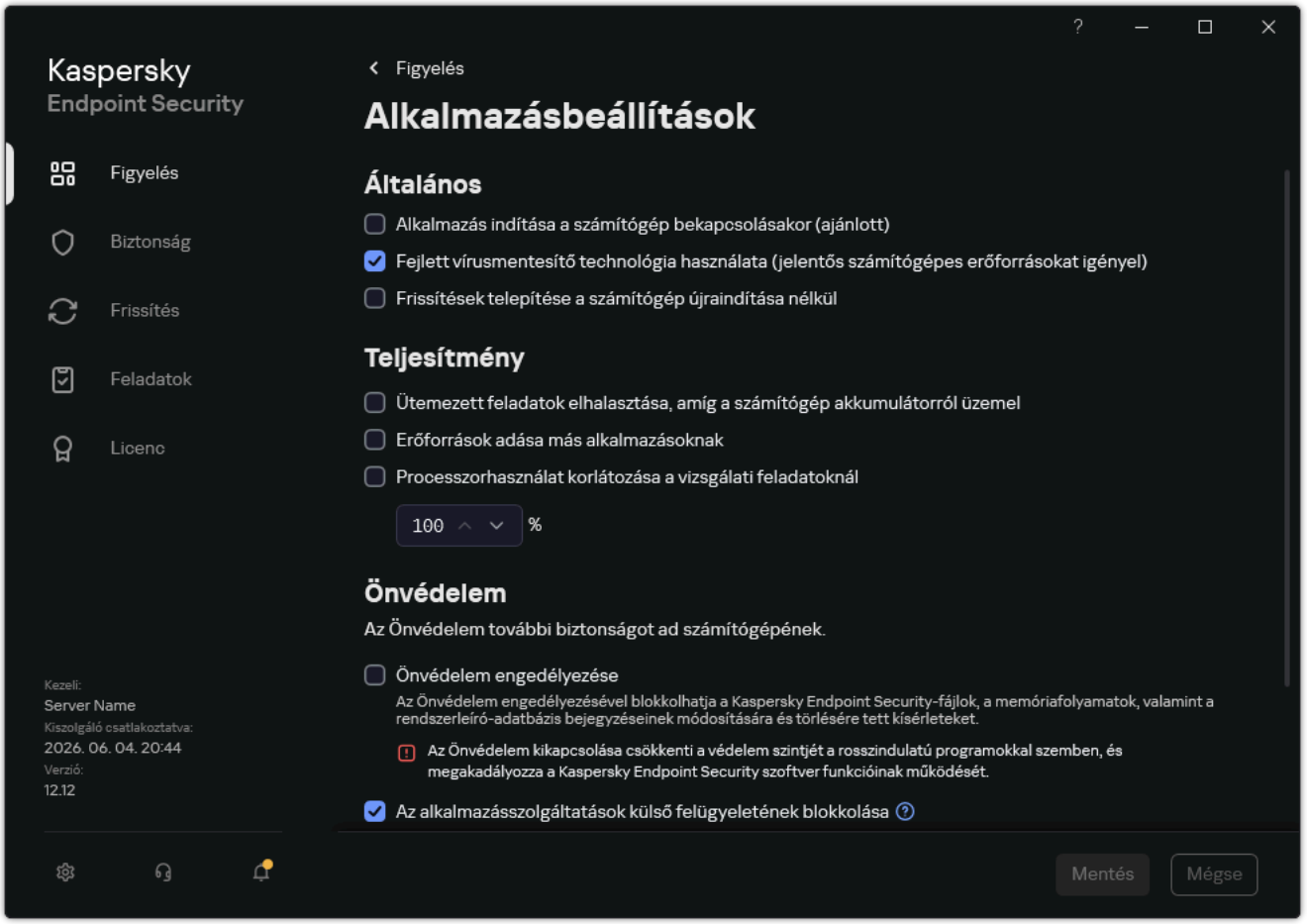
Az energiatakarékos mód engedélyezése vagy letiltása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Performance** elemet.
5. A(z) **Postpone or skip scheduled tasks while running on battery power** blokkban a(z) **Postpone or skip scheduled tasks while running on battery power (depends on OS)** jelölőnégyzet aktiválásával engedélyezheti vagy letilthatja az energiatakarékos módot.
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az energiatakarékos mód engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. A **Teljesítmény** részben használja az **Ütemezett feladatok elhalasztása, amíg a számítógép akkumulátorról üzemel** jelölőnégyzetet az energiatakarékos mód engedélyezéséhez vagy letiltásához.
4. Mentse el a módosításokat.

Erőforrások más alkalmazásoknak történő átadásának engedélyezése és letiltása

A számítógép erőforrásainak Kaspersky Endpoint Security általi felhasználása a számítógép átvizsgálása során növelheti a processzor és a merevlemez alrendszereinek terhelését. Ez lassíthatja más alkalmazások működését. A teljesítmény optimalizálása céljából a Kaspersky Endpoint Security biztosítja *az erőforrások más alkalmazásoknak történő átadásának módját*. Ebben az üzemmódban az operációs rendszer csökkentheti a Kaspersky Endpoint Security vizsgálati feladatszálainak prioritását, ha a processzorterhelés magas. Ez lehetővé teszi az operációs rendszer erőforrásainak más alkalmazások számára történő újraelosztását. Így a vizsgálati feladatok kevesebb processzoridőt kapnak. Ennek eredményeképpen a Kaspersky Endpoint Security számára tovább tart a számítógép vizsgálata. Az alkalmazás alapértelmezés szerint úgy van beállítva, hogy az erőforrásokat átadja más alkalmazásoknak.

Az erőforrások más alkalmazásoknak történő átadásának engedélyezése vagy letiltása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. A **Teljesítmény** részben jelölje be az **Erőforrások adása más alkalmazásoknak** jelölőnégyzetet az erőforrások más alkalmazásoknak való átadása engedélyezéséhez vagy letiltásához.
5. Mentse el a módosításokat.

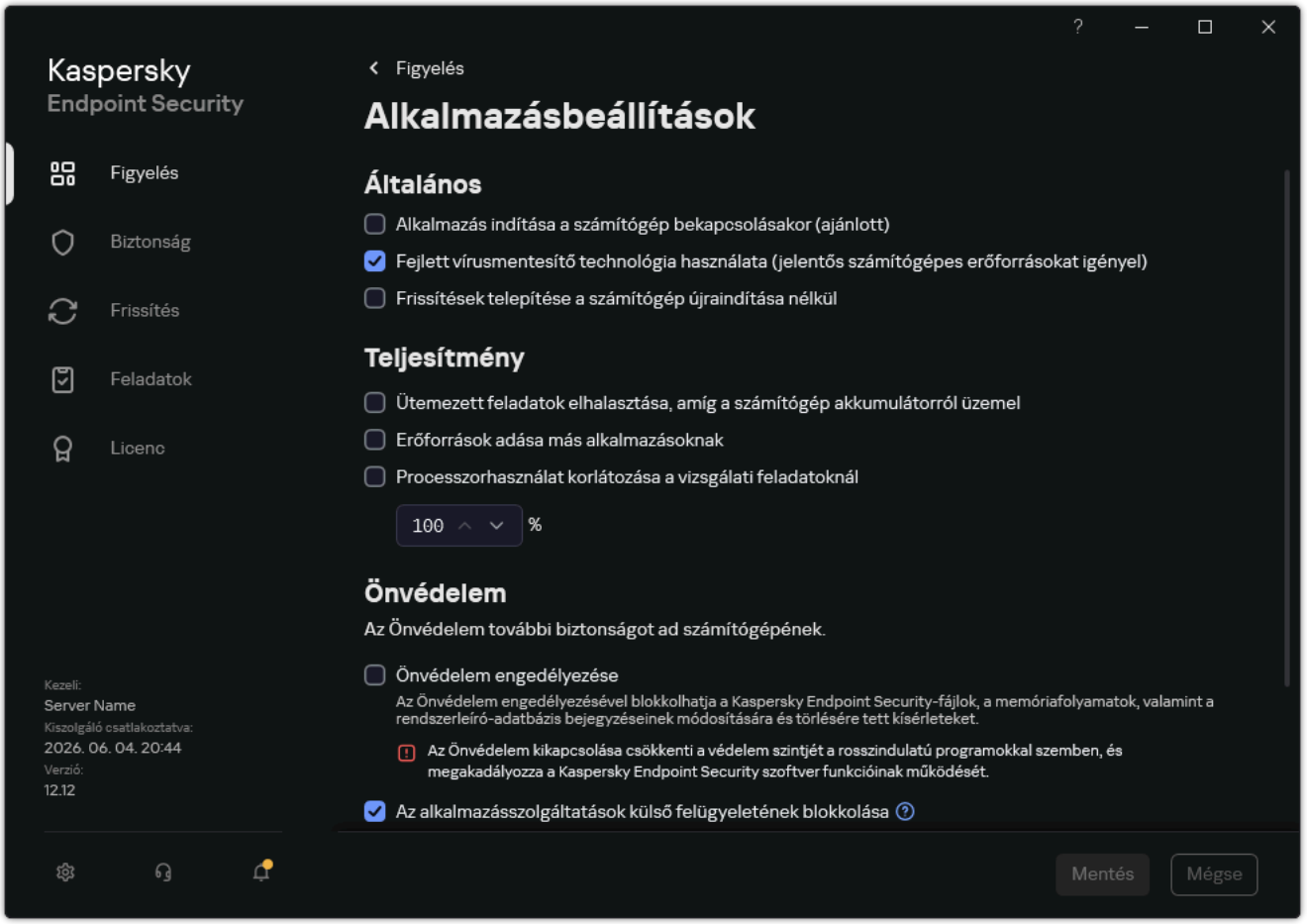
Az erőforrások más alkalmazásoknak történő átadásának engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Performance** elemet.
5. A(z) **Yield resources to other applications** blokkban a(z) **Yield resources to other applications** kapcsolóval engedélyezheti vagy letilthatja az erőforrások más alkalmazásoknak való átengedését.
6. Mentse el a módosításokat.

Az erőforrások más alkalmazásoknak történő átadásának engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. A **Teljesítmény** részben jelölje be az **Erőforrások adása más alkalmazásoknak** jelölőnégyzetet az erőforrások más alkalmazásoknak való átadása engedélyezéséhez vagy letiltásához.
4. Mentse el a módosításokat.

Ajánlott eljárások a Kaspersky Endpoint Security teljesítményének optimalizálásához

A Kaspersky Endpoint Security for Windows telepítésekor a következő javaslatok segítségével konfigurálhatja a számítógép védelmét és optimalizálhatja a teljesítményt. A számítógép teljesítményével kapcsolatos hibák megoldásáról szóló további információkért tekintse meg a Terméktámogatási tudásbázist.

Általános

Konfigurálja az alkalmazás általános beállításait a következő ajánlások szerint:

1. Frissítse a Kaspersky Endpoint Security alkalmazást a legújabb verzióra.

   Az alkalmazás újabb verzióiban javítottuk a hibákat, növeltük a stabilitást, és optimalizáltuk a teljesítményt.

2. Engedélyezze a védelmi összetevőket az alapértelmezett beállításokkal.

   Az alapértelmezett beállítások tekinthetők optimálisnak. A Kaspersky szakértői ezeket a beállításokat ajánlják. Az alapértelmezett beállítások biztosítják az ajánlott védelmi szintet és az optimális erőforrás-felhasználást. Ha szükséges, visszaállíthatja az alkalmazás alapértelmezett beállításait.

3. Engedélyezze az alkalmazásteljesítmény-optimalizálási funkciókat.

   Az alkalmazás teljesítmény-optimalizálási funkciókkal rendelkezik: energiatakarékos mód és erőforrások átengedése más alkalmazásoknak. Győződjön meg arról, hogy ezek a beállítások engedélyezve vannak.

Kártevő vizsgálata munkaállomásokon

Ajánlott a háttérbeli vizsgálat engedélyezése a rosszindulatú programok vizsgálatához a munkaállomásokon. A *Vizsgálat a háttérben* a Kaspersky Endpoint Security egy olyan vizsgálati módja, ami nem jeleníti meg az értesítéseket a felhasználónak. A Vizsgálat a háttérben kevesebb számítógépes erőforrást igényel, mint az egyéb típusú vizsgálatok (például a teljes vizsgálat). Ebben a módban a Kaspersky Endpoint Security megvizsgálja az indítási objektumokat, a rendszerindító szektort, a rendszermemóriát és a rendszerpartíciót. A háttérbeli vizsgálat beállításai tekinthetők optimálisnak. A Kaspersky szakértői ezeket a beállításokat ajánlják. Így a Kártevő vizsgálata a számítógépen csak a háttérbeli vizsgálat módot használhatja egyéb vizsgálati feladatok nélkül.

Ha a háttérbeli vizsgálat nem felel meg az Ön igényeinek, konfigurálja a *Kártevő vizsgálata* feladatot az alábbi ajánlásoknak megfelelően:

1. Állítson be korlátozást a CPU erőforrás-használatára a számítógép vizsgálata közben.

   Korlátozhatja a CPU-használatot a *Kártevő vizsgálata* feladat futtatásakor. Ehhez az alkalmazás beállításaiban adja meg az összes processzormag maximális terhelésének százalékos arányát, amelyet a számítógép vizsgálata során használhat. Ez megnövelheti a számítógép vizsgálatának idejét.

2. Állítsa be az optimális számítógép-vizsgálati ütemezést.

   Konfigurálhatja a feladatot, hogy akkor fusson, amikor a számítógép minimális terhelés mellett működik. Például beállíthatja, hogy a feladat csak éjszaka vagy hétvégén fusson.

   Ha a felhasználók munkaidőn kívül kikapcsolják a számítógépet, engedélyezheti a Hálózati ébresztés funkciót. A Wake-on-LAN funkció lehetővé teszi a számítógép távoli bekapcsolását speciális jelet küldve annak a helyi hálózaton keresztül. A funkció használatához engedélyeznie kell a Wake-on-LAN funkciót a BIOS beállításaiban. Azt is beállíthatja, hogy a számítógép automatikusan kikapcsoljon a vizsgálat befejezése után.

   Ha nem tudta konfigurálni az optimális vizsgálati ütemezést, állítsa be a feladatokat úgy, hogy azok csak akkor fussanak, amikor a számítógép üresjáratban van. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították.

3. Határozzon meg egy vizsgálati hatókört.

Válassza ki a következő objektumokat vizsgálatra (a vizsgálat hatókörének minimális készlete):

- Kernelmemória
- A futó folyamatok és indítási objektumok
- Rendszerindító szektorok
- %systemroot% (almappák nélkül)
- %systemroot%\System (almappák nélkül)
- %systemroot%\System32 (almappák nélkül)
- %systemroot%\System32\drivers (almappák nélkül)
- %systemroot%\SysWOW64 (almappák nélkül)
- %systemroot%\SysWOW64\drivers (almappák nélkül)

4. Kapcsolja be az iSwift és az iChecker technológiákat.

   - iSwift technológia.

     Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.

   - iChecker technológia.

     Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

   Az iSwift és az iChecker technológiákat csak az Adminisztrációs konzolon (MMC) és a Kaspersky Endpoint Security felületén kapcsolhatja be. Ezek a technológiák nem kapcsolhatók be a Kaspersky Security Center Web Console-ban.

5. Tiltsa le a jelszóval védett archívumok vizsgálatát.

   Ha a jelszóval védett archívumok vizsgálata engedélyezve van, akkor az archívum vizsgálata előtt megjelenik egy jelszóbekérő ablak. Mivel a feladatot a munkaidőn kívülre ajánlott ütemezni, a felhasználó nem tudja megadni a jelszót. Lehetőség van a jelszóval védett archívumok manuális vizsgálatára is.

6. Több vizsgálati feladat egyidejű indításának letiltása.

   A Kaspersky Endpoint Security várólistába sorolja az új vizsgálati feladatokat, ha az aktuális vizsgálat folytatódik. Ez segíti a számítógép terhelésének optimalizálását.

Kártevő vizsgálata a kiszolgálókon

Konfigurálja a *Kártevő vizsgálata* feladatot az alábbi ajánlásoknak megfelelően:

1. Állítson be korlátozást a CPU erőforrás-használatára a számítógép vizsgálata közben.

   Korlátozhatja a CPU-használatot a *Kártevő vizsgálata* feladat futtatásakor. Ehhez az alkalmazás beállításaiban adja meg az összes processzormag maximális terhelésének százalékos arányát, amelyet a számítógép vizsgálata során használhat. Ez megnövelheti a számítógép vizsgálatának idejét.

2. Állítsa be az optimális számítógép-vizsgálati ütemezést.

   Konfigurálhatja a feladatot, hogy akkor fusson, amikor a számítógép minimális terhelés mellett működik. Például beállíthatja, hogy a feladat csak éjszaka vagy hétvégén fusson.

3. Kapcsolja be az iSwift és az iChecker technológiákat.

   - iSwift technológia.

     Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.

   - iChecker technológia.

     Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

   Az iSwift és az iChecker technológiákat csak az Adminisztrációs konzolon (MMC) és a Kaspersky Endpoint Security felületén kapcsolhatja be. Ezek a technológiák nem kapcsolhatók be a Kaspersky Security Center Web Console-ban.

4. Tiltsa le a jelszóval védett archívumok vizsgálatát.

   Ha a jelszóval védett archívumok vizsgálata engedélyezve van, akkor az archívum vizsgálata előtt megjelenik egy jelszóbekérő ablak. Mivel a feladatot a munkaidőn kívülre ajánlott ütemezni, a felhasználó nem tudja megadni a jelszót. Lehetőség van a jelszóval védett archívumok manuális vizsgálatára is.

5. Több vizsgálati feladat egyidejű indításának letiltása.

   A Kaspersky Endpoint Security várólistába sorolja az új vizsgálati feladatokat, ha az aktuális vizsgálat folytatódik. Ez segíti a számítógép terhelésének optimalizálását.

Kaspersky Security Network

A számítógép védelmének fokozása érdekében a Kaspersky Endpoint Security a felhasználóktól a világ minden tájáról kapott adatokat használja. A Kaspersky Security Network feladata ezen adatok fogadása.

A *Kaspersky Security Network (KSN)* felhőalapú szolgáltatások egy olyan infrastruktúrája, amely hozzáférést nyújt a Kaspersky online tudásbázisához, ahonnan információkat kaphat fájlok, webes erőforrások és szoftverek megbízhatóságáról. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban reagál az új típusú fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken. Ha tagja a Kaspersky Security Networknek, a KSN szolgáltatások a Kaspersky Endpoint Security számára információkat nyújtanak a vizsgált webcímek megbízhatóságáról, valamint a vizsgált fájlok kategóriájáról és megbízhatóságáról.

Szerkessze a Kaspersky Security Network beállításait a következő ajánlások szerint:

1. Tiltsa le a kiterjesztett KSN módot.

   A *Kiterjesztett KSN mód* egy olyan mód, melyben a Kaspersky Endpoint Security további adatokat küld a Kaspersky számára.

2. Konfigurálja a Privát Kaspersky Security Network szolgáltatást.

   A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről.

3. Felhő mód engedélyezése.

   A *Felhő mód* arra az alkalmazásműveleti módra vonatkozik, amiben a Kaspersky Endpoint Security az antivírus adatbázisok egyszerű verzióját használja. A Kaspersky Security Network támogatja az alkalmazásműveletet, ha az antivírus adatbázisok egyszerű verziója van használva. Az antivírus adatbázisok egyszerű verziójával körülbelül fele annyi RAM-ot használ a számítógépen, amit az átlagos adatbázisokkal használna. Ha nem vesz részt a Kaspersky Security Networkben, vagy ha a felhő mód ki van kapcsolva, a Kaspersky Endpoint Security letölti az antivírus adatbázisok teljes verzióját a Kaspersky szerverekről.

Kártevő vizsgálata

A Kártevő vizsgálata a számítógép biztonsága szempontjából létfontosságú. A rosszindulatú programok rendszeresen elvégzett vizsgálata kizárja az olyan rosszindulatú programok terjedésének lehetőségét, amelyeket a védelmi összetevők nem észleltek az alacsony biztonsági szint miatt, vagy egyéb okokból.

A Kaspersky Endpoint Security nem vizsgálja a OneDrive felhőtárhelyen tárolt fájlok tartalmát, és a létrehozott naplóbejegyzésekben pedig jelzi, hogy ezen fájlok vizsgálatára nem került sor.

Teljes vizsgálat

Az egész számítógép alapos vizsgálata. A Kaspersky Endpoint Security az alábbi objektumokat vizsgálja:

- Kernelmemória
- Az operációs rendszer indulásakor betöltött objektumok
- Rendszerindító szektorok
- Az operációs rendszer biztonsági mentése
- Minden merevlemez és cserélhető meghajtó

A Kaspersky szakértői javasolják, hogy ne módosítsa a *Teljes vizsgálat* feladat hatókörét.

A számítógépes erőforrások megtakarításához javasolt használni a háttérvizsgálati feladatot a teljes vizsgálati feladat helyett. Ez nem csökkenti a számítógép biztonsági szintjét.

Kritikus területek vizsgálata

A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.

A Kaspersky szakértői javasolják, hogy ne módosítsa a *Kritikus területek vizsgálata* feladat hatókörét.

Egyéni vizsgálat

A Kaspersky Endpoint Security a felhasználó által kiválasztott objektumokat vizsgálja. Az alábbi listáról bármely objektumot megvizsgálhatja:

- Rendszermemória
- Az operációs rendszer indulásakor betöltött objektumok
- Az operációs rendszer biztonsági mentése
- Merevlemezek, cserélhető meghajtók és hálózati meghajtók
- Bármely kiválasztott fájl

Vizsgálat a háttérben

A *Vizsgálat a háttérben* a Kaspersky Endpoint Security egy olyan vizsgálati módja, ami nem jeleníti meg az értesítéseket a felhasználónak. A Vizsgálat a háttérben kevesebb számítógépes erőforrást igényel, mint az egyéb típusú vizsgálatok (például a teljes vizsgálat). Ebben a módban a Kaspersky Endpoint Security megvizsgálja az indítási objektumokat, a rendszerindító szektort, a rendszermemóriát és a rendszerpartíciót.

Alkalmazás integritás-ellenőrzése

A Kaspersky Endpoint Security ellenőrzi, hogy az alkalmazásmodulok nem sérültek vagy módosultak-e.

Számítógép vizsgálata

A vizsgálat a számítógép biztonsága szempontjából létfontosságú. A rosszindulatú programok rendszeresen elvégzett vizsgálata kizárja az olyan rosszindulatú programok terjedésének lehetőségét, amelyeket a védelmi összetevők nem észleltek az alacsony biztonsági szint miatt, vagy egyéb okokból. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

A Kaspersky Endpoint Security következő standard feladatai előre meghatározottak: *Teljes vizsgálat*, *Kritikus területek vizsgálata*, *Egyéni vizsgálat*. Ha a vállalata telepítette a Kaspersky Security Center adminisztrációs rendszerét, akkor létrehozhat egy *Kártevő vizsgálata* feladatot, és konfigurálhatja a vizsgálatot.

Vizsgálati feladat futtatása az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.

3. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.

   Ha szükséges, hozza létre a *Kártevő vizsgálata* feladatot.

4. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.

5. Konfigurálja a vizsgálati feladatot (lásd az alábbi táblázatot).

   Ha szükséges, konfigurálja a vizsgálati feladat ütemezését.

6. Mentse el a módosításokat.

7. Futtassa a vizsgálati feladatot.

A Kaspersky Endpoint Security elindítja a számítógép vizsgálatát. Ha a felhasználó megszakította a feladat végrehajtását (például a számítógép kikapcsolásával), a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol a vizsgálatot megszakították.

Vizsgálati feladat futtatása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Konfigurálja a vizsgálati feladatot (lásd az alábbi táblázatot).

   Ha szükséges, konfigurálja a vizsgálati feladat ütemezését.

5. Mentse el a módosításokat.

6. Futtassa a vizsgálati feladatot.

A Kaspersky Endpoint Security elindítja a számítógép vizsgálatát. Ha a felhasználó megszakította a feladat végrehajtását (például a számítógép kikapcsolásával), a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol a vizsgálatot megszakították.

Vizsgálati feladat futtatása az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.

2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.

3. Konfigurálja a vizsgálati feladatot (lásd az alábbi táblázatot).

   Ha szükséges, konfigurálja a vizsgálati feladat ütemezését.

4. Mentse el a módosításokat.

5. Futtassa a vizsgálati feladatot.

A Kaspersky Endpoint Security elindítja a számítógép vizsgálatát. Az alkalmazás mutatja a vizsgálat előrehaladását, a megvizsgált fájlok számát és a még hátralévő vizsgálati időt. A feladatot bármikor leállíthatja a **Leállítás** gombra kattintva. Ha a vizsgálati feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

A Kaspersky Endpoint Security teljesítményének optimalizálása céljából a számítógép vizsgálata során felügyelheti a *Teljes vizsgálat feladat* speciális beállításait, és korlátozhatja a processzor erőforrásainak használatát.

A Kaspersky Security Center alkalmazásban használhatja a *Háttérbeli vizsgálat* feladat helyett a *Teljes vizsgálat* feladatot az alkalmazás teljesítményének optimalizálására. Ez nem csökkenti a számítógép biztonsági szintjét. A háttérben végzett vizsgálat nem konfigurálható.

Ennek eredményeként a Kaspersky Endpoint Security átvizsgálja a számítógépet, és ha fenyegetést észlel, végrehajtja az alkalmazás beállításaiban konfigurált műveletet. Az alkalmazás általában megpróbálja vírusmentesíteni a fertőzött fájlokat. Ennek eredményeként a fertőzött fájlok a következő állapotokat kaphatják:

- **Elhalasztott**. A fertőzött fájlt nem lehetett vírusmentesíteni. Az alkalmazás a számítógép újraindítása után törli a fertőzött fájlt.
- **Naplózott**. A fertőzött fájlt nem lehetett vírusmentesíteni. Az alkalmazás hozzáadja az észlelt fertőzött fájlokról szóló információkat az aktív fenyegetések listájához.
- **Az írás nem támogatott** vagy **Írási hiba**. A fertőzött fájlt nem lehetett vírusmentesíteni. Az alkalmazásnak nincs írási jogosultsága.
- **Már feldolgozva**. Az alkalmazás korábban észlelt egy fertőzött fájlt. Az alkalmazás a számítógép újraindítása után vírusmentesíti vagy törli a fertőzött fájlt.

Vizsgálati beállítások

Paraméter	Leírás
Biztonsági szint	A Kaspersky Endpoint Security különböző beállításcsoportokat használhat a vizsgálat futtatásához. Ezek az alkalmazásban tárolt beállításcsoportokat *biztonsági szinteknek* nevezzük: • **Magas**. A Kaspersky Endpoint Security minden típusú fájlt megvizsgál. Összetett fájlok vizsgálatakor az alkalmazás megvizsgálja az archívumokat, a terjesztési csomagokat, az Office formátumú fájlokat, de nem vizsgálja a jelszóval védett archívumokat. Ha ez a biztonsági szint be van állítva, az alkalmazás heurisztikus elemzést használ az **Alapos vizsgálat** részletezési szinttel. • **Ajánlott**. A Kaspersky Endpoint Security minden típusú fájlt megvizsgál. Összetett fájlok vizsgálatakor az alkalmazás megvizsgálja az archívumokat, a terjesztési csomagokat, az Office formátumú fájlokat, de nem vizsgálja a jelszóval védett archívumokat. Ha ez a biztonsági szint be van állítva, az alkalmazás heurisztikus elemzést használ a **Közepes vizsgálat** részletezési szinttel. • **Alacsony**. A Kaspersky Endpoint Security csak a megadott fájlformátumokat vizsgálja. Összetett fájlok vizsgálatakor az alkalmazás megvizsgálja az archívumokat, a terjesztési csomagokat, az Office formátumú fájlokat, de nem vizsgálja a jelszóval védett archívumokat. Ha ez a biztonsági szint be van állítva, az alkalmazás heurisztikus elemzést használ az **Egyszerű vizsgálat** részletezési szinttel. Kiválaszthatja az előre beállított biztonsági szintek egyikét, de kézileg is megadhatja a beállításokat. Ha módosítja a biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.

Paraméter	Leírás
Művelet fenyegetés észlelésekor	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt. **Vírusmentesítés, értesítés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához. **Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor. Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, az alkalmazás létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz. Windows Store-alkalmazás részét alkotó fertőzött fájlok észlelése esetén a Kaspersky Endpoint Security megkísérli törölni a fájlt.
Fejlett vírusmentesítés futtatása azonnal *(csak a Kaspersky Security Center konzolon érhető el)*	A Fejlett vírusmentesítés csak akkor van alkalmazva a vírusvizsgálat alatt, ha a Fejlett vírusmentesítés funkció engedélyezve van a számítógépen alkalmazott irányelv tulajdonságaiban. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security azonnal vírusmentesíti az aktív fertőzést, miután észlelte azt a vírusvizsgálati feladat végrehajtása során. Az aktív fertőzés vírusmentesítése után a Kaspersky Endpoint Security a felhasználó megkérdezése nélkül újraindítja a számítógépet. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem vírusmentesíti az aktív fertőzést, miután észlelte azt a vírusvizsgálati feladat végrehajtása során. A Kaspersky Endpoint Security aktív fertőzési eseményeket hoz létre a helyi alkalmazásjelentésekben és a Kaspersky Security Center oldalán. Az aktív fertőzés vírusmentesíthető, ha a vírusvizsgálati feladatot újból futtatja a Fejlett vírusmentesítés funkció bekapcsolásával. Ily módon a rendszergazda kiválaszthatja a megfelelő időt a fejlett vírusmentesítés elvégzésére, majd ezt követően automatikusan újraindíthatja a számítógépeket.
Vizsgálat hatóköre	A Kaspersky Endpoint Security által a vizsgálati feladat végrehajtása során vizsgált objektumok listája. A vizsgálat hatókörébe tartozó objektumok között szerepelhet a rendszermag memóriája, a futó folyamatok, a rendszerindító szektorok, a rendszer másolattároló, a merevlemez, a cserélhető meghajtó vagy a hálózati meghajtó, egy-egy mappa, illetve fájl. A Kaspersky Endpoint Security for Windows 12.12-ben az e-mailek nem tartoznak az alkalmazás vizsgálati hatókörébe. A bejövő és kimenő e-mail-üzenetek vizsgálatát a Levelezésvédelem összetevő végzi. Ha az adminisztrációs bővítmény korábbi verzióját használja, az alkalmazás kizárja az e-maileket a vizsgálatból, még akkor is, ha a házirend tartalmazza azokat.
Vizsgálat ütemezése	**Manually**. A futásmód, amelyben manuálisan elindíthatja a vizsgálatot, amikor az Önnek kényelmes. **By schedule**. A vizsgálati feladatoknak ebben a futásmódjában az alkalmazás a feladatot a létrehozott ütemtervnek megfelelően futtatja. A vizsgálati feladat ezen futásmódjának kiválasztása esetén a vizsgálati feladat elindítható kézileg is.
Futtatás elhalasztása az alkalmazásindítás után N percre	A vizsgálati feladat elhalasztása az alkalmazás elindulása után. Az operációs rendszer indításakor számos folyamat fut, ezért előnyös a vizsgálati feladat futtatását elhalasztani, ahelyett, hogy közvetlenül a Kaspersky Endpoint Security indítása után futtatná.
Kihagyott vizsgálatok futtatása	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott feladatot azonnal elindítja, amint lehetségessé válik. A feladat például akkor hagyható ki, ha a számítógép az ütemezett feladat indítási időpontjában ki volt kapcsolva. Amikor az alkalmazás lehetőséget kap a kihagyott feladatok végrehajtására, egy adott időintervallumon belül véletlenszerűen futtatja a feladatokat, hogy elossza a számítógép terhelését. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott feladatokat. Ehelyett a következő feladatot a jelenlegi ütemezésnek megfelelően futtatja.
Csak akkor fusson, ha a számítógép üresjáratban van	A feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították. Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.

Paraméter	Leírás
Vizsgálat futtatása mint	Alapértelmezés szerint az alkalmazás a vizsgálati feladatot annak a felhasználónak a nevében futtatja, akinek a jogosultságaival Ön regisztrálva van az operációs rendszerben. A védelem hatóköre magában foglalhatja a hálózati meghajtókat vagy más objektumokat, amelyek eléréséhez speciális hozzáférési jogokra van szükség. Az alkalmazás beállításaiban megadhat egy olyan felhasználót, aki rendelkezik a szükséges jogokkal, és a vizsgálati feladatot e felhasználói fiók alatt futtathatja.
Fájltípusok	A Kaspersky Endpoint Security a kiterjesztés nélküli fájlokat végrehajthatónak tekinti. Az alkalmazás a végrehajtható fájlokat mindig megvizsgálja, függetlenül a vizsgálatra kiválasztott fájltípusoktól. **Minden fájl**. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül). **Formátum alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejlécet a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres. **Kiterjesztés alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg. A Kaspersky Endpoint Security alapértelmezés szerint a formátumuk alapján vizsgálja a fájlokat. A fájlok kiterjesztés szerinti vizsgálata kevésbé biztonságos, mert elképzelhető, hogy egy rosszindulatú fájl kiterjesztése nem szerepel a potenciálisan fertőzöttek listáján (pl. `.123`).
Csak új és módosult fájlok vizsgálata	Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.
Fájlok kihagyása, ha a vizsgálat több mint N mp	A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.
Ne futtasson több vizsgálati feladatot egyszerre!	Vizsgálati feladatok elhalasztott indítása, ha egy vizsgálat már fut. A Kaspersky Endpoint Security várólistába sorolja az új vizsgálati feladatokat, ha az aktuális vizsgálat folytatódik. Ez segíti a számítógép terhelésének optimalizálását. Feltételezzük például, hogy az alkalmazás az ütemezésnek megfelelően Teljes vizsgálatot indított el. Ha egy felhasználó megpróbál fájlvizsgálatot indítani az alkalmazás felületéről, a Kaspersky Endpoint Security sorba állítja ezt a gyorsvizsgálati feladatot, majd automatikusan elindítja ezt a feladatot, miután a Teljes vizsgálati feladat befejeződött. Ugyanakkor a Kaspersky Endpoint Security azonnal elindítja a vizsgálati feladatot akkor is, ha a következő vizsgálati feladatok közül az egyik fut: • Cserélhető meghajtók vizsgálata csatlakozáskor. • Vizsgálat a helyi menüből. • Kritikus területek vizsgálata, amely egy biztonsági sérülés indikátor (IoC) észlelés alapján indult. Ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security hagyja, hogy egyszerre több vizsgálati feladatot futtasson. Több vizsgálati feladat futtatása több számítógépes erőforrást igényel.
Archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.
Terjesztési csomagok vizsgálata	Harmadik féltől származó alkalmazások terjesztőcsomagjainak vizsgálata.
Microsoft Office formátumú fájlok vizsgálata	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.

Paraméter	Leírás
E-mail formátumú fájlok vizsgálata	Az e-mail formátumú fájlok és a levéladatbázis átvizsgálása. Az alkalmazás ellenőrzi az MS Outlook és a Windows Mail levelezőprogramok által használt PST- és OST-fájlokat, valamint az EML-fájlokat. A Kaspersky Endpoint Security nem támogatja a Microsoft Outlook levelezőprogram 64 bites verzióját. Ez azt jelenti, hogy a Kaspersky Endpoint Security nem vizsgálja át a Microsoft Outlook-fájlokat (PST- és OST-fájlokat), ha a számítógépre a Microsoft Outlook 64 bites verziója van telepítve, még akkor sem, ha az e-mailek szerepelnek a vizsgálat hatókörében. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security az e-mail formátumú fájlt felbontja összetevőire (fejléc, szövegtörzs, mellékletek), és megvizsgálja bennük a fenyegetéseket. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security az e-mail formátumú fájlt egyetlen fájlként vizsgálja meg. Ha a rendszer rosszindulatú objektumot észlel a PST vagy OST fájlokban, a Kaspersky Endpoint Security a kiválasztott műveletnek (például a fájl vírusmentesítése vagy törlése) megfelelően ártalmatlanná teszi azt. Ha más levelezőprogramok (például a Mozilla Thunderbird) fájljaiban rosszindulatú fájlt észlel, a Kaspersky Endpoint Security csak a fertőzött üzenetet jelöli meg. A fertőzött mellékletet tartalmazó üzenetet manuálisan kell törölnie.
Jelszóvédett archívumok vizsgálata	Ha a jelölőnégyzet be van jelölve, az alkalmazás vizsgálja a jelszóval védett archívumokat. Mielőtt az archívumokban lévő fájlokat vizsgálatára sor kerülhetne, a rendszer felkéri a jelszó megadására. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás kihagyja a jelszóval védett archívumok vizsgálatát.
Ne csomagoljon ki nagy összetett fájlokat	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás minden összetett fájlt megvizsgál. Az alkalmazás megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.
Gépi tanulás és aláíráselemzés	A gépi tanulási és aláírás-elemzési módszer a Kaspersky Endpoint Security adatbázisait használja, melyek az ismert fenyegetések leírásait és semlegesítésük módszereit tartalmazzák. Az ezt a módszert alkalmazó védelem biztosítja a minimális elfogadható biztonsági szintet. A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.
Heurisztikus elemzés	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
iSwift Technológia *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.
iChecker Technológia *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

Cserélhető meghajtók vizsgálata a számítógéphez történő csatlakoztatásukkor

A Kaspersky Endpoint Security az összes futtatott vagy másolt fájlt megvizsgálja, még akkor is, ha a fájl cserélhető meghajtón található (a Fájl védelem összetevő). A vírusok és más rosszindulatú programok terjedésének megakadályozásához beállíthatja a cserélhető meghajtók automatikus vizsgálatát a számítógéphez történő csatlakoztatáskor. A Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security törli a fájlokat. Az összetevő gépi tanulást, heurisztikus elemzést (magas szintű) és aláírás-elemzést használó vizsgálatok futtatásával gondoskodik a számítógép-biztonságról. A Kaspersky Endpoint Security emellett iSwift és iChecker vizsgálatoptimalizálási technológiákat is alkalmaz. Ezek a technológiák mindig aktívak, és nem tilthatók le.

A cserélhető meghajtók vizsgálati futtatásának konfigurálása az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakban válassza a **Helyi feladatok** → **Cserélhető meghajtók vizsgálata** részt.
4. A **Cserélhető meghajtó csatlakoztatásakor végzendő művelet** legördülő listából válassza a **Részletes vizsgálat** vagy a **Gyors vizsgálat** lehetőséget.
5. Konfigurálja a cserélhető meghajtók vizsgálatának speciális beállításait (lásd az alábbi táblázatot).
6. Mentse el a módosításokat.

A cserélhető meghajtók vizsgálati futtatásának konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Removable Drives Scan** elemet.
5. A **Removable Drives Scan ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Az **Scan type** területen válassza a **Detailed Scan** vagy a **Quick Scan** opciót.
7. Konfigurálja a cserélhető meghajtók vizsgálatának speciális beállításait (lásd az alábbi táblázatot).
8. Mentse el a módosításokat.

A cserélhető meghajtók vizsgálati futtatásának konfigurálása az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.
2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.

3. A **Cserélhető meghajtók vizsgálata** kapcsolóval engedélyezheti vagy letilthatja a cserélhető meghajtók vizsgálatát a számítógéphez való csatlakozáskor.

4. Konfigurálja a cserélhető meghajtók vizsgálatának speciális beállításait (lásd az alábbi táblázatot).

5. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Endpoint Security futtatja a Cserélhető meghajtók vizsgálatát a megadott maximális méretnél nem nagyobb cserélhető meghajtókon. Ha a *Cserélhető meghajtók vizsgálata* feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

Cserélhető meghajtók vizsgálatának beállításai

Paraméter	Leírás
Scan type	**Detailed Scan**. Ha ez az opció van kiválasztva, a Kaspersky Endpoint Security cserélhető meghajtó csatlakoztatásakor az összes fájlt megvizsgálja, beleértve az összetett objektumokba ágyazott fájlokat, az archívumokat, a terjesztőcsomagokat és az Office formátumú fájlokat. A Kaspersky Endpoint Security nem vizsgál levélformátumú fájlokat vagy jelszóval védett archívumokat. **Quick Scan**. Ha ez a lehetőség van kiválasztva, akkor a cserélhető meghajtó csatlakoztatását követően a Kaspersky Endpoint Security csak az adott kiterjesztésű fájlokat vizsgálja, amelyek a fertőzésekkel szemben a leginkább sebezhetők, és nem csomagolja ki az összetett objektumokat.
Maximum drive size (MB)	Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kiválasztott műveletet a megadott maximális meghajtóméretet meg nem haladó méretű cserélhető meghajtókon hajtja végre. Ha a cserélhető meghajtó mérete meghaladja a beállított értéket, a Kaspersky Endpoint Security kihagyja a vizsgálatot. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security a kiválasztott műveletet bármilyen méretű cserélhető meghajtón végrehajtja.
Hide scan progress bar	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a cserélhető meghajtók vizsgálatának állapotát külön ablakban és a **Feladatok** ablakban jeleníti meg. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security a cserélhető meghajtók vizsgálatát a háttérben hajtja végre.
Prevent users from stopping the scan	Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security helyi felületén, a Cserélhető meghajtók vizsgálata feladatnál a **Feladatok** szakasz **Leállítás** gombja és a Cserélhető meghajtók vizsgálata ablak **Leállítás** gombja nem lesz elérhető.

Vizsgálat a háttérben

A *Vizsgálat a háttérben* a Kaspersky Endpoint Security egy olyan vizsgálati módja, ami nem jeleníti meg az értesítéseket a felhasználónak. A Vizsgálat a háttérben kevesebb számítógépes erőforrást igényel, mint az egyéb típusú vizsgálatok (például a teljes vizsgálat). Ebben a módban a Kaspersky Endpoint Security megvizsgálja az indítási objektumokat, a rendszerindító szektort, a rendszermemóriát és a rendszerpartíciót.

A számítógépes erőforrások fenntartására javasolt használni a háttérvizsgálati feladatot a teljes vizsgálati feladat helyett. Ez nem csökkenti a számítógép biztonsági szintjét. Ezek a feladatok ugyan azzal a vizsgálati hatókörrel rendelkeznek. A számítógép terhelésének optimalizálása érdekében az alkalmazás nem futtat egyszerre teljes vizsgálati és háttérvizsgálati feladatot. Ha már lefuttatta a teljes vizsgálat feladatot, a Kaspersky Endpoint Security a teljes vizsgálat befejezésétől számított hét napig nem indít vizsgálatot a háttérben.

Háttérvizsgálat a következő esetekben indítható:

- Antivírus adatbázisok frissítése után.
- A Kaspersky Endpoint Security indítása után 30 perccel.
- Hat óránként.
- Ha a számítógép öt percig vagy tovább tétlen (a számítógép zárolva van, vagy a képernyővédő be van kapcsolva).

Amikor a számítógép készenléti üzemmódban van, a háttérvizsgálat megszakad, ha a következő feltételek egyike teljesül:

- A számítógép aktív módba váltott.

  Amikor már több mint tíz napja nem volt háttérvizsgálat futtatva, akkor a vizsgálat nem fog megszakadni.

- A számítógép (laptop) akkumulátor üzemmódba váltott.

Ha a háttérvizsgálatot végez, a Kaspersky Endpoint Security nem vizsgálja meg azokat a fájlokat, amik tartalma a OneDrive felhőtárhelyen van.

A háttérvizsgálat engedélyezése az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakban válassza a **Helyi feladatok** → **Vizsgálat a háttérben** részt.
4. A **Háttérbeli vizsgálat engedélyezése** jelölőnégyzettel kapcsolhatja be vagy ki a vizsgálatot a háttérben.
5. Mentse el a módosításokat.

A háttérvizsgálat engedélyezése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Navigáljon ide: **Host Threat Protection** → **File Threat Protection**.
5. A(z) **Background Scan** területen a(z) **Background Scan ENABLED** kapcsolóval engedélyezheti vagy tilthatja le a háttérben futó vizsgálatot.
6. Mentse el a módosításokat.

A háttérvizsgálat engedélyezése az alkalmazás felületén

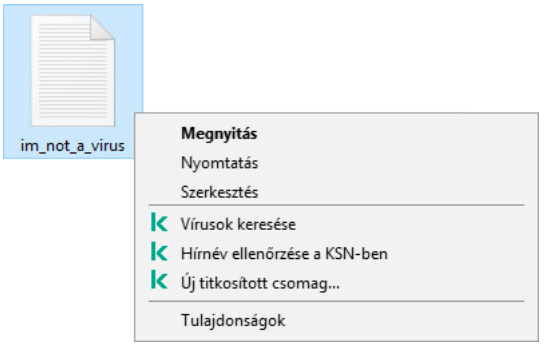
1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.
2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.
3. A **Vizsgálat a háttérben** kapcsolóval kapcsolhatja be vagy ki a háttérvizsgálatot.
4. Mentse el a módosításokat.

Ha a *Vizsgálat a háttérben* nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

Vizsgálat a helyi menüből

A Kaspersky Endpoint Security segítségével vírusokat kereshet egyéni fájlokban, valamint egyéb rosszindulatú programokat is a helyi menüből (lásd az alábbi ábrát).

Ha a helyi menüből történő vizsgálatot végez, a Kaspersky Endpoint Security nem vizsgálja meg azokat a fájlokat, amik tartalma a OneDrive felhőtárhelyen van.



Vizsgálat a helyi menüből

A Vizsgálat a helyi menüből feladat konfigurálása az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Helyi feladatok → Vizsgálat a helyi menüből** lehetőséget.
4. A Vizsgálat a helyi menüből feladat konfigurálása (lásd az alábbi táblázatot).
5. Mentse el a módosításokat.

A Vizsgálat a helyi menüből feladat konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Navigáljon ide: **Host Threat Protection → File Threat Protection**.
5. A **Scan from Context Menu** területen konfigurálhatja a vizsgálatot a helyi menüből (lásd az alábbi táblázatot).
6. Mentse el a módosításokat.

A Vizsgálat a helyi menüből feladat konfigurálása az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.
2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.
3. A Vizsgálat a helyi menüből feladat konfigurálása (lásd az alábbi táblázatot).
4. Mentse el a módosításokat.

Ha a *Vizsgálat a helyi menüből* feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

A helyi menüből való vizsgálat beállításai

Paraméter	Leírás
Biztonsági szint	A Kaspersky Endpoint Security különböző beállításcsoportokat használhat a vizsgálat futtatásához. Ezek az alkalmazásban tárolt beállításcsoportokat *biztonsági szinteknek* nevezzük: • **Magas**. A Kaspersky Endpoint Security minden típusú fájlt megvizsgál. Összetett fájlok vizsgálatakor az alkalmazás megvizsgálja az archívumokat, a terjesztési csomagokat, az Office formátumú fájlokat, de nem vizsgálja a jelszóval védett archívumokat. Ha ez a biztonsági szint be van állítva, az alkalmazás heurisztikus elemzést használ az **Alapos vizsgálat** részletezési szinttel. • **Ajánlott**. A Kaspersky Endpoint Security minden típusú fájlt megvizsgál. Összetett fájlok vizsgálatakor az alkalmazás megvizsgálja az archívumokat, a terjesztési csomagokat, az Office formátumú fájlokat, de nem vizsgálja a jelszóval védett archívumokat. Ha ez a biztonsági szint be van állítva, az alkalmazás heurisztikus elemzést használ a **Közepes vizsgálat** részletezési szinttel. • **Alacsony**. A Kaspersky Endpoint Security csak a megadott fájlformátumokat vizsgálja. Összetett fájlok vizsgálatakor az alkalmazás megvizsgálja az archívumokat, a terjesztési csomagokat, az Office formátumú fájlokat, de nem vizsgálja a jelszóval védett archívumokat. Ha ez a biztonsági szint be van állítva, az alkalmazás heurisztikus elemzést használ az **Egyszerű vizsgálat** részletezési szinttel.
Művelet fenyegetés észlelésekor	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt. **Vírusmentesítés, értesítés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához. **Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.
Fájltípusok	A Kaspersky Endpoint Security a kiterjesztés nélküli fájlokat végrehajthatónak tekinti. Az alkalmazás a végrehajtható fájlokat mindig megvizsgálja, függetlenül a vizsgálatra kiválasztott fájltípusoktól. **Minden fájl**. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül). **Formátum alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejlécet a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres. **Kiterjesztés alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg. A Kaspersky Endpoint Security alapértelmezés szerint a formátumuk alapján vizsgálja a fájlokat. A fájlok kiterjesztés szerinti vizsgálata kevésbé biztonságos, mert elképzelhető, hogy egy rosszindulatú fájl kiterjesztése nem szerepel a potenciálisan fertőzöttek listáján (pl. `.123`).
Csak új és módosult fájlok vizsgálata	Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.
Fájlok kihagyása, ha a vizsgálat több mint N mp	A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.
Archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.

Paraméter	Leírás
Terjesztési csomagok vizsgálata	A jelölőnégyzet engedélyezi vagy letiltja a terjesztőcsomagok vizsgálatát.
Microsoft Office formátumú fájlok vizsgálata	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.
E-mail formátumú fájlok vizsgálata	Az e-mail formátumú fájlok és a levéladatbázis átvizsgálása. Az alkalmazás ellenőrzi az MS Outlook és a Windows Mail levelezőprogramok által használt PST- és OST-fájlokat, valamint az EML-fájlokat. A Kaspersky Endpoint Security nem támogatja a Microsoft Outlook levelezőprogram 64 bites verzióját. Ez azt jelenti, hogy a Kaspersky Endpoint Security nem vizsgálja át a Microsoft Outlook-fájlokat (PST- és OST-fájlokat), ha a számítógépre a Microsoft Outlook 64 bites verziója van telepítve, még akkor sem, ha az e-mailek szerepelnek a vizsgálat hatókörében. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security az e-mail formátumú fájlt felbontja összetevőire (fejléc, szövegtörzs, mellékletek), és megvizsgálja bennük a fenyegetéseket. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security az e-mail formátumú fájlt egyetlen fájlként vizsgálja meg. Ha a rendszer rosszindulatú objektumot észlel a PST vagy OST fájlokban, a Kaspersky Endpoint Security a kiválasztott műveletnek (például a fájl vírusmentesítése vagy törlése) megfelelően ártalmatlanná teszi azt. Ha más levelezőprogramok (például a Mozilla Thunderbird) fájljaiban rosszindulatú fájlt észlel, a Kaspersky Endpoint Security csak a fertőzött üzenetet jelöli meg. A fertőzött mellékletet tartalmazó üzenetet manuálisan kell törölnie.
Jelszóvédett archívumok vizsgálata	Ha a jelölőnégyzet be van jelölve, az alkalmazás vizsgálja a jelszóval védett archívumokat. Mielőtt az archívumokban lévő fájlokat vizsgálatára sor kerülhetne, a rendszer felkéri a jelszó megadására. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás kihagyja a jelszóval védett archívumok vizsgálatát.
Ne csomagoljon ki nagy összetett fájlokat	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás minden összetett fájlt megvizsgál. Az alkalmazás megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.
Gépi tanulás és aláíráselemzés	A gépi tanulási és aláírás-elemzési módszer a Kaspersky Endpoint Security adatbázisait használja, melyek az ismert fenyegetések leírásait és semlegesítésük módszereit tartalmazzák. Az ezt a módszert alkalmazó védelem biztosítja a minimális elfogadható biztonsági szintet. A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.
Heurisztikus elemzés	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
iSwift Technológia	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.
iChecker Technológia	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

Alkalmazás integritás-ellenőrzése

A Kaspersky Endpoint Security ellenőrzi, hogy az alkalmazásmodulok nem sérültek vagy módosultak-e. Például, ha egy alkalmazáskönyvtár digitális aláírása hibás, akkor az sérültnek minősül. Az *Alkalmazás integritás-ellenőrzése* feladat az alkalmazásfájlok ellenőrzésére való. Futtassa az *Alkalmazás integritás-ellenőrzése* feladatot, ha a Kaspersky Endpoint Security rosszindulatú objektumot észlelt, de nem hatástalanította azt.

Alkalmazás integritás-ellenőrzése feladatot csak a Kaspersky Security Center Web Console-on és az Adminisztrációs konzolon hozhat létre. Nem lehet feladatot létrehozni a Kaspersky Security Center Cloud Console helyen.

Alkalmazásintegritással kapcsolatos biztonsági incidens a következő esetekben történhet:

- Ha egy rosszindulatú objektum módosítja a Kaspersky Endpoint Security fájljait. Ebben az esetben végezze el a Kaspersky Endpoint Security visszaállítási folyamatát az operációs rendszer eszközeinek segítségével. A visszaállítás után futtasson teljes vizsgálatot a számítógépen, majd ismételje meg az integritás-ellenőrzést.
- A digitális aláírás lejárt. Ebben az esetben frissítse a Kaspersky Endpoint Security alkalmazást.

Alkalmazásintegritás-ellenőrzés futtatásának menete az Adminisztrációs Konzolon (MMC) keresztül

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Alkalmazás integritás-ellenőrzése** elemet.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. lépés Feladatindítási ütemezés konfigurálása

Állítson be ütemezést egy adott feladat elindításához, például kézi indítást vagy vírusfertőzés esetén bekövetkezőt.

4. lépés A feladat nevének megadása

Adja meg a feladat nevét, például: *Integritás-ellenőrzés a számítógép megfertőződése után*.

5. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Ennek eredményeképp a Kaspersky Endpoint Security ellenőrzi az alkalmazás integritását. Megadhatja az alkalmazás integritás-ellenőrzési ütemtervét a feladat tulajdonságaiban (lásd az alábbi táblázatot).

Alkalmazásintegritás-ellenőrzés futtatásának menete a Web Console-on keresztül

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Application Integrity Check** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például: *Alkalmazás integritásának ellenőrzése a számítógép megfertőződése után*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. Válassza ki a feladat melletti jelölőnégyzetet.

Ennek eredményeképp a Kaspersky Endpoint Security ellenőrzi az alkalmazás integritását. Megadhatja az alkalmazás integritás-ellenőrzési ütemtervét a feladat tulajdonságaiban (lásd az alábbi táblázatot).

Integritás-ellenőrzés futtatása az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.
2. Ezzel megnyitja a feladatlistát; itt válassza ki az *Alkalmazás integritás-ellenőrzése* feladatot, majd kattintson a **Futtatás** elemre.

Ennek eredményeképp a Kaspersky Endpoint Security ellenőrzi az alkalmazás integritását. Megadhatja az alkalmazás integritás-ellenőrzési ütemtervét a feladat tulajdonságaiban (lásd az alábbi táblázatot). Ha az *Alkalmazás integritás-ellenőrzése* feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

Integritás-ellenőrzési feladat beállításai

Paraméter	Leírás
Vizsgálat ütemezése	**Manually**. A futásmód, amelyben manuálisan elindíthatja a vizsgálatot, amikor az Önnek kényelmes. **Ütemezés szerint** A vizsgálati feladatoknak ebben a futásmódjában az alkalmazás a feladatot a létrehozott ütemtervnek megfelelően futtatja. A vizsgálati feladat ezen futásmódjának kiválasztása esetén a vizsgálati feladat elindítható kézileg is.
Kihagyott vizsgálatok futtatása	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott feladatot azonnal elindítja, amint lehetségessé válik. A feladat például akkor hagyható ki, ha a számítógép az ütemezett feladat indítási időpontjában ki volt kapcsolva. Amikor az alkalmazás lehetőséget kap a kihagyott feladatok végrehajtására, egy adott időintervallumon belül véletlenszerűen futtatja a feladatokat, hogy elossza a számítógép terhelését. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott feladatokat. Ehelyett a következő feladatot a jelenlegi ütemezésnek megfelelően futtatja.
Csak akkor fusson, ha a számítógép üresjáratban van	A feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították. Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.

A vizsgálat hatókörének szerkesztése

A *Vizsgálat hatóköre* olyan mappák és más elemek elérési útjainak listája, amelyeket a Kaspersky Endpoint Security megvizsgál a feladat végrehajtása során. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

A vizsgálat hatókörének szerkesztéséhez ajánlott az *Egyéni vizsgálat* feladatot használni. A Kaspersky szakértői javasolják, hogy ne módosítsa a *Teljes vizsgálat* és a *Kritikus területek vizsgálata* feladatok hatókörét.

A Kaspersky Endpoint Security a következő előre definiált objektumokat tartalmazza a vizsgálat hatókörének részeként:

- **Rendszermemória**.
- **A futó folyamatok és indítási objektumok**.

  A rendszerindításkor elinduló folyamatok és az alkalmazás által futtatható fájlok által lefoglalt memória.
- **Lemez rendszerindító szektorai**.

  A merevlemez és a cserélhető lemezek rendszerindító szektorai.

- **Biztonsági mentés a rendszerről**.

  A rendszerkötet információit tartalmazó mappa tartalma.

- **Összes külső eszköz**.

- **Összes merevlemez**.

- **Összes hálózati meghajtó**.

> A Kaspersky Endpoint Security for Windows 12.12-ben az e-mailek nem tartoznak az alkalmazás vizsgálati hatókörébe. A bejövő és kimenő e-mail-üzenetek vizsgálatát a Levelezésvédelem összetevő végzi. Ha az adminisztrációs bővítmény korábbi verzióját használja, az alkalmazás kizárja az e-maileket a vizsgálatból, még akkor is, ha a házirend tartalmazza azokat.

> Javasoljuk, hogy hozzon létre egy külön vizsgálati feladatot a hálózati meghajtók vagy megosztott mappák ellenőrzéséhez. A *Kártevő vizsgálata* feladat beállításaiban adjon meg egy olyan felhasználót, akinek írási hozzáférése van ehhez a meghajtóhoz; ez szükséges az észlelt fenyegetések mérsékléséhez. Ha a kiszolgáló, ahol a hálózati meghajtó található, saját biztonsági eszközökkel rendelkezik, ne futtassa a vizsgálati feladatot az adott meghajtón. Ily módon elkerülheti az objektum kétszeri ellenőrzését, és javíthatja a kiszolgáló teljesítményét.

Ha ki szeretne zárni mappákat vagy fájlokat a vizsgálat hatóköréből, adja hozzá az adott mappát vagy fájlt a megbízható zónához.

Vizsgálat hatókörének szerkesztése az Adminisztrációs Konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.
3. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.

   Ha szükséges, hozza létre a *Kártevő vizsgálata* feladatot.
4. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.
5. A **Vizsgálat hatóköre** részen kattintson a **Beállítások** elemre.
6. A megnyíló ablakban válassza ki azokat az objektumokat, amelyeket hozzá kíván adni a vizsgálat hatóköréhez vagy ki szeretne zárni abból.
7. Ha egy új objektumot szeretne hozzáadni a vizsgálat hatóköréhez:

   a. Kattintson **Hozzáadás** gombra.

   b. Az **Objektum** mezőbe írja be a mappa vagy fájl elérési útját.

maszkok használata:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

A maszkokat bárhol használhatja a fájl vagy mappa elérési útjában. Ha például a vizsgálat hatókörét szeretné kiterjeszteni a számítógépen található összes felhasználói fiók Letöltések mappájára, írja be a `C:\Users\*\Downloads\` maszkot.

Az **Ez a PC** objektum a számítógép fájlerőforrásainak listáján a következő objektumokat tartalmazza: **Minden merevlemez**, **Minden hálózati meghajtó** és **Minden cserélhető meghajtó**.

Kizárhat egy objektumot a vizsgálatokból anélkül, hogy törölné azt a vizsgálati hatókörbe tartozó objektumok listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Vizsgálat hatókörének szerkesztése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

   Megnyílik a feladatok tulajdonságai ablak. Ha szükséges, hozza létre a(z) *Malware Scan* feladatot.

3. Válassza ki az **Application settings** lapot.

4. A **Scan scope** részen válassza ki azokat az objektumokat, amelyeket hozzá kíván adni a vizsgálat hatóköréhez, vagy ki szeretne zárni abból.

5. Ha egy új objektumot szeretne hozzáadni a vizsgálat hatóköréhez:

   a. Kattintson az **Add** gombra.

   b. Adja meg a mappa vagy fájl elérési útját.

maszkok használata:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

A maszkokat bárhol használhatja a fájl vagy mappa elérési útjában. Ha például a vizsgálat hatókörét szeretné kiterjeszteni a számítógépen található összes felhasználói fiók Letöltések mappájára, írja be a `C:\Users\*\Downloads\` maszkot.

Kizárhat egy objektumot a vizsgálatokból anélkül, hogy törölné azt a vizsgálati hatókörbe tartozó objektumok listájáról. Ehhez állítsa a mellette lévő kapcsolót kikapcsolt helyzetbe.

6. Mentse el a módosításokat.

Vizsgálat hatókörének szerkesztése az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.

2. Ezzel megnyitja a feladatlistát; válassza ki az *Egyéni vizsgálat* feladatot, majd kattintson a **Kiválasztás** lehetőségre.

   Szerkesztheti más feladatok vizsgálati hatókörét is. A Kaspersky szakértői javasolják, hogy ne módosítsa a *Teljes vizsgálat* és a *Kritikus területek vizsgálata* feladatok hatókörét.

3. A megnyíló ablakban válassza ki azokat az objektumokat, amelyeket hozzá kíván adni a vizsgálat hatóköréhez.

4. Mentse el a módosításokat.

Ha a vizsgálati feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

Ütemezett vizsgálat futtatása

A *Rosszindulatú programok vizsgálata* feladattal végzett rosszindulatú programok keresése időigényes lehet, és megnövelheti a Kaspersky Endpoint Security számítógép-erőforrásainak használatát. Ezért célszerű olyan időpontot választani a feladat futtatására, amely minimálisra csökkenti a többi alkalmazás teljesítményre gyakorolt hatását.

Például, ha a cég alkalmazottai fix munkaidőben dolgoznak, beállíthatja, hogy a számítógépes vizsgálat éjszaka vagy hétvégén fusson. Ha a feladat futtatása valamilyen okból (például a számítógép abban az időpontban nem volt bekapcsolva) nem volt lehetséges, beállíthatja a kimaradt feladatot úgy is, hogy automatikusan elinduljon, amint lehet. Ezt a funkciót óvatosan érdemes használni, mert lelassíthatja az alkalmazásokat a felhasználó számítógépén, amikor reggel bekapcsolja a gépet.

Ha nem sikerül olyan optimális vizsgálati ütemezést meghatározni, amely megfelel az Ön igényeinek, beállíthatja, hogy a vizsgálat akkor fusson le, amikor az alábbi különleges feltételek valamelyike teljesül:

- Adatbázis-frissítés után.

  A Kaspersky Endpoint Security frissített aláírási adatbázisokkal futtatja a számítógép vizsgálatát.

- Az alkalmazás elindulása után.

  A Kaspersky Endpoint Security az alkalmazás indítását követően egy előre meghatározott idő elteltével futtatja a számítógép vizsgálatát. Az operációs rendszer indításakor számos folyamat fut, ezért előnyös a vizsgálati feladat futtatását elhalasztani, ahelyett, hogy közvetlenül a Kaspersky Endpoint Security indítása után futtatná.

- Wake-on-LAN szolgáltatás.

  A Kaspersky Endpoint Security ütemezetten futtatja a számítógép vizsgálatát, még akkor is, ha a számítógép ki van kapcsolva. Ehhez az alkalmazás az operációs rendszer Wake-on-LAN funkcióját használja. A Wake-on-LAN funkció lehetővé teszi a számítógép távoli bekapcsolását speciális jelet küldve annak a helyi hálózaton keresztül. A funkció használatához engedélyeznie kell a Wake-on-LAN funkciót a BIOS beállításaiban.

  A Wake-on-LAN használatával történő vizsgálat futtatását csak a *Kártevő vizsgálata* feladathoz konfigurálhatja a Kaspersky Security Centerben. Nem engedélyezheti a Wake-on-LAN funkciót a számítógép vizsgálatához az alkalmazás felületén.

- Amikor a számítógép üresjáratban van.

  A Kaspersky Endpoint Security ütemezetten futtatja a számítógép vizsgálatát, amikor a képernyővédő aktív, vagy a képernyő zárolva van. Ha a felhasználó feloldja a számítógép zárolását, a Kaspersky Endpoint Security leállítja a vizsgálatot. Ebben az esetben a Teljes vizsgálat több napot is igénybe vehet.

- Amikor a feladatot kihagyták.

  A Kaspersky Endpoint Security, amint lehetséges, futtatja a kihagyott feladatot. A feladat például akkor hagyható ki, ha a számítógép az ütemezett feladat indítási időpontjában ki volt kapcsolva. Amikor az alkalmazás lehetőséget kap a kihagyott feladatok végrehajtására, egy adott időintervallumon belül véletlenszerűen futtatja a feladatokat, hogy elossza a számítógép terhelését.

A vizsgálat ütemezés konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.

4. Állítsa be a vizsgálati feladat ütemezését.

5. Adja meg a kiválasztott gyakoriság függvényében a feladatfutás ütemezését meghatározó speciális beállításokat (lásd az alábbi táblát).

6. Mentse el a módosításokat.

Vizsgálati ütemezés konfigurálása az alkalmazás felületén

A vizsgálat ütemezését csak akkor konfigurálhatja, ha a házirend nincs alkalmazva a számítógépen. A házirend hatálya alá tartozó számítógépeknél a *Kártevő vizsgálata* feladat ütemezését a Kaspersky Security Centerben konfigurálhatja.

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.
2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.

   Beállíthatja a Teljes vizsgálat, a Kritikus területek vizsgálata és az Integritás-ellenőrzés feladatokat. Egyéni vizsgálat csak manuálisan futtatható.
3. Kattintson a **Vizsgálat ütemezése** gombra.
4. A megnyíló ablakban konfigurálja a vizsgálati feladat futásának ütemezését.
5. Adja meg a kiválasztott gyakoriság függvényében a feladatfutás ütemezését meghatározó speciális beállításokat (lásd az alábbi táblát).
6. Mentse el a módosításokat.

Vizsgálati ütemezés beállításai

Paraméter	Leírás
Vizsgálat ütemezése	**Manually**. A futásmód, amelyben manuálisan elindíthatja a vizsgálatot, amikor az Önnek kényelmes. **Ütemezés szerint** A vizsgálati feladatoknak ebben a futásmódjában az alkalmazás a feladatot a létrehozott ütemtervnek megfelelően futtatja. A vizsgálati feladat ezen futásmódjának kiválasztása esetén a vizsgálati feladat elindítható kézileg is.
Futtatás elhalasztása az alkalmazásindítás után N percre	A vizsgálati feladat elhalasztása az alkalmazás elindulása után. Az operációs rendszer indításakor számos folyamat fut, ezért előnyös a vizsgálati feladat futtatását elhalasztani, ahelyett, hogy közvetlenül a Kaspersky Endpoint Security indítása után futtatná.
Kihagyott vizsgálatok futtatása	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott feladatot azonnal elindítja, amint lehetségessé válik. A feladat például akkor hagyható ki, ha a számítógép az ütemezett feladat indítási időpontjában ki volt kapcsolva. Amikor az alkalmazás lehetőséget kap a kihagyott feladatok végrehajtására, egy adott időintervallumon belül véletlenszerűen futtatja a feladatokat, hogy elossza a számítógép terhelését. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott feladatokat. Ehelyett a következő feladatot a jelenlegi ütemezésnek megfelelően futtatja.
Csak akkor fusson, ha a számítógép üresjáratban van	A feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították. Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.
Use automatically randomized delay for task starts *(csak a Kaspersky Security Center konzolon érhető el)*	Ha a jelölőnégyzet be van jelölve, akkor a feladat nem szigorúan ütemezés szerint, hanem véletlenszerűen fut egy bizonyos időközön belül, vagyis a feladat indítási időpontjai szét vannak osztva. A véletlenszerű indítási időpontok segítenek elkerülni, hogy a feladatok ütemezett futtatásakor sok számítógép férjen hozzá egyszerre a felügyeleti kiszolgálóhoz. A véletlenszerű indítási időpontok automatikusan kiszámításra kerülnek a feladat létrehozásakor, attól függően, hogy hány számítógép van hozzárendelve a feladathoz. Ezt követően a feladat mindig a kiszámított indítási időpontban fut. A feladatbeállítások módosításakor vagy a feladat manuális futtatásakor azonban a számított indítási időpont megváltozik. Ha a jelölőnégyzet nincs bejelölve, a feladat pontosan az ütemezett időpontban fut.
Use randomized delay for task starts within an interval of (min)	Ha ez a jelölőnégyzet be van jelölve, a feladat egy bizonyos időtartamon belüli véletlenszerű időpontban fut le a számítógépeken. A véletlenszerű indítási időpontok segítenek elkerülni, hogy a feladatok ütemezett futtatásakor sok számítógép férjen hozzá egyszerre a felügyeleti kiszolgálóhoz. Ha a jelölőnégyzet nincs bejelölve, a feladat pontosan az ütemezett időpontban fut.

Paraméter	Leírás
Stop the task if it runs longer than (min) *(csak a Kaspersky Security Center konzolon érhető el)*	A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint. A feladat végrehajtási idejének csökkentéséhez pl. konfigurálhatja a vizsgálat hatókörét vagy optimalizálhatja a vizsgálatot.
Turn on devices by using the Wake-on-LAN function before starting the task (min) *(csak a Kaspersky Security Center konzolon érhető el)*	Ha a jelölőnégyzet be van jelölve, a számítógép operációs rendszere meghatározott átfutási időt kap az indítás befejezésére a feladat futtatása előtt. Az alapértelmezett átfutási idő 5 perc. Jelölje be a jelölőnégyzetet, ha a feladatot minden számítógépen szeretné futtatni, beleértve a kikapcsolt számítógépeket is.
Shut down the devices after completing the task *(csak a Kaspersky Security Center konzolon érhető el)*	Például engedélyezheti ezt a funkciót a számítógép vizsgálatához pénteken, munkaidő után. A feladat végeztével az alkalmazás kikapcsolja a számítógépet a hétvégére.
Feladat felfüggesztése	Megadhat egy időintervallumot, amely alatt a korábban ütemezett feladat végrehajtása szünetel. Amint a megadott időtartam lejár, a feladat folytatódik. Erre például azért lehet szükség, hogy minimalizáljuk a Kaspersky Endpoint Security hatását a számítógép teljesítményére a csúcsforgalmi időszakokban.
Ütemezés letiltásának kezdete	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a megadott dátumtól kezdve nem fogja tovább futtatni az ütemezett feladatot. A feladat **Kézi** üzemmódba kerül.

Vizsgálat futtatása más felhasználóként

Alapértelmezés szerint az alkalmazás a vizsgálati feladatot annak a felhasználónak a nevében futtatja, akinek a jogosultságaival Ön regisztrálva van az operációs rendszerben. A védelem hatóköre magában foglalhatja a hálózati meghajtókat vagy más objektumokat, amelyek eléréséhez speciális hozzáférési jogokra van szükség. Az alkalmazás beállításaiban megadhat egy olyan felhasználót, aki rendelkezik a szükséges jogokkal, és a vizsgálati feladatot e felhasználói fiók alatt futtathatja.

A következő vizsgálatokat más felhasználóként is futtathatja:

- Kritikus területek vizsgálata.
- Teljes vizsgálat.
- Egyéni vizsgálat.
- Vizsgálat a helyi menüből.

Nem konfigurálhatja a felhasználói jogokat a Cserélhető meghajtók vizsgálata, a Vizsgálat a háttérben és az Integritás-ellenőrzés futtatásakor.

Vizsgálat futtatása más felhasználóként az Adminisztrációs Konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Tasks** lapot.
4. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.
5. Válassza ki a számítógép tulajdonságainak ablakában az **Account** részt.

6. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a vizsgálati feladat futtatásához.

7. Mentse el a módosításokat.

Vizsgálat futtatása más felhasználóként a Web Console vagy a Cloud Console szolgáltatásban

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Settings** lapot.

4. A **Account** részen kattintson a **Settings** gombra.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a vizsgálati feladat futtatásához.

6. Mentse el a módosításokat.

Vizsgálat futtatása más felhasználóként az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.

2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.

3. A feladat tulajdonságainál válassza a **Speciális beállítások** → **Vizsgálat futtatása másként** elemet.

4. A megnyíló ablakban adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a vizsgálati feladat futtatásához.

5. Mentse el a módosításokat.

Ha a vizsgálati feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

Vizsgálatoptimalizáció

A CPU-használat korlátozása a számítógép vizsgálata közben

Korlátozhatja a CPU-használatot a *Kártevő vizsgálata* feladat futtatásakor. Ez megnövelheti a számítógép vizsgálatának idejét.

A CPU-használat korlátozása a számítógép vizsgálatakor a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.

4. A **Teljesítmény** részen jelölje be a **Vizsgálati feladatok CPU-használatának korlátozása** jelölőnégyzetet, és adja meg a CPU erőforrás-használatának átlagos értékét százalékban.

5. Mentse el a módosításokat.

A CPU-használat korlátozása a számítógép vizsgálatakor a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Performance** elemet.

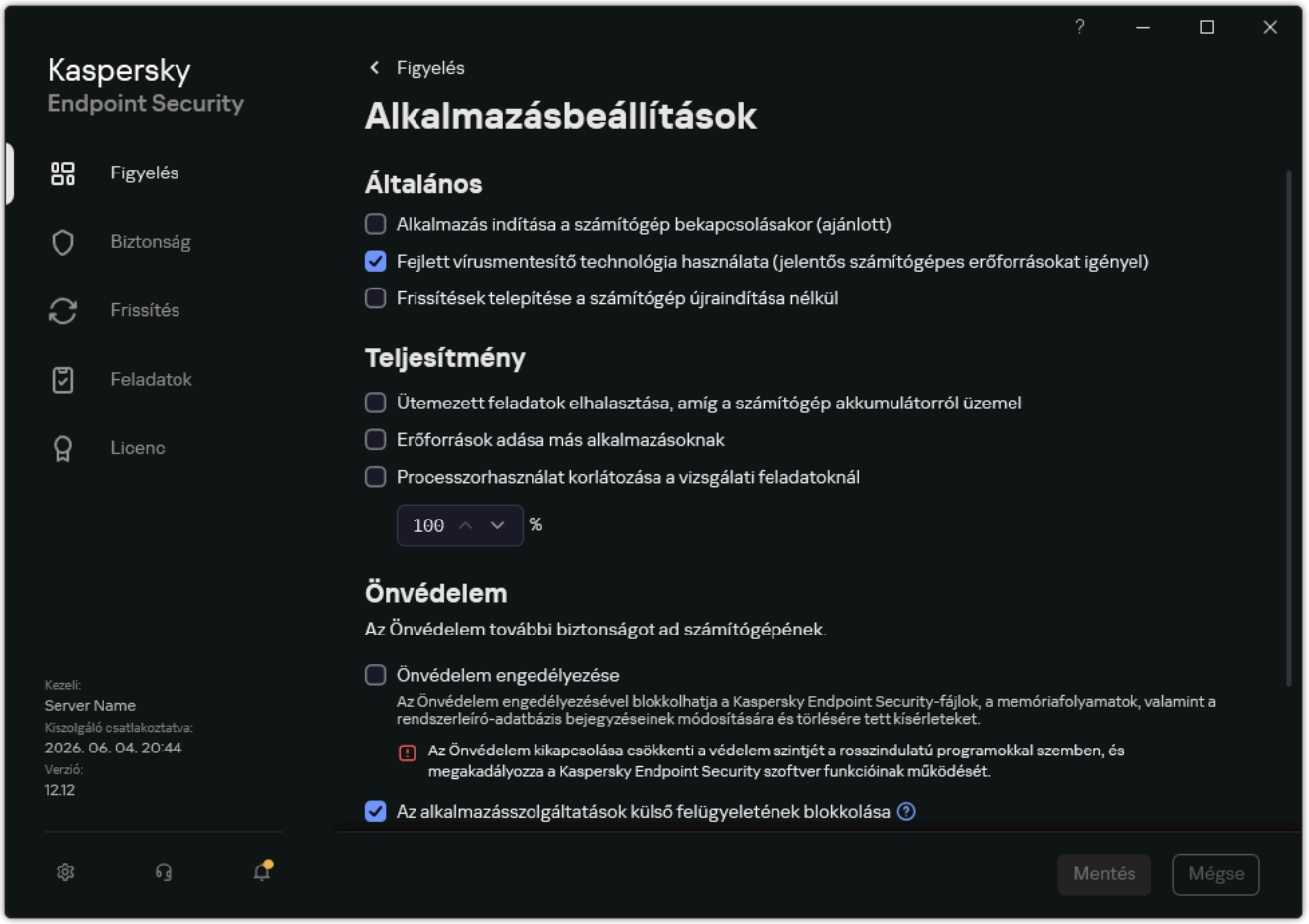
5. A(z) **Limit CPU usage for scan tasks** területen állítsa a kapcsolót **Limit CPU usage for scan tasks** állásba, és adja meg a CPU erőforrás-használatának átlagos értékét százalékban.

6. Mentse el a módosításokat.

A CPU-használat korlátozása a számítógép vizsgálatakor az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. A **Teljesítmény** részen jelölje be a **Vizsgálati feladatok CPU-használatának korlátozása** jelölőnégyzetet, és adja meg a CPU erőforrás-használatának átlagos értékét százalékban.

4. Mentse el a módosításokat.

A Kártevő-ellenőrzés speciális beállításainak konfigurálása.

Optimalizálhatja a fájlvizsgálatot: csökkentheti a vizsgálat idejét, és növelheti a Kaspersky Endpoint Security működési sebességét. Ez úgy érhető el, hogy az alkalmazás csak az új és a legutóbbi vizsgálat óta megváltozott fájlokat vizsgálja. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes. Időkorlátot is beállíthat egy fájl vizsgálatához. Ha letelik a megadott időtartam, a Kaspersky Endpoint Security a fájlt kizárja az aktuális vizsgálatból (kivéve az archívumokat és a több fájlból álló objektumokat).

A vírusok és egyéb rosszindulatú programok álcázásának gyakori módja az összetett fájlokba, pl. archívumokba vagy adatbázisokba történő beágyazás. Az ilyen módon elrejtett vírusok és rosszindulatú programok felismeréséhez az összetett fájlt ki kell csomagolni, ami csökkentheti a vizsgálat sebességét. Korlátozhatja a vizsgálandó összetett fájlok típusát, így felgyorsíthatja a vizsgálatot.

Bekapcsolhatja az iChecker és az iSwift technológiát is. Az iChecker és iSwift technológiák oly módon optimalizálják a fájlok vizsgálatának sebességét, hogy kizárják a legutóbbi vizsgálat óta nem módosult fájlokat.

A vizsgálat optimalizálása az Adminisztrációs Konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Tasks** lehetőséget.

3. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.

   Ha szükséges, hozza létre a *Kártevő vizsgálata* feladatot.

4. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.

5. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Ezzel nyitható meg a vizsgálati feladat beállításainak ablaka.

6. Az **Optimalizálás** részen konfigurálja a vizsgálati beállításokat:

   - **Csak az új és módosított fájlok vizsgálata**. Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.

     Beállíthatja az új fájlok vizsgálatát is típus szerint. Például vizsgálhatja az összes terjesztőcsomagot, illetve csak az új archívumokat és az Office-formátumú fájlokat is.

- **Fájlok kihagyása, amelyek hosszabb ideje van vizsgálva, mint N mp**. A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

- **Ne futtasson több vizsgálati feladatot egyszerre!** Vizsgálati feladatok elhalasztott indítása, ha egy vizsgálat már fut. A Kaspersky Endpoint Security várólistába sorolja az új vizsgálati feladatokat, ha az aktuális vizsgálat folytatódik. Ez segíti a számítógép terhelésének optimalizálását. Feltételezzük például, hogy az alkalmazás az ütemezésnek megfelelően Teljes vizsgálatot indított el. Ha egy felhasználó megpróbál fájlvizsgálatot indítani az alkalmazás felületéről, a Kaspersky Endpoint Security sorba állítja ezt a gyorsvizsgálati feladatot, majd automatikusan elindítja ezt a feladatot, miután a Teljes vizsgálati feladat befejeződött.

7. Kattintson a **További** gombra.

   Ez megnyitja az összetett fájlok vizsgálati beállításainak ablakát.

8. A **Méretkorlát** részben jelölje be a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet. A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

   A Kaspersky Endpoint Security az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzet be van-e jelölve.

9. Kattintson az **OK** gombra.

10. Nyissa meg a **További** lapot.

11. A **Vizsgálati technológiák** blokkban jelölje be a jelölőnégyzeteket azon technológiák neve mellett, amelyeket egy vizsgálat során használni szeretne:

    - **iSwift technológia**. Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.

    - **iChecker Technológia**. Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

12. Mentse el a módosításokat.

Vizsgálat optimalizálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

   Megnyílik a feladatok tulajdonságai ablak. Ha szükséges, hozza létre a(z) *Malware Scan* feladatot.

3. Válassza ki az **Application settings** lapot.

4. A **Action on threat detection** részen jelölje be az **Scan only new and modified files** jelölőnégyzetet. Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.

   Beállíthatja az új fájlok vizsgálatát is típus szerint. Például vizsgálhatja az összes terjesztőcsomagot, illetve csak az új archívumokat és az Office-formátumú fájlokat is.

5. A **Scan optimization** részen jelölje be az **Do not unpack large compound files** jelölőnégyzetet. A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

   A Kaspersky Endpoint Security az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Do not unpack large compound files** jelölőnégyzet be van-e jelölve.

6. Tegyen jelölést a **Do not run multiple scan tasks at the same time** jelölőnégyzetbe. Vizsgálati feladatok elhalasztott indítása, ha egy vizsgálat már fut. A Kaspersky Endpoint Security várólistába sorolja az új vizsgálati feladatokat, ha az aktuális vizsgálat folytatódik. Ez segíti a számítógép terhelésének optimalizálását. Feltételezzük például, hogy az alkalmazás az ütemezésnek megfelelően Teljes vizsgálatot indított el. Ha egy felhasználó megpróbál fájlvizsgálatot indítani az alkalmazás felületéről, a Kaspersky Endpoint Security sorba állítja ezt a gyorsvizsgálati feladatot, majd automatikusan elindítja ezt a feladatot, miután a Teljes vizsgálati feladat befejeződött.

7. A **Advanced settings** részen jelölje be az **Skip file that is scanned for longer than (sec)** jelölőnégyzetet. A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

8. Mentse el a módosításokat.

A vizsgálat optimalizálása az alkalmazás felületén

1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.

2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a ⚙ elemre.

3. Kattintson a **Speciális beállítások** elemre.

4. Az **Optimalizálás** részen konfigurálja a vizsgálati beállításokat:

   - **Csak az új és módosított fájlok vizsgálata**. Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.

     Beállíthatja az új fájlok vizsgálatát is típus szerint. Például vizsgálhatja az összes terjesztőcsomagot, illetve csak az új archívumokat és az Office-formátumú fájlokat is.

- **Fájl kihagyása, ha a vizsgálat több mint N mp**. A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

- **Ne futtasson több vizsgálati feladatot egyszerre!** Vizsgálati feladatok elhalasztott indítása, ha egy vizsgálat már fut. A Kaspersky Endpoint Security várólistába sorolja az új vizsgálati feladatokat, ha az aktuális vizsgálat folytatódik. Ez segíti a számítógép terhelésének optimalizálását. Feltételezzük például, hogy az alkalmazás az ütemezésnek megfelelően Teljes vizsgálatot indított el. Ha egy felhasználó megpróbál fájlvizsgálatot indítani az alkalmazás felületéről, a Kaspersky Endpoint Security sorba állítja ezt a gyorsvizsgálati feladatot, majd automatikusan elindítja ezt a feladatot, miután a Teljes vizsgálati feladat befejeződött.

5. A **Méretkorlát** részben jelölje be a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet. A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

   A Kaspersky Endpoint Security az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzet be van-e jelölve.

6. A **Vizsgálati technológiák** blokkban jelölje be a jelölőnégyzeteket azon technológiák neve mellett, amelyeket egy vizsgálat során használni szeretne:

   - **iSwift technológia**. Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.

   - **iChecker Technológia**. Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

7. Mentse el a módosításokat.

Ha a vizsgálati feladat nem jelenik meg, a rendszergazda megtiltotta a helyi feladatok használatát a házirendben.

Adatbázisok és alkalmazás-szoftvermodulok frissítése

A Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítése biztosítja a számítógép védelmének naprakész állapotát. Nap mint nap jelentős számú új vírus és más típusú rosszindulatú program jelenik meg világszerte. A fenyegetésekről és a semlegesítésük módjáról a Kaspersky Endpoint Security adatbázisai tartalmaznak információkat. A fenyegetések gyors észlelése érdekében javasoljuk, hogy rendszeresen frissítse az adatbázisokat és az alkalmazásmodulokat.

Elképzelhető, hogy a frissítési funkciók (beleértve a vírusirtó aláírások és a kódbázis frissítéseit) nem lesznek elérhetők a szoftverben az Egyesült Államok területén.

A rendszeres frissítéshez működő licenc szükséges. Ha nincs aktuális licence, csak egyetlen alkalommal végezhet frissítést.

A frissítési csomagoknak a Kaspersky frissítési kiszolgálóiról való sikeres letöltéséhez a számítógépnek csatlakoznia kell az internethez. Alapértelmezés szerint az alkalmazás automatikusan észleli az internetkapcsolat beállításait. Ha proxykiszolgálót használ, konfigurálnia kell a proxykiszolgáló beállításait.

A frissítések HTTPS protokollon keresztül töltődnek le. HTTP protokollon is le lehet tölteni őket, ha nem lehet HTTPS protokollon frissítéseket letölteni.

Frissítés végrehajtásakor az alkalmazás letölti és telepíti az alábbi objektumokat a számítógépre:

- A Kaspersky Endpoint Security adatbázisai. A számítógép védelme olyan adatbázisokra épül, amelyek tartalmazzák a vírusok és egyéb fenyegetések aláírásait, valamint a semlegesítésükre vonatkozó információkat. A védelmi összetevők ezen információk segítségével keresik meg és semlegesítik a számítógépen található fertőzött fájlokat. Az adatbázisok folyamatosan kiegészülnek az új fenyegetések adataival és hatástalanításuk módszereivel. Emiatt javasoljuk, hogy rendszeresen frissítse az adatbázisokat.

  A Kaspersky Endpoint Security adatbázisai mellett frissülnek azok a hálózati illesztőprogramok is, amelyek segítségével az alkalmazás összetevői elfoghatják a hálózati forgalmat.

- Alkalmazásmodulok. A Kaspersky Endpoint Security adatbázisai mellett az alkalmazásmodulok is frissíthetők. Az alkalmazásmodulok frissítései kiküszöbölik a Kaspersky Endpoint Security sebezhetőségeit, új funkciókat adnak hozzá, illetve meglévő funkciókat bővítenek ki.

Frissítéskor az alkalmazás összehasonlítja a számítógépen található alkalmazásmodulokat és adatbázisokat a frissítési forráson található naprakész változatokkal. Ha az érvényes adatbázisok és alkalmazásmodulok eltérnek a naprakész verzióktól, a frissítés telepíti a hiányzó részeket a számítógépre.

Ha az adatbázisok elavultak, a frissítőcsomag nagy méretű lehet, és további internetforgalmat (több tucat MB) generálhat.

A Kaspersky Endpoint Security adatbázisok aktuális állapotával kapcsolatos információk az alkalmazás főablakában vagy az elemleírásban jelennek meg, amelyet akkor láthat, ha a kurzort az értesítési területen lévő alkalmazásikon fölé viszi.

A frissítés eredményeit és a frissítési feladat végrehajtása során történt eseményeket a Kaspersky Endpoint Security egy jelentésben naplózza.

Ha az alkalmazás Light Agent üzemmódban működik, az alkalmazás adatbázisainak és moduljainak frissítése különleges megfontolásokat igényel.

Adatbázis- és alkalmazásmodul frissítésének lehetőségei

A Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítése biztosítja a számítógép védelmének naprakész állapotát. Nap mint nap jelentős számú új vírus és más típusú rosszindulatú program jelenik meg világszerte. A fenyegetésekről és a semlegesítésük módjáról a Kaspersky Endpoint Security adatbázisai tartalmaznak információkat. A fenyegetések gyors észlelése érdekében javasoljuk, hogy rendszeresen frissítse az adatbázisokat és az alkalmazásmodulokat.

A következő objektumok frissülnek a felhasználói számítógépeken:

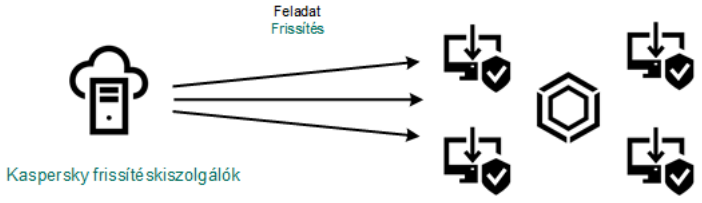
- Antivírus adatbázisok. Az antivírus adatbázisok közé tartoznak a rosszindulatú programok aláírásainak adatbázisai, az adathalász és rosszindulatú webcímek adatbázisai, a reklámcsíkok adatbázisai, a levélszemét-észlelő adatbázisok és egyéb adatok.

- Alkalmazásmodulok. A modulfrissítések az alkalmazás sebezhetőségeinek elkerülésére, valamint a számítógép védelmi módszereinek fejlesztésére szolgálnak. A modulfrissítések megváltoztathatják az alkalmazás összetevők magatartását, hozzáadhatnak új képességeket.

A Kaspersky Endpoint Security a következő lehetőségeket támogatja az adatbázisok és az alkalmazásmodulok frissítésére:

- A Kaspersky kiszolgálókról érkező frissítések.

  A Kaspersky frissítéskiszolgálók a világ számos országában megtalálhatók. Ez biztonságossá teszi a frissítéseket. Ha egy frissítést nem lehet végrehajtani egy kiszolgálóról, a Kaspersky Endpoint Security átvált a következő kiszolgálóra.



A Kaspersky kiszolgálókról érkező frissítések

- Központosított frissítés.

  A központosított frissítés csökkenti a külső internetes forgalmat, valamint biztosítja a frissítés kényelmes megfigyelését.

  A központosított frissítés a következő lépésekből áll:

  1. Töltse le a frissítési csomagot a szervezet hálózatának egy tárhelyére.

     A frissítési csomag letöltődött a tárhelyre a *Download updates to the Administration Server repository* nevű felügyeleti kiszolgálói feladat által.

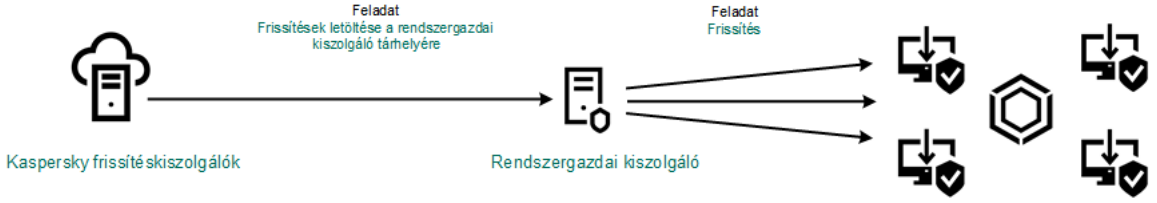
  2. Töltse le a frissítési csomagot a megosztott mappába (opcionális).

A következő módszerekkel töltheti le a frissítési csomagot a megosztott mappába:

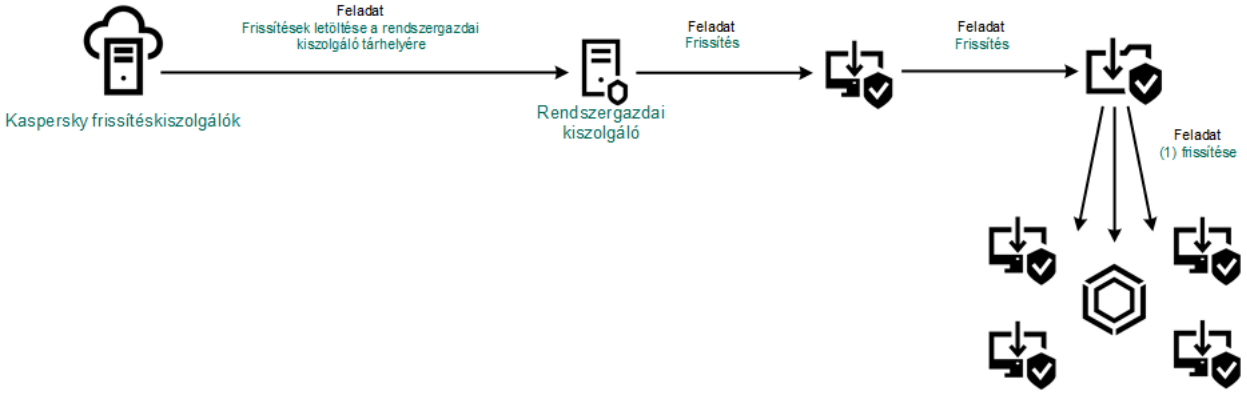
- A Kaspersky Endpoint Security *Adatbázisok és alkalmazásmodulok frissítése* feladatának használata. A feladat a helyi vállalati hálózaton lévő egy számítógépre lett szánva.
- A Kaspersky Update Utility használata. A Kaspersky Update Utility használatával kapcsolatos további információkért lásd: Kaspersky Tudásbázis.

3. A frissítési csomag megosztása az ügyfélszámítógépekkel.

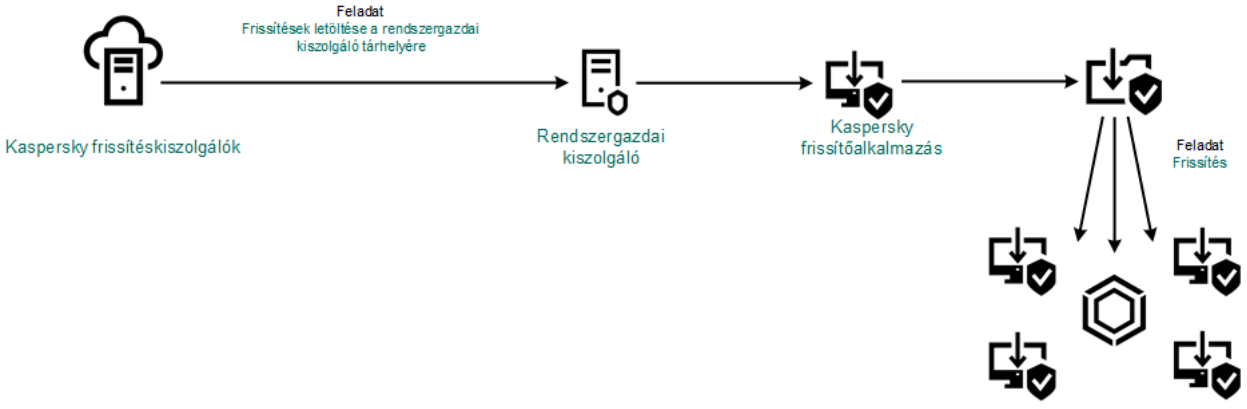
   A frissítési csomagot a Kaspersky Endpoint Security *Adatbázisok és alkalmazásmodulok frissítése* feladata megosztja az ügyfélszámítógépekkel. Korlátlan számú frissítési feladatot hozhat létre az adminisztrációs csoportokhoz.



Frissítés a kiszolgáló tárhelyéből



Megosztott mappából való frissítés



Frissítés a Kaspersky Update Utility használatával

A Kaspersky Security Center esetében a frissítésforrások alapértelmezett listáján a Kaspersky Security Center felügyeleti kiszolgáló és a Kaspersky frissítéskiszolgálói szerepelnek. A Kaspersky Security Center Cloud Console esetében a frissítésforrások alapértelmezett listáján a Kaspersky frissítéskiszolgálói és a terjesztőpontok szerepelnek. Az elosztói pontokkal kapcsolatos további részletekért lásd a Kaspersky Security Center Cloud Console Súgót. Felvehet más frissítésforrásokat is a listába. Frissítésforrásként megadhat HTTP-/FTP-kiszolgálókat és megosztott meghajtókat. Ha egy frissítést nem lehet végrehajtani egy frissítésforrásról, a Kaspersky Endpoint Security átvált a következő kiszolgálóra.

A frissítések letöltődnek a Kaspersky frissítéskiszolgálókról vagy egyéb FTP vagy HTTP kiszolgálókról, szabványos hálózati protokollokon keresztül. Ha egy proxykiszolgáló-kapcsolat szükséges a frissítés forrásának eléréséhez, akkor meghatározhatja a proxykiszolgáló beállításait a Kaspersky Endpoint Security rendszabály beállításaiban.

Frissítés a kiszolgáló tárhelyéből

Az internetes forgalom megőrzéséhez egy kiszolgáló tárhelyről konfigurálhatja a szervezet helyi hálózaton lévő számítógépein történő adatbázisok és alkalmazásmodulok frissítését. Ehhez a Kaspersky Security Centernek le kell töltenie egy frissítési csomagot a tárhelyre (FTP vagy HTTP kiszolgáló, hálózati vagy helyi mappa) a Kaspersky frissítéskiszolgálókból. A szervezet helyi hálózatán lévő egyéb számítógépek fogadhatnak frissítési csomagot a kiszolgáló tárhelyből.

A kiszolgáló tárhelyről történő adatbázis és alkalmazásmodul-frissítések konfigurálása két lépésből áll:

1. Frissítőcsomag letöltésének konfigurálása a felügyeleti kiszolgáló tárhelyére (*Download updates to the Administration Server repository* feladat).

   A *Download updates to the Administration Server repository* feladatot a Felügyeleti kiszolgáló gyorsindító varázslója automatikusan létrehozza, és ennek a feladatnak csak egyetlen példánya lehet. A Kaspersky Security Center alapértelmezés szerint a következő mappába másolja a frissítőcsomagot: `\\<server name>\KLSHARE\Updates`. A frissítéseknek a Felügyeleti kiszolgáló adattárába történő letöltésével kapcsolatos további információkat a Kaspersky Security Center súgójában találja.

2. A megadott kiszolgáló tárhely adatbázisainak és alkalmazásmodul-frissítéseinek konfigurálása a helyi hálózat fennmaradó számítógépeire (*Adatbázisok és alkalmazásmodulok frissítése* feladat).

   A Kaspersky Endpoint Security megadott kiszolgálói tárhelyről történő frissítésének konfigurálása a Felügyeleti kiszolgálói konzolban (MMC)

   1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

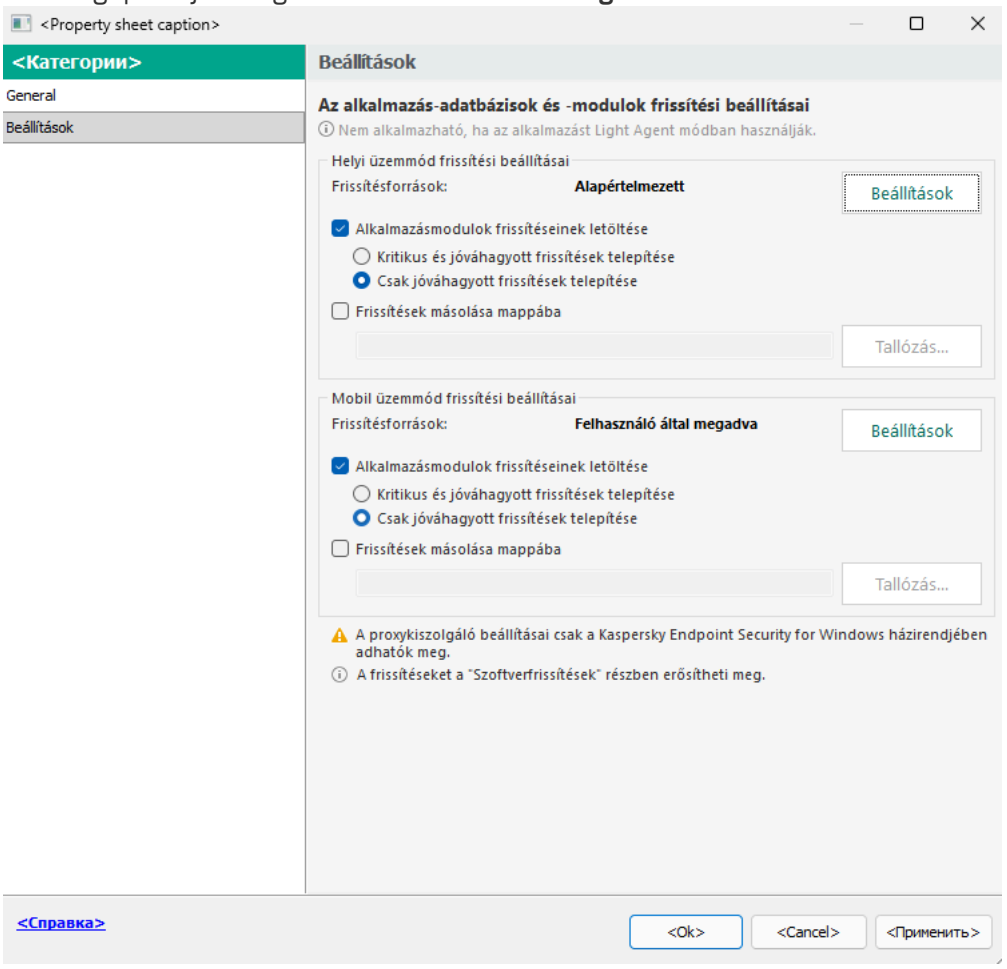
      A konzolfán válassza ki a **Tasks** lehetőséget.

   2. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

      Megnyílik a feladatok tulajdonságai ablak.

      Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki a számítógép tulajdonságainak ablakában az **Settings** részt.



Az Adatbázisok és alkalmazásmodulok frissítése feladat beállításai

4. A **Helyi üzemmód frissítési beállításai** részen kattintson a **Beállítások** gombra.

5. A frissítési források listájában győződjön meg arról, hogy a **Kaspersky Security Center** forrásból származó frissítés engedélyezve van. Ezenkívül a **Kaspersky Security Center** forrásnak kell a legmagasabb prioritást élveznie.

6. Ha szükséges, adja hozzá a frissítési forrásokat:

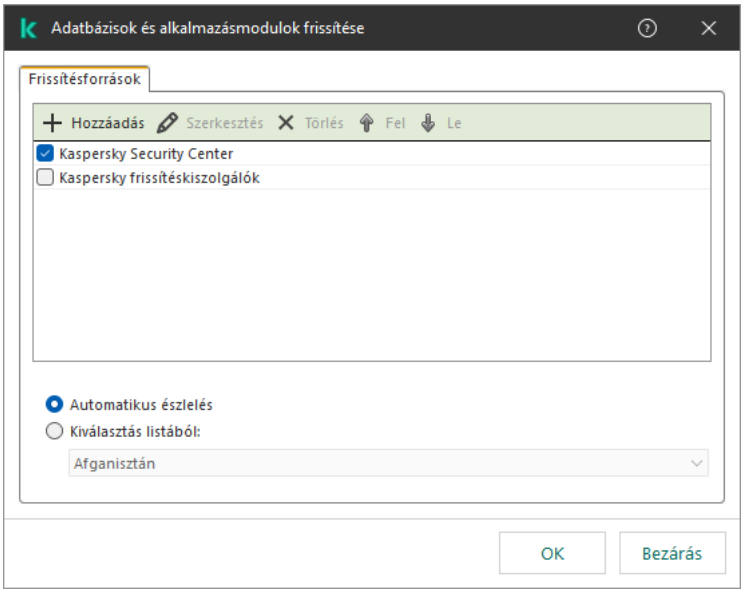
   a. A frissítési források listájában kattintson a **Add** gombra.

   b. A **Frissítésforrások** mezőben adja meg az FTP vagy HTTP kiszolgáló, a hálózati vagy helyi mappa címét, ahol a Kaspersky Security Center lemásolja a Kaspersky kiszolgálóitól kapott frissítési csomagot.

   > A frissítés forrásának címének meg kell egyeznie a **Folder for storing updates** mezőben megadott címmel, amikor a frissítéseknek a kiszolgáló tárhelyére történő letöltését konfigurálta (a *Download updates to the Administration Server repository* feladat).

   c. Kattintson az **OK** gombra.

A frissítésforrást kizárhatja anélkül, hogy eltávolítaná a frissítésforrások listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.



Frissítési források

7. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

8. A feladat tulajdonságai ablakban válassza ki a **Schedule** szakaszt, és konfigurálja a feladat futásmódját.

9. A Kaspersky Endpoint Security alapértelmezés szerint kézi módban futtatja a feladatot.

10. Mentse el a módosításokat.

A Kaspersky Endpoint Security megadott kiszolgálói tárhelyről történő frissítésének konfigurálása a Web Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Update** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

   A *Update* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki az **Application settings** → **Local mode** lapot.

4. A frissítési források listájában győződjön meg arról, hogy a **Kaspersky Security Center** forrásból származó frissítés engedélyezve van. Ezenkívül a **Kaspersky Security Center** forrásnak a legmagasabb prioritással kell rendelkeznie.

5. Ha szükséges, adja hozzá a frissítési forrásokat:

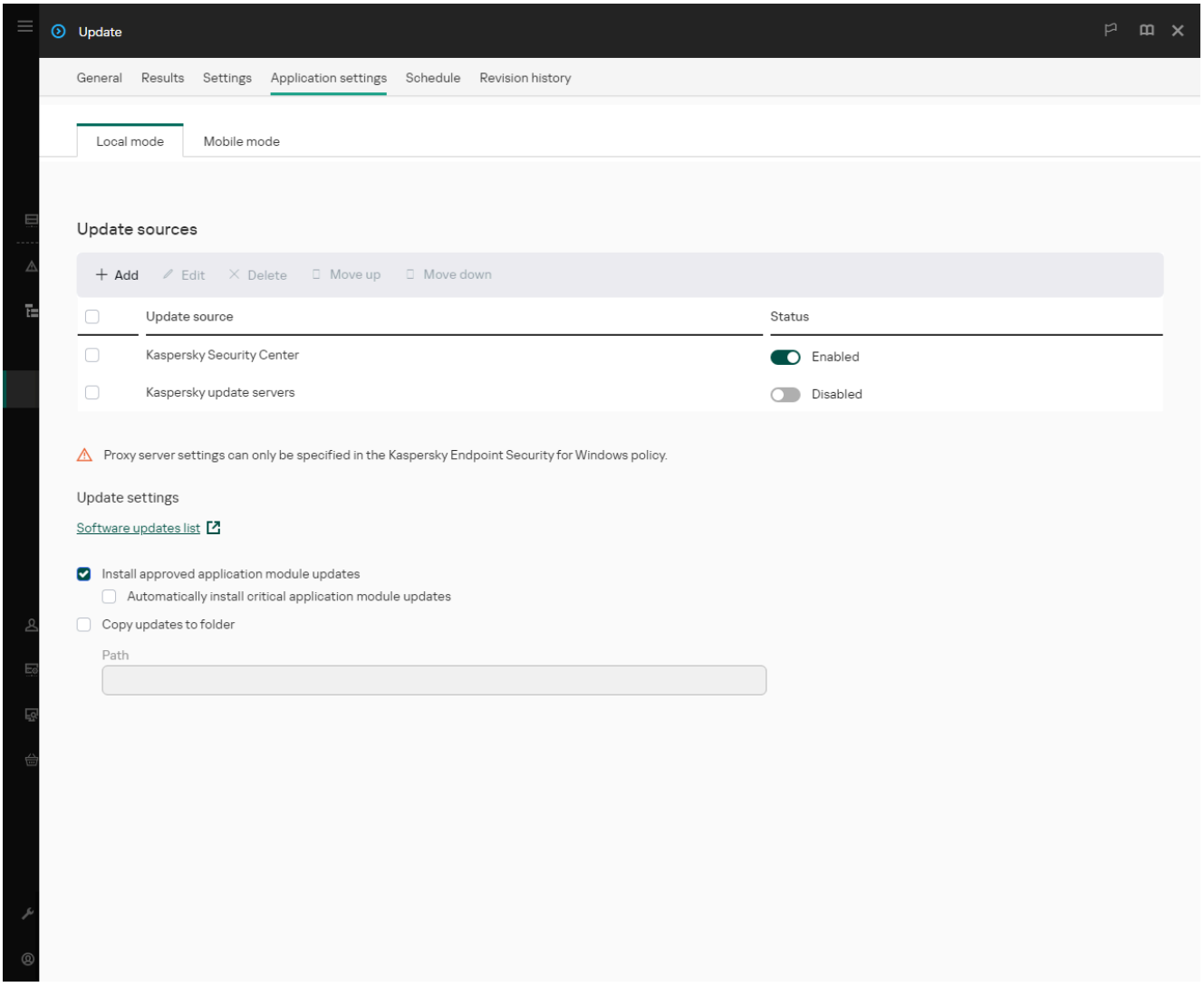
   a. A frissítési források listájában kattintson a **Add** gombra.

   b. A(z) **Update sources** mezőben adja meg az FTP- vagy HTTP-kiszolgáló, a hálózati vagy helyi mappa címét, ahol a Kaspersky Security Center lemásolja a Kaspersky kiszolgálóitól kapott frissítési csomagot.

   > A frissítés forrásának címének meg kell egyeznie a **Folder for storing updates** mezőben megadott címmel, amikor a frissítéseknek a kiszolgáló tárhelyére történő letöltését konfigurálta (a *Download updates to the Administration Server repository* feladat).

   c. Kattintson az **Save** gombra.

A frissítésforrást kizárhatja anélkül, hogy eltávolítaná a frissítésforrások listájáról. Ehhez állítsa a mellette lévő kapcsolót kikapcsolt helyzetbe.



Frissítési források

6. Adja meg a frissítésforrások prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

7. A feladat tulajdonságai ablakban válassza ki a **Schedule** szakaszt, és konfigurálja a feladat futásmódját.

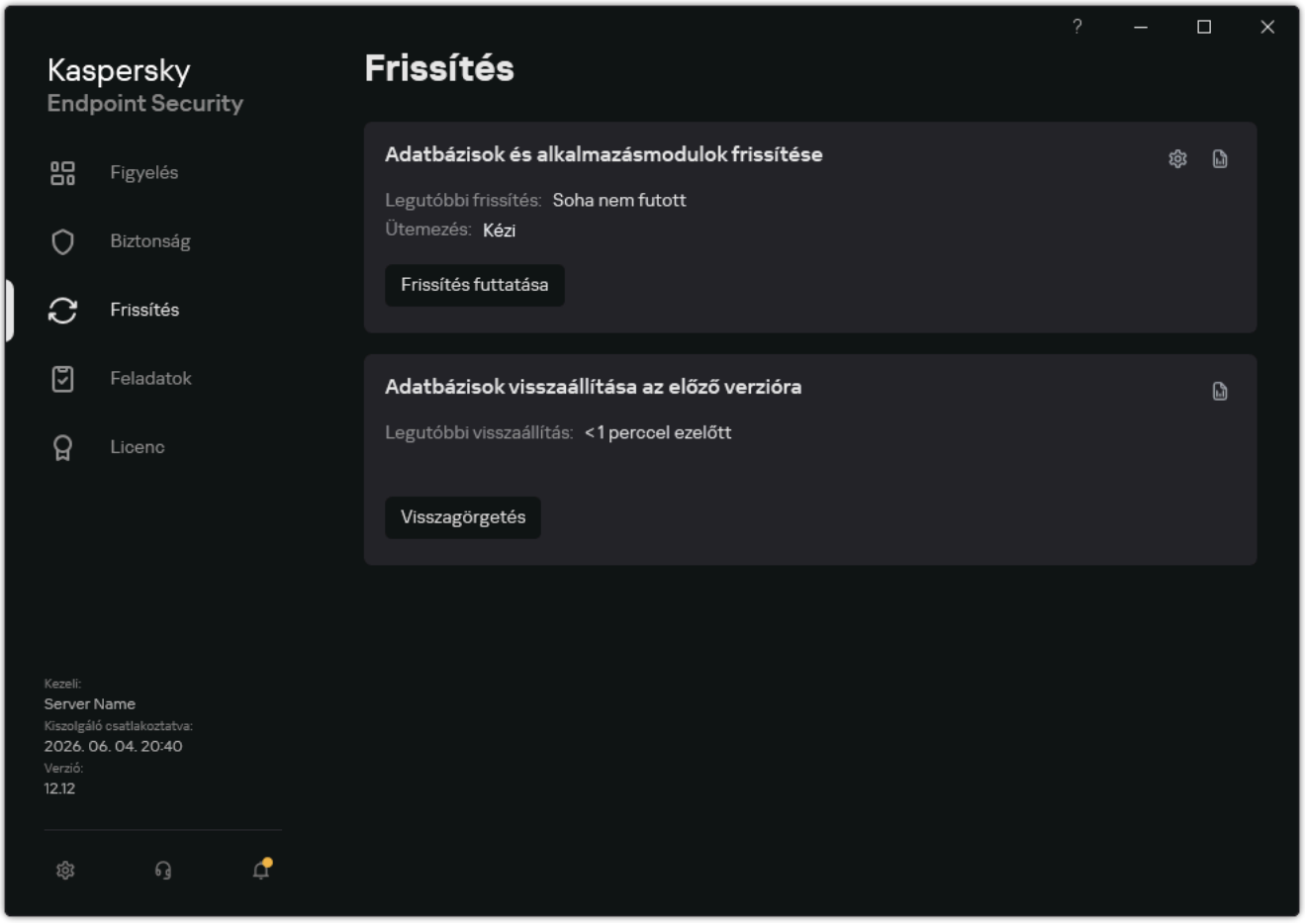
8. A Kaspersky Endpoint Security alapértelmezés szerint kézi módban futtatja a feladatot.

9. Mentse el a módosításokat.

A Kaspersky Endpoint Security megadott kiszolgálói tárhelyről történő frissítésének konfigurálása az alkalmazás felületén

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

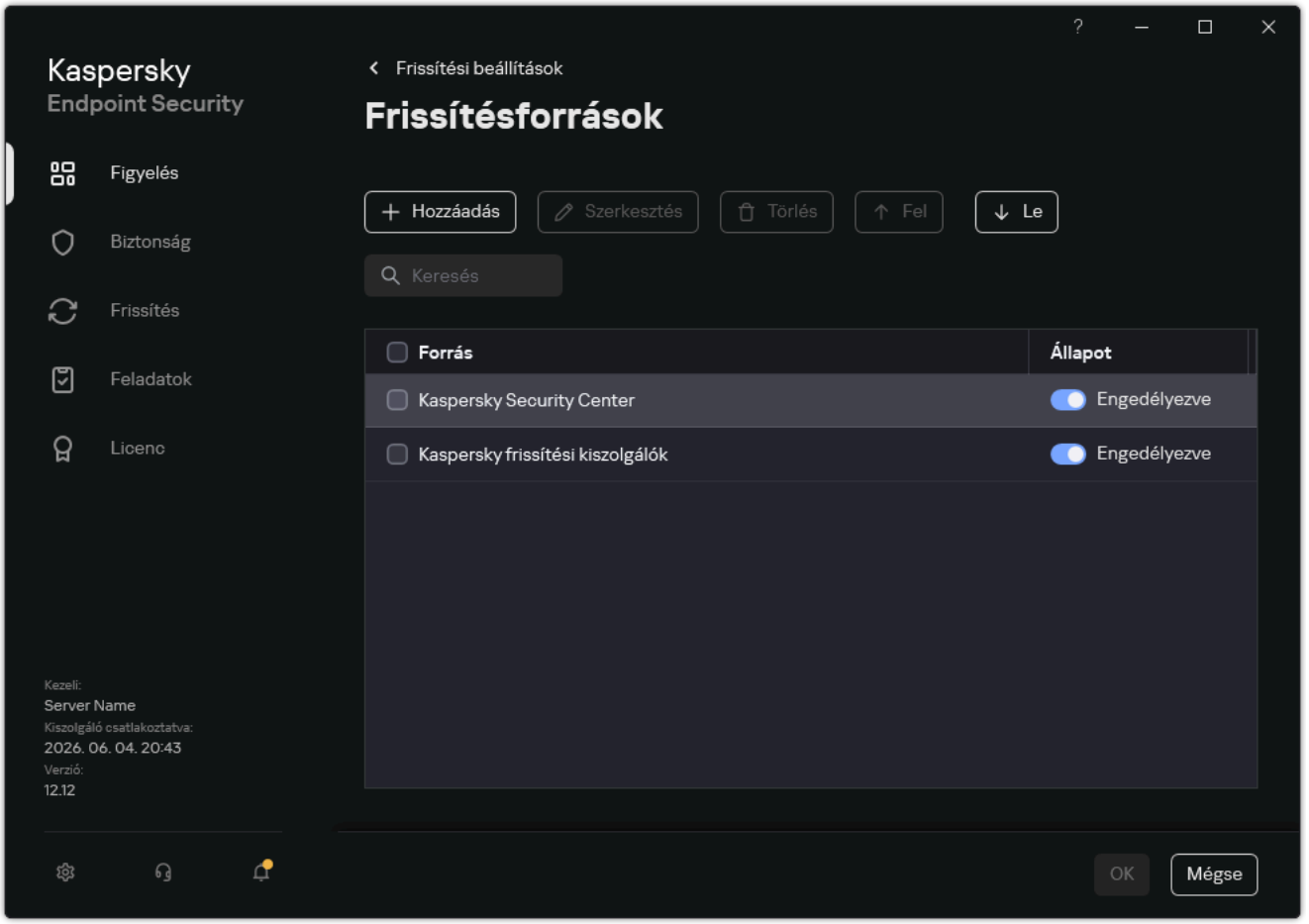
   Megnyílik a feladatok tulajdonságai ablak.

3. A feladat tulajdonságai ablakban kattintson a **Frissítésforrások kiválasztása** elemre.

4. A frissítési források listájában győződjön meg arról, hogy a **Kaspersky Security Center** forrásból származó frissítés engedélyezve van. Ezenkívül a **Kaspersky Security Center** forrásnak kell a legmagasabb prioritást élveznie.

5. Ha szükséges, adja hozzá a frissítési forrásokat:

   a. A frissítési források listájában kattintson a **Add** gombra.



Frissítési források

   a. Adja meg annak az FTP- vagy HTTP-kiszolgálónak, hálózati mappának vagy helyi mappának a címét, ahová a Kaspersky Security Center a Kaspersky frissítési kiszolgálóktól kapott frissítőcsomagot másolja.

   A frissítés forrásának címének meg kell egyeznie a **Folder for storing updates** mezőben megadott címmel, amikor a frissítéseknek a kiszolgáló tárhelyére történő letöltését konfigurálta (a *Download updates to the Administration Server repository* feladat).

   b. Kattintson **Kijelölés** gombra.

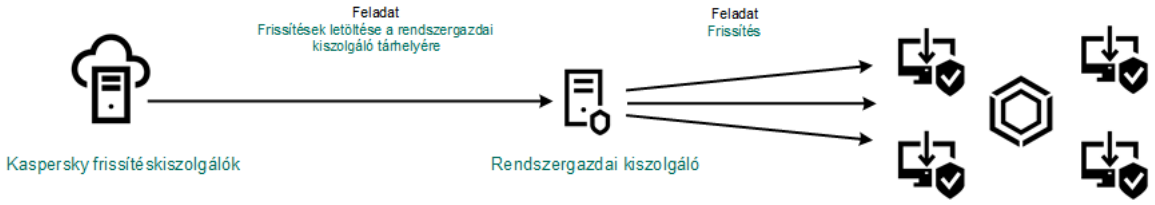
   A frissítésforrást kizárhatja anélkül, hogy eltávolítaná a frissítésforrások listájáról. Ehhez állítsa a mellette lévő kapcsolót kikapcsolt helyzetbe.

6. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

   Ha egy számítógépet a Kaspersky Security Center felügyel, akkor nem lehet konfigurálni a futásmódot az *Adatbázisok és alkalmazásmodulok frissítése* feladathoz. A feladatot csak manuálisan futtathatja.

7. Mentse el a módosításokat.



Frissítés a kiszolgáló tárhelyéből

Megosztott mappából való frissítés

Az internetes forgalom megőrzéséhez egy megosztott mappából konfigurálhatja a szervezet LAN hálózatának számítógépein lévő adatbázisok és alkalmazásmodulok frissítését. Ehhez a helyi hálózaton lévő egyik számítógép frissítési csomagokat fogad a Kaspersky Security Center felügyeleti kiszolgálójától vagy a Kaspersky frissítéskiszolgálóitól, majd a kapott frissítési csomagot egy megosztott mappába másolja. A szervezet helyi hálózatán lévő egyéb számítógépek fogadhatnak frissítési csomagot ebből a megosztott mappából.

A frissítőcsomagot megosztott mappába másoló Kaspersky Endpoint Security alkalmazás verziójának és lokalizációjának meg kell egyeznie a megosztott mappából adatbázisokat frissítő alkalmazás verziójával és honosításával. Ha az alkalmazások verziói vagy honosításai nem egyeznek meg, az adatbázis frissítése hibával zárulhat.

A megosztott mappák adatbázis és alkalmazásmodul-frissítéseinek konfigurálása két lépésből áll:

1. Adatbázisok és alkalmazásmodul-frissítések konfigurálása a kiszolgáló tárhelyéből.

2. A frissítési csomag másolásának engedélyezése a helyi hálózaton lévő egyik számítógép valamelyik megosztott mappájába.

   A frissítőcsomag másolásának engedélyezése a megosztott mappába az Adminisztrációs konzolban (MMC)

   1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

   2. A konzolfán válassza ki a **Tasks** lehetőséget.

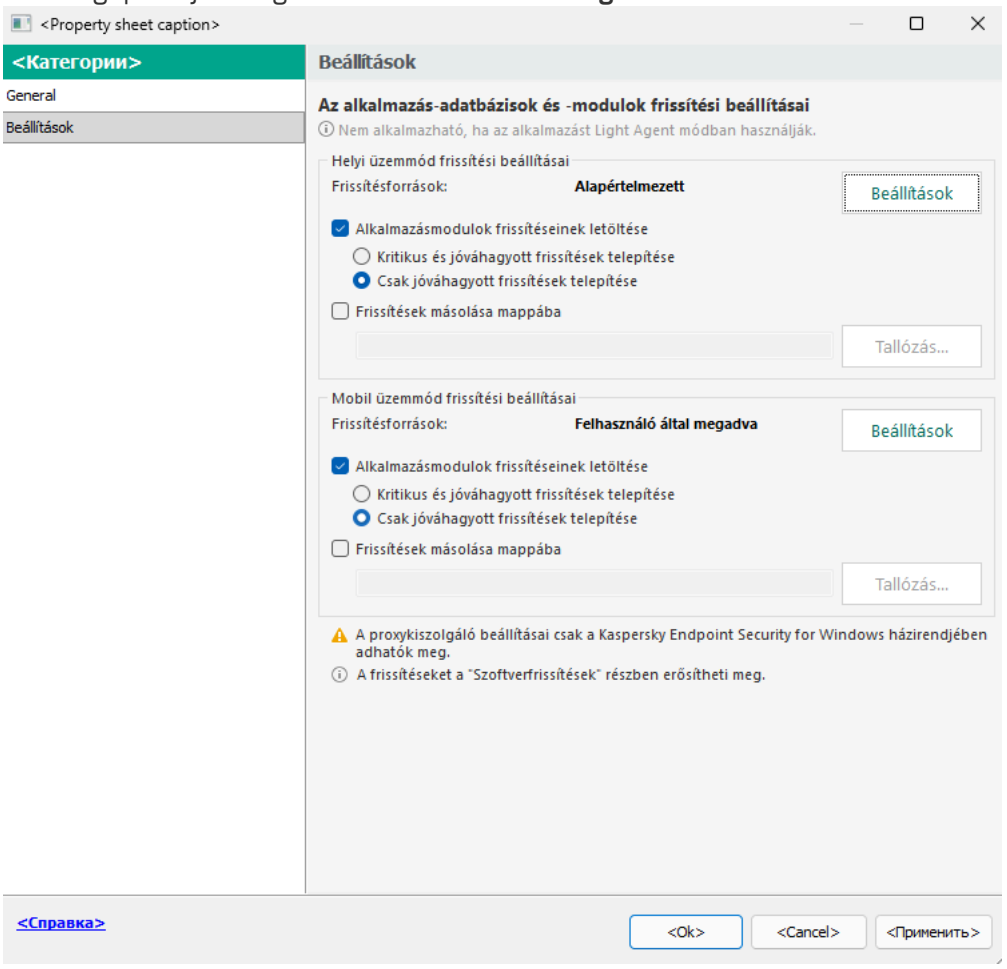
      Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot egy olyan számítógéphez kell hozzárendelni, ami a frissítések forrásaként működik.

   3. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

      Megnyílik a feladatok tulajdonságai ablak.

      Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

4. Válassza ki a számítógép tulajdonságainak ablakában az **Settings** részt.



Az Adatbázisok és alkalmazásmodulok frissítése feladat beállításai

5. A **Helyi üzemmód frissítési beállításai** részen kattintson a **Beállítások** gombra.

6. A frissítések forrásainak beállítása.

   A frissítések forrásai lehetnek Kaspersky frissítéskiszolgálók, a Kaspersky Security Center felügyeleti kiszolgálója, egyéb FTP vagy HTTP kiszolgálók, helyi mappák vagy hálózati mappák.

7. Jelölje be a **Frissítések másolása mappába** jelölőnégyzetet.

8. A **Mappa elérési útja** mezőben adja meg a megosztott mappa UNC-útvonalát (például `\\<server name>\KLSHARE\Updates`).

   Ha a mező üres marad, a Kaspersky Endpoint Security a frissítési csomagot a `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` mappába másolja.

9. Mentse el a módosításokat.

A frissítőcsomag másolásának engedélyezése a Web Console és a Cloud Console megosztott mappájába

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

   A *Update* feladatot egy olyan számítógéphez kell hozzárendelni, ami a frissítések forrásaként működik.

2. Kattintson a Kaspersky Endpoint Security **Update** feladatára.

Megnyílik a feladatok tulajdonságai ablak.

A *Update* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki az **Application settings** → **Local mode** lapot.

4. A frissítések forrásainak beállítása.

   A frissítések forrásai lehetnek Kaspersky frissítéskiszolgálók, a Kaspersky Security Center felügyeleti kiszolgálója, egyéb FTP vagy HTTP kiszolgálók, helyi mappák vagy hálózati mappák.

5. Tegyen jelölést a **Copy updates to folder** jelölőnégyzetbe.

6. Az **Path** mezőben adja meg a megosztott mappa UNC-útvonalát (például `\\<server name>\KLSHARE\Updates`).

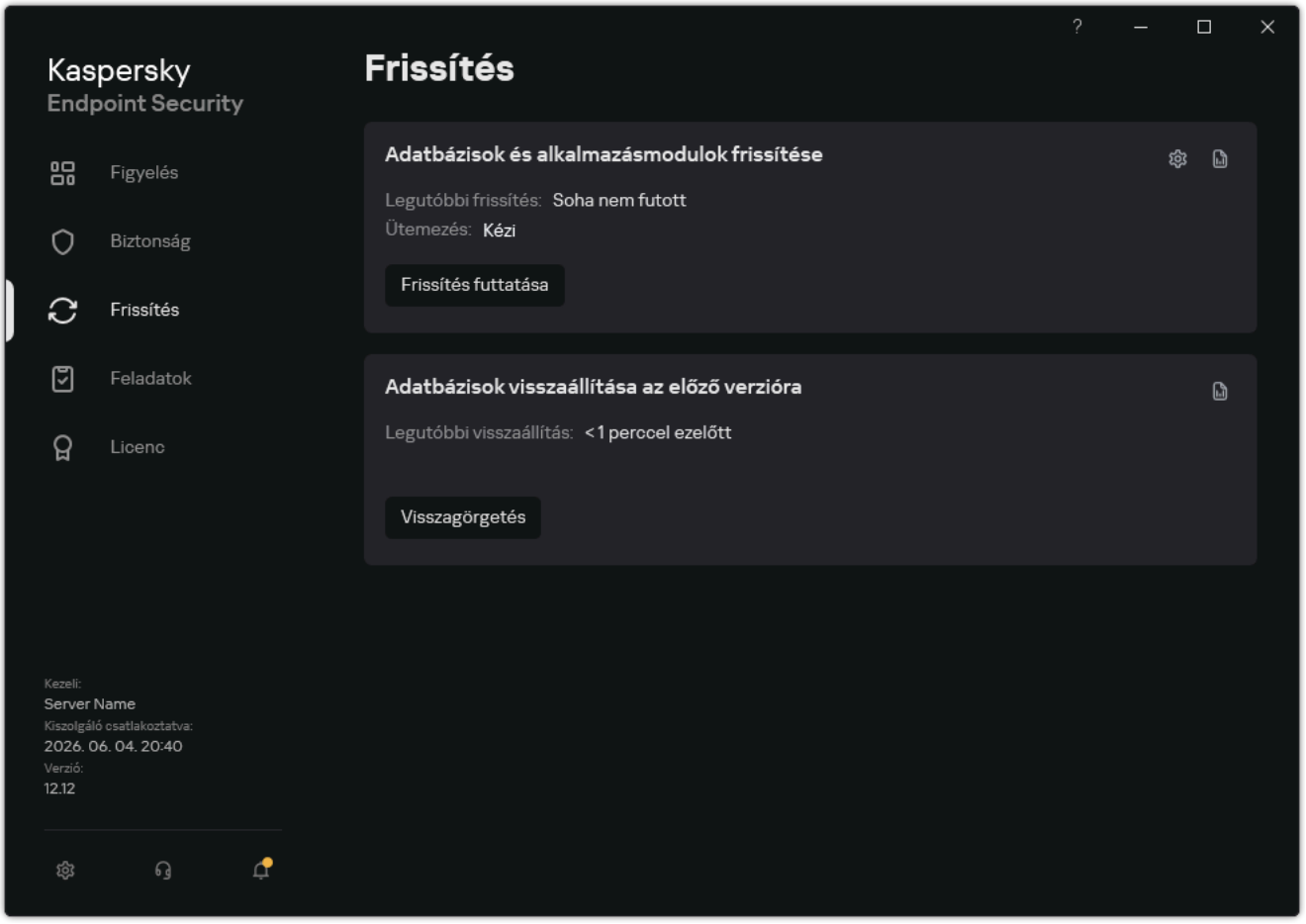
   Ha a mező üres marad, a Kaspersky Endpoint Security a frissítési csomagot a `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` mappába másolja.

7. Mentse el a módosításokat.

A frissítőcsomag másolásának engedélyezése a megosztott mappába az alkalmazás felületén

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. A **Frissítések terjesztése** blokkban jelölje be a **Frissítések másolása mappába** jelölőnégyzetet.

4. Adja meg a megosztott mappa UNC-útvonalát (például, `\\<server name>\KLSHARE\Updates`).

5. Mentse el a módosításokat.

3. A megadott megosztott mappa adatbázisainak és alkalmazásmodul-frissítéseinek konfigurálása a helyi hálózat fennmaradó számítógépeire.

Frissítések konfigurálása a megosztott mappából az Administration Console-on (MMC)

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki **Adatbázisok és alkalmazásmodulok frissítése** elemet.

4. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

5. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Adatbázisok és alkalmazásmodulok frissítése** elemet.

2. lépés: Frissítésforrások kiválasztása

Új frissítésforrás hozzáadása: megosztott mappa. A forráscímnek egyeznie kell azzal a címmel, amit korábban, az **Mappa elérési útja** mezőben adott meg, amikor beállította a frissítési csomag másolását a megosztott mappába. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot a helyi hálózat számítógépeihez hozzá kell rendelni, kivéve ahhoz, ami a frissítés forrásaként működik.

4. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válasszon ki egy fiókot az *Adatbázisok és alkalmazásmodulok frissítése* feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

5. lépés Feladatindítási ütemezés konfigurálása

Adjon meg ütemtervet a feladat indításához, például kézileg vagy azután, hogy az antivírus adatbázisok letöltődtek a könyvtárba.

6. lépés A feladat nevének megadása

Írja be a feladat nevét, pl. *Frissítés megosztott mappából*.

7. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Ennek eredményeképpen a frissítési feladat végre lesz hajtva a felhasználók számítógépén a megadott ütemezés alapján.

Frissítések konfigurálása a megosztott mappából a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Update** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például *Frissítés megosztott mappából*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

   > A *Update* feladatot a helyi hálózat számítógépeihez hozzá kell rendelni, kivéve ahhoz, ami a frissítés forrásaként működik.

4. Válassza ki az eszközöket a kiválasztott feladathatókör lehetőségének megfelelően, majd ugorjon a következő lépésre.

5. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok táblázatában.

6. Kattintson az újonnan létrehozott *Update* feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

7. Válassza ki az **Application settings** → **Local mode** lapot.

8. A **Update sources** részen kattintson a **Add** gombra.

9. A megnyíló ablakban adja be a megosztott mappa útvonalát.

   > A forráscímnek egyeznie kell azzal a címmel, amit korábban, a(z) **Path** mezőben adott meg, amikor beállította a frissítési csomag másolását a megosztott mappába (lásd a fenti utasításokat).

10. Kattintson az **OK** gombra.

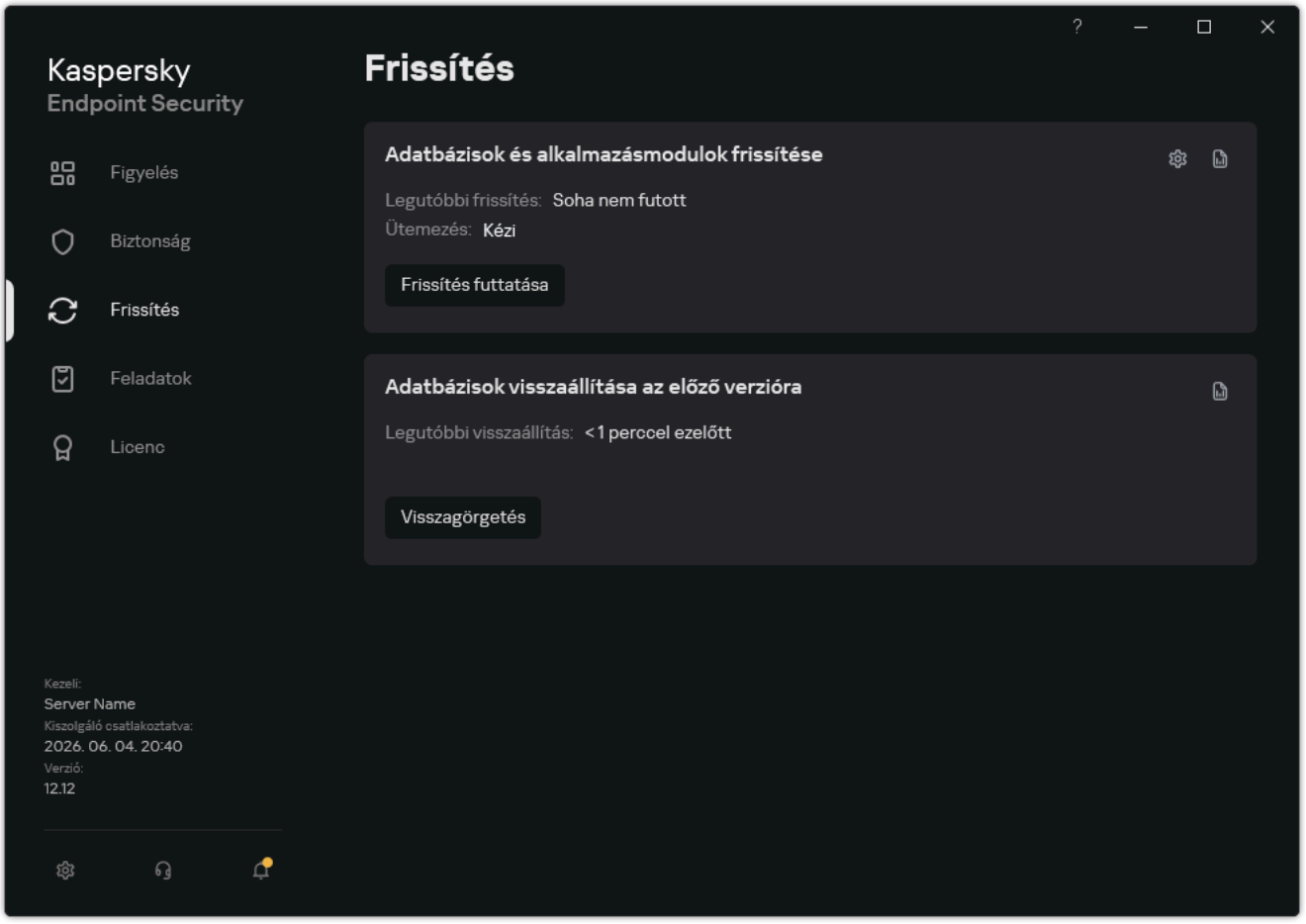
11. Adja meg a frissítésforrások prioritásait a **Up** és **Down** gombokkal.

12. Mentse el a módosításokat.

Frissítések konfigurálása a megosztott mappából az alkalmazás felületén

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Kattintson a **Frissítési források kiválasztása** gombra.

4. Az ablakban kattintson a **Hozzáadás** gombra.

5. A megnyíló ablakban adja be a megosztott mappa útvonalát.

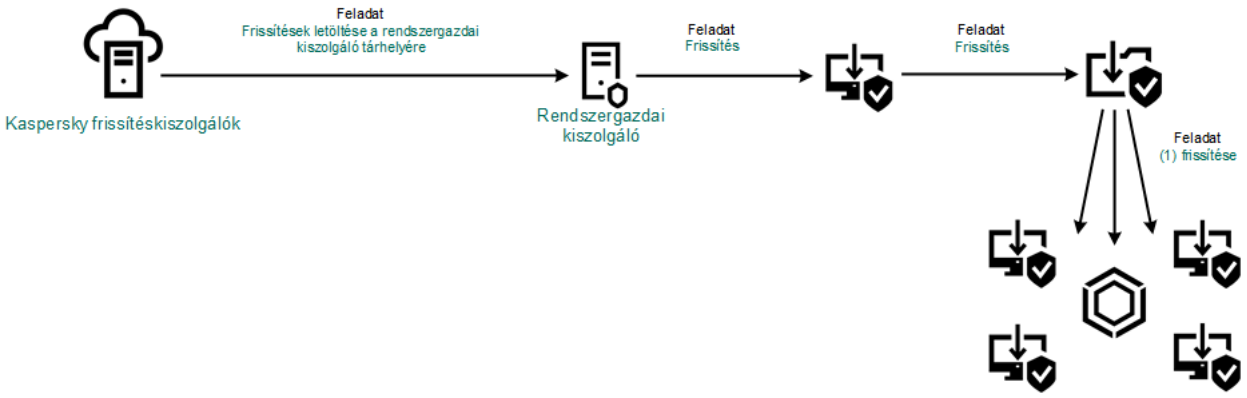
   A forráscímnek egyeznie kell azzal a címmel, amit korábban adott meg, amikor beállította a frissítési csomag másolását a megosztott mappába (lásd a fenti utasításokat).

6. Kattintson **Kijelölés** gombra.

7. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

8. Mentse el a módosításokat.



Megosztott mappából való frissítés

Frissítés a Kaspersky Update Utility használatával

Az internetes forgalom megőrzéséhez egy megosztott mappából konfigurálhatja a szervezet LAN hálózatának számítógépein lévő adatbázisok és alkalmazásmodulok frissítését Kaspersky Update Utility használatával. Ehhez a helyi hálózaton lévő egyik számítógép frissítési csomagokat fogad a Kaspersky Security Center felügyeleti kiszolgálójától vagy a Kaspersky frissítéskiszolgálóitól, majd a kapott frissítési csomagot egy megosztott mappába másolja a segédprogram használatával. A szervezet helyi hálózatán lévő egyéb számítógépek fogadhatnak frissítési csomagot ebből a megosztott mappából.

A frissítőcsomagot megosztott mappába másoló Kaspersky Endpoint Security alkalmazás verziójának és lokalizációjának meg kell egyeznie a megosztott mappából adatbázisokat frissítő alkalmazás verziójával és honosításával. Ha az alkalmazások verziói vagy honosításai nem egyeznek meg, az adatbázis frissítése hibával zárulhat.

A megosztott mappák adatbázis és alkalmazásmodul-frissítéseinek konfigurálása két lépésből áll:

1. Adatbázisok és alkalmazásmodul-frissítések konfigurálása a kiszolgáló tárhelyéből.

2. Telepítse a Kaspersky Update Utility programot a szervezet LAN-hálózatán lévő egyik számítógépre.

3. Állítsa be a frissítési csomag másolását a megosztott mappába a Kaspersky Update Utility beállításokban.

   Letöltheti a Kaspersky Update Utility terjesztőcsomagot a Kaspersky Terméktámogatás weboldaláról. A segédprogram telepítése után válassza ki a frissítésforrást (például az Adminisztrációs kiszolgáló tárhelye) és a megosztott mappát, ahová a Kaspersky Update Utility másolni fogja a frissítési csomagokat. A Kaspersky Update Utility használatával kapcsolatos további információkért lásd: Kaspersky Tudásbázis.

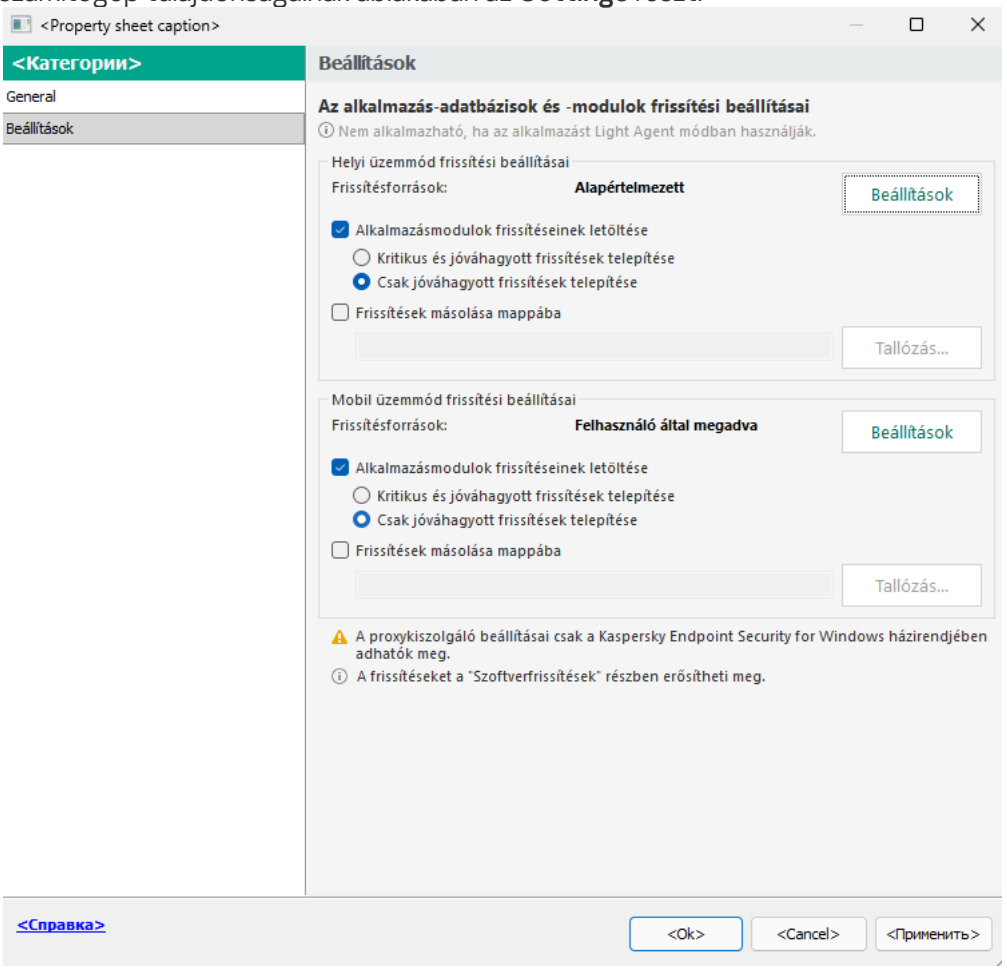
4. A megadott megosztott mappa adatbázisainak és alkalmazásmodul-frissítéseinek konfigurálása a helyi hálózat fennmaradó számítógépeire.

Frissítések konfigurálása a megosztott mappából az Administration Console-on (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.
3. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

   Megnyílik a feladatok tulajdonságai ablak.

   Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.
4. Válassza ki a számítógép tulajdonságainak ablakában az **Settings** részt.



Az Adatbázisok és alkalmazásmodulok frissítése feladat beállításai

5. A **Helyi üzemmód frissítési beállításai** részen kattintson a **Beállítások** gombra.
6. A frissítési források listájában kattintson a **Add** gombra.
7. A megnyíló ablakban adja be a megosztott mappa UNC-útvonalát (például: `\\<server name>\KLSHARE\Updates`).

   A forráscímnek egyeznie kell a Kaspersky Update Utility beállításaiban megadott címmel.
8. Kattintson az **OK** gombra.

9. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

10. Mentse el a módosításokat.

Frissítések konfigurálása a megosztott mappából a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Update** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

   A *Update* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki az **Application settings** → **Local mode** lapot.

4. A frissítési források listájában kattintson a **Add** gombra.

5. A megnyíló ablakban adja be a megosztott mappa UNC-útvonalát (például: `\\<server name>\KLSHARE\Updates`).

   > A forráscímnek egyeznie kell a Kaspersky Update Utility beállításaiban megadott címmel.

6. Kattintson az **OK** gombra.

7. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

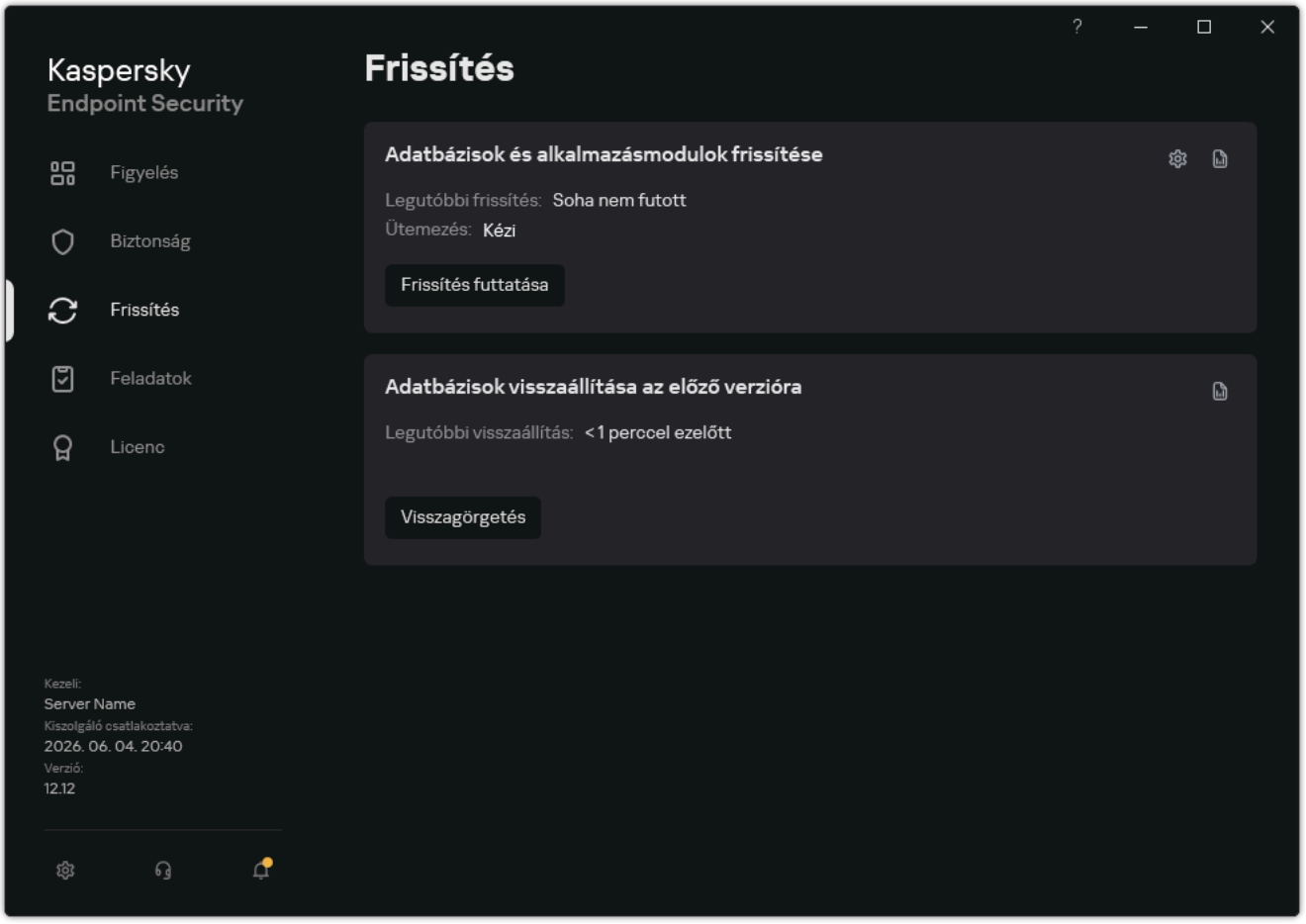
   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

8. Mentse el a módosításokat.

Frissítések konfigurálása a megosztott mappából az alkalmazás felületén

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



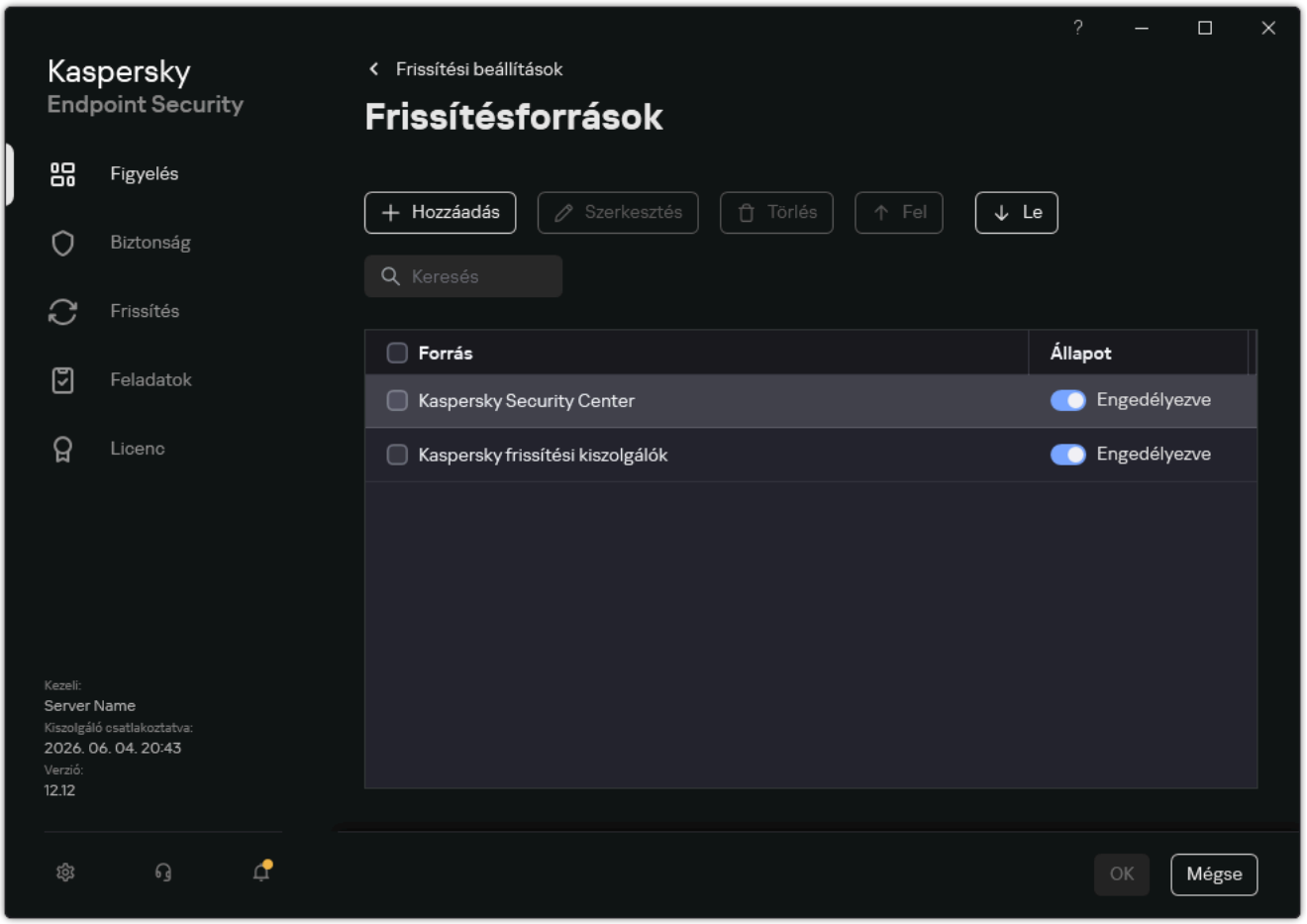
Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. A feladat tulajdonságai ablakban kattintson a **Frissítésforrások kiválasztása** elemre.

4. A frissítési források listájában kattintson a **Add** gombra.



Frissítési források

5. Adja meg a megosztott mappa UNC-útvonalát (például, `\\<server name>\KLSHARE\Updates`).

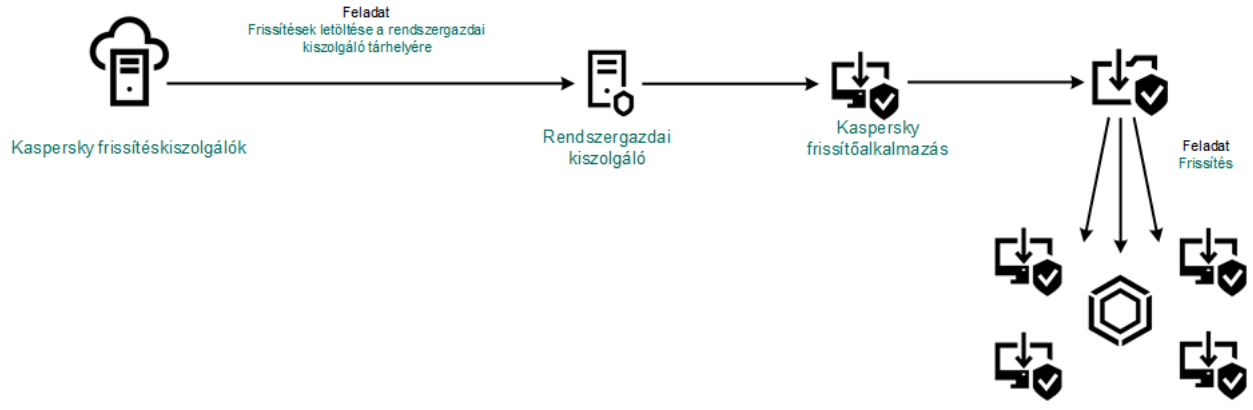
A forráscímnek egyeznie kell a Kaspersky Update Utility beállításaiban megadott címmel.

6. Kattintson **Kijelölés** gombra.

7. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

8. Mentse el a módosításokat.



Frissítés a Kaspersky Update Utility használatával

Frissítés mobil módban

A *Mobil mód* a Kaspersky Endpoint Security egy olyan működési módja, ahol a számítógép elhagyja a szervezet hálózatának területét (*offline számítógépek*). Az offline számítógépekkel és az irodán kívüli felhasználókkal való együttműködéssel kapcsolatos további tudnivalókért lásd a Kaspersky Security Center súgót.

A szervezeten kívüli offline számítógép nem tud csatlakozni az Adminisztrációs kiszolgálóhoz, hogy adatbázisokat és alkalmazásmodulokat frissítsen. Alapértelmezetten a Kaspersky frissítéskiszolgálói a frissítések forrásaiként vannak használva az adatbázisok és alkalmazásmodulok frissítéséhez mobil módban. A proxykiszolgáló internethez történő csatlakozását egy speciális házon kívüli rendszabály szabja meg. A házon kívüli szabályt külön kell létrehozni. Ha a Kaspersky Endpoint Security mobil üzemmódra van kapcsolva, a frissítési feladat két óránként elindul.

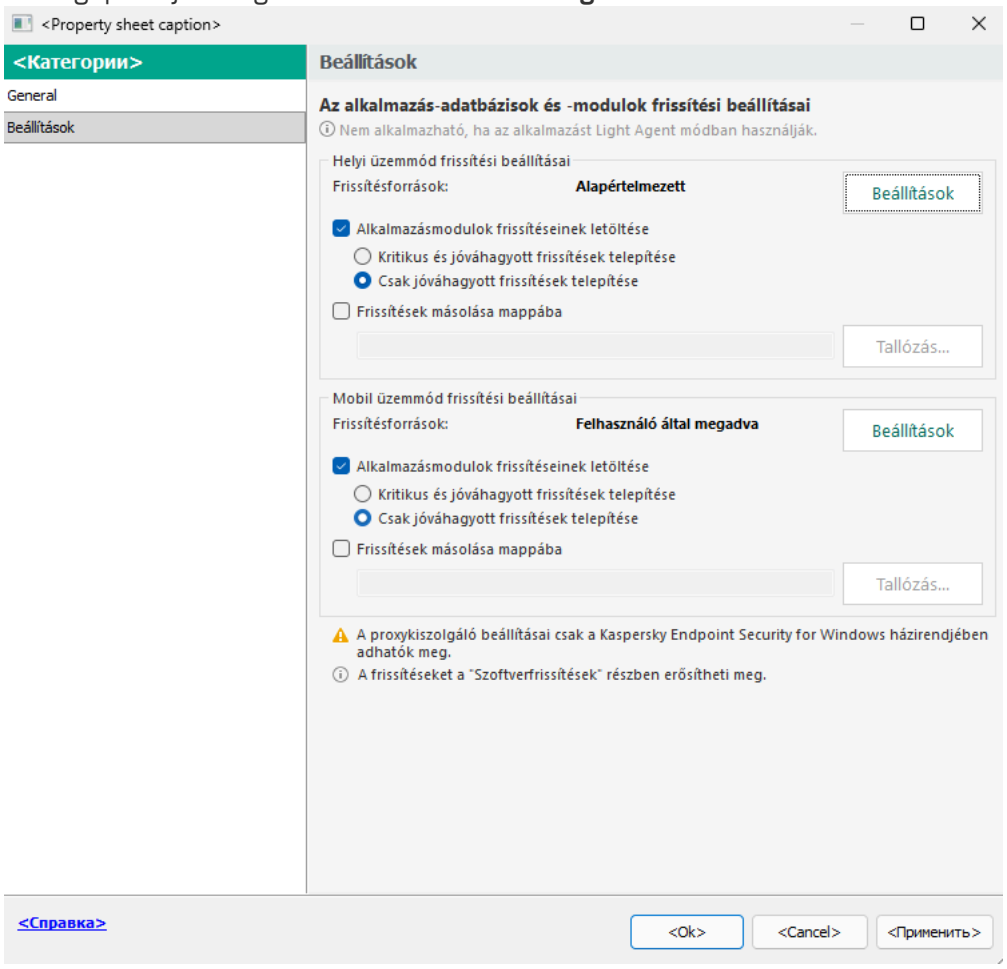
Mobil üzemmód frissítési beállításainak konfigurálása az Administration Console-on (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.
3. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

   Megnyílik a feladatok tulajdonságai ablak.

   Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

4. Válassza ki a számítógép tulajdonságainak ablakában az **Settings** részt.



Az Adatbázisok és alkalmazásmodulok frissítése feladat beállításai

5. A **Mobil üzemmód frissítési beállításai** részen kattintson a **Beállítások** gombra.

6. A frissítések forrásainak beállítása. A frissítések forrásai lehetnek Kaspersky frissítéskiszolgálók, egyéb FTP és HTTP kiszolgálók, helyi mappák vagy hálózati mappák.

7. Mentse el a módosításokat.

Mobil üzemmód frissítési beállításainak konfigurálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Update** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

   A *Update* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki az **Application settings** → **Mobile mode** lapot.

4. A frissítések forrásainak beállítása. A frissítések forrásai lehetnek Kaspersky frissítéskiszolgálók, egyéb FTP és HTTP kiszolgálók, helyi mappák vagy hálózati mappák.

5. Mentse el a módosításokat.

Ennek eredményeképpen az adatbázisok és az alkalmazásmodulok frissülnek a felhasználók számítógépén, ha átváltanak mobil üzemmódra.

A frissítési feladatok elindítása és leállítása

A kiválasztott frissítési feladat futásmódjától függetlenül a Kaspersky Endpoint Security frissítési feladatai bármikor elindíthatók és leállíthatók.

Frissítési feladat elindítása és leállítása:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Az **Adatbázisok és alkalmazásmodulok frissítése** csempén kattintson a **Frissítés** gombra, ha el szeretné indítani a frissítési feladatot.

   A Kaspersky Endpoint Security megkezdi az alkalmazásmodulok és adatbázisok frissítését. Az alkalmazás megjeleníti a feladat előrehaladását, a letöltött fájlok méretét és a frissítésforrást. A feladatot bármikor leállíthatja a **Frissítés leállítása** gombra kattintva.

Frissítési feladat elindítása és leállítása az egyszerűsített alkalmazásfelület megjelenése közben:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.
2. A helyi menüben a **Feladatok** legördülő listán végezze el az alábbi műveletek közül valamelyiket:
   - az elindításhoz válasszon ki egy nem futó frissítési feladatot
   - a leállításhoz válasszon ki egy futó frissítési feladatot
   - a folytatáshoz vagy újraindításhoz válasszon ki egy szünetelő frissítési feladatot

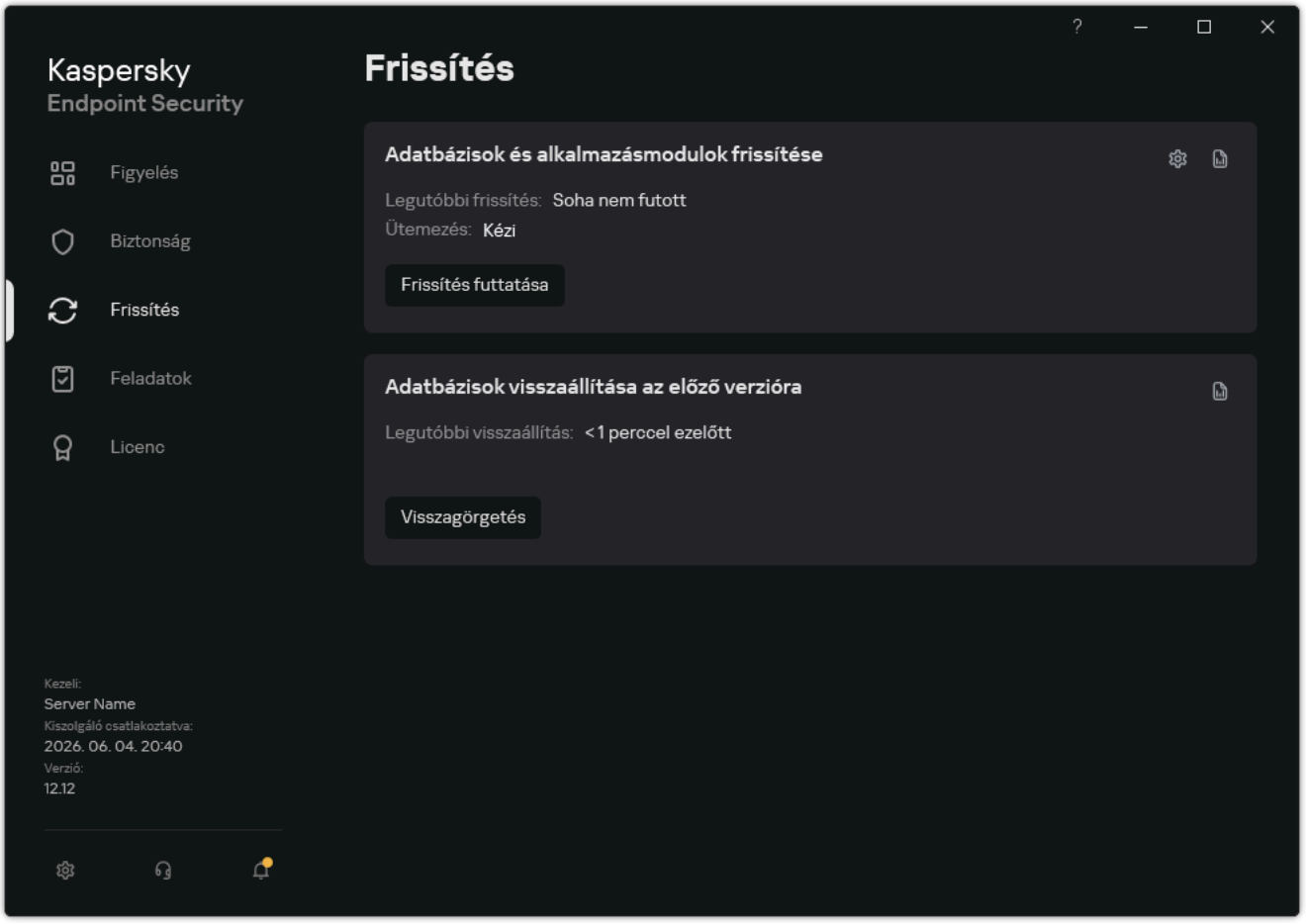
Frissítési feladat elindítása másik felhasználói fiók jogosultságaival

A Kaspersky Endpoint Security frissítési feladata alapértelmezés szerint ugyanannak a felhasználónak a nevében indul el, akinek a fiókjával bejelentkezett az operációs rendszerbe. A Kaspersky Endpoint Security azonban frissíthető olyan forrásból is, amelyhez a felhasználó a szükséges jogosultságok hiányában (például frissítési csomagot tartalmazó megosztott mappából), vagy egy olyan frissítésforrással, melyhez a proxykiszolgáló hitelesítése nincs konfigurálva, nem férhet hozzá. Az alkalmazás beállításaiban megadhat egy olyan felhasználót, aki rendelkezik ezekkel a jogosultságokkal, és a Kaspersky Endpoint Security frissítési feladatát elindíthatja ennek a felhasználói fióknak a nevében.

Frissítési feladat elindítása egy másik felhasználó fiókjában:

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Kattintson az **Adatbázis-frissítések futtatása felhasználói jogokkal** gombra.

4. A megnyíló ablakban válassza a **Másik felhasználó** lehetőséget.

5. Adja meg a frissítésforrás eléréséhez szükséges jogosultságokkal rendelkező felhasználói fiók bejelentkezési adatait.

6. Mentse el a módosításokat.

Frissítési feladat futásmódjának kiválasztása

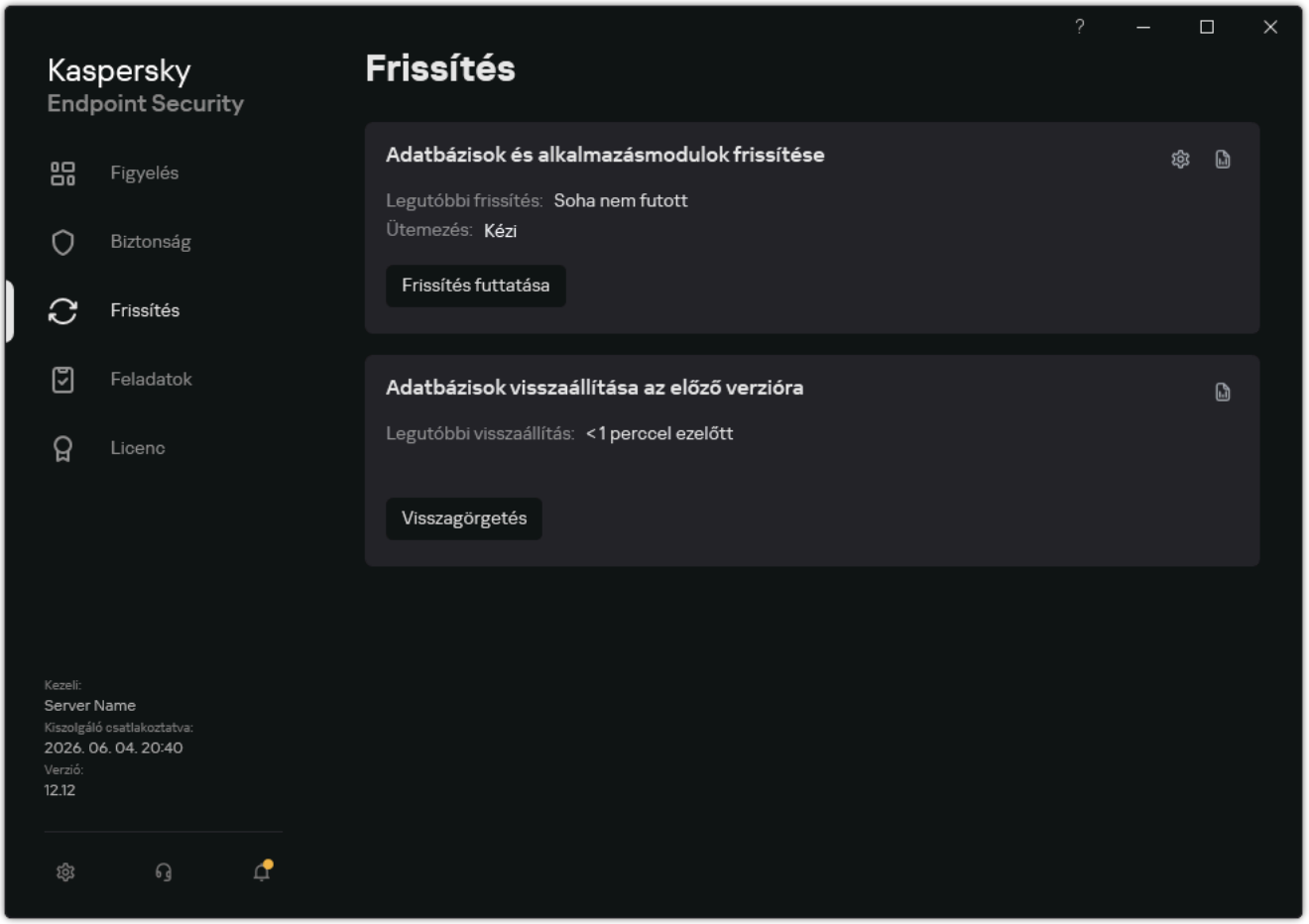
Ha a frissítési feladat futtatása valamilyen okból (például a számítógép abban az időpontban nem volt bekapcsolva) nem volt lehetséges, beállíthatja a kimaradt feladatot úgy is, hogy automatikusan elinduljon, amint lehet.

A frissítési feladat alkalmazásindítást követő elindulását el is halaszthatja, ha a frissítési feladat **Ütemezés szerint** futásmódját választja ki, és a Kaspersky Endpoint Security kezdési időpontja egyezik a frissítési feladat indítási ütemezésével. Az frissítési feladatok futtatására csak akkor kerülhet sor, ha letelik a megadott időtartam a Kaspersky Endpoint Security elindulása után.

Frissítési feladat futásmódjának kiválasztása:

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Kattintson a **Futásmód** lehetőségre.

4. A megnyíló ablakban válassza ki a frissítési feladat futásának módját:

   - Ha azt szeretné, hogy a Kaspersky Endpoint Security a frissítési feladatot attól függően futtassa, hogy a frissítési forrástól beszerezhető-e frissítési csomag, válassza az **Automatikus** lehetőséget. Vírusjárványok kirobbanásakor a Kaspersky Endpoint Security gyakrabban ellenőrzi a frissítési csomagokat, máskor pedig ritkábban.

   - Ha kézileg szeretne frissítési feladatot indítani, válassza ki a **Kézi** lehetőséget.

   - Ha be szeretné állítani a frissítési feladat futtatási ütemezését, válasszon másik opciót. Konfigurálja a speciális beállításokat a frissítési feladat indításához:

     - Adja meg a **Futtatás elhalasztása az alkalmazásindítás után N percre** mezőben azt az időközt, amellyel a frissítési feladat elkezdését elhalasztja a Kaspersky Endpoint Security indítása után.

     - Válassza az **Ütemezett vizsgálat futtatása a következő napon, ha a számítógép ki van kapcsolva** lehetőséget, ha azt szeretné, hogy a Kaspersky Endpoint Security az első alkalommal futtassa a kimaradt frissítési feladatokat. Amikor az alkalmazás lehetőséget kap a kihagyott feladatok végrehajtására, egy adott időintervallumon belül véletlenszerűen futtatja a feladatokat, hogy elossza a számítógép terhelését.

5. Mentse el a módosításokat.

Frissítésforrás hozzáadása

A *frissítésforrás* a Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítéseit tartalmazó erőforrás.

A frissítési források közé a Kaspersky Security Center kiszolgálója, a Kaspersky frissítési kiszolgálói, valamint hálózati vagy helyi mappák tartoznak.

Ha a Kaspersky frissítési kiszolgálói nem érhetők el, a Kaspersky Endpoint Security alternatív tartományokat használhat az adatbázisok és alkalmazásmodulok frissítéséhez. Részletes információkért tekintse meg a Terméktámogatási tudásbázist.

A frissítésforrások alapértelmezett listáján a Kaspersky Security Center és a Kaspersky frissítéskiszolgálói szerepelnek. Felvehet más frissítésforrásokat is a listába. Frissítésforrásként megadhat HTTP-/FTP-kiszolgálókat és megosztott meghajtókat.

A Kaspersky Endpoint Security csak akkor támogatja a frissítéseket HTTPS-kiszolgálókról, ha azok a Kaspersky saját frissítési kiszolgálói.

Ha több forrás van kiválasztva frissítésforrásként, a Kaspersky Endpoint Security egymás után próbál kapcsolatot létesíteni azokkal a lista első elemétől kezdve, és úgy végzi el a frissítési feladatot, hogy az első elérhető forrásról letölti a frissítőcsomagot.

Alapértelmezés szerint a Kaspersky Endpoint Security a Kaspersky Security Center kiszolgálóját használja első frissítési forrásként. Ez segít megőrizni az adatforgalmat a frissítés során. Ha a számítógépre nem vonatkozik házirend, az *Adatbázisok és alkalmazásmodulok frissítése* helyi feladat beállításaiban a Kaspersky-kiszolgálók kerülnek kiválasztásra első frissítési forrásként, mivel előfordulhat, hogy az alkalmazás nem fér hozzá a Kaspersky Security Center kiszolgálójához.

Ha az alkalmazás Light Agent üzemmódban fut, az SVM egyik mappája lesz kiválasztva frissítésforrásként.

Frissítési forrás hozzáadása az Administration Console-on (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

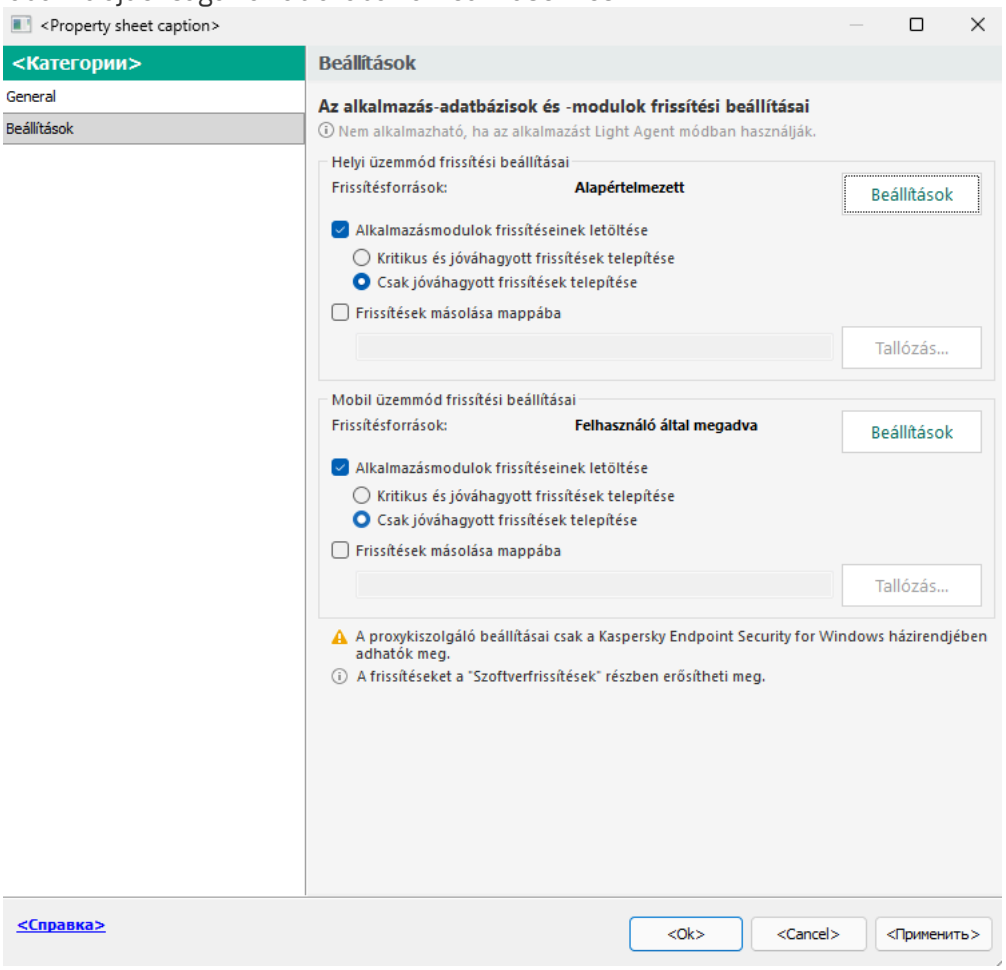
   A konzolfán válassza ki a **Tasks** lehetőséget.

2. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

   Megnyílik a feladatok tulajdonságai ablak.

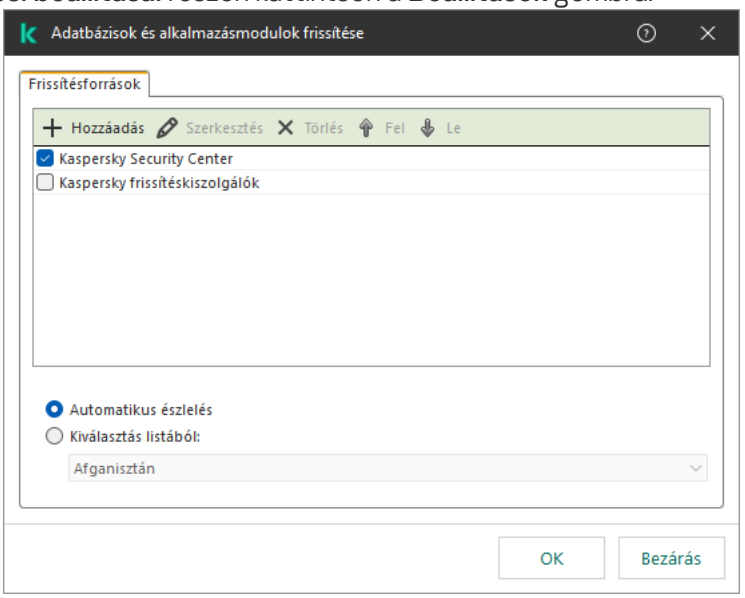
   Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.



Az Adatbázisok és alkalmazásmodulok frissítése feladat beállításai

4. A **Helyi üzemmód frissítési beállításai** részen kattintson a **Beállítások** gombra.



Frissítési források

5. A frissítési források listájában kattintson a **Add** gombra.

6. A **Frissítésforrások** mezőben adja meg az FTP vagy a HTTP-kiszolgáló címét, illetve a frissítési csomagot tartalmazó hálózati mappát vagy a helyi mappát.

   Az elérési utat a frissítési források esetében a következő formátumban kell megadni:

   - FTP- vagy HTTP-kiszolgáló esetén adja meg a webcímet vagy az IP-címet.

     Például: `http://dnl-01.geo.kaspersky.com/` vagy `93.191.13.103`.

     FTP-kiszolgáló esetén megadhatja a hitelesítési beállításokat a webcímben a következő formátumban: `ftp://<user name>:<password>@<node>:<port>`.

   - Hálózati mappához adja meg az UNC-útvonalat

     Például: `\\Server\Share\Update distribution`.

   - Helyi mappa esetén adja meg a mappa teljes elérési útvonalát.

     Például: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   A frissítésforrást kizárhatja anélkül, hogy eltávolítaná a frissítésforrások listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

7. Kattintson az **OK** gombra.

8. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

9. Ha szükséges, adjon hozzá egy frissítésforrást a mobil üzemmódhoz. A *Mobil mód* a Kaspersky Endpoint Security egy olyan működési módja, ahol a számítógép elhagyja a szervezet hálózatának területét (*offline számítógépek*).

10. Mentse el a módosításokat.

Frissítésforrás hozzáadása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

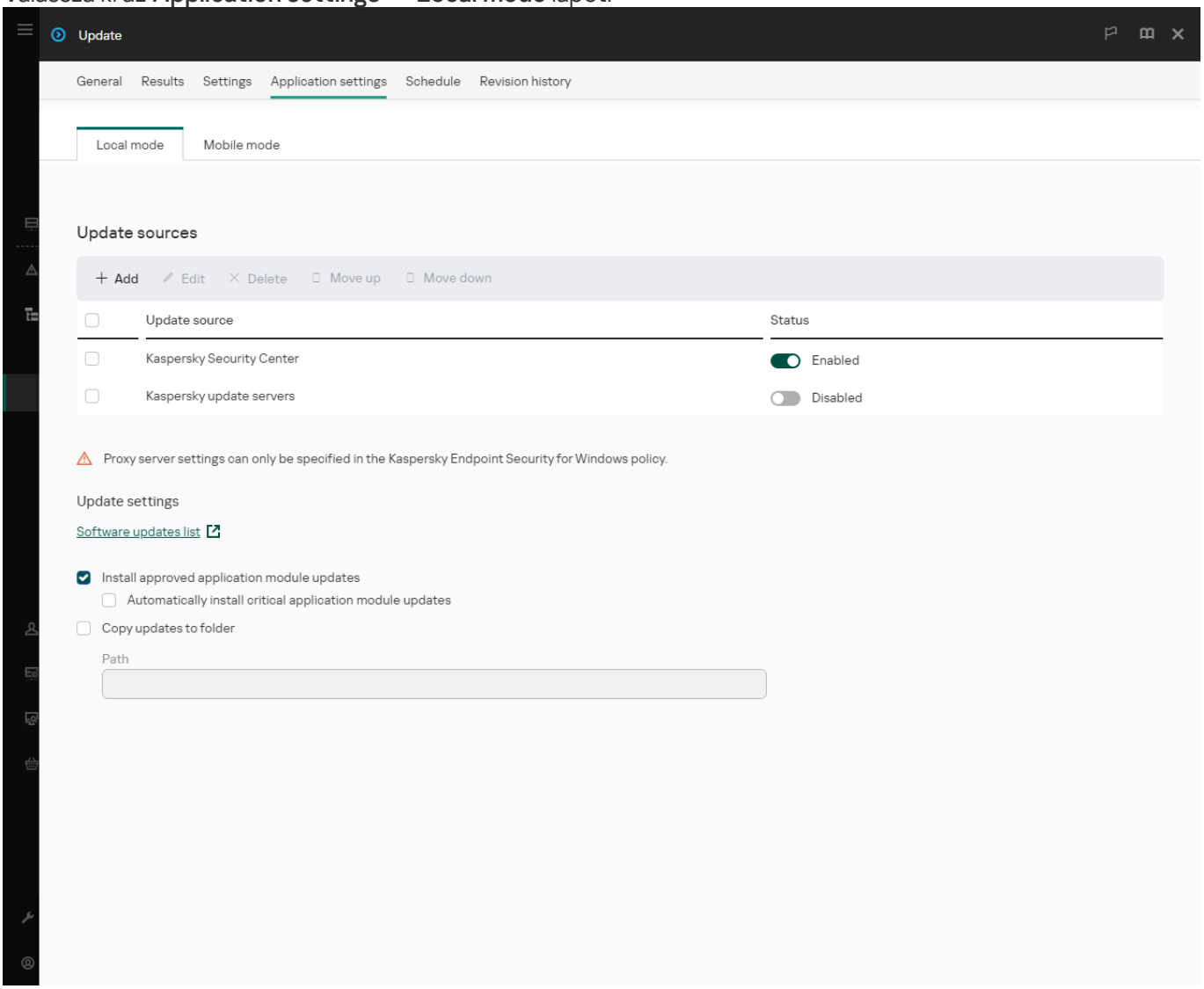
   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Update** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

   A *Update* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki az **Application settings** → **Local mode** lapot.



Frissítési források

4. A frissítési források listájában kattintson a **Add** gombra.

5. A megnyíló ablakban adja meg az FTP vagy a HTTP szerver címét, illetve a frissítési csomagot tartalmazó hálózati mappát vagy a helyi mappát.

   Az elérési utat a frissítési források esetében a következő formátumban kell megadni:

   - FTP- vagy HTTP-kiszolgáló esetén adja meg a webcímet vagy az IP-címet.

     Például: `http://dnl-01.geo.kaspersky.com/` vagy `93.191.13.103`.

FTP-kiszolgáló esetén megadhatja a hitelesítési beállításokat a webcímben a következő formátumban: `ftp://<user name>:<password>@<node>:<port>`.

- Hálózati mappához adja meg az UNC-útvonalat

  Például: `\\Server\Share\Update distribution`.

- Helyi mappa esetén adja meg a mappa teljes elérési útvonalát.

  Például: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

A frissítésforrást kizárhatja anélkül, hogy eltávolítaná a frissítésforrások listájáról. Ehhez állítsa a mellette lévő kapcsolót kikapcsolt helyzetbe.

6. Kattintson az **OK** gombra.

7. Adja meg a frissítésforrások prioritásait a **Up** és **Down** gombokkal.

   Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

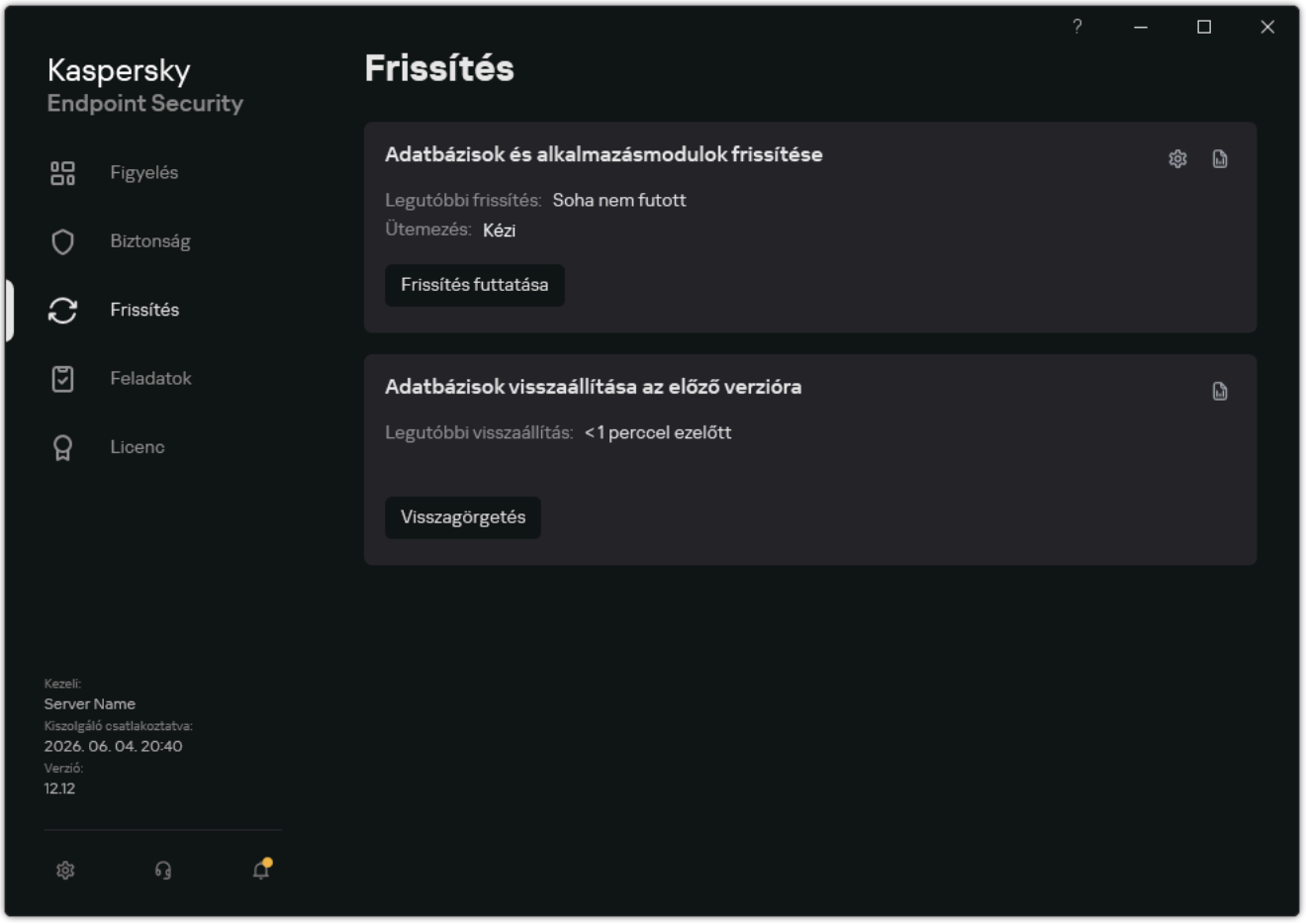
8. Ha szükséges, adjon hozzá egy frissítésforrást a mobil üzemmódhoz. A *Mobil mód* a Kaspersky Endpoint Security egy olyan működési módja, ahol a számítógép elhagyja a szervezet hálózatának területét (*offline számítógépek*).

9. Mentse el a módosításokat.

Frissítésforrás hozzáadása az alkalmazás felületén

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



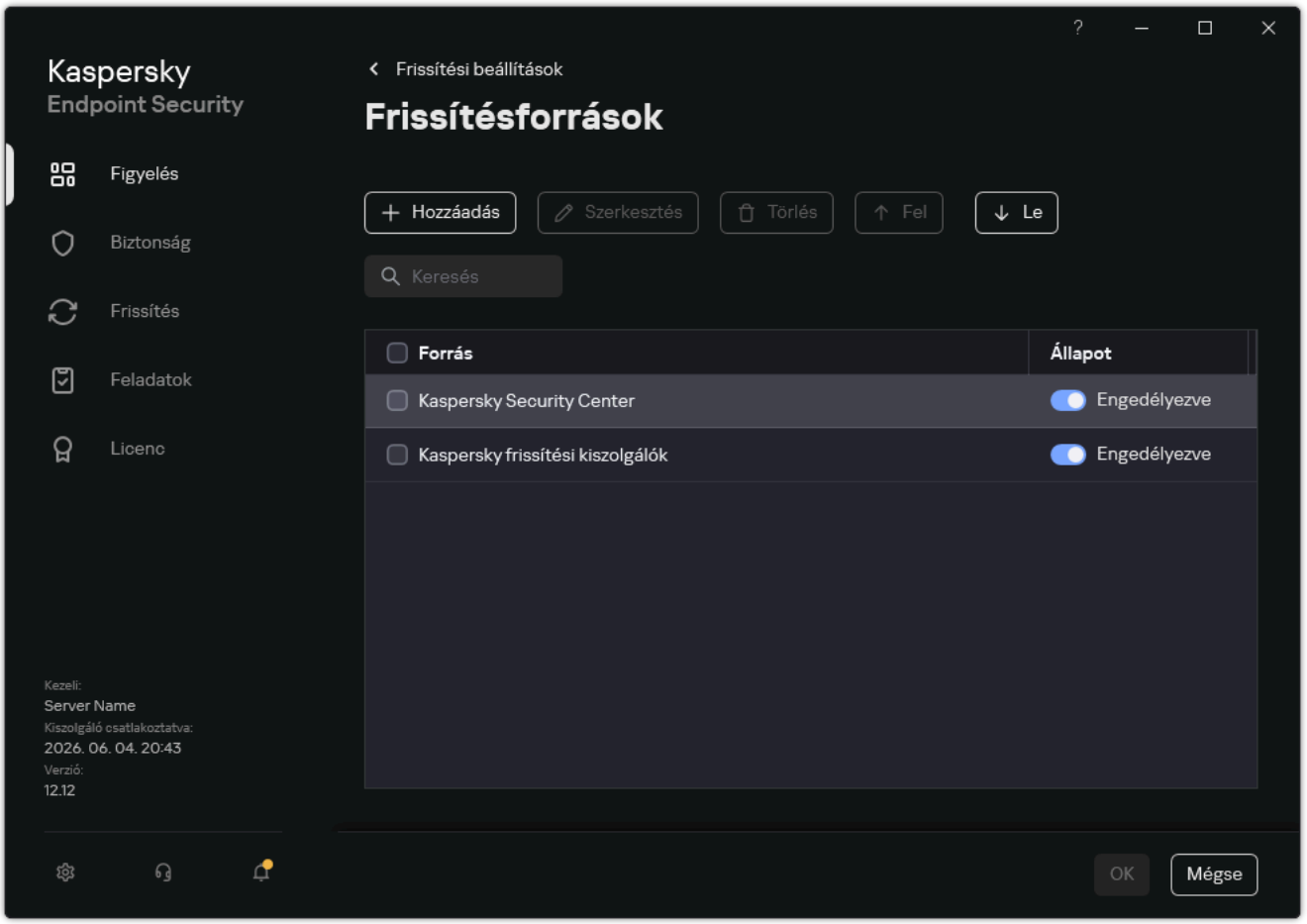
Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Kattintson a **Frissítési források kiválasztása** gombra.

4. Az ablakban kattintson a **Hozzáadás** gombra.



Frissítési források

5. A megnyíló ablakban adja meg az FTP vagy a HTTP szerver címét, illetve a frissítési csomagot tartalmazó hálózati mappát vagy a helyi mappát.

   Az elérési utat a frissítési források esetében a következő formátumban kell megadni:

   - FTP- vagy HTTP-kiszolgáló esetén adja meg a webcímet vagy az IP-címet.

     Például: `http://dnl-01.geo.kaspersky.com/` vagy `93.191.13.103`.

     FTP-kiszolgáló esetén megadhatja a hitelesítési beállításokat a webcímben a következő formátumban: `ftp://<user name>:<password>@<node>:<port>`.

   - Hálózati mappához adja meg az UNC-útvonalat

     Például: `\\Server\Share\Update distribution`.

   - Helyi mappa esetén adja meg a mappa teljes elérési útvonalát.

     Például: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Kattintson **Kijelölés** gombra.

7. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

8. Mentse el a módosításokat.

Alkalmazásmodulok frissítése

Az alkalmazás modulfrissítései kijavítják a hibákat, javítják a teljesítményt és új szolgáltatásokat tartalmaznak. Amikor egy új alkalmazás modulfrissítés elérhetővé válik, meg kell erősítenie a frissítés telepítését. Az alkalmazás modulfrissítés telepítését az alkalmazás felületén vagy a Kaspersky Security Centerben erősítheti meg. Amikor egy frissítés érhető el, az alkalmazás értesítést jelenít meg a Kaspersky Endpoint Security főablakában: . Ha az alkalmazásmodul-frissítésekhez át kell tekinteni és el kell fogadni a Végfelhasználói licencszerződés feltételeit, akkor az alkalmazás csak ennek megtörténte után telepíti a frissítéseket.

Az alkalmazásfrissítés telepítése után szükség lehet a számítógép újraindítására.

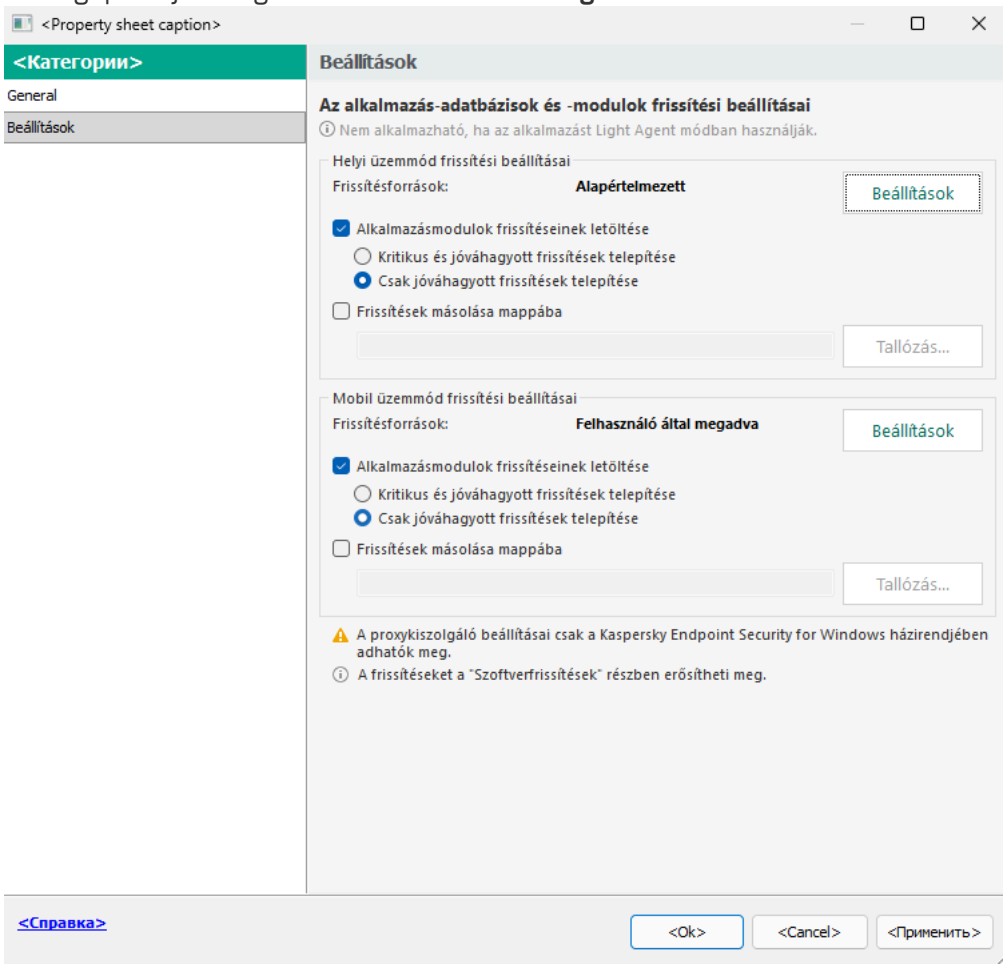
Az alkalmazás modulfrissítéseinek konfigurálása a felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.
3. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

   Megnyílik a feladatok tulajdonságai ablak.

   Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

4. Válassza ki a számítógép tulajdonságainak ablakában az **Settings** részt.



Az Adatbázisok és alkalmazásmodulok frissítése feladat beállításai

5. A **Helyi üzemmód frissítési beállításai** részen jelölje be az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzet.

   Ha meg szeretné akadályozni, hogy az alkalmazásmodul frissítései letöltődjenek, törölje az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzet bejelölését, és megtilthatja a helyi feladatok felhasználó általi használatát.

6. Válassza ki a telepíteni kívánt alkalmazás modulfrissítéseket.

   - **Kritikus és jóváhagyott frissítések telepítése**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security automatikusan telepíti a létfontosságú frissítéseket, a többit pedig csak akkor, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről.

   - **Csak jóváhagyott frissítések telepítése**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security csak akkor telepíti őket, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről. Alapértelmezésben ez a lehetőség van kiválasztva.

7. Szükség esetén konfigurálja az alkalmazás modulfrissítéseit mobil üzemmódban. A *Mobil mód* a Kaspersky Endpoint Security egy olyan működési módja, ahol a számítógép elhagyja a szervezet hálózatának területét (*offline számítógépek*).

8. Mentse el a módosításokat.

Az alkalmazás modulfrissítéseinek konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

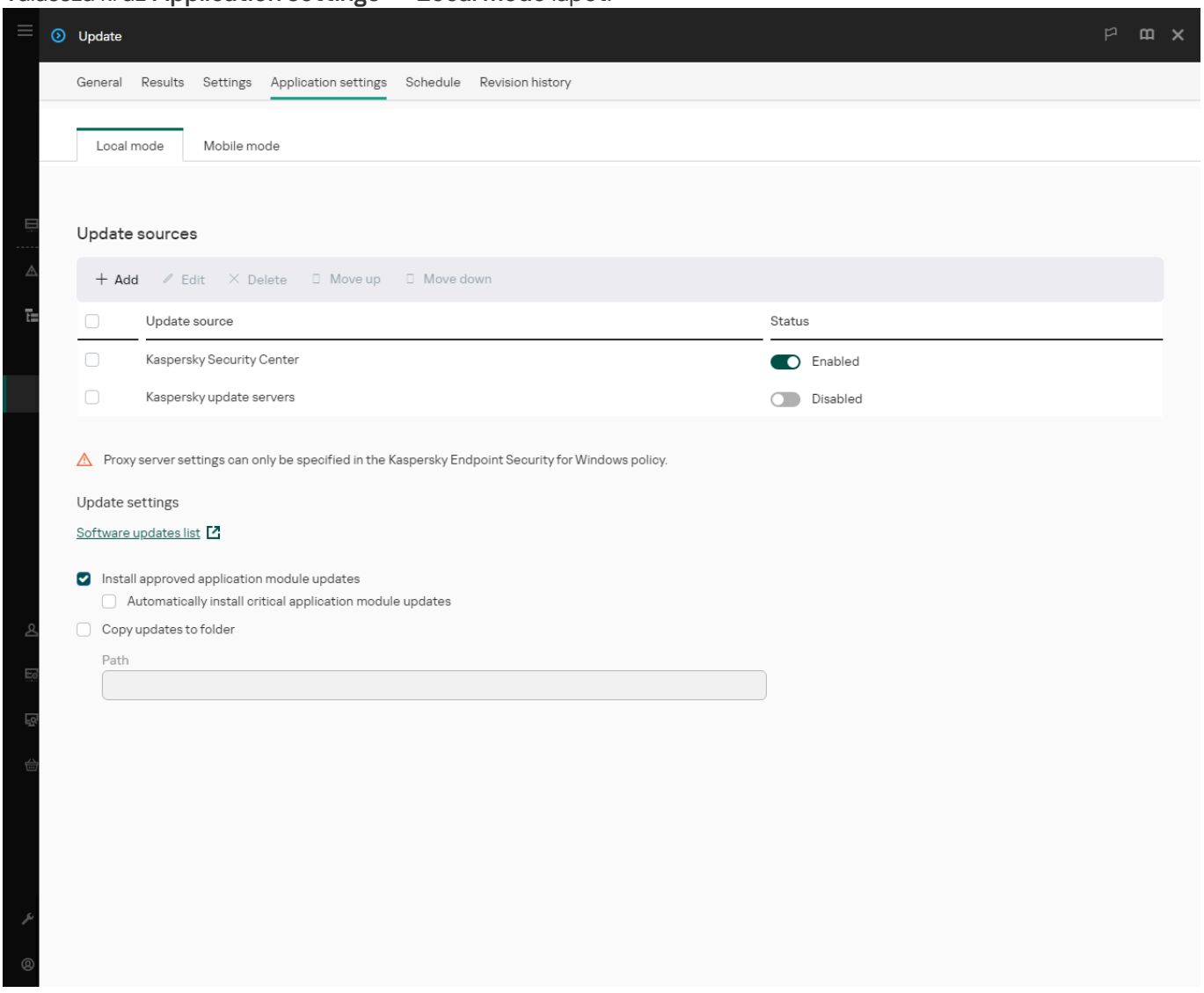
   Megnyílik a feladatok listája.

2. Kattintson az **Adatbázisok és alkalmazásmodulok frissítése** feladatra a Kaspersky Endpoint Security alkalmazásban.

   Megnyílik a feladatok tulajdonságai ablak.

   Az *Adatbázisok és alkalmazásmodulok frissítése* feladatot automatikusan létrehozza a Felügyeleti kiszolgáló gyorsindítási varázslója. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows Management Plug-in, miközben futtatja a Varázslót.

3. Válassza ki az **Application settings** → **Local mode** lapot.



Update feladatbeállítások

4. Az **Update settings** területen válassza ki a telepíteni kívánt alkalmazásmodul-frissítéseket:

   - **Install approved application module updates**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security csak akkor telepíti őket, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről. Alapértelmezésben ez a lehetőség van kiválasztva.

   - **Automatically install critical application module updates**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security automatikusan telepíti a létfontosságú frissítéseket, a többit pedig csak akkor, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről.

   Ha meg szeretné akadályozni, hogy az alkalmazásmodul frissítései letöltődjenek, törölje az **Install approved application module updates** és az **Automatically install critical application module updates** négyzetek jelölését, és megtilthatja a helyi feladatok felhasználó általi használatát.

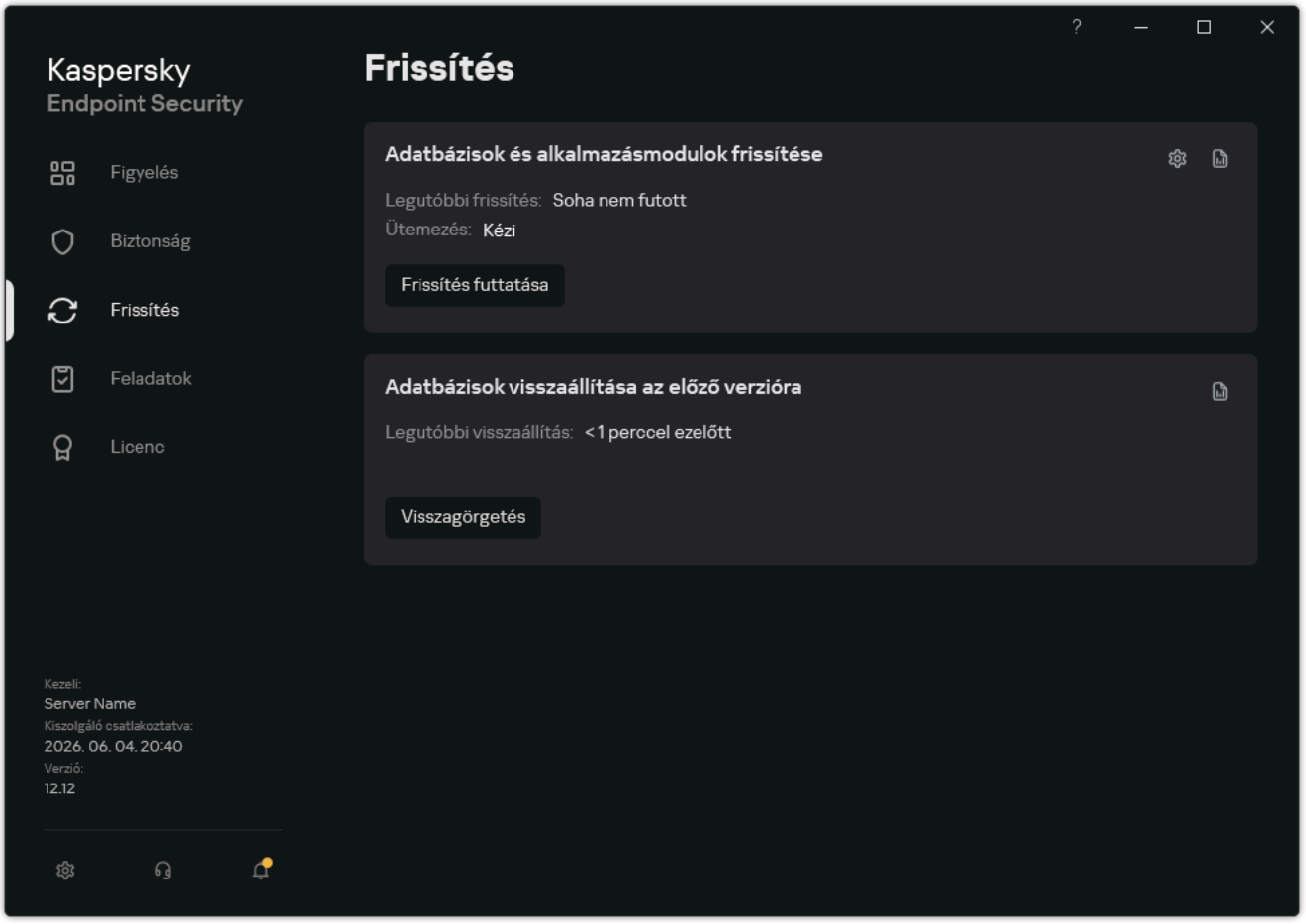
5. Szükség esetén konfigurálja az alkalmazás modulfrissítéseit mobil üzemmódban. A *Mobil mód* a Kaspersky Endpoint Security egy olyan működési módja, ahol a számítógép elhagyja a szervezet hálózatának területét (*offline számítógépek*).

6. Mentse el a módosításokat.

Az alkalmazás modulfrissítéseinek konfigurálása az alkalmazás felületén

Nem konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* csoportfeladatot az alkalmazás felületén. Csak egy helyi frissítési feladat – az *Adatbázisok és alkalmazásmodulok frissítése* – érhető el a felhasználó számára. Ha az *Adatbázisok és alkalmazásmodulok frissítése* feladat nem jelenik meg, az azt jelenti, hogy az adminisztrátor megtiltotta a helyi feladatok használatát a házirendben.

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Ez megnyitja a feladatlistát; válassza ki az *Adatbázisok és alkalmazásmodulok frissítése* feladatot, majd kattintson a ⚙ ikonra.

   Megnyílik a feladatok tulajdonságai ablak.

3. Az **Alkalmazásmodulok frissítéseinek letöltése és telepítése** blokkban jelölje be az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzetet.

4. Válassza ki a telepíteni kívánt alkalmazás modulfrissítéseket.

   - **Kritikus és jóváhagyott frissítések telepítése**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security automatikusan telepíti a létfontosságú frissítéseket, a többit pedig csak akkor, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről.

   - **Csak jóváhagyott frissítések telepítése**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security csak akkor telepíti őket, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről. Alapértelmezésben ez a lehetőség van kiválasztva.

5. Mentse el a módosításokat.

Proxykiszolgáló használata a frissítésekhez

Lehet, hogy meg kell adnia proxykiszolgáló beállításokat, hogy adatbázist és alkalmazásmodul-frissítéseket töltsön le a frissítési forrásából. Ha több frissítési forrás van, a proxykiszolgáló beállításai minden forráshoz alkalmazva lesznek. Ha nem szükséges proxykiszolgáló bizonyos frissítési forrásokhoz, akkor kikapcsolhatja a használatukat a rendszabály-tulajdonságok. A Kaspersky Endpoint Security a proxykiszolgálók használatával is megpróbál hozzáférni a Kaspersky Security Network alkalmazáshoz és az aktivációs kiszolgálókhoz.

Kapcsolat konfigurálásához, hogy proxykiszolgálón keresztül frissítsen forrásokat:

1. A Web Console főablakában kattintson a(z) ⚙ lehetőségre.

   Megnyílik az Adminisztrációs kiszolgáló tulajdonságok ablak.

2. Nyissa meg a **Configuring internet access** szakaszt.

3. Tegyen jelölést a **Use proxy server** jelölőnégyzetbe.

4. Adja meg a proxykiszolgáló kapcsolat beállításait: proxykiszolgáló cím, port és a hitelesítési beállításai (felhasználónév és jelszó).

5. Mentse el a módosításokat.

A proxykiszolgálók használatának kikapcsolásához bizonyos adminisztrációs csoportok számára:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Network Settings** elemet.

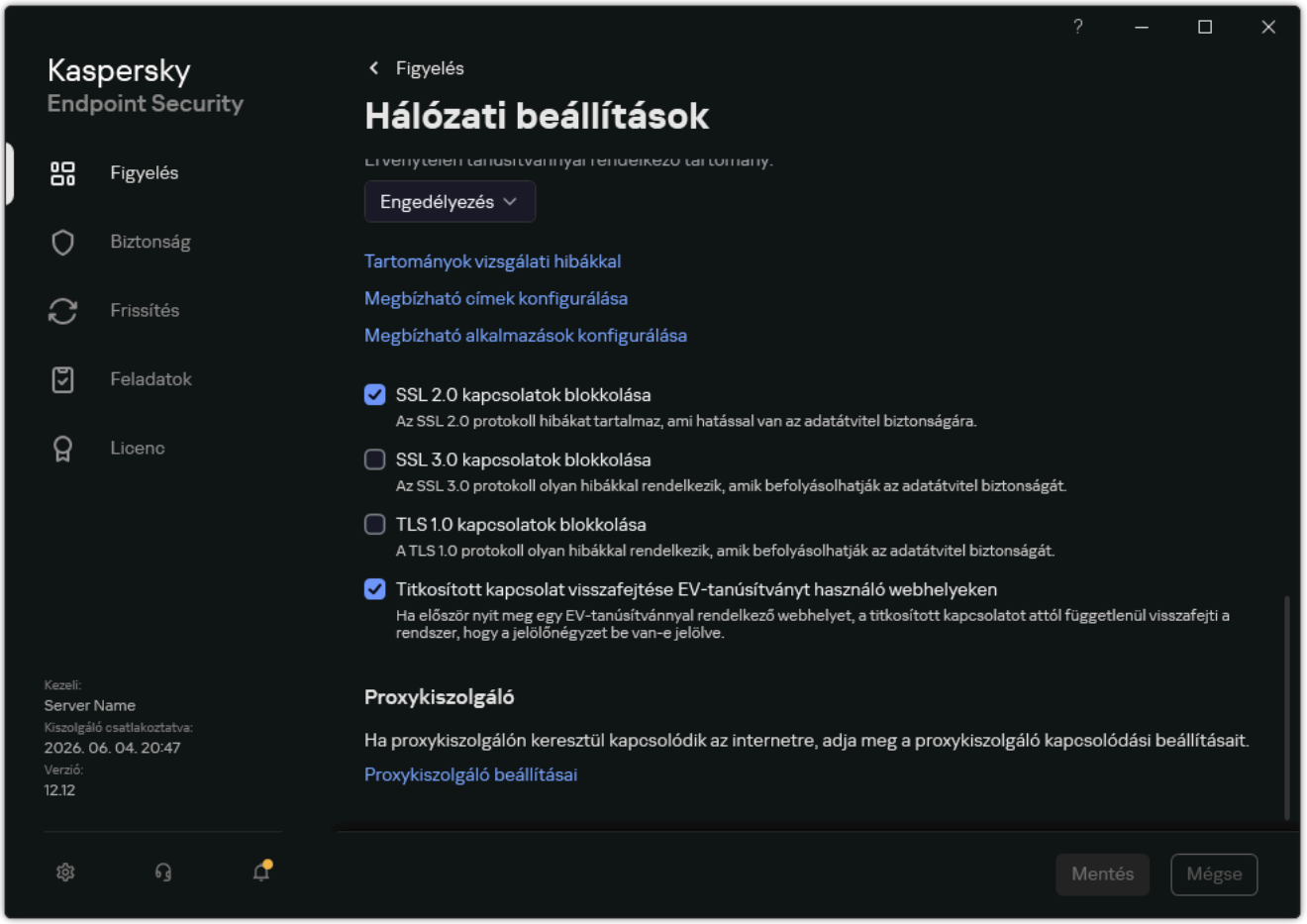
5. A **Proxy server** részen kattintson a **Settings** gombra.

6. A megnyíló ablakban jelölje be a **Bypass a proxy server for local addresses** négyzetet.

7. Mentse el a módosításokat.

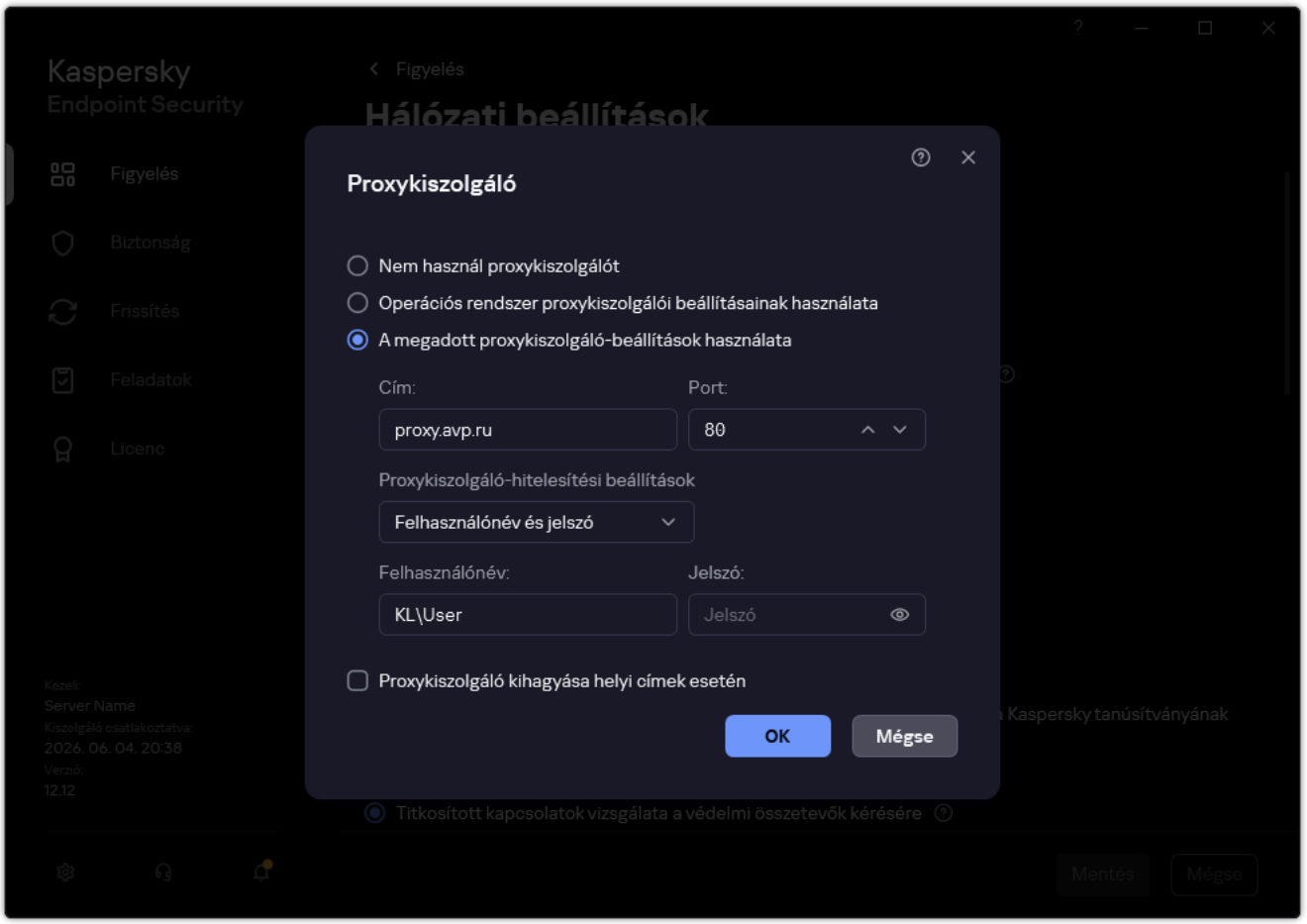
A proxykiszolgáló beállításainak konfigurálása az alkalmazás felületén:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.



Alkalmazások hálózati beállításai

3. A **Proxykiszolgáló** blokkban kattintson a **Proxykiszolgáló beállításai** hivatkozásra.



Proxykiszolgáló csatlakozási beállításai

4. A megnyíló ablakban a proxykiszolgáló címének meghatározása céljából válassza ki az alábbi lehetőségek egyikét:

   - **Az operációs rendszer proxykiszolgáló-beállításainak használata**.

     Alapértelmezésben ez a lehetőség van kiválasztva. A Kaspersky Endpoint Security az operációs rendszer beállításaiban megadott proxykiszolgáló-beállításokat használja.

   - **A megadott proxykiszolgáló-beállítások használata**.

     Ha ezt az opciót választotta, adja meg a proxykiszolgálóhoz való csatlakozás beállításait: proxykiszolgáló címe és portja.

5. Válassza ki, hogy az alkalmazás hogyan végezzen hitelesítést a proxykiszolgálón. Alapértelmezés szerint az alkalmazás az aktuális felhasználó tartományi NTLM hitelesítését használja.

6. Ha le kívánja tiltani a proxykiszolgáló-használatot az adatbázisok és alkalmazásmodulok frissítése közben, ha az megosztott mappából történik, tegyen jelölést a **Proxykiszolgáló kihagyása helyi címek esetén** jelölőnégyzetben.

7. Mentse el a módosításokat.

Ennek eredményeképpen a Kaspersky Endpoint Security a proxykiszolgálót fogja használni az alkalmazásmodul és az adatbázis-frissítések letöltéséhez. A Kaspersky Endpoint Security a proxykiszolgálók használatával is megpróbál hozzáférni a KSN alkalmazáshoz és a Kaspersky aktiváló kiszolgálókhoz. Ha a proxykiszolgálón hitelesítésre van szükség, de a felhasználói fiók hitelesítő adatai nem lettek megadva vagy hibásak, a Kaspersky Endpoint Security kérni fogja a felhasználónevet és a jelszót.

Utolsó frissítés visszagörgetése

Az adatbázisok és alkalmazásmodulok első frissítése után elérhetővé válik az adatbázisok és az alkalmazásmodulok korábbi verzióinak visszagörgetésére szolgáló funkció.

A frissítési folyamat minden egyes indításakor a Kaspersky Endpoint Security biztonsági mentést készít az aktuális adatbázisokról és alkalmazásmodulokról. Ennek köszönhetően szükség esetén az adatbázisokat és az alkalmazásmodulokat vissza lehet görgetni korábbi verziójukra. A legutóbbi frissítés visszagörgetése például akkor hasznos, ha egy új adatbázis-verzió téves riasztást okoz, aminek következtében a Kaspersky Endpoint Security blokkol egy biztonságos alkalmazást.

A Kaspersky Endpoint Security Light Agent üzemmódban nem támogatja a *Frissítés visszaállítása* feladatot.

Az utolsó frissítés visszaállítása az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

1. Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Frissítés visszaállítása** elemet.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. lépés Feladatindítási ütemezés konfigurálása

Konfigurálja a feladat ütemezését, például manuálisan.

4. lépés A feladat nevének megadása

Adja meg a feladat nevét.

7. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Az utolsó frissítés visszaállítása a Web Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Update rollback** lehetőséget.

   c. A(z) **Task name** mezőben adjon meg egy rövid leírást (például: *Frissítés visszaállítása*).

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

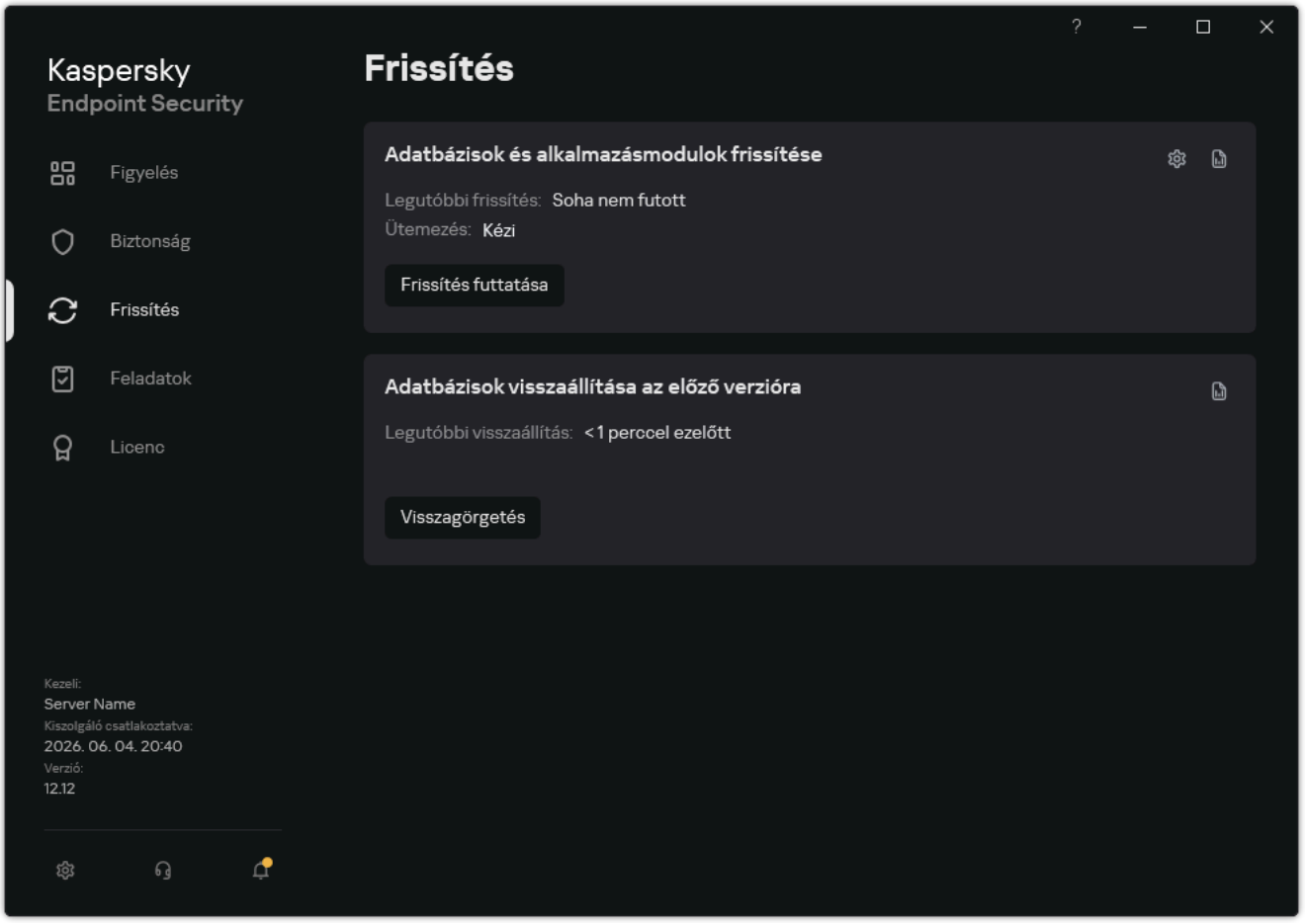
7. Egy új feladat jelenik meg a feladatok listájában.

8. Válassza ki a feladat melletti jelölőnégyzetet.

9. Kattintson az **Start** gombra.

Az utolsó frissítés visszaállítása az alkalmazás felületén

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.



Helyi frissítési feladatok

2. Az **Adatbázisok visszaállítása az előző verzióra** csempén kattintson a **Visszagörgetés** gombra.

A Kaspersky Endpoint Security megkezdi az utolsó adatbázisfrissítés visszagörgetését. Az alkalmazás megjeleníti a visszagörgetés előrehaladását, a letöltött fájlok méretét és a frissítésforrást. A feladatot bármikor leállíthatja a **Frissítés leállítása** gombra kattintva.

Fejlett vírusmentesítő technológia

Az aktív fenyegetések kezeléséhez a Kaspersky Endpoint Security a Fejlett vírusmentesítő technológiát használja. A Fejlett vírusmentesítés másként működik munkaállomásokon és kiszolgálókon. A fejlett vírusmentesítést a *Kártevő vizsgálata* feladat beállításaiban és az alkalmazásbeállításokban konfigurálhatja.

Ha a Kaspersky Endpoint Security nem tudja leállítani egy rosszindulatú program futtatását, használhatja a Fejlett vírusmentesítő technológiát. A szabályzat hatálya alá tartozó számítógépek esetében a Fejlett vírusmentesítés alapértelmezés szerint ki van kapcsolva, mivel ez a technológia jelentős mértékű számítógép-erőforrást használ fel. A szabályzat hatálya alá nem tartozó számítógépeken alapértelmezés szerint a Fejlett vírusmentesítés engedélyezve van.

A Fejlett vírusmentesítés másként működik munkaállomásokon és kiszolgálókon. A technológia kiszolgálókon történő használatához engedélyeznie kell az azonnali fejlett vírusmentesítést a *Kártevő vizsgálata* feladat tulajdonságaiban. Ez az előfeltétel nem szükséges a technológia munkaállomásokon történő használatához.

A Fejlett vírusmentesítő technológia engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. Az **Általános** részen a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le a Fejlett vírusmentesítő technológiát.
5. Mentse el a módosításokat.

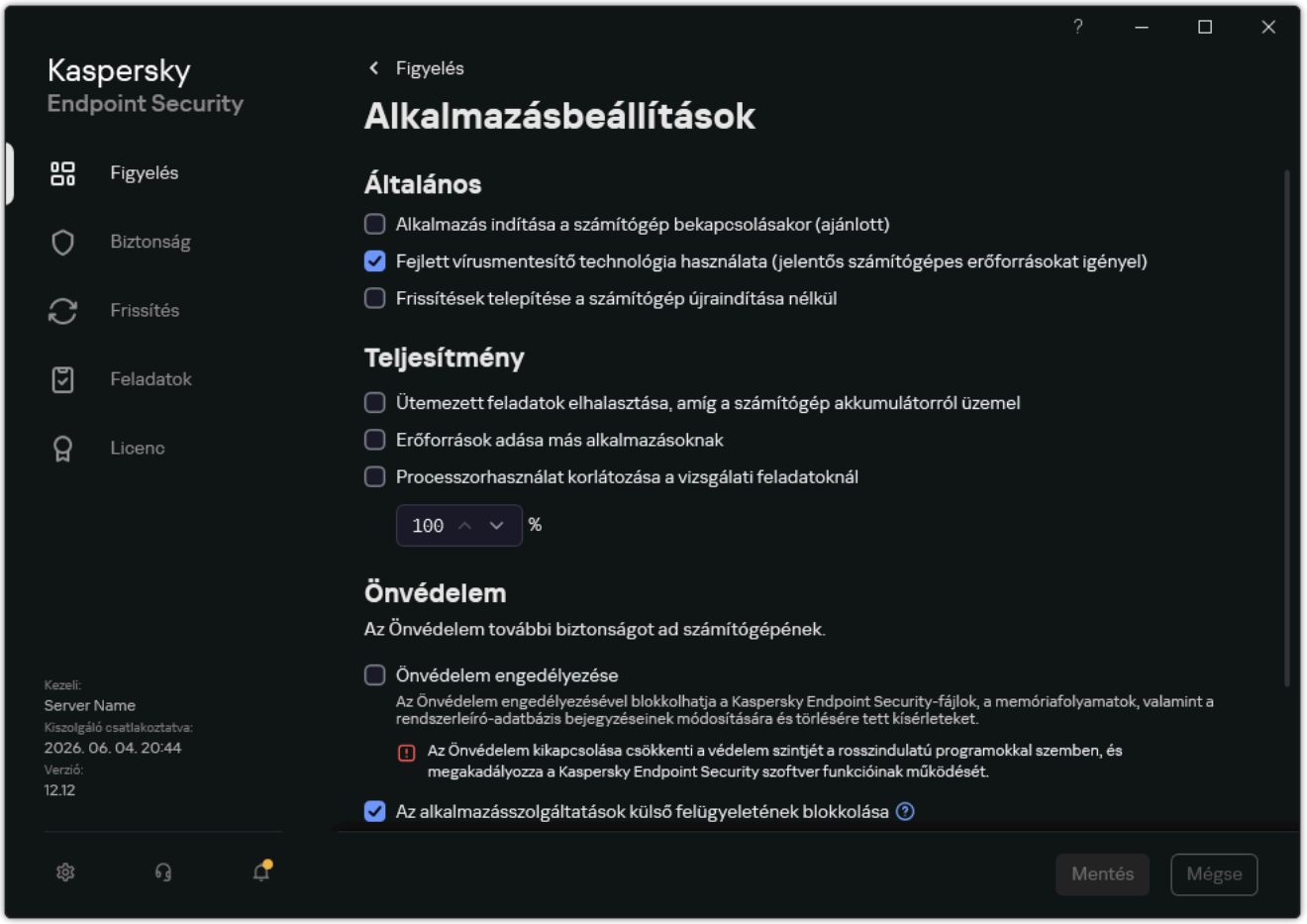
A Fejlett vírusmentesítő technológia engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Válassza az **General Settings** → **Detection Settings** lehetőséget.
5. A(z) **Advanced Disinfection Technology** területen kapcsolja be vagy ki a(z) **Advanced Disinfection Technology ENABLED** kapcsolót a Fejlett vírusmentesítő technológia engedélyezéséhez vagy letiltásához.
6. Mentse el a módosításokat.

A Fejlett vírusmentesítő technológia engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

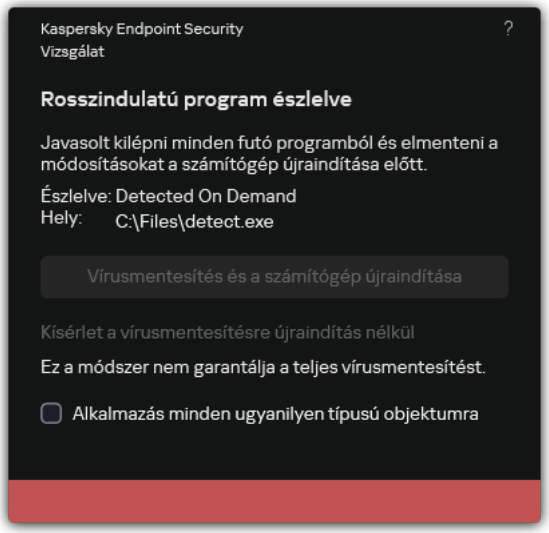
3. Az **Általános** részen a **Fejlett vírusmentesítő technológia használata (jelentős számítógépes erőforrásokat igényel)** jelölőnégyzet bejelölésével vagy a jelölés törlésével engedélyezze vagy tiltsa le a Fejlett vírusmentesítő technológiát.
4. Mentse el a módosításokat.

Ennek eredményeként a felhasználó nem tudja használni az operációs rendszer legtöbb funkcióját, miközben a Fejlett vírusmentesítés folyamatban van. A vírusmentesítés befejezése után a számítógép újraindul.

Aktív fenyegetések vírusmentesítése munkaállomásokon

Ha munkaállomásokon szeretne kezelni aktív fenyegetéseket, engedélyezze a Fejlett vírusmentesítő technológiát az alkalmazásbeállításokban. Ezután konfigurálja a felhasználói élményt a *Kártevő vizsgálata* feladat tulajdonságaiban. A feladat tulajdonságaiban található a **Fejlett vírusmentesítés futtatása azonnal** jelölőnégyzet. Ha a jelölő be van állítva, a Kaspersky Endpoint Security a felhasználó értesítése nélkül végzi a vírusmentesítést. A vírusmentesítés befejezése után a számítógép újraindul. Ha a jelölő nincs beállítva, a Kaspersky Endpoint Security értesítést jelenít meg az aktív fenyegetésekről (lásd az alábbi ábrát). Az értesítést nem lehet bezárni a fájl feldolgozása nélkül.

A Fejlett vírusmentesítés csak akkor van alkalmazva a vírusvizsgálat alatt, ha a Fejlett vírusmentesítés funkció engedélyezve van a számítógépen alkalmazott irányelv tulajdonságaiban.



Értesítés aktív fenyegetésről

Az aktív fenyegetések vírusmentesítése a kiszolgálókon

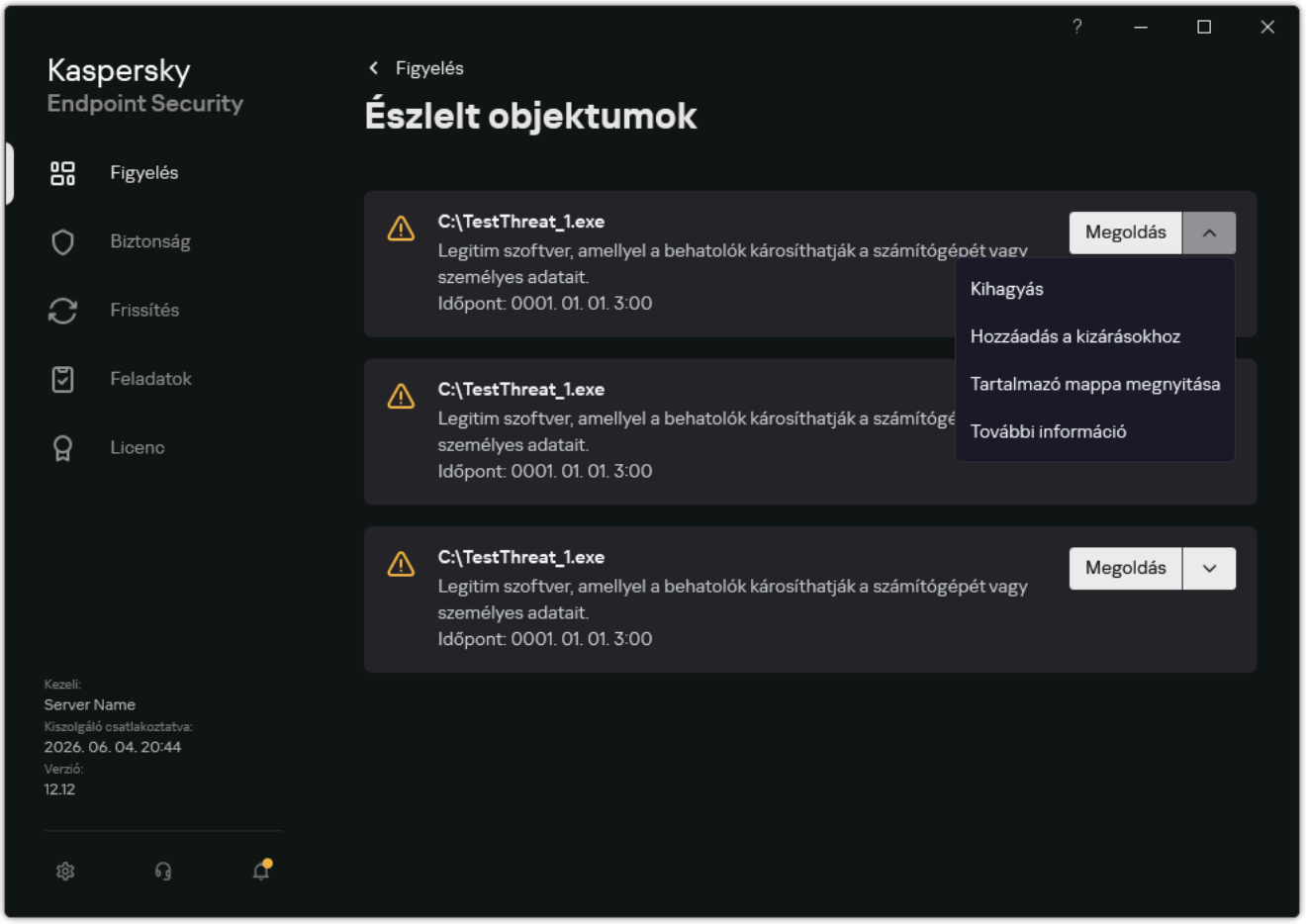
A kiszolgálókon lévő aktív fenyegetések kezeléséhez a következőket kell tennie:

- engedélyezze a Fejlett vírusmentesítő technológiát az alkalmazás beállításaiban;
- engedélyezze az azonnali fejlett vírusmentesítést a *Kártevő vizsgálata* feladat tulajdonságaiban.

Ha a Kaspersky Endpoint Security alkalmazás Windows for Servers operációs rendszert futtató számítógépre van telepítve, a Kaspersky Endpoint Security nem jeleníti meg az értesítést. Ezért Ön nem választhatja ki az aktív fenyegetés vírusmentesítésére szolgáló műveletet. A fenyegetések vírusmentesítéséhez engedélyeznie kell a fejlett vírusmentesítő technológiát az alkalmazásbeállításokban, és engedélyeznie kell az azonnali fejlett vírusmentesítést a *Kártevő vizsgálata* feladat beállításaiban. Ezután el kell indítania a *Kártevő vizsgálata* feladatot.

Feldolgozatlan fenyegetések megszüntetése

Kaspersky Endpoint Security naplózza az olyan fájlokra vonatkozó adatokat, amelyeket valamilyen okból fel nem dolgozott fel. Ezek az adatok az aktív fenyegetések listájára események formájában kerülnek fel (lásd az alábbi ábrát).



Az aktív fenyegetések listája

A fertőzött fájl *feldolgozottnak* tekinthető, ha a Kaspersky Endpoint Security vírusmentesítette a fájlt, vagy eltávolította a fenyegetést, miközben vírusokat és más rosszindulatú programokat keresett a számítógépen.

A Kaspersky Endpoint Security akkor helyezi a fájlt az aktív fenyegetések listájára, ha valamilyen okból nem végzett rajtuk semmilyen műveletet a megadott alkalmazásbeállításoknak megfelelően, miközben a számítógépen vírusok és egyéb fenyegetések jelenlétét vizsgálta.

Ez a helyzet az alábbi esetekben lehetséges:

- A vizsgált fájl nem érhető el (például nem írható hálózati meghajtón vagy cserélhető meghajtón található).
- A *Kártevő vizsgálata* feladat beállításainál a fenyegetésészlelési művelet **Értesítés** állapotra van beállítva. Ezután, amikor a fertőzött fájlról szóló értesítés megjelent a képernyőn, a felhasználó a **Kihagyás** gombot választotta.

Ha vannak feldolgozatlan fenyegetések, a Kaspersky Endpoint Security az ikont a következőre változtatja: . Az alkalmazás főablakában megjelenik a fenyegetésről szóló értesítés (lásd az alábbi ábrát). A Kaspersky Security Center konzolban a számítógép állapota a következőre módosul: *Critical* – .

Fenyegetések feldolgozása a Felügyeleti konzolon

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Advanced** → **Repositories** → **Active threats** mappát.

   Megnyílik az aktív fenyegetések listája.

2. Jelölje ki a feldolgozni kívánt objektumot.

3. Válassza ki, hogyan szeretné kezelni a fenyegetést:

   - **Disinfect**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Delete**. Ha ezt a lehetőséget választja, az alkalmazás törli az észlelt fertőzött fájlokat az aktív fenyegetések tárából. Ebben az esetben az alkalmazás az észlelt fájlt a számítógép memóriájában tárolja. A fenyegetés számítógépről való eltávolításához válassza a **Disinfect**lehetőséget.

Fenyegetések feldolgozása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza az **Operations** → **Repositories** → **Active threats** lehetőséget.

   Megnyílik az aktív fenyegetések listája.

2. Jelölje ki a feldolgozni kívánt objektumot.

3. Válassza ki, hogyan szeretné kezelni a fenyegetést:

   - **Disinfect**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Delete**. Ha ezt a lehetőséget választja, az alkalmazás törli az észlelt fertőzött fájlokat az aktív fenyegetések tárából. Ebben az esetben az alkalmazás az észlelt fájlt a számítógép memóriájában tárolja. A fenyegetés számítógépről való eltávolításához válassza a **Disinfect**lehetőséget.

Fenyegetések feldolgozása az alkalmazás felületén

1. Az alkalmazás főablakának **Monitoring** részén kattintson **Protection is at risk** csempére.

   Megnyílik az aktív fenyegetések listája.

2. Jelölje ki a feldolgozni kívánt objektumot.

3. Válassza ki, hogyan szeretné kezelni a fenyegetést:

   - **Resolve**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Add exclusions**. Ha ezt a műveletet választja, a Kaspersky Endpoint Security javasolja a fájl hozzáadását a vizsgálati kizárások listájához. A kizárás beállításainak konfigurálása automatikusan megtörténik. Ha a kizárás hozzáadása nem érhető el, az azt jelenti, hogy a rendszergazda letiltotta a kizárások hozzáadását a házirend-beállításokban.

   - **Kihagyás**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security törli a bejegyzést az aktív fenyegetések listájáról. Ha nincs több aktív fenyegetés a listán, a számítógép állapota *OK*-ra változik. Ha ismét észleli az objektumot, a Kaspersky Endpoint Security új bejegyzésként adja hozzá az aktív fenyegetések listájához.

- **Tartalmazó mappa megnyitása**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security megnyitja a fájlkezelőben az objektumot tartalmazó mappát. Ezután az kézzel törölhető vagy áthelyezhető egy olyan mappába, ami kívül esik a védelem hatókörén.

- **További információ**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security megnyitja a Kaspersky sebezhetőségek és fenyegetések adatbázis webhelyét.

Az aktív fenyegetések Kaspersky Security Center konzolon történő feldolgozásához engedélyeznie kell a feldolgozatlan fájlokkal kapcsolatos információk átvitelét az adminisztrációs kiszolgálóra. Az adatátvitel alapértelmezés szerint engedélyezve van.

A feldolgozatlan fájladatok átvitelének engedélyezése az Adminisztrációs konzolon (MMC)

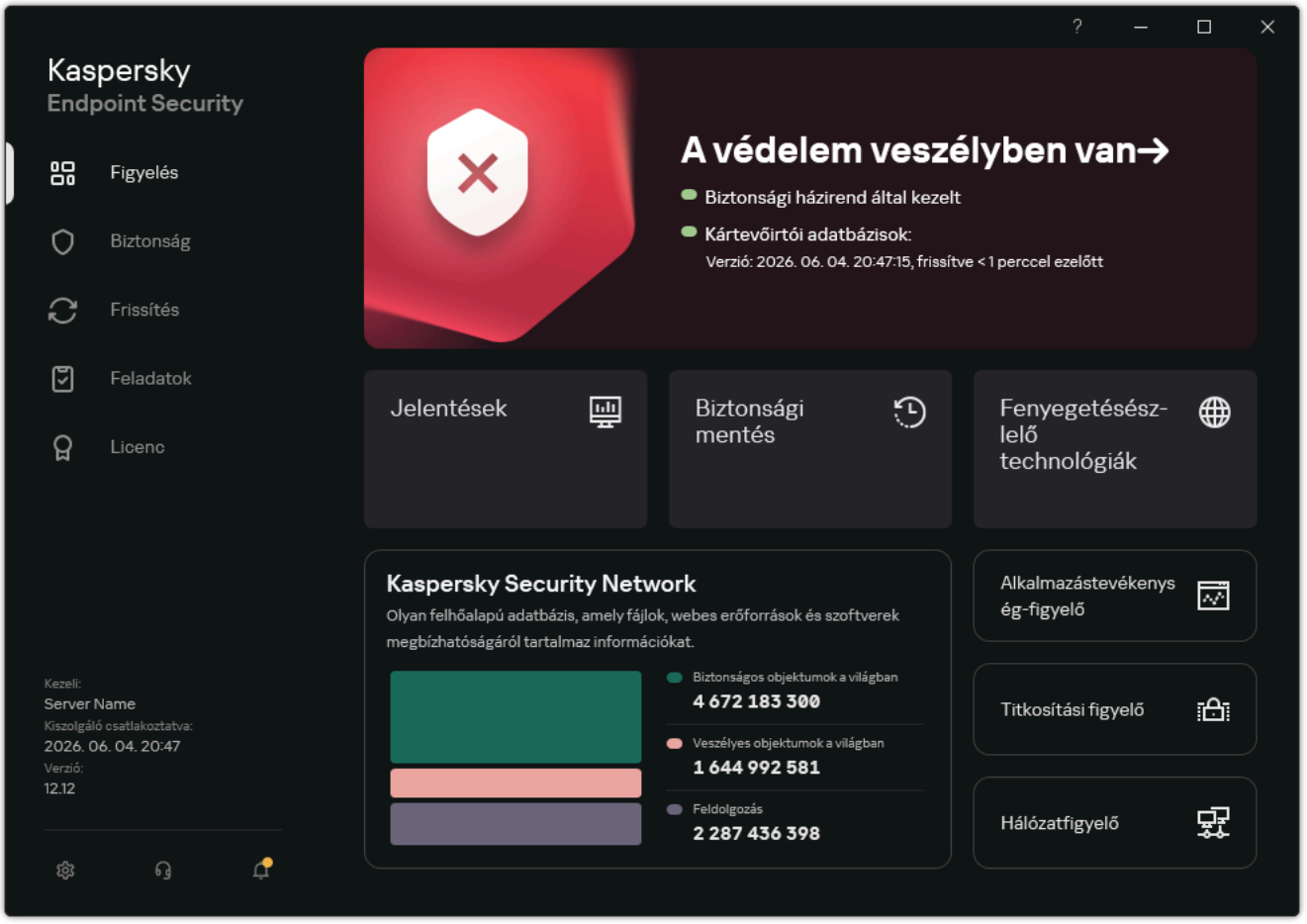
1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirendek ablakában válassza az **Általános beállítások → Jelentések és tároló** lehetőséget.
4. Az **Adatátvitel az adminisztrációs kiszolgálóra** részen kattintson a **Beállítások** gombra.
5. Jelölje be **Feldolgozatlan fájlok** négyzetet.
6. Mentse el a módosításokat.

A feldolgozatlan fájladatok átvitelének engedélyezése a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings → KSC Integration** elemet.

5. A **Data transfer to Administration Server** részen jelölje be az **About unprocessed files** jelölőnégyzetet.

6. Mentse el a módosításokat.



Fő alkalmazásablak fenyegetés észlelésekor

Számítógépvédelem

Fájl védelem

A Fájl védelem összetevő lehetővé teszi a számítógép fájlrendszerében a fertőzések megelőzését. Alapértelmezés szerint a Fájl védelem összetevő állandóan a számítógép RAM-jában található, és valós időben vizsgálja az összes megnyitott, mentett és futtatott fájlt. Ez az összetevő megvizsgálja a számítógép összes meghajtóján lévő fájlokat, beleértve a csatlakoztatott meghajtókat is. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

Az összetevő megvizsgálja a felhasználó és az alkalmazás által elért fájlokat. Ha az alkalmazás kártékony fájlt észlel, a Kaspersky Endpoint Security blokkolja a fájl működését. Az alkalmazás ezután kártevőmentesíti vagy törli a kártékony fájlt a „Fájl védelem" összetevő beállításainak megfelelően.

Amikor egy olyan fájlhoz próbál hozzáférni, amelynek tartalma OneDrive felhőalapú tárhelyen található, a Kaspersky Endpoint Security letölti és megvizsgálja a fájl tartalmát.

A Fájl védelem engedélyezése és letiltása

A Fájl védelem összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. A Fájl védelemhez a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezeket az alkalmazásban mentett beállításcsoportokat *biztonsági szinteknek* nevezzük: **magas**, **ajánlott**, **alacsony**. Az **Ajánlott** biztonsági szint beállításai tekinthetők optimálisnak, és a Kaspersky szakértői is ezeket ajánlják (lásd az alábbi táblázatot). Kiválaszthatja az előre beállított biztonsági szintek egyikét, de kézileg is megadhatja a beállításokat. Ha módosítja a biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.

A Fájlvédelem összetevő a más alkalmazás-összetevőktől kapott adatokat használja fel. Ezen összetevők engedélyezése opcionális. A további adatokat szolgáltató összetevők a következők:

- Kaspersky Security Network.
- Behatolásmegelőző rendszer.
- Viselkedésészlelés.

A Fájl védelem összetevő engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Fájl védelem** lehetőséget.
4. A **Fájl védelem** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.

5. Ha engedélyezte az összetevőt, tegye az alábbiak egyikét a **Biztonsági szint** részben:

   - Ha valamelyik előtelepített biztonsági szintet szeretné alkalmazni, válassza ki a csúszkával:

     - **Magas**. A Fájl védelem összetevő ennél a fájlbiztonsági szintnél ellenőrzi a legszigorúbban a megnyitott, mentett és elindított fájlokat. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján lévő összes fájltípust megvizsgálja. Ezenkívül vizsgálja az archívumokat, a telepítőcsomagokat és a beágyazott OLE-objektumokat is.

     - **Ajánlott**. A Kaspersky Lab szakértői ezt a fájlbiztonsági szintet ajánlják. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján csak a megadott fájlformátumokat és a beágyazott OLE objektumokat vizsgálja meg. A Fájl védelem összetevő nem vizsgálja az archívumokat és a telepítőcsomagokat.

     - **Alacsony**. E fájlbiztonsági szint beállításai biztosítják a maximális vizsgálati sebességet. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján csak a megadott kiterjesztésű fájlokat vizsgálja meg. A Fájl védelem összetevő nem vizsgálja az összetett fájlokat.

   - Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, és adja meg a saját összetevőbeállításait.

     Az előre beállított biztonsági szintek értékeit az **Alapértelmezett** gombra kattintva állíthatja vissza.

6. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a rosszindulatú objektumokon végez:

   - **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés sikertelen, az alkalmazás blokkolja a fájlt.

   - **Blokkolás**. Ha ezt a beállítást választja, az alkalmazás automatikusan blokkolja a fertőzött fájlt anélkül, hogy megpróbálná vírusmentesíteni vagy törölni azt.

   - **Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.

   Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, az alkalmazás létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.

7. Mentse el a módosításokat.

A Fájl védelem összetevő engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Navigáljon ide: **Host Threat Protection** → **File Threat Protection**.

5. A **File Threat Protection ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Ha egy új objektumot szeretne hozzáadni a védelem hatóköréhez:

   a. A **Advanced settings** területen válassza a **Protection scope** lapot.

   b. Kattintson az **Add** gombra.

   c. A megnyíló ablakban válassza ki azokat az objektumokat, amelyeket hozzá kíván adni a vizsgálat hatóköréhez.

   maszkok használata:

   - A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

   - Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

   - A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

   A maszkokat bárhol használhatja a fájl vagy mappa elérési útjában. Ha például a vizsgálat hatókörét szeretné kiterjeszteni a számítógépen található összes felhasználói fiók Letöltések mappájára, írja be a `C:\Users\*\Downloads\` maszkot.

   Egy objektumot anélkül is kizárhat a védelemből, hogy eltávolítaná azt a védelem hatókörébe tartozó objektumok listájáról. Ehhez állítsa a mellette lévő kapcsolót kikapcsolt helyzetbe.

   d. Mentse el a módosításokat.

7. Válassza ki a **Action on threat detection** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a rosszindulatú objektumokon végez:

   - **Disinfect, delete if disinfection fails**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Disinfect, block if disinfection fails**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés sikertelen, az alkalmazás blokkolja a fájlt.

   - **Block**. Ha ezt a beállítást választja, az alkalmazás automatikusan blokkolja a fertőzött fájlt anélkül, hogy megpróbálná vírusmentesíteni vagy törölni azt.

   Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, az alkalmazás létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.

8. Ha szükséges, szerkessze a Fájl védelem speciális beállításait.

9. Mentse el a módosításokat.

A Fájl védelem összetevő engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.

3. A **Fájl védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Ha engedélyezte az összetevőt, tegye az alábbiak egyikét a **Biztonsági szint** részben:

   - Ha valamelyik előtelepített biztonsági szintet szeretné alkalmazni, válassza ki a csúszkával:

     - **Magas**. A Fájl védelem összetevő ennél a fájlbiztonsági szintnél ellenőrzi a legszigorúbban a megnyitott, mentett és elindított fájlokat. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján lévő összes fájltípust megvizsgálja. Ezenkívül vizsgálja az archívumokat, a telepítőcsomagokat és a beágyazott OLE-objektumokat is.

     - **Ajánlott**. A Kaspersky Lab szakértői ezt a fájlbiztonsági szintet ajánlják. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján csak a megadott fájlformátumokat és a beágyazott OLE objektumokat vizsgálja meg. A Fájl védelem összetevő nem vizsgálja az archívumokat és a telepítőcsomagokat.

     - **Alacsony**. E fájlbiztonsági szint beállításai biztosítják a maximális vizsgálati sebességet. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján csak a megadott kiterjesztésű fájlokat vizsgálja meg. A Fájl védelem összetevő nem vizsgálja az összetett fájlokat.

   - Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Speciális beállítások** gombra, és adja meg a saját összetevői beállításokat.

     Az előre beállított biztonsági szintek értékeit az **Ajánlott biztonsági szint visszaállítása** gombra kattintva állíthatja vissza.

5. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a rosszindulatú objektumokon végez:

   - **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés sikertelen, az alkalmazás blokkolja a fájlt.

   - **Blokkolás**. Ha ezt a beállítást választja, az alkalmazás automatikusan blokkolja a fertőzött fájlt anélkül, hogy megpróbálná vírusmentesíteni vagy törölni azt.

   - **Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.

Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, az alkalmazás létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.

6. Mentse el a módosításokat.

A Fájl védelem Kaspersky szakértői által ajánlott beállításai (ajánlott biztonsági szint)

Paraméter	Érték	Leírás
Fájltípusok	**Formátum alapján vizsgált fájlok**	Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejlécet a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres.
Heurisztikus elemzés	**Egyszerű vizsgálat**	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
Csak új és módosult fájlok vizsgálata	**Be**	Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.
Használja az iSwift technológiát	**Be**	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.
Használja az iChecker technológiát	**Be**	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).
Microsoft Office formátumú fájlok vizsgálata	**Be**	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.
E-mail formátumú fájlok vizsgálata	**Be**	E-mail formátumú fájlok vizsgálata. Az alkalmazás megvizsgálja az MSG és EML típusú fájlokat. Az e-mail formátumú fájlok az OLE-objektumokat és MHT-fájlokat is magukban foglalják. A Kaspersky Endpoint Security megvizsgálja az archívumokból kibontott, 1 MB-nál kisebb, e-mail formátumú fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.
Vizsgálat módja	**Intelligens mód**	Ebben a módban a Fájl védelem az objektumot az azon végzett műveletek elemzése alapján vizsgálja meg. Ha például egy Microsoft Office dokumentummal dolgozik, a Kaspersky Endpoint Security a fájlt első megnyitásakor és utolsó bezárásakor vizsgálja meg. A fájlt felülíró köztes műveletek nem váltanak ki vizsgálatot.
Művelet fenyegetés észlelésekor	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**	Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

A Fájl védelem automatikus szüneteltetése

Beállíthatja, hogy a Fájl védelem automatikusan szüneteltesse működését egy megadott időpontban, illetve adott alkalmazások kezelésekor.

A Fájl védelem szüneteltetését csak végső megoldásként szabad igénybe venni, ha alkalmazásokkal ütközik. Ha bármilyen ütközés lép fel egy összetevő futása közben, javasolt felvenni a kapcsolatot a Kaspersky Terméktámogatással. A terméktámogatási szakemberek segítséget nyújtanak a Fájl védelem összetevő beállításában, így az más alkalmazásokkal egy időben is futhat a számítógépen.

A Fájl védelem automatikus szüneteltetésének beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. A **Fájl védelem szüneteltetése** blokkban kattintson a **Fájl védelem szüneteltetése** hivatkozásra.
5. A megnyíló ablakban konfigurálja a beállításokat a Fájl védelem szüneteltetéséhez:
   a. Konfiguráljon ütemezést a Fájl védelem automatikus szüneteltetéséhez.
   b. Hozzon létre egy listát azokról az alkalmazásokról, amelyek működésének hatására a Fájl védelem szünetelteti a tevékenységeit.
6. Mentse el a módosításokat.

A Fájl védelem összetevő által fertőzött fájl észlelésekor elvégzett művelet módosítása

Alapértelmezett esetben a Fájl védelem összetevő automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Fájl védelem összetevő törli ezeket.

A Fájl védelem összetevő által fertőzött fájl észlelésekor elvégzett művelet módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.

3. Válassza ki a megfelelő lehetőséget a **Művelet fenyegetés észlelésekor** részben:

   - **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt.

   - **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés sikertelen, az alkalmazás blokkolja a fájlt.

   - **Blokkolás**. Ha ezt a beállítást választja, az alkalmazás automatikusan blokkolja a fertőzött fájlt anélkül, hogy megpróbálná vírusmentesíteni vagy törölni azt.

   Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, az alkalmazás létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.

4. Mentse el a módosításokat.

A Fájl védelem összetevő védelmi hatókörének kialakítása

A védelmi hatókör azon objektumok körére utal, amelyeket az összetevő vizsgál, ha engedélyezve van. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak. A vizsgálandó fájlok helye és típusa a Fájl védelem összetevő védelmi hatókörének tulajdonságai. Alapértelmezés szerint a Fájl védelem összetevő csak a merevlemezekről, cserélhető meghajtókról és hálózati meghajtókról futtatott potenciálisan megfertőzhető fájlokat vizsgálja.

A vizsgálandó fájltípusok kiválasztásakor vegye figyelembe az alábbiakat:

1. Bizonyos formátumok esetében kicsi a valószínűsége annak, hogy a fájl és annak aktiválása rosszindulatú kódot futtat (ilyen például a TXT formátum). Ugyanakkor vannak olyan fájlformátumok (például .exe, .dll), amelyekben végrehajtható kódot található. A végrehajtható kód tartalmazhat olyan fájlformátumokat is, amelyek eredetileg nem erre a célra szolgálnak (ilyen például a DOC formátum). A rosszindulatú kódok behatolásának és aktiválódásának kockázata az ilyen fájloknál magas.

2. Egy behatoló vírust vagy egyéb rosszindulatú alkalmazást küldhet a számítógépre egy olyan végrehajtható fájlban, amely .txt kiterjesztésűre lett átnevezve. Ha a fájlok kiterjesztés alapján történő vizsgálatát választja, az alkalmazás kihagyja az ilyen fájlt a vizsgálatból. Ha a formátum alapján történő vizsgálat van kiválasztva, a Kaspersky Endpoint Security a kiterjesztéstől függetlenül elemzi a fájl fejlécét. Ha ez az elemzés azt jelzi, hogy a fájl formátuma futtatható fájl (például .EXE), akkor az alkalmazás megvizsgálja.

A védelem hatókörének létrehozása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.

3. Kattintson a **Speciális beállítások** elemre.

4. A **Fájltípusok** részben adja meg azokat a fájltípusokat, amelyeket a Fájl védelem összetevőnek meg kell vizsgálnia:

   - **Minden fájl**. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül).

   - **Formátum alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejlécet a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres.

   - **Kiterjesztés alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.

5. Kattintson a **Védelem hatókörének szerkesztése** hivatkozásra.

6. A megnyíló ablakban válassza ki azokat az objektumokat, amelyeket hozzá kíván adni a védelem hatóköréhez vagy ki szeretne zárni abból.

   Az védelem alapértelmezett hatókörébe tartozó objektumokat nem lehet eltávolítani, illetve szerkeszteni.

7. Ha egy új objektumot szeretne hozzáadni a védelem hatóköréhez:

   a. Kattintson **Hozzáadás** gombra.

      A mappafa nyílik meg.

   b. Az **Elérési út** mezőbe írja be a mappa vagy fájl elérési útját.

      maszkok használata:

      - A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

      - Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

      - A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

      A maszkokat bárhol használhatja a fájl vagy mappa elérési útjában. Ha például a vizsgálat hatókörét szeretné kiterjeszteni a számítógépen található összes felhasználói fiók Letöltések mappájára, írja be a `C:\Users\*\Downloads\` maszkot.

      Az **Ez a PC** objektum a számítógép fájlerőforrásainak listáján a következő objektumokat tartalmazza: **Minden merevlemez**, **Minden hálózati meghajtó** és **Minden cserélhető meghajtó**.

   Kizárhat egy objektumot a vizsgálatokból anélkül, hogy törölné azt a vizsgálati hatókörbe tartozó objektumok listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

8. Mentse el a módosításokat.

A vizsgálatmódok használata

A Kaspersky Endpoint Security egy Gépi tanulás és aláírás-elemzés nevű vizsgálati technikát alkalmaz. Az aláírások elemzése során a Kaspersky Endpoint Security az észlelt objektumot egyezteti az adatbázisában lévő bejegyzésekkel. A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.

A védelem hatékonyságának fokozása érdekében használható a heurisztikus elemzés. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.

Heurisztikus elemzés használatának beállítása a Fájl védelem összetevő működése során:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. Ha azt szeretné, hogy az alkalmazás heurisztikus elemzést használjon a fájlfenyegetések elleni védelemhez, jelölje be a **Heurisztikus elemzés** jelölőnégyzetet a **Vizsgálatmódok** blokkban. Ezután állítsa be a csúszkával a heurisztikus elemzés szintjét: **Egyszerű vizsgálat**, **Közepes vizsgálat** vagy **Alapos vizsgálat**.
5. Mentse el a módosításokat.

Vizsgálati technológiák használata a Fájl védelem összetevő működése során

Vizsgálati technológiák használatának beállítása a Fájl védelem összetevő működése során:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.

4. A **Vizsgálati technológiák** blokkban jelölje be a jelölőnégyzeteket azon technológiák neve mellett, amelyeket a fájl védelemhez használni szeretne.

   - **iSwift technológia használata**. Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.

   - **iChecker technológia használata**. Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).

5. Mentse el a módosításokat.

A fájlvizsgálat optimalizálása

Optimalizálhatja a Fájl védelem összetevő által végzett fájlvizsgálatot: csökkentheti a vizsgálat idejét, és növelheti a Kaspersky Endpoint Security működési sebességét. Ez úgy érhető el, hogy az alkalmazás csak az új és a legutóbbi vizsgálat óta megváltozott fájlokat vizsgálja. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.

Engedélyezheti az iChecker és az iSwift technológiák alkalmazását is, melyek oly módon optimalizálják a fájlok vizsgálatának sebességét, hogy kizárják a legutóbbi vizsgálat óta nem módosult fájlokat.

A fájlvizsgálat optimalizálása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.

3. Kattintson a **Speciális beállítások** elemre.

4. Az **Optimalizálás** részen jelölje be a **Csak az új és módosított fájlok vizsgálata** jelölőnégyzetet.

5. Mentse el a módosításokat.

Az összetett fájlok vizsgálata

A vírusok és egyéb rosszindulatú programok álcázásának gyakori módja az összetett fájlokba, pl. archívumokba vagy adatbázisokba történő beágyazás. Az ilyen módon elrejtett vírusok és rosszindulatú programok felismeréséhez az összetett fájlt ki kell csomagolni, ami csökkentheti a vizsgálat sebességét. Korlátozhatja a vizsgálandó összetett fájlok típusát, így felgyorsíthatja a vizsgálatot.

A fertőzött összetett fájl feldolgozásának módszere (vírusmentesítés vagy törlés) a fájl típusától függ.

A Fájl védelem összetevő vírusmentesíti a ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR és ICE formátumokban lévő összetett fájlokat, az összes többi formátumban lévő fájlokat pedig törli (kivéve a levelezési adatbázisokat).

Az összetett fájlok vizsgálatának beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. Adja meg az **Összetett fájlok vizsgálata** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, terjesztőcsomagok, e-mailek vagy Office formátumú fájlok.
5. Ha az új és módosított fájlok vizsgálata le van tiltva, adja meg az egyes összetett fájlok vizsgálati beállításait: az összes ilyen típusú fájlt vagy csak az új fájlokat.

   Ha az új és módosított fájlok vizsgálata engedélyezve van, a Kaspersky Endpoint Security csak az összetett fájlok összes típusának új és módosított fájljait vizsgálja.
6. Konfigurálja az összetett fájlok vizsgálatának speciális beállításait.

   - **Ne csomagoljon ki nagy összetett fájlokat**.

     Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket.

     Ha a négyzet nincs bejelölve, a Kaspersky Endpoint Security mindenfajta méretű összetett fájlt megvizsgál.

     A Kaspersky Endpoint Security az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzet be van-e jelölve.

   - **Összetett fájlok kicsomagolása a háttérben**.

     Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security hozzáférést biztosít az összetett fájlokhoz, amelyek mérete meghaladja a fájlvizsgálatban meghatározott méret értékét. Ilyenkor a Kaspersky Endpoint Security a háttérben csomagolja ki és vizsgálja meg az összetett fájlokat.

     A Kaspersky Endpoint Security csak e fájlok kicsomagolása és vizsgálata után biztosít hozzáférést az ennél kisebb méretű összetett fájlokhoz.

Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security csak akkor biztosít hozzáférést bármilyen méretű fájlhoz, ha kicsomagolta és átvizsgálta a fájlokat.

7. Mentse el a módosításokat.

Vizsgálatmód megváltoztatása

A *Vizsgálat módja* azt a feltételt jelenti, amely elindítja a Fájl védelem összetevő által végrehajtott víruskeresést. A Kaspersky Endpoint Security alapértelmezés szerint okos módban vizsgálja a fájlokat. Ebben a fájlvizsgálati módban a Fájl védelem összetevő azt követően dönt egy fájl vizsgálatáról, hogy elemezte a felhasználó, illetve a felhasználó nevében egy alkalmazás (a bejelentkezéshez használt vagy más felhasználói fiókkal) vagy az operációs rendszer által a fájlon végzett műveleteket. Ha például egy Microsoft Office Word-dokumentummal dolgozik, a Kaspersky Endpoint Security a fájlt első megnyitásakor és utolsó bezárásakor vizsgálja meg. A fájlt felülíró köztes műveletek nem váltanak ki vizsgálatot.

A fájlvizsgálati mód módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. A **Vizsgálat módja** részben válassza ki a kívánt módot:
   - **Intelligens mód**. Ebben a módban a Fájl védelem az objektumot az azon végzett műveletek elemzése alapján vizsgálja meg. Ha például egy Microsoft Office dokumentummal dolgozik, a Kaspersky Endpoint Security a fájlt első megnyitásakor és utolsó bezárásakor vizsgálja meg. A fájlt felülíró köztes műveletek nem váltanak ki vizsgálatot.
   - **Hozzáféréskor és módosításkor**. Ebben a módban a Fájl védelem megnyitási és módosítási kísérletek esetén mindig megvizsgálja az objektumokat.
   - **Hozzáféréskor**. Ebben a módban a Fájl védelem az objektumokat csak a megnyitási kísérletek esetén vizsgálja meg.
   - **Végrehajtáskor**. Ebben a módban a Fájl védelem az objektumokat csak a futtatási kísérletek esetén vizsgálja meg.
5. Mentse el a módosításokat.

Tárolóvizsgálat

A *tároló* egy elszigetelt környezet, amelyben az alkalmazások az operációs rendszerrel való közvetlen interakció nélkül futhatnak. A tárolók használata a következő kockázatokkal jár:

- Előfordulhat, hogy a hackerek a tárolóban található sebezhetőségeket kihasználva feltörhetik a tárolón belüli alkalmazásokat.
- A hackerek a tárolókörnyezet nem biztonságos konfigurációját kihasználva illetéktelenül hozzáférhetnek a számítógépen lévő adatokhoz, vagy megzavarhatják a rendszer integritását.

- Egy tároló elleni sikeres támadás lehetővé teheti a hacker számára, hogy hozzáférjen a számítógépen lévő adatokhoz.
- A hackerek a hálózati sebezhetőségeket kihasználva lehallgathatják a hálózati forgalmat.

A Kaspersky Endpoint Security nem csak a lemezeken, hanem a tárolókon belül is vizsgálja a fájlokat. Vagyis a Kaspersky Endpoint Security egy külső eszköz, amellyel a tárolókon belüli rosszindulatú tevékenységeket lehet észlelni. Ez lehetővé teszi a tárolók teljesítményének fenntartását, és megelőzi a tárolón belüli más alkalmazásokkal való ütközést. A Kaspersky Endpoint Security tárolón belüli telepítése nem támogatott.

A tárolóbiztonság mellett a Kaspersky Endpoint Security lehetővé teszi az alkalmazások tárolókon belüli kezelését is az Alkalmazásfelügyelő használatával. Az Alkalmazásfelügyelő a tárolók esetében ugyanúgy konfigurálható, mint a számítógépre telepített alkalmazások esetében. A Rendszerintegritás-felügyelet tárolókat is támogat.

A tárolókra vonatkozó követelmények

- A tárolónak Docker-tárolónak kell lennie. Más tárolóeszközök nem támogatottak.
- A tárolónak folyamat-elkülönítési üzemmódban kell futnia. A Hyper-V elkülönítési üzemmód nem támogatott.
- A tárolót Windows Server 2016, 2019 vagy 2022 rendszerű kiszolgálón kell elhelyezni (Docker Host).
- A tárolónak tartalmaznia kell egy Windows lemezképet (Docker Image). A Windows 10 és 11 nem támogatott. A Linux rendszerű lemezképek nem támogatottak.

Művelet fenyegetés észlelésekor

Ha a rendszer fenyegetést észlel egy tárolón belül, az alkalmazás alkalmazza a a Fájl védelem összetevőhöz kiválasztott művelet. A Tárolóvizsgálat további beállításokat tartalmaz (tekintse meg az alábbi utasításokat). Ha a rendszer fenyegetést észlel, az alkalmazás blokkolja a rosszindulatú tevékenységet, és végrehajtja a kiválasztott műveletet (például megkísérli az objektum vírusmentesítését). A Kaspersky Endpoint Security le tudja állítani a tárolót, ha az észlelt objektum nem vírusmentesíthető. Alapértelmezés szerint a tároló leállítása funkció le van tiltva.

Tárolók vizsgálatának konfigurálása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** lehetőséget.
4. Kattintson a **Beállítások** gombra.
5. A megnyíló ablakban válassza a **További** lapot.

6. **A Windows-tárolókban végrehajtott fájlműveletek vizsgálata** részen konfigurálja a tárolók vizsgálati beállításait:

   - **A tároló leállítása, ha a vírusmentesítés sikertelen**. Előfordulhat, hogy az alkalmazás nem rendelkezik elegendő olvasási és írási jogosultsággal az észlelt objektumnál. Ebben az esetben az észlelt objektum vírusmentesítése vagy törlése nem lehetséges. Ha ez a jelölőnégyzet be van jelölve, az alkalmazás blokkolja az észlelt objektumot, és leállítja a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás csak az észlelt objektumot blokkolja.

   - **Ne vizsgálja a Windows-tárolókban végrehajtott fájlműveleteket**. Ha ez a négyzet be van jelölve, az alkalmazás csak a tároló indításakor vizsgálja meg a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás folyamatosan, valós időben vizsgálja a tárolót.

7. Mentse el a módosításokat.

Tárolók vizsgálatának konfigurálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Navigáljon ide: **Host Threat Protection** → **File Threat Protection**.

5. A **Advanced settings** területen válassza a **Performance** lapot.

6. A **Scan optimization** részen konfigurálhatja a tárolók vizsgálati beállításait:

   - **Stop container if disinfection fails**. Előfordulhat, hogy az alkalmazás nem rendelkezik elegendő olvasási és írási jogosultsággal az észlelt objektumnál. Ebben az esetben az észlelt objektum vírusmentesítése vagy törlése nem lehetséges. Ha ez a jelölőnégyzet be van jelölve, az alkalmazás blokkolja az észlelt objektumot, és leállítja a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás csak az észlelt objektumot blokkolja.

   - **Do not scan file operations executed in Windows containers**. Ha ez a négyzet be van jelölve, az alkalmazás csak a tároló indításakor vizsgálja meg a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás folyamatosan, valós időben vizsgálja a tárolót.

7. Mentse el a módosításokat.

A tárolók vizsgálatának konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájl védelem** opciót.

3. **A Windows-tárolókban végrehajtott fájlműveletek vizsgálata** részen konfigurálja a tárolók vizsgálati beállításait:

   - **A tároló leállítása, ha a vírusmentesítés sikertelen**. Előfordulhat, hogy az alkalmazás nem rendelkezik elegendő olvasási és írási jogosultsággal az észlelt objektumnál. Ebben az esetben az észlelt objektum vírusmentesítése vagy törlése nem lehetséges. Ha ez a jelölőnégyzet be van jelölve, az alkalmazás blokkolja az észlelt objektumot, és leállítja a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás csak az észlelt objektumot blokkolja.

   - **Ne vizsgálja a Windows-tárolókban végrehajtott fájlműveleteket**. Ha ez a négyzet be van jelölve, az alkalmazás csak a tároló indításakor vizsgálja meg a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás folyamatosan, valós időben vizsgálja a tárolót.

4. Mentse el a módosításokat.

Behatolásmegelőző rendszer

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

A Behatolásmegelőző rendszer összetevő megelőzi, hogy az alkalmazások az operációs rendszerre esetleg veszélyes műveletbe kezdjenek, így felügyelve a hozzáférést az operációs rendszer erőforrásaihoz és a személyes adatokhoz. Az összetevő antivírus adatbázisok és a Kaspersky Security Network felhőszolgáltatás segítségével biztosít védelmet a számítógépnek.

Az összetevő *alkalmazásjogosultságok* használatán keresztül felügyeli az alkalmazások működését. Az alkalmazásjogosultságok a következő hozzáférési paramétereket tartalmazzák:

- hozzáférés az operációs rendszer erőforrásaihoz (például automatikus rendszerindítási beállításokhoz, beállításkulcsokhoz);
- Hozzáférés a személyes adatokhoz (például fájlokhoz és alkalmazásokhoz).

Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

Az alkalmazás első indítása során a „Behatolásmegelőző rendszer” összetevő a következő műveleteket hajtja végre:

1. Ellenőrzi az alkalmazás biztonságát letöltött antivírus adatbázisok segítségével.
2. Ellenőrzi az alkalmazás biztonságát a Kaspersky Security Networkben.

   Javasoljuk, hogy vegyen részt a Kaspersky Security Networkben, amivel eredményesebbé teheti a „Behatolásmegelőző rendszer” összetevő működését is.

3. Az alkalmazást a megbízhatósági csoportok valamelyikébe helyezi: *Megbízható*, *Alacsony korlátozás*, *Magas korlátozás*, *Nem megbízható*.

A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére használ. A Kaspersky Endpoint Security egy alkalmazást az alapján helyez megbízhatósági csoportba, hogy az alkalmazás milyen veszélyességi szintet képvisel a számítógép szempontjából.

A Kaspersky Endpoint Security az alkalmazásokat a Tűzfal és a Behatolásmegelőző rendszer összetevő számára helyezi megbízhatósági csoportba. Nem lehet módosítani a megbízhatósági csoportot kizárólag a Tűzfal vagy a Behatolásmegelőző rendszer esetében.

Ha nem vesz részt a KSN rendszerében vagy nincs hálózat, a Kaspersky Endpoint Security a Behatolásmegelőző rendszer összetevő beállításai alapján helyezi az alkalmazást megbízhatósági csoportba. Miután megérkezett az alkalmazás megítélése a KSN hálózattól, a rendszer automatikusan módosíthatja az alkalmazás megbízhatósági csoportját.

4. Blokkolja az alkalmazás műveleteit a megbízhatósági csoporttól függően. Például a *Magas korlátozás* megbízhatósági csoportba sorolt alkalmazások nem kapnak hozzáférést az operációs rendszer moduljaihoz.

Az alkalmazás következő indításakor a Kaspersky Endpoint Security ellenőrzi annak integritását. Amennyiben az alkalmazás nem változott meg, az összetevő használni fogja a meglevő alkalmazásjogot. Ha az alkalmazás módosult, a Kaspersky Endpoint Security ugyanúgy végigelemzi, mintha az első elindítására kerülne sor.

A Behatolásmegelőző rendszer be- és kikapcsolása

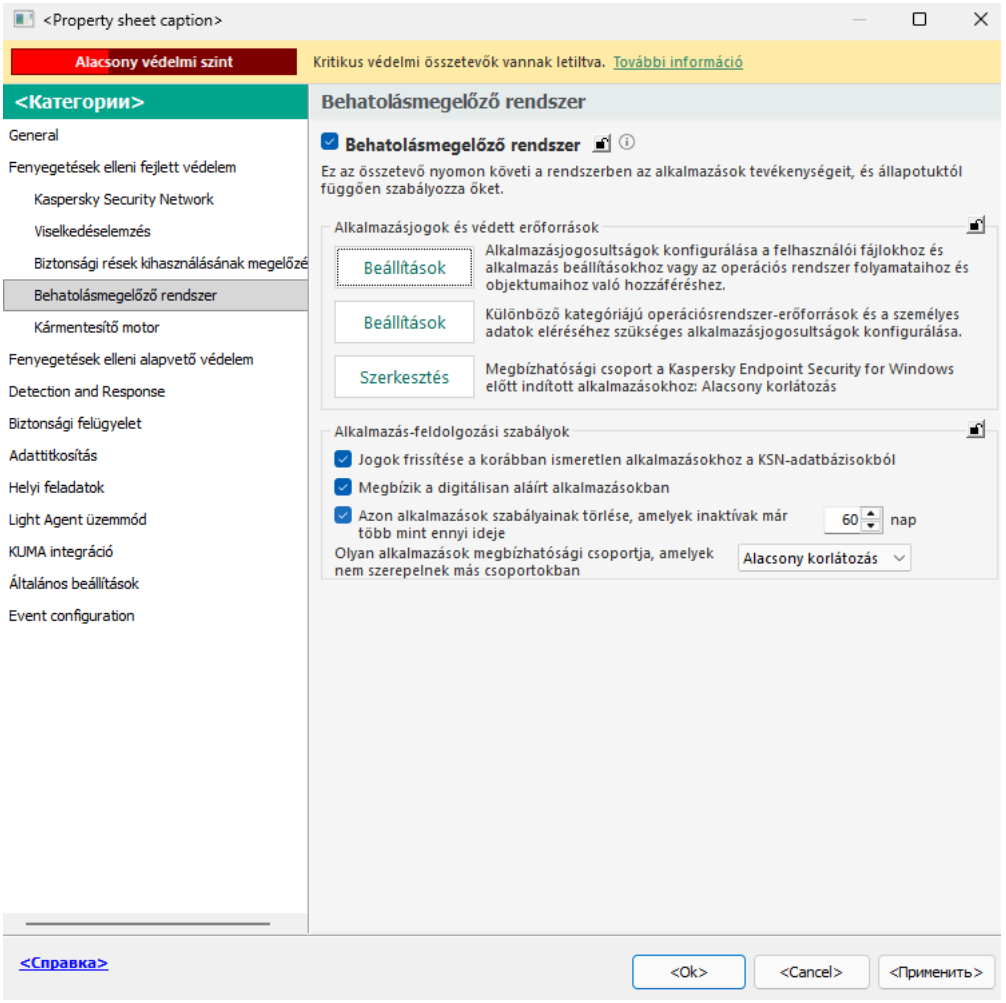
A Behatolásmegelőző rendszer összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik.

A Behatolásmegelőző rendszer összetevő engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. A **Behatolásmegelőző rendszer** jelölőnégyzet használatával engedélyezze vagy tiltsa le az összetevőt.

5. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Behatolásmegelőző rendszer összetevő engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection → Host Intrusion Prevention** elemet.

5. A **Host Intrusion Prevention ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Mentse el a módosításokat.

A Behatolásmegelőző rendszer összetevő engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection → Host Intrusion Prevention** opciót.
3. A **Behatolásmegelőző rendszer** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ha a Behatolásmegelőző rendszer összetevő be van kapcsolva, a Kaspersky Endpoint Security egy alkalmazást az alapján helyez megbízhatósági csoportba, hogy az alkalmazás milyen veszélyességi szintet képvisel a számítógép szempontjából. A Kaspersky Endpoint Security ezután a megbízhatósági csoporttól függően blokkolja az alkalmazás műveleteit.

Az alkalmazások megbízhatósági csoportjainak kezelése

Az egyes alkalmazások első elindulásakor a Behatolásmegelőző rendszer megvizsgálja az adott alkalmazás biztonságát, és besorolja egy megbízhatósági csoportba.

Az alkalmazás vizsgálatának első szakaszában a Kaspersky Endpoint Security rákeres az ismert alkalmazásokat tartalmazó belső adatbázisban az egyező bejegyzésekre, és ugyanakkor kérést küld a Kaspersky Security Network adatbázisának (ha van internetkapcsolat). A belső adatbázisban és a Kaspersky Security Network adatbázisában végzett keresés eredményei alapján az alkalmazás egy megbízhatósági csoportba kerül. Az alkalmazás utólagos indításakor a Kaspersky Endpoint Security minden alkalommal újabb lekérdezést küld a KSN adatbázis részére, és ha az alkalmazás reputációja megváltozott a KSN adatbázisban, más megbízhatósági csoportba helyezi át az alkalmazást.

Kiválaszthat olyan megbízhatósági csoportot, amelybe a Kaspersky Endpoint Security minden ismeretlen alkalmazást automatikusan besorol. A Kaspersky Endpoint Security indítása előtt már futó alkalmazások automatikusan a Behatolásmegelőző rendszer beállításai által beállított megbízhatósági csoportba kerülnek.

A Kaspersky Endpoint Security előtt elindított alkalmazások esetén csak a hálózati tevékenység van felügyelet alatt. A felügyelet a Tűzfal beállításaiban meghatározott hálózati szabályoknak megfelelően történik.

Egy alkalmazás megbízhatósági csoportjának módosítása

Az egyes alkalmazások első elindulásakor a Behatolásmegelőző rendszer megvizsgálja az adott alkalmazás biztonságát, és besorolja egy megbízhatósági csoportba.

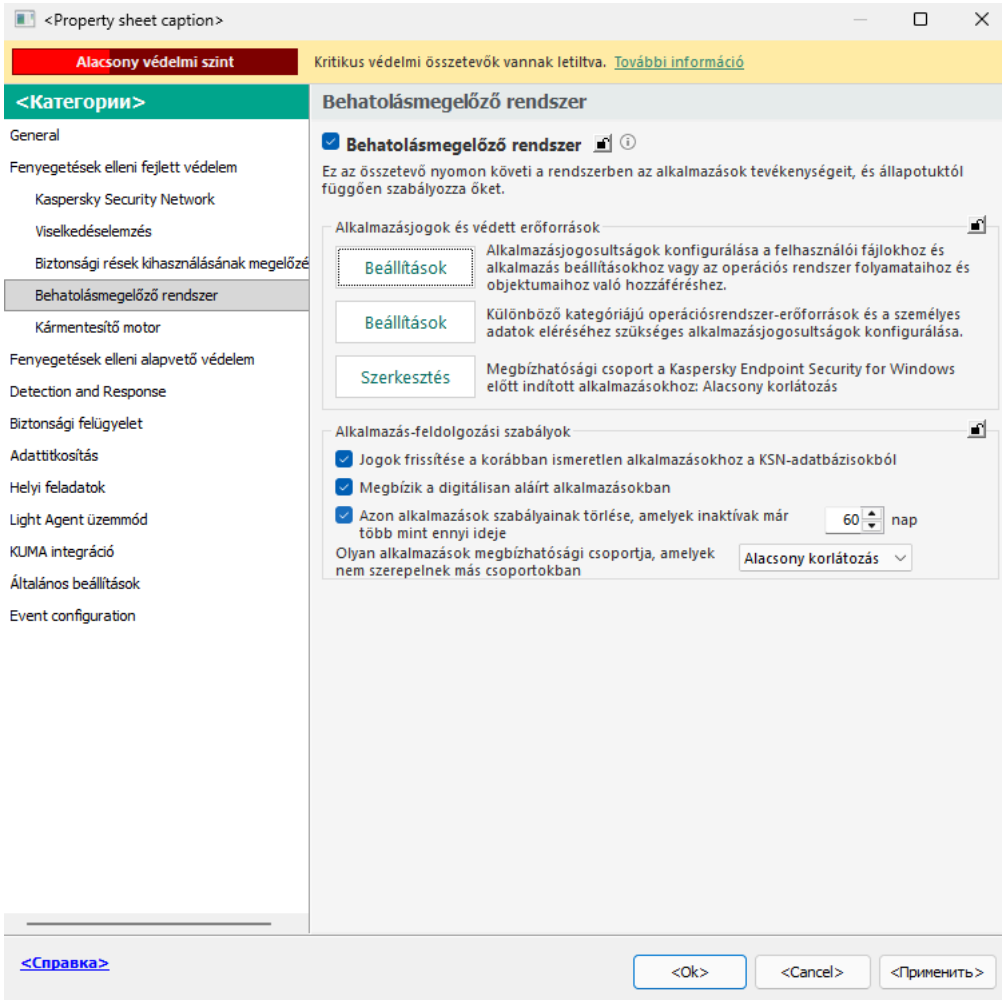
A Kaspersky szakemberei nem javasolják az alkalmazások áthelyezését az automatikusan kiosztott megbízhatósági csoportból másik megbízhatósági csoportba. Ehelyett módosíthatja az egyes alkalmazások jogait, ha szükséges.

Egy alkalmazás megbízhatósági csoportjának módosítása az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

5. Válassza ki az **Application rights** fület.

6. Kattintson **Hozzáadás** gombra.

7. A megnyíló ablakban írja be annak az alkalmazásnak a keresési feltételeit, amelynek megbízhatósági csoportját módosítani kívánja.

   Megadhatja az alkalmazás nevét vagy a gyártó nevét is. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

8. Kattintson a **Frissítés**.

   A Kaspersky Endpoint Security megkeresi az alkalmazást a felügyelt számítógépekre telepített alkalmazások összesített listáján. A Kaspersky Endpoint Security megjeleníti azon alkalmazások listáját, amelyek megfelelnek a keresési feltételeknek.

9. Válassza ki a szükséges alkalmazást.

10. A **Kijelölt alkalmazás hozzáadása a megbízhatósági csoporthoz** legördülő listában válassza ki az alkalmazáshoz szükséges megbízhatósági csoportot.

11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Egy alkalmazás megbízhatósági csoportjának módosítása a Web Console-ban, illetve a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection** → **Host Intrusion Prevention** elemet.

5. A **Application rights and protected resources** részen kattintson a **Application rights and protected resources** hivatkozásra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

6. Válassza ki az **Application rights** lapot.

   Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.

7. Kattintson az **Add** gombra.

   Ezután elindul a varázsló, amellyel hozzáadhat egy alkalmazást egy megbízhatósági csoporthoz.

8. Válassza ki az alkalmazás megfelelő megbízhatósági csoportját.

9. Válassza ki az **Application** típust. Lépjen a következő lépésre.

   Ha több alkalmazás megbízhatósági csoportját szeretné módosítani, válassza ki a **Group** típust, és adjon egy nevet az alkalmazáscsoportnak.

10. Az alkalmazások megnyílt listájában válassza ki azokat az alkalmazásokat, amelyeknél módosítaná a megbízhatósági csoportot.

    Használjon szűrőt. Megadhatja az alkalmazás nevét vagy a gyártó nevét is. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

11. Lépjen ki a varázslóból.

    A rendszer hozzáadja az alkalmazást a megbízhatósági csoporthoz.

12. Mentse el a módosításokat.

Egy alkalmazás megbízhatósági csoportjának módosítása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection** → **Host Intrusion Prevention** opciót.

3. Kattintson az **Alkalmazások kezelése** elemre.

   Ezzel megnyitja a telepített alkalmazások listáját.

4. Válassza ki a szükséges alkalmazást.

5. Az alkalmazás helyi menüjében kattintson a **Korlátozások** → **<megbízhatósági csoport>** elemre.

6. Mentse el a módosításokat.

Ennek eredményeként az alkalmazás a másik megbízhatósági csoportba kerül. A Kaspersky Endpoint Security ezután a megbízhatósági csoporttól függően blokkolja az alkalmazás műveleteit. A *(felhasználó által definiált)* állapot lesz hozzárendelve az alkalmazáshoz. Ha az alkalmazás megbízhatósága változik a Kaspersky Security Networkben, a Behatolásmegelőző rendszer változatlanul hagyja az alkalmazás bizalmi csoportját.

A megbízhatósági csoport jogainak konfigurálása

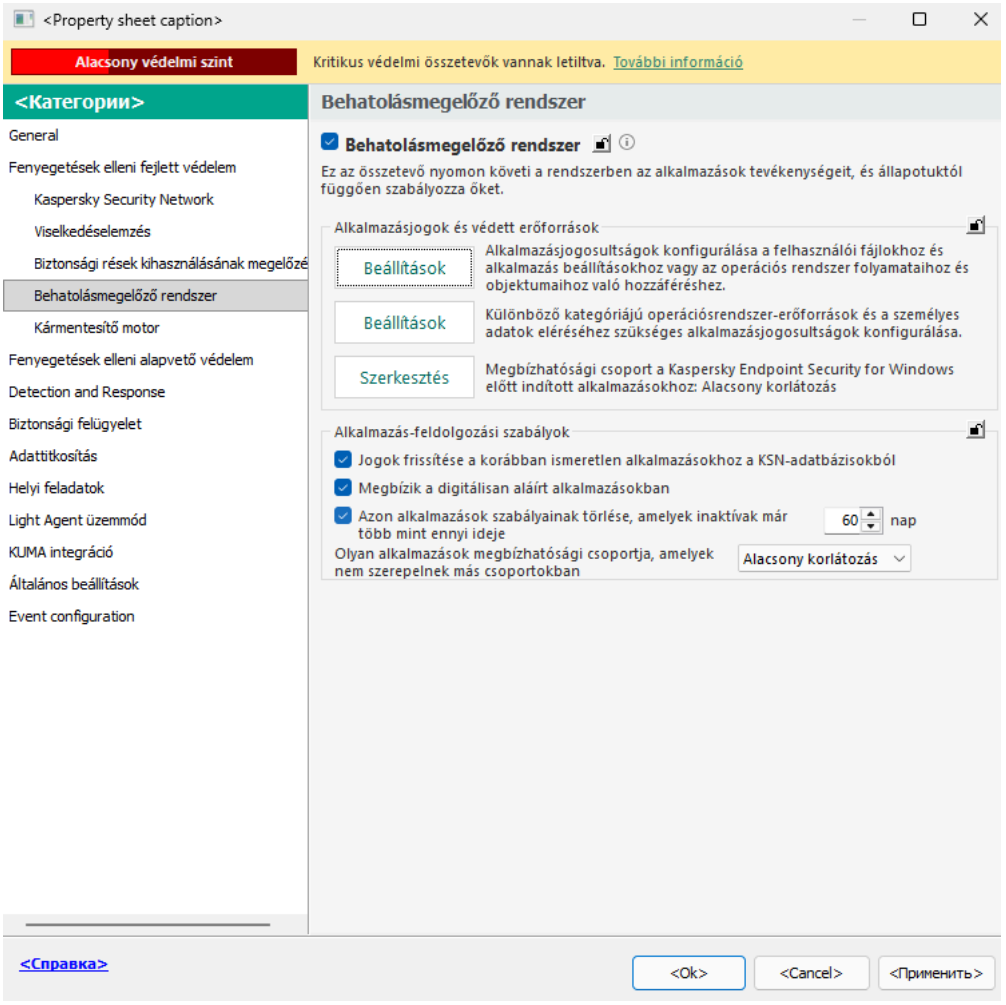
A különböző megbízhatósági csoportok optimális alkalmazásjogai alapértelmezés szerint létrejönnek. A megbízhatósági csoportokban lévő alkalmazáscsoportok jogainak beállításai a megbízhatósági csoportok jogainak beállításainak értékeit öröklik.

Megbízhatósági csoport jogainak módosítása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

5. Nyissa meg az **Alkalmazásjogok** fület.

6. Válassza ki a szükséges megbízhatósági csoportot.

7. A megbízhatósági csoport helyi menüjében válassza ki a **Csoportjogok** elemet.

   Ez megnyitja a megbízhatósági csoport tulajdonságait.

8. Végezze el az alábbiak egyikét:

   - Ha módosítani kívánja az operációs rendszer beállításjegyzékével, a felhasználói fájlokkal és az alkalmazásbeállításokkal végzett műveleteket szabályozó megbízhatósági csoportok jogait, válassza ki a **Fájlok és rendszerleíró adatbázis** lehetőséget.

   - Ha módosítani szeretné az operációs rendszer folyamataihoz és objektumaihoz való hozzáférést szabályozó megbízhatósági csoportok jogait, válassza ki a **Jogok** lapot.

   Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

9. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában, és válassza ki a szükséges lehetőséget: **Öröklés**, **Engedélyezés** (✓) vagy **Blokkolás** (⊘).

10. Ha szeretné figyelemmel követni a számítógép erőforrásainak használatát, válassza ki az **Események naplózása** (✓ / ⊘) lehetőséget.

    A Kaspersky Endpoint Security rögzíti a Behatolásmegelőző rendszer összetevő működésére vonatkozó információkat. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Megbízhatósági csoport jogainak módosítása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection** → **Host Intrusion Prevention** elemet.

5. A **Application rights and protected resources** részen kattintson a **Application rights and protected resources** hivatkozásra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

6. Nyissa meg a **Application rights** lapot.

   Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.

7. Az ablak bal oldalán válassza ki a megfelelő megbízhatósági csoportot.

8. Az ablak jobb oldalán a legördülő listában végezze el a következő műveletek egyikét:

   - Ha módosítani kívánja az operációs rendszer beállításjegyzékével, a felhasználói fájlokkal és az alkalmazásbeállításokkal végzett műveleteket szabályozó megbízhatósági csoportok jogait, válassza ki a **Files and system registry** lehetőséget.
   - Ha módosítani szeretné az operációs rendszer folyamataihoz és objektumaihoz való hozzáférést szabályozó megbízhatósági csoportok jogait, válassza ki a **Rights** lapot.

   Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

9. A megfelelő erőforrás és a megfelelő művelet oszlopában válassza ki a szükséges opciót:**Inherit**, **Allow** ( ) vagy **Block** ( ).

10. Ha szeretné figyelemmel követni a számítógép erőforrásainak használatát, válassza ki az **Log events** (/) lehetőséget.

    A Kaspersky Endpoint Security rögzíti a Behatolásmegelőző rendszer összetevő működésére vonatkozó információkat. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

11. Mentse el a módosításokat.

Megbízhatósági csoport jogainak módosítása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection → Host Intrusion Prevention** opciót.
3. Kattintson az **Alkalmazások kezelése** elemre.

   Ezzel megnyitja a telepített alkalmazások listáját.

4. Válassza ki a szükséges megbízhatósági csoportot.
5. A megbízhatósági csoport helyi menüjében válassza ki a **Részletek és szabályok** elemet.

   Ez megnyitja a megbízhatósági csoport tulajdonságait.

6. Végezze el az alábbiak egyikét:

   - Ha módosítani kívánja az operációs rendszer beállításjegyzékével, a felhasználói fájlokkal és az alkalmazásbeállításokkal végzett műveleteket szabályozó megbízhatósági csoportok jogait, válassza ki a **Fájlok és rendszerleíró adatbázis** lehetőséget.
   - Ha módosítani szeretné az operációs rendszer folyamataihoz és objektumaihoz való hozzáférést szabályozó megbízhatósági csoportok jogait, válassza ki a **Jogok** lapot.

   Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

7. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában, és válassza ki a szükséges lehetőséget: **Öröklés**, **Engedélyezés** ( ) vagy **Tiltás** ( ).

8. Ha szeretné figyelemmel követni a számítógép erőforrásainak használatát, válassza ki az **Események naplózása** (📊) lehetőséget.

   A Kaspersky Endpoint Security rögzíti a Behatolásmegelőző rendszer összetevő működésére vonatkozó információkat. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

9. Mentse el a módosításokat.

A megbízhatósági csoport jogai megváltoznak. A Kaspersky Endpoint Security ezután a megbízhatósági csoporttól függően blokkolja az alkalmazás műveleteit. Az ■ állapot (*Egyéni beállítások*) a megbízhatósági csoporthoz lesz hozzárendelve.

A Kaspersky Endpoint Security előtt indított alkalmazások megbízhatósági csoportjának kiválasztása

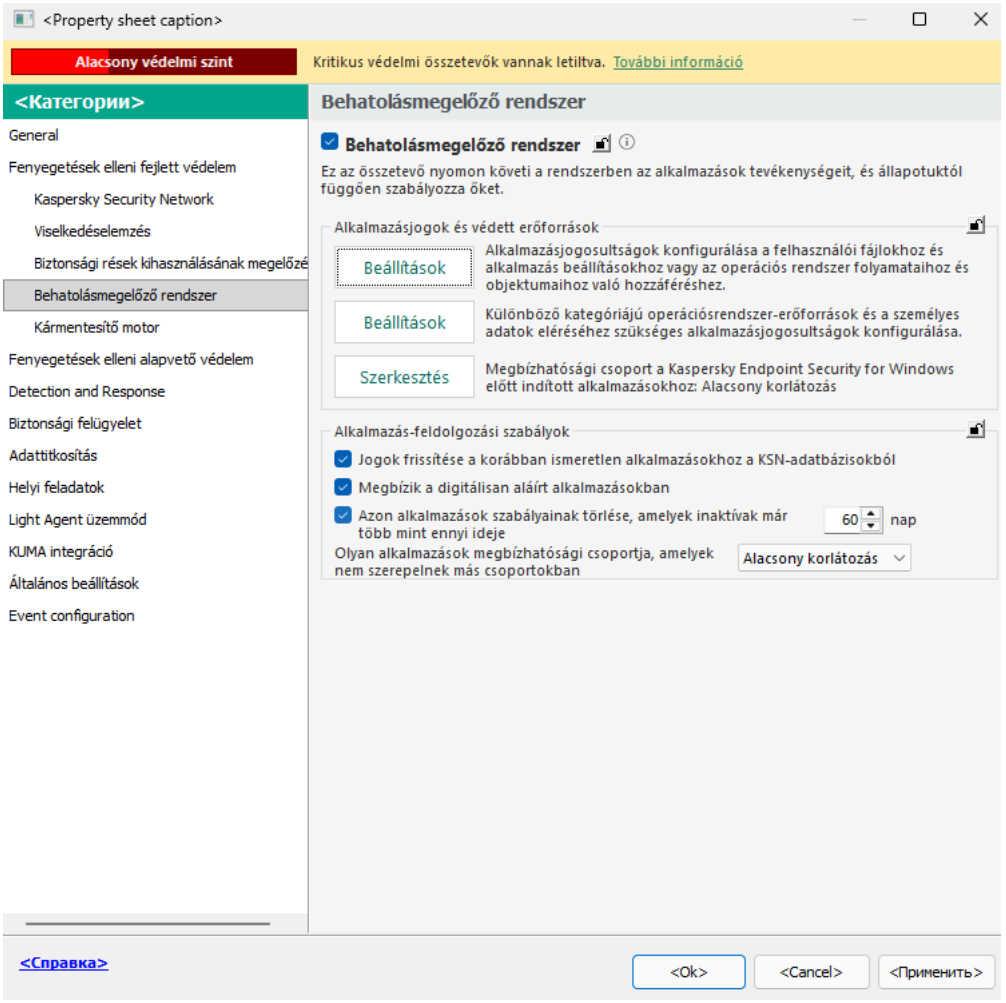
A Kaspersky Endpoint Security előtt elindított alkalmazások esetén csak a hálózati tevékenység van felügyelet alatt. A felügyelet a Tűzfal beállításaiban meghatározott hálózati szabályoknak megfelelően történik. Annak megadásához, hogy az ilyen alkalmazások hálózati tevékenységei figyelésénél melyik hálózati szabályokat kell alkalmazni, ki kell választani egy megbízhatósági csoportot.

Megbízhatósági csoport kiválasztása a Kaspersky Endpoint Security előtt elindított alkalmazásokhoz az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. Az **Alkalmazásjogok és védett erőforrások** részen kattintson a **Szerkesztés** gombra.

5. A(z) **Trust group for applications started before Kaspersky Endpoint Security** beállításhoz válassza ki a megfelelőt megbízhatósági csoportot.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Megbízhatósági csoport kiválasztása a Kaspersky Endpoint Security előtt elindított alkalmazásokhoz a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection → Host Intrusion Prevention** elemet.

5. A(z) **Trust group for applications started before Kaspersky Endpoint Security** beállításhoz válassza ki a megfelelőt megbízhatósági csoportot.

6. Mentse el a módosításokat.

Megbízhatósági csoport kiválasztása a Kaspersky Endpoint Security előtt elindított alkalmazásokhoz az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection → Host Intrusion Prevention** opciót.
3. A **Megbízhatósági csoport a Kaspersky Endpoint Security előtt indított alkalmazásokhoz** részen válassza ki a megfelelő megbízhatósági csoportot.
4. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Endpoint Security előtt elindított alkalmazás bekerül a másik megbízhatósági csoportba. A Kaspersky Endpoint Security ezután a megbízhatósági csoporttól függően blokkolja az alkalmazás műveleteit.

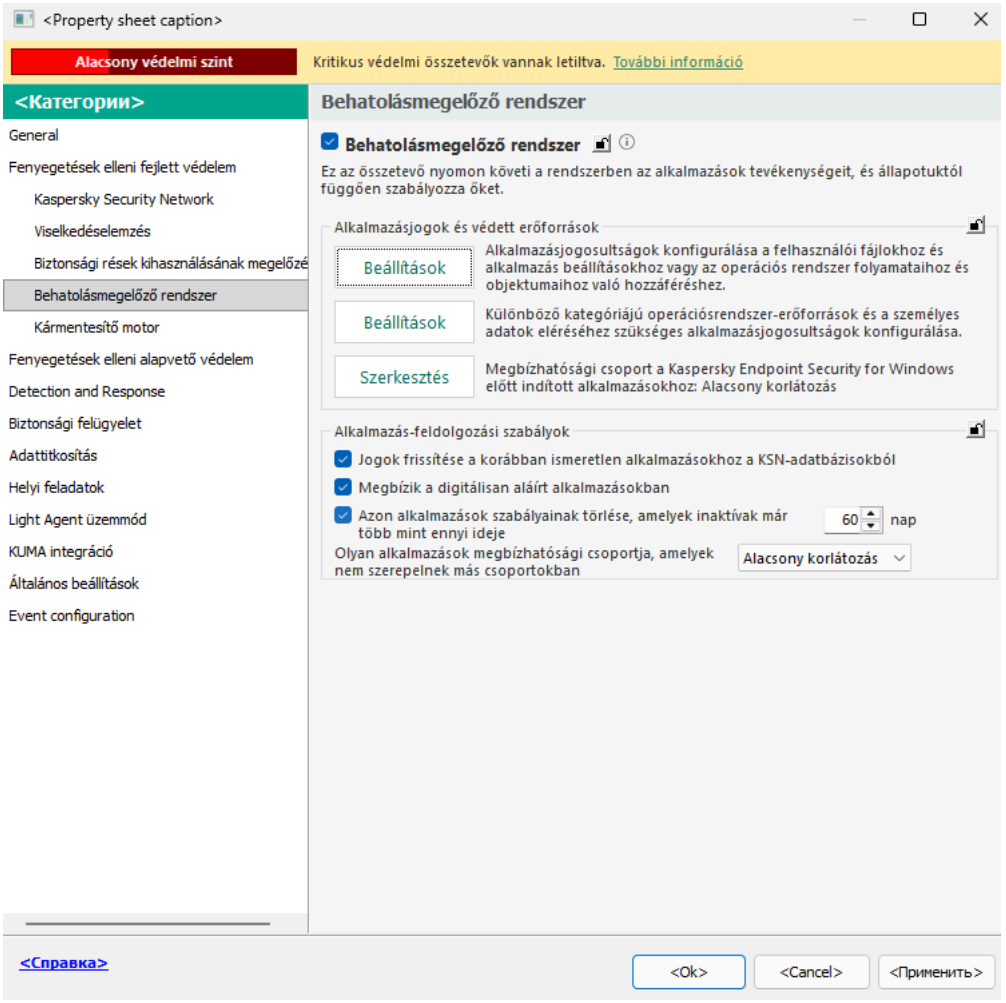
Megbízhatósági csoport kiválasztása ismeretlen alkalmazásokhoz

Az alkalmazás első indításakor a Behatolásmegelőző rendszer összetevő meghatározza az alkalmazáshoz tartozó megbízhatósági csoportot. Ha nincs internetkapcsolat, vagy a Kaspersky Security Network nem rendelkezik információval erről az alkalmazásról, a Kaspersky Endpoint Security alapértelmezés szerint az *alacsony korlátozású* csoportba helyezi az alkalmazást. Ha a Kaspersky Endpoint Security egy korábban ismeretlen alkalmazásról észlel információt a KSN-ben, frissíti az adott alkalmazás jogait. Ezután kézzel szerkesztheti az alkalmazás jogait.

Megbízhatósági csoport kiválasztása ismeretlen alkalmazásokhoz az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. A(z) **Application processing rules** területen a(z) **Trust group for applications not included in other groups** legördülő listából válassza ki a szükséges megbízhatósági csoportot.

   Ha Kaspersky Security Network is enabled, a Kaspersky Endpoint Security minden alkalommal kérést küld a KSN-nek az alkalmazások megbízhatóságára vonatkozóan az adott alkalmazás elindításakor. A kapott válasz alapján az alkalmazás a Behatolásmegelőző rendszer összetevő beállításaiban megadottól eltérő megbízhatósági csoportba kerülhet.

5. A(z) **Update rights for previously unknown applications from KSN database** jelölőnégyzettel konfigurálhatja az ismeretlen alkalmazások jogainak automatikus frissítését.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Megbízhatósági csoport kiválasztása ismeretlen alkalmazásokhoz a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection → Host Intrusion Prevention** elemet.

5. A(z) **Application processing rules** területen a(z) **Trust group for applications not included in other groups** legördülő listából válassza ki a szükséges megbízhatósági csoportot.

   Ha Kaspersky Security Network is enabled, a Kaspersky Endpoint Security minden alkalommal kérést küld a KSN-nek az alkalmazások megbízhatóságára vonatkozóan az adott alkalmazás elindításakor. A kapott válasz alapján az alkalmazás a Behatolásmegelőző rendszer összetevő beállításaiban megadottól eltérő megbízhatósági csoportba kerülhet.

6. A(z) **Update rights for previously unknown applications from KSN database** jelölőnégyzettel konfigurálhatja az ismeretlen alkalmazások jogainak automatikus frissítését.

7. Mentse el a módosításokat.

Megbízhatósági csoport kiválasztása ismeretlen alkalmazásokhoz az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection** → **Host Intrusion Prevention** opciót.

3. Az **Alkalmazás-feldolgozási szabályok** részen válassza ki a megfelelő megbízhatósági csoportot.

   Ha Kaspersky Security Network is enabled, a Kaspersky Endpoint Security minden alkalommal kérést küld a KSN-nek az alkalmazások megbízhatóságára vonatkozóan az adott alkalmazás elindításakor. A kapott válasz alapján az alkalmazás a Behatolásmegelőző rendszer összetevő beállításaiban megadottól eltérő megbízhatósági csoportba kerülhet.

4. Használja a **Szabályok frissítése a korábban ismeretlen alkalmazásokhoz a KSN-ről** jelölőnégyzetet az ismeretlen alkalmazások jogainak automatikus frissítéséhez.

5. Mentse el a módosításokat.

Megbízhatósági csoport kiválasztása digitálisan aláírt alkalmazásokhoz

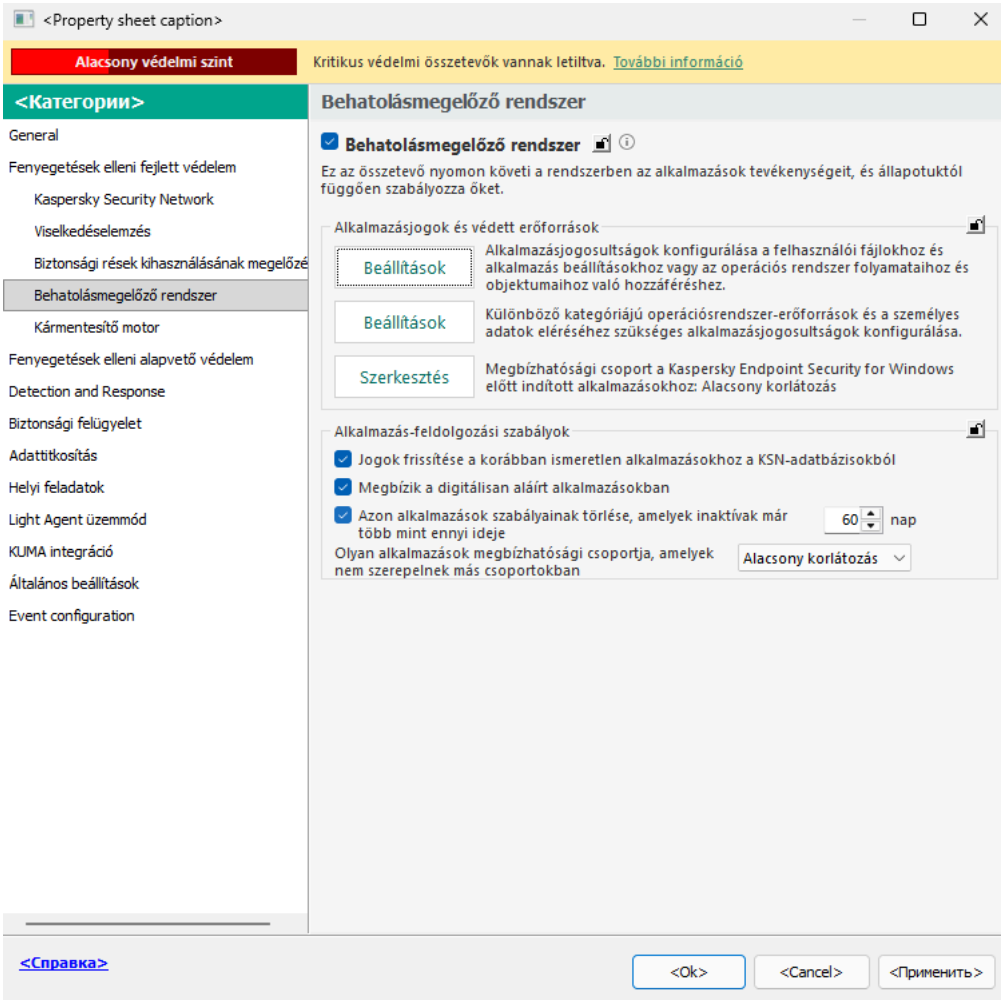
A Kaspersky Endpoint Security a Microsoft tanúsítványokkal vagy Kaspersky tanúsítványokkal rendelkező alkalmazásokat mindig a *Megbízható* csoportba teszi.

Megbízhatósági csoport kiválasztása digitálisan aláírt alkalmazásokhoz az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. A(z) **Application processing rules** területen használja a(z) **Trust digitally signed applications jelölőnégyzetet a megbízható gyártók digitális aláírásait tartalmazó alkalmazások Trusted megbízható csoporthoz történő automatikus hozzárendelésének engedélyezése vagy letiltása céljából.**

   A *megbízható gyártók* olyan szoftvergyártók, amelyeket a Kaspersky megbízható csoportba helyezett. A gyártói tanúsítványt manuálisan is hozzáadhatja a megbízható rendszertanúsítvány-tárolóhoz.

   Ha a jelölőnégyzet nincs bejelölve, a Behatolásmegelőző rendszer összetevő a digitális aláírással rendelkező alkalmazásokat nem tekinti megbízhatónak, és más paraméterek alapján dönti el megbízhatósági csoportjukat.

5. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Megbízhatósági csoport kiválasztása digitálisan aláírt alkalmazásokhoz a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection → Host Intrusion Prevention** elemet.

5. A(z) **Application processing rules** területen használja a(z) **Trust digitally signed applications jelölőnégyzetet a megbízható gyártók digitális aláírásait tartalmazó alkalmazások Trusted megbízható csoporthoz történő automatikus hozzárendelésének engedélyezése vagy letiltása céljából.**

   A *megbízható gyártók* olyan szoftvergyártók, amelyeket a Kaspersky megbízható csoportba helyezett. A gyártói tanúsítványt manuálisan is hozzáadhatja a megbízható rendszertanúsítvány-tárolóhoz.

   Ha a jelölőnégyzet nincs bejelölve, a Behatolásmegelőző rendszer összetevő a digitális aláírással rendelkező alkalmazásokat nem tekinti megbízhatónak, és más paraméterek alapján dönti el megbízhatósági csoportjukat.

6. Mentse el a módosításokat.

Megbízhatósági csoport kiválasztása digitálisan aláírt alkalmazásokhoz az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection → Host Intrusion Prevention** opciót.

3. A(z) **Application processing rules** területen használja a(z) **Trust digitally signed applications jelölőnégyzetet a megbízható gyártók digitális aláírásait tartalmazó alkalmazások Trusted megbízható csoporthoz történő automatikus hozzárendelésének engedélyezése vagy letiltása céljából.**

   A *megbízható gyártók* olyan szoftvergyártók, amelyeket a Kaspersky megbízható csoportba helyezett. A gyártói tanúsítványt manuálisan is hozzáadhatja a megbízható rendszertanúsítvány-tárolóhoz.

   Ha a jelölőnégyzet nincs bejelölve, a Behatolásmegelőző rendszer összetevő a digitális aláírással rendelkező alkalmazásokat nem tekinti megbízhatónak, és más paraméterek alapján dönti el megbízhatósági csoportjukat.

4. Mentse el a módosításokat.

Alkalmazásjogok kezelése

Alapértelmezés szerint az alkalmazástevékenység felügyelete azon megbízhatósági csoporthoz meghatározott alkalmazásjogok alapján történik, amelybe a Kaspersky Endpoint Security az alkalmazást annak első indításakor besorolta. Szükség esetén szerkesztheti az alkalmazásjogokat a teljes megbízhatósági csoport szintjén, egyes alkalmazásonként, illetve a megbízhatósági csoportban található alkalmazások csoportja szerint.

A manuálisan definiált alkalmazásjogok a megbízhatósági csoporthoz meghatározott alkalmazásjogoknál magasabb prioritással rendelkeznek. Más szóval, ha a manuálisan definiált alkalmazásjogok eltérnek a megbízhatósági csoporthoz meghatározott alkalmazásjogoktól, a Behatolásmegelőző rendszer összetevő a manuálisan definiált alkalmazásjogok szerint felügyeli az alkalmazás tevékenységét.

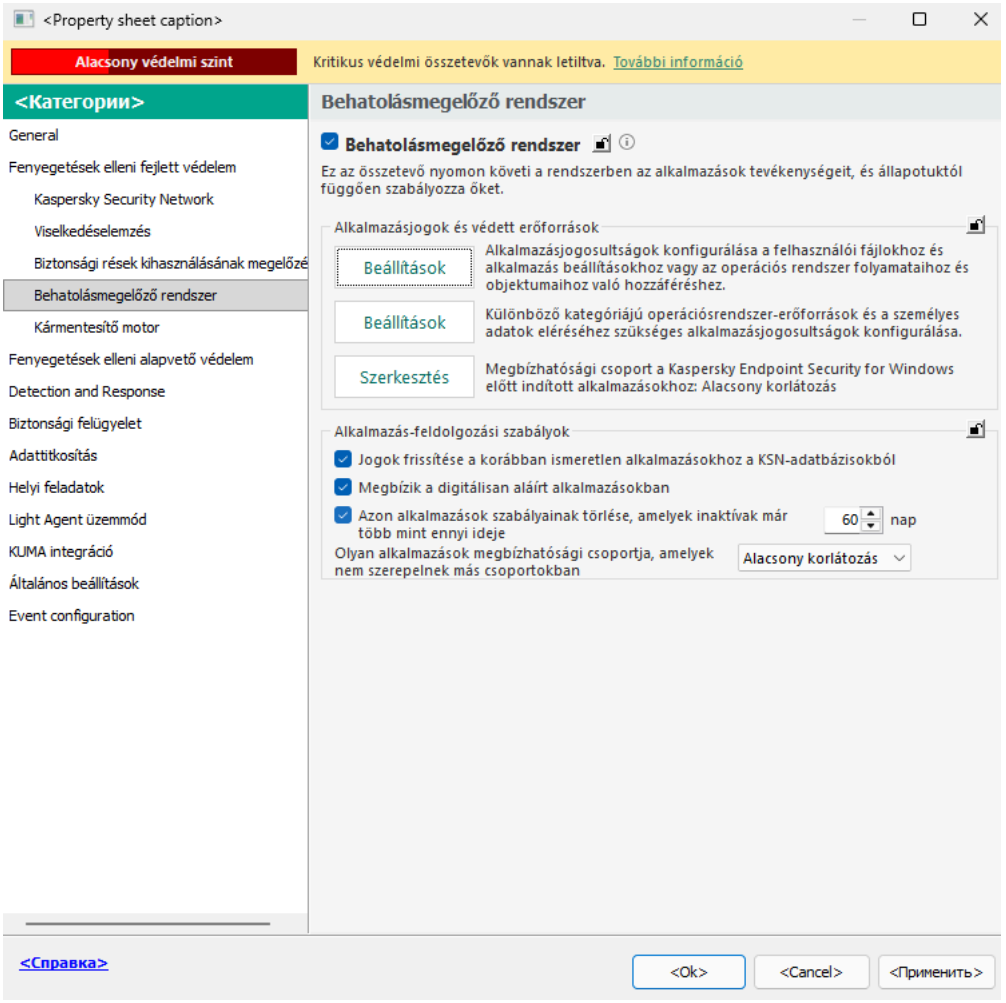
Az alkalmazásokhoz létrehozott szabályokat öröklik a gyermek alkalmazások. Például ha minden hálózati tevékenységet megtilt a cmd.exe részére, ez meg lesz tiltva a notepad.exe részére is, ha az a cmd.exe használatával indul el. Ha egy alkalmazás nem az azt futtató alkalmazás gyermeke, a szabályok nem öröklődnek.

Alkalmazásjogok módosítása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

5. Nyissa meg az **Alkalmazásjogok** fület.

6. Kattintson **Hozzáadás** gombra.

7. A megnyíló ablakban írja be annak az alkalmazásnak a keresési feltételeit, amelynek alkalmazásjogait módosítani kívánja.

   Megadhatja az alkalmazás nevét vagy a gyártó nevét is. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

8. Kattintson a **Frissítés**.

   A Kaspersky Endpoint Security megkeresi az alkalmazást a felügyelt számítógépekre telepített alkalmazások összesített listáján. A Kaspersky Endpoint Security megjeleníti azon alkalmazások listáját, amelyek megfelelnek a keresési feltételeknek.

9. Válassza ki a szükséges alkalmazást.

10. A **Kijelölt alkalmazás hozzáadása a megbízhatósági csoporthoz** legördülő listában válassza ki az **Alapértelmezett csoportok** lehetőséget, majd kattintson az **OK** gombra.

    A rendszer hozzáadja az alkalmazást az alapértelmezett csoporthoz.

11. Válassza ki a megfelelő alkalmazást, majd válassza az **Alkalmazásjogok** lehetőséget az alkalmazás helyi menüjében.

    Ez megnyitja az alkalmazás tulajdonságait.

12. Végezze el az alábbiak egyikét:

    - Ha módosítani kívánja az operációs rendszer beállításjegyzékével, a felhasználói fájlokkal és az alkalmazásbeállításokkal végzett műveleteket szabályozó megbízhatósági csoportok jogait, válassza ki a **Fájlok és rendszerleíró adatbázis** lehetőséget.

    - Ha módosítani szeretné az operációs rendszer folyamataihoz és objektumaihoz való hozzáférést szabályozó megbízhatósági csoportok jogait, válassza ki a **Jogok** lapot.

    Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

13. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában, és válassza ki a szükséges lehetőséget: **Öröklés**, **Engedélyezés** (✓) vagy **Blokkolás** (⊘).

14. Ha szeretné figyelemmel követni a számítógép erőforrásainak használatát, válassza ki az **Események naplózása** (✓ / ⊘) lehetőséget.

    A Kaspersky Endpoint Security rögzíti a Behatolásmegelőző rendszer összetevő működésére vonatkozó információkat. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

15. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Alkalmazásjogok módosítása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection** → **Host Intrusion Prevention** elemet.

5. A **Application rights and protected resources** részen kattintson a **Application rights and protected resources** hivatkozásra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

6. Nyissa meg a **Application rights** lapot.

   Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.

7. Kattintson az **Add** gombra.

   Ezután elindul a varázsló, amellyel hozzáadhat egy alkalmazást egy megbízhatósági csoporthoz.

8. Válassza ki az alkalmazás megfelelő megbízhatósági csoportját.

9. Válassza ki az **Application** típust. Lépjen a következő lépésre.

   Ha több alkalmazás megbízhatósági csoportját szeretné módosítani, válassza ki a **Group** típust, és adjon egy nevet az alkalmazáscsoportnak.

10. Az alkalmazások megnyílt listájában válassza ki azokat az alkalmazásokat, amelyeknél módosítaná az alkalmazásjogokat.

    Használjon szűrőt. Megadhatja az alkalmazás nevét vagy a gyártó nevét is. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

11. Lépjen ki a varázslóból.

    A rendszer hozzáadja az alkalmazást a megbízhatósági csoporthoz.

12. Az ablak bal oldalán válassza ki a megfelelő alkalmazást.

13. Az ablak jobb oldalán a legördülő listában végezze el a következő műveletek egyikét:

    - Ha módosítani kívánja az operációs rendszer beállításjegyzékével, a felhasználói fájlokkal és az alkalmazásbeállításokkal végzett műveleteket szabályozó megbízhatósági csoportok jogait, válassza ki a **Files and system registry** lehetőséget.
    - Ha módosítani szeretné az operációs rendszer folyamataihoz és objektumaihoz való hozzáférést szabályozó megbízhatósági csoportok jogait, válassza ki a **Rights** lapot.

    Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

14. A megfelelő erőforrás és a megfelelő művelet oszlopában válassza ki a szükséges opciót:**Inherit**, **Allow** ( ) vagy **Block** ( ).

15. Ha szeretné figyelemmel követni a számítógép erőforrásainak használatát, válassza ki az **Log events** (/) lehetőséget.

    A Kaspersky Endpoint Security rögzíti a Behatolásmegelőző rendszer összetevő működésére vonatkozó információkat. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

16. Mentse el a módosításokat.

Alkalmazásjogok módosítása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection → Host Intrusion Prevention** opciót.
3. Kattintson az **Alkalmazások kezelése** elemre.

   Ezzel megnyitja a telepített alkalmazások listáját.

4. Válassza ki a szükséges alkalmazást.
5. Az alkalmazás helyi menüjében válassza ki a **Részletek és szabályok** elemet.

   Ez megnyitja az alkalmazás tulajdonságait.

6. Végezze el az alábbiak egyikét:

   - Ha módosítani kívánja az operációs rendszer beállításjegyzékével, a felhasználói fájlokkal és az alkalmazásbeállításokkal végzett műveleteket szabályozó megbízhatósági csoportok jogait, válassza ki a **Fájlok és rendszerleíró adatbázis** lehetőséget.

   - Ha módosítani szeretné az operációs rendszer folyamataihoz és objektumaihoz való hozzáférést szabályozó megbízhatósági csoportok jogait, válassza ki a **Jogok** lapot.

7. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában, és válassza ki a szükséges lehetőséget: **Öröklés**, **Engedélyezés** (✓) vagy **Tiltás** (!).

8. Ha szeretné figyelemmel követni a számítógép erőforrásainak használatát, válassza ki az **Események naplózása** (📊) lehetőséget.

   A Kaspersky Endpoint Security rögzíti a Behatolásmegelőző rendszer összetevő működésére vonatkozó információkat. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

9. Válassza ki a **Kizárások** lapot, és konfigurálja az alkalmazás speciális beállításait (lásd az alábbi táblát).

10. Mentse el a módosításokat.

Az alkalmazás speciális beállításai

Paraméter	Leírás
Ne vizsgálja meg az alkalmazás által megnyitott fájlokat	Az alkalmazás által megnyitott összes fájl ki van zárva a Kaspersky Endpoint Security általi vizsgálatból. Például, ha alkalmazásokat használ fájlok biztonsági mentésére, ez a szolgáltatás segít csökkenteni a Kaspersky Endpoint Security erőforrás-felhasználását.
Ne figyelje az alkalmazástevékenységet	A Kaspersky Endpoint Security nem fogja figyelni az alkalmazás fájl- és hálózati tevékenységét az operációs rendszerben. Beállíthatja az alkalmazástevékenység-figyelést a Kaspersky Endpoint Security különböző összetevőihez: • **Ne figyelje a védelmi és felügyeleti összetevőket**. Az alkalmazástevékenységet a következő összetevők figyelik: Behavior analysis, Biztonsági rések kihasználásának megelőzése, Behatolásmegelőző rendszer, Kármentesítő motor és Tűzfal. • **Ne figyelje a Managed Detection and Response és az Endpoint Detection and Response megoldásokat**. Az alkalmazások tevékenységét figyeli a beépített MDR agent és beépített EDR (KATA) agent. • **Ne szerezze meg a konzol interaktív bemenetét az Endpoint Detection and Response esetében**. A Kaspersky Endpoint Security nem küld telemetriai adatokat az alkalmazás konzolon történő kezeléséről. A telemetriai adatokat Kaspersky Anti Targeted Attack Platform (EDR) használja.
Ne örökölje a szülőfolyamat (alkalmazás) korlátozásait	A szülői folyamathoz konfigurált korlátozásokat a Kaspersky Endpoint Security nem alkalmazza utódfolyamatra. A szülői folyamatot egy olyan alkalmazás indítja, amelyhez konfigurálva vannak az alkalmazásjogok (Behatolásmegelőző rendszer) és az alkalmazás hálózati szabályai (Tűzfal).
Ne figyelje a gyermek alkalmazás tevékenységét	A Kaspersky Endpoint Security nem figyeli az ezen alkalmazás által elindított alkalmazások fájl- vagy hálózati tevékenységét. A kizárást rekurzívan is alkalmazhatja. Annak érdekében, hogy az alkalmazás ne figyelje a gyermekalkalmazások teljes láncának tevékenységét.
Interakció engedélyezése a Kaspersky Endpoint Security for Windows felületével	A Kaspersky Endpoint Security Önvédelem blokkolja az alkalmazásszolgáltatások távoli számítógépről történő kezelésének minden kísérletét. Ha a jelölőnégyzet be van jelölve, a távoli hozzáférési alkalmazás a Kaspersky Endpoint Security beállításait a Kaspersky Endpoint Security felületen keresztül kezelheti.
Ne vizsgálja a titkosított forgalmat / **Ne vizsgálja a teljes forgalmat**	Az alkalmazás által kezdeményezett hálózati forgalom ki lesz zárva a Kaspersky Endpoint Security vizsgálataiból. A vizsgálatokból kizárhatja a teljes forgalmat vagy csak a titkosított forgalmat. Kizárhatja az egyes IP-címeket és portszámokat is a vizsgálatokból. A Kaspersky Endpoint Security 14.0 vagy annál korábbi verziói nem támogatják a hálózati forgalom kizárását, ha egy megbízható alkalmazáshoz elérési út helyett kivonatot adnak meg.

Operációsrendszer-erőforrások és személyes adatok védelme

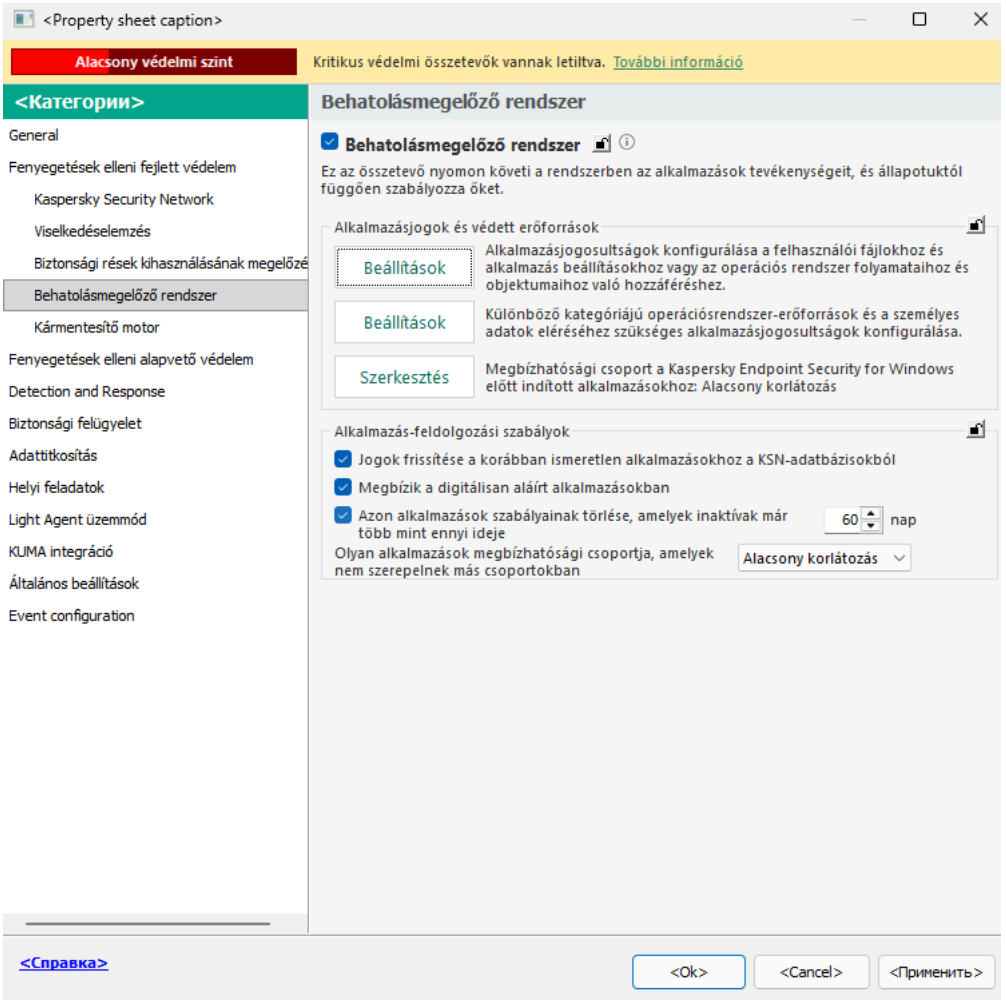
A Behatolásmegelőző rendszer összetevő kezeli az alkalmazások jogosultságát az operációs rendszer különböző kategóriákba sorolt erőforrásain és a személyes adatokon végzett műveletekre. A Kaspersky szakemberei előre kialakított kategóriákba sorolták a védett erőforrásokat. Például az *Operációs rendszer* kategóriának van egy *Indítási beállítások* alkategóriája, amely felsorolja az alkalmazások automatikus futtatásához társított összes beállításkulcsot. A védett erőforrások előre kialakított kategóriái és az alapértelmezés szerint ezekbe a kategóriákba tartozó erőforrások nem szerkeszthetők és nem törölhetők.

Védett erőforrás hozzáadásának menete az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

5. Nyissa meg a **Védett erőforrások** fület.

   Az ablak bal oldalán megjelenik a védett erőforrások listája és az ezekhez az erőforrásokhoz való hozzáférés megfelelő jogai az adott megbízhatósági csoporttól függően.

6. Jelölje ki a védett erőforrások azon kategóriáját, amelyhez új védett erőforrást szeretne hozzáadni.

   Ha alkategóriát szeretne hozzáadni, kattintson a **Add** → **Category** elemre.

7. Kattintson a **Hozzáadás** gombra. A legördülő listában válassza ki a hozzáadni kívánt erőforrás típusát: **Fájl vagy mappa** vagy **Beállításkulcs**.

8. A megnyíló ablakban válasszon ki egy fájlt, mappát vagy beállításkulcsot.

   Megtekintheti az alkalmazások hozzáadott erőforrásokhoz tartozó hozzáférési jogait. Ehhez válasszon egy hozzáadott erőforrást az ablak bal oldalán, és a Kaspersky Endpoint Security megmutatja az adott megbízhatósági csoport hozzáférési jogait. Az új erőforrás melletti jelölőnégyzet használatával letilthatja az alkalmazástevékenység erőforrásokkal történő vezérlését is.

9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Védett erőforrás hozzáadásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection** → **Host Intrusion Prevention** elemet.

5. A **Application rights and protected resources** részen kattintson a **Application rights and protected resources** hivatkozásra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

6. Nyissa meg a **Protected resources** lapot.

   Az ablak bal oldalán megjelenik a védett erőforrások listája és az ezekhez az erőforrásokhoz való hozzáférés megfelelő jogai az adott megbízhatósági csoporttól függően.

7. Kattintson az **Add** gombra.

   Elindul az Új erőforrás varázsló.

8. A(z) **Group name** területen válassza ki a védett erőforrások azon kategóriáját, amelyhez új védett erőforrást szeretne hozzáadni.

   Ha alkategóriát szeretne hozzáadni, válassza ki a **Category of protected resources** lehetőséget.

9. Válassza ki a hozzáadni kívánt erőforrás típusát: **File or folder** vagy **Registry key**.

10. Válasszon ki egy fájlt, mappát vagy beállításkulcsot.

11. Lépjen ki a varázslóból.

    Megtekintheti az alkalmazások hozzáadott erőforrásokhoz tartozó hozzáférési jogait. Ehhez válasszon egy hozzáadott erőforrást az ablak bal oldalán, és a Kaspersky Endpoint Security megmutatja az adott megbízhatósági csoport hozzáférési jogait. Az **Status** oszlopban található jelölőnégyzetet is használhatja az alkalmazástevékenység erőforrásokkal történő vezérlésének letiltására.

12. Mentse el a módosításokat.

Védett erőforrás hozzáadásának menete az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection → Host Intrusion Prevention** opciót.
3. Kattintson az **Erőforrások kezelése** gombra.

   Megnyílik a védett erőforrások listája.
4. Jelölje ki a védett erőforrások azon kategóriáját, amelyhez új védett erőforrást szeretne hozzáadni.

   Ha alkategóriát szeretne hozzáadni, kattintson a **Add → Category** elemre.
5. Kattintson a **Hozzáadás** gombra. A legördülő listában válassza ki a hozzáadni kívánt erőforrás típusát: **Fájl vagy mappa** vagy **Beállításkulcs**.
6. A megnyíló ablakban válasszon ki egy fájlt, mappát vagy beállításkulcsot.

   Megtekintheti az alkalmazások hozzáadott erőforrásokhoz tartozó hozzáférési jogait. Ehhez válasszon egy hozzáadott erőforrást az ablak bal oldalán, és a Kaspersky Endpoint Security megmutatja az alkalmazások listáját és az egyes alkalmazások hozzáférési jogait. Az alkalmazástevékenységek erőforrásokkal történő vezérlését le is tilthatja a **Felügyelet engedélyezése** gombra kattintva az **Állapot** oszlopban.
7. Mentse el a módosításokat.

A Kaspersky Endpoint Security szabályozza az operációs rendszer hozzáadott erőforrásaihoz és a személyes adatokhoz való hozzáférést. A Kaspersky Endpoint Security az adott alkalmazáshoz rendelt megbízhatósági csoport alapján szabályozza az alkalmazás erőforrásokhoz való hozzáférését. Ezenkívül módosíthatja az alkalmazás megbízhatósági csoportját is.

Nem használt alkalmazásokra vonatkozó adatok törlése

A Kaspersky Endpoint Security az alkalmazásjogokkal szabályozza az alkalmazások tevékenységét. Az alkalmazások jogait a megbízhatósági csoportok határozzák meg. A Kaspersky Endpoint Security az adott alkalmazás első indításakor megbízhatósági csoportba helyezi az alkalmazást. Manuálisan is módosíthatja az alkalmazás megbízhatósági csoportját. Manuálisan is konfigurálhatja az egyéni alkalmazások jogait. A Kaspersky Endpoint Security az alkalmazások következő információit tárolja: a megbízhatósági csoportja, valamint a jogai.

A Kaspersky Endpoint Security automatikusan törli a nem használt alkalmazások adatait, hogy számítógépes erőforrásokat spóroljon. A Kaspersky Endpoint Security a következő szabályok alapján törli az alkalmazások információit:

- Ha az alkalmazás megbízhatósági csoportja és jogai automatikusan ki lettek választva, a Kaspersky Endpoint Security 30 nap után törli ezeket az adatokat. Nem lehet módosítani az alkalmazás információinak tárolási feltételeit, illetve nem lehet kikapcsolni az automatikus törlést.
- Ha manuálisan rak be egy alkalmazást egy megbízhatósági csoportba vagy így ad hozzáférési jogokat, a Kaspersky Endpoint Security 60 nap után törli az alkalmazás információit (alapértelmezett tárolási feltétel). Módosíthatja az alkalmazás információinak tárolási feltételeit, illetve kikapcsolhatja az automatikus törlést (lásd az alábbi utasítást).

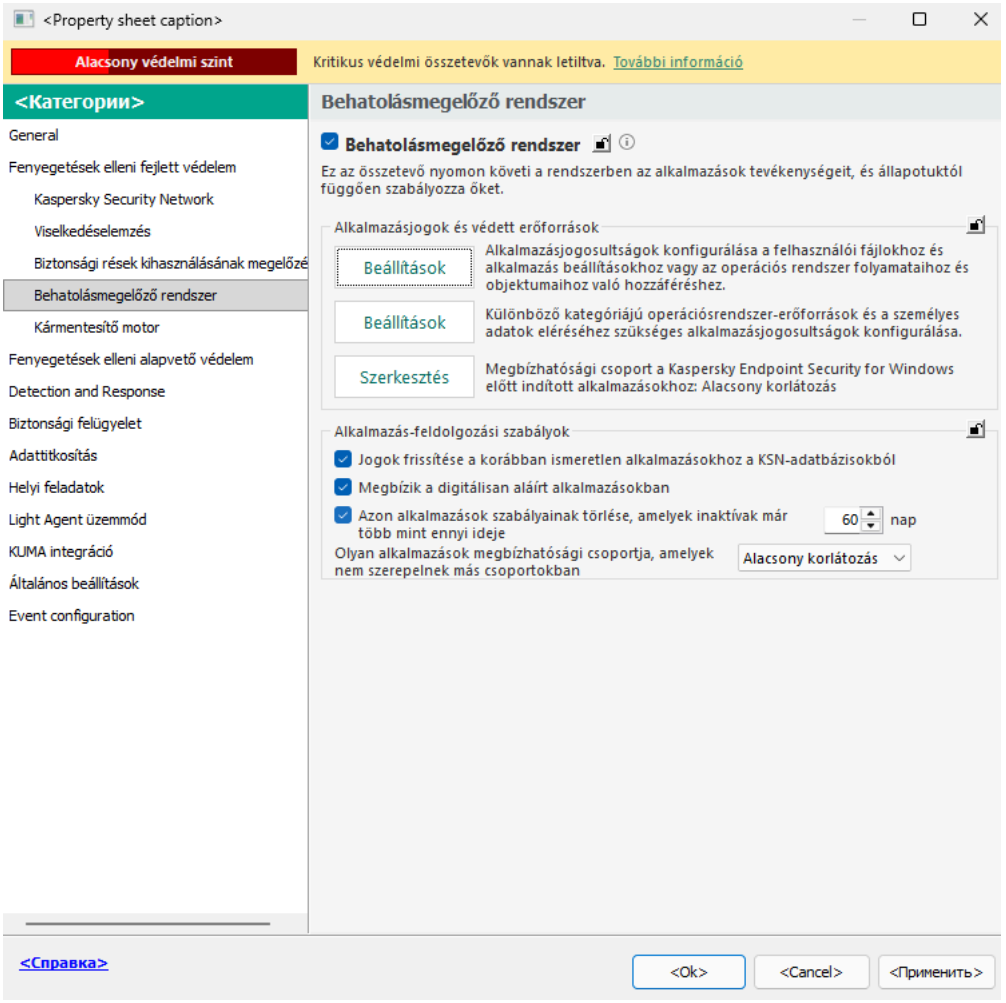
Ha először indít el olyan alkalmazást, melynek információi törlésre kerültek, a Kaspersky Endpoint Security úgy elemzi annak adatait, mintha legelőször indítaná el.

A nem használt alkalmazások információi automatikus törlésének konfigurálása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.



Behatolásmegelőző rendszer beállításai

4. Az **Application processing rules** részen végezze el az alábbiak egyikét:

- Ha be szeretné állítani az automatikus törlést, jelölje be az **Azon alkalmazások szabályainak törlése, amelyek inaktívak már több mint N napja** jelölőnégyzetet, és adja meg a napok számát.

  A Kaspersky Endpoint Security a megadott számú nap elteltével törli az azokra az alkalmazásokra vonatkozó adatokat, amelyeket Ön helyezett kézzel egy megbízható csoportba vagy amelyek hozzáférési jogosultságait Ön kézzel konfigurálta. A Kaspersky Endpoint Security 30 nap elteltével az azokra az alkalmazásokra vonatkozó adatokat is törli, amelyek megbízható csoportba történő felvétele, valamint alkalmazáselérési jogosultságainak megadása automatikusan zajlott.

- Ha ki szeretné kapcsolni az automatikus törlést, törölje az **Azon alkalmazások szabályainak törlése, amelyek inaktívak már több mint N napja** jelölőnégyzet kijelölését.

  Az olyan alkalmazásoknak az információit, amelyeket Ön manuálisan helyezett megbízhatósági csoportokba vagy így adott nekik hozzáférési jogokat, a Kaspersky Endpoint Security korlátlan ideig őrzi, tárolási feltételek nélkül. A Kaspersky Endpoint Security csak azon alkalmazások információit törli 30 nap elteltével, amelyek megbízható csoportba való beosztását és alkalmazásjogosultságait a rendszer automatikusan kezelte.

5. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A nem használt alkalmazások információi automatikus törlésének konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Host Intrusion Prevention** elemet.
5. A **Application processing rules** részen hajtsa végre a következő műveletek valamelyikét:

   - Ha automatikus törlést szeretne beállítani, jelölje be a(z) **Delete rules for applications that have not been started for longer than (days, 1 to 90)** a négyzetet, és adja meg a napok számát.

     A Kaspersky Endpoint Security a megadott számú nap elteltével törli az azokra az alkalmazásokra vonatkozó adatokat, amelyeket Ön helyezett kézzel egy megbízható csoportba vagy amelyek hozzáférési jogosultságait Ön kézzel konfigurálta. A Kaspersky Endpoint Security 30 nap elteltével az azokra az alkalmazásokra vonatkozó adatokat is törli, amelyek megbízható csoportba történő felvétele, valamint alkalmazáselérési jogosultságainak megadása automatikusan zajlott.

   - Ha ki szeretné kapcsolni az automatikus törlést, törölje a **Delete rules for applications that have not been started for longer than (days, 1 to 90)** négyzet jelölését.

     Az olyan alkalmazásoknak az információit, amelyeket Ön manuálisan helyezett megbízhatósági csoportokba vagy így adott nekik hozzáférési jogokat, a Kaspersky Endpoint Security korlátlan ideig őrzi, tárolási feltételek nélkül. A Kaspersky Endpoint Security csak azon alkalmazások információit törli 30 nap elteltével, amelyek megbízható csoportba való beosztását és alkalmazásjogosultságait a rendszer automatikusan kezelte.

6. Mentse el a módosításokat.

A nem használt alkalmazások információi automatikus törlésének konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazásbeállítások ablakban válassza az **Advanced Threat Protection** → **Host Intrusion Prevention** opciót.

3. Az **Application processing rules** részen végezze el az alábbiak egyikét:

   - Ha be szeretné állítani az automatikus törlést, jelölje be az **Azon alkalmazások szabályainak törlése, amelyek inaktívak már több mint N napja (1–90)** négyzetet, és adja meg a napok számát.

     A Kaspersky Endpoint Security a megadott számú nap elteltével törli az azokra az alkalmazásokra vonatkozó adatokat, amelyeket Ön helyezett kézzel egy megbízható csoportba vagy amelyek hozzáférési jogosultságait Ön kézzel konfigurálta. A Kaspersky Endpoint Security 30 nap elteltével az azokra az alkalmazásokra vonatkozó adatokat is törli, amelyek megbízható csoportba történő felvétele, valamint alkalmazáselérési jogosultságainak megadása automatikusan zajlott.

   - Ha ki szeretné kapcsolni az automatikus törlést, törölje az **Azon alkalmazások szabályainak törlése, amelyek inaktívak már több mint Nnapja (1–90)** négyzet jelölését.

     Az olyan alkalmazásoknak az információit, amelyeket Ön manuálisan helyezett megbízhatósági csoportokba vagy így adott nekik hozzáférési jogokat, a Kaspersky Endpoint Security korlátlan ideig őrzi, tárolási feltételek nélkül. A Kaspersky Endpoint Security csak azon alkalmazások információit törli 30 nap elteltével, amelyek megbízható csoportba való beosztását és alkalmazásjogosultságait a rendszer automatikusan kezelte.

4. Mentse el a módosításokat.

Behatolásmegelőző rendszer figyelése

Jelentéseket kaphat a Behatolásmegelőző rendszer összetevő működéséről. A jelentések információkat tartalmaznak az alkalmazás által a számítógép erőforrásaival végzett műveletekről (engedélyezve vagy tiltva). A jelentések információkat tartalmaznak az egyes erőforrásokat használó alkalmazásokról is.

A Behatolásmegelőző rendszer működésének figyeléséhez engedélyeznie kell a jelentések rögzítését. Például engedélyezheti az egyes alkalmazásokhoz tartozó jelentések továbbítását a Behatolásmegelőző rendszer összetevő beállításaiban.

A Behatolásmegelőző rendszer figyelésének konfigurálásakor vegye figyelembe az esetleges hálózati terhelést, amikor eseményeket továbbít a Kaspersky Security Centerbe. Csak a jelentések mentését is engedélyezheti a Kaspersky Endpoint Security helyi naplójában.

A hang- és videórögzítéshez való hozzáférés védelme

Az audiojel-védelmi funkció és a webkamera hozzáférés-védelmi funkciója nem támogatott az ARM-alapú számítógépeken.

Az internetes bűnözők megkísérelhetnek speciális programokkal hozzáférést szerezni olyan eszközökhöz, amelyek hangot és videót rögzítenek (például mikrofonok vagy webkamerák). A Kaspersky Endpoint Security felügyeli az alkalmazások hang- és video-adatfolyamának fogadását, és megvédi az adatokat az illetéktelen elfogástól.

Alapértelmezés szerint a Kaspersky Endpoint Security csak a *Megbízható* csoportba tartozó alkalmazások számára engedélyezi a hang- és videostreamek fogadását. Az *Alacsony korlátozás*, *Magas korlátozás* és *Nem megbízható* csoportok alkalmazásai nem fogadhatják az audio- és videostreamet az eszközökről. Manuálisan engedélyezheti az alkalmazásoknak a hang- és video-adatfolyam fogadását.

A hang-adatfolyam védelemének speciális jellemzői

A hang-adatfolyam védelme az alábbi speciális jellemzőkkel rendelkezik:

- A funkció működéséhez engedélyezve kell lennie a Behatolásmegelőző rendszer összetevőnek.
- Ha az alkalmazás a Behatolásmegelőző rendszer összetevő indítása előtt elkezdett hang-adatfolyamot fogadni, a Kaspersky Endpoint Security lehetővé teszi, hogy az alkalmazás fogadja a hang-adatfolyamot, és nem jelenít meg értesítést.
- Ha az alkalmazás az hang-adatfolyamot fogadását követően a *Nem megbízható* vagy a *Magas korlátozás* csoportba került, a Kaspersky Endpoint Security lehetővé teszi, hogy az alkalmazás fogadja a hang-adatfolyamot, és nem jelenít meg értesítést.
- Az alkalmazás hangrögzítő eszközhöz való hozzáférési beállításainak módosítását követően (például ha az alkalmazásnak meg lett tiltva a hang-adatfolyam fogadása) az alkalmazást újra kell indítani, hogy többé ne fogadja a hang-adatfolyamot.
- A hangrögzítő eszközök hangadatfolyamaihoz való hozzáférés felügyelete nem függ az alkalmazás webkamerához való hozzáférésére vonatkozó beállításaitól.
- A Kaspersky Endpoint Security csak a beépített és külső mikrofonokhoz való hozzáférést védi. Egyéb hang-adatfolyamot biztosító eszközöket nem támogat.
- A Kaspersky Endpoint Security nem garantálja azon hang-adatfolyamok védelmét, amelyek DSLR kamerákból, hordozható videokamerákból és akciókamerákból érkeznek.
- Amikor a Kaspersky Endpoint Security telepítése után először hang- vagy videorögzítő, illetve -lejátszó alkalmazásokat futtat, előfordulhat, hogy a hang- vagy videorögzítés, illetve -lejátszás megszakad. Ez az alkalmazások számára a hangrögzítő eszközökhöz való hozzáférést vezérlő funkciók engedélyezéséhez szükséges. A hanghardvert vezérlő rendszerszolgáltatás a Kaspersky Endpoint Security első futásakor újraindul.

A webkamera hozzáférési védelmének speciális jellemzői az alkalmazásban

A webkamera hozzáférési védelmére az alábbi különleges szempontok és korlátozások vonatkoznak:

- Az alkalmazás a webkamera adatainak feldolgozásából származó mozgó- és állóképeket ellenőrzi.
- Az alkalmazás akkor vezérli a hang-adatfolyamot, ha az a webkamerából érkező videoadatfolyam része.
- Az alkalmazás csak olyan webkamerákat vezérel, amelyek USB vagy IEEE1394 felületen keresztül csatlakoznak és Képeszközök néven jelennek meg a Windows Eszközkezelőben.
- A Kaspersky Endpoint Security az alábbi webkamerákat támogatja:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210

- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

A Kaspersky a listán nem szereplő webkamerák támogatását nem tudja garantálni.

BadUSB védelem

Egyes vírusok az USB eszközök firmware-ét módosítva becsapják az operációs rendszert, így az az USB eszközt billentyűzetként észleli. Ennek eredményeképpen a vírus parancsokat hajthat végre az Ön felhasználói fiókja alatt, például rosszindulatú programok letöltésére.

A BadUSB védelem összetevő megakadályozza azt, hogy a billentyűzetet emuláló fertőzött USB eszközök a számítógéphez csatlakozzanak.

Ha egy USB eszközt a számítógéphez való csatlakoztatásakor az operációs rendszer billentyűzetként azonosít, akkor felkéri a felhasználót, hogy írjon be ezen a billentyűzeten vagy a képernyőn megjelenő billentyűzeten, ha elérhető, egy általa előállított számkódot (lásd az alábbi táblázatot). Ezt az eljárást nevezik billentyűzethitelesítésnek.

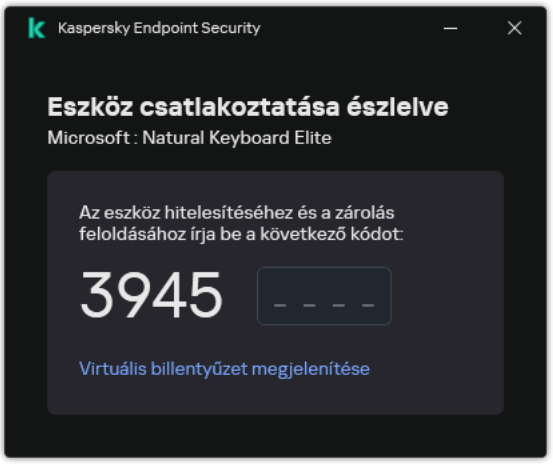
A kód megfelelő beírása esetén az alkalmazás menti az azonosító paramétereket — a billentyűzet VID/PID azonosítóját és a csatlakoztatás portszámát — a hitelesített billentyűzetek listájára. A billentyűzethitelesítést a billentyűzet ismételt csatlakoztatásakor és az operációs rendszer újraindításakor nem kell újra elvégezni.

Ha a hitelesített billentyűzetet a számítógép egy másik USB portjához csatlakoztatja, az alkalmazás megjeleníti a billentyűzet újbóli hitelesítési kérését.

Ha a számkód beírása nem sikerül, az alkalmazás új kódot állít elő. Beállíthatja a számkód beírására tett kísérletek számát. Ha a számkódot többször helytelenül adják meg, vagy a billentyűzethitelesítés engedélyezési ablaka be van zárva (lásd az alábbi ábrát), az alkalmazás letiltja a billentyűzetről történő bevitelt. Amikor letelik az USB-eszköz blokkolási ideje, vagy az operációs rendszer újraindul, az alkalmazás ismét felkéri a felhasználót, hogy végezze el a billentyűzet hitelesítését.

Az alkalmazás a hitelesített billentyűzet használatát engedélyezi, a nem hitelesítettét pedig blokkolja.

A BadUSB védelem összetevőt alapértelmezés szerint nem telepíti a rendszer. Ha szüksége van a BadUSB védelem összetevőre, hozzáadhatja az alkalmazás telepítése előtt a telepítőcsomag tulajdonságaiban, vagy módosíthatja az elérhető alkalmazásösszetevőket az alkalmazás telepítését után.



Billentyűzethitelesítés

BadUSB védelem be- és kikapcsolása

Az operációs rendszer által billentyűzetként felismert, a BadUSB védelem összetevő telepítése előtt a számítógéphez csatlakoztatott USB eszközök az összetevő telepítését követően hitelesítettnek minősülnek.

A BadUSB védelem összetevő engedélyezése vagy letiltása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → BadUSB védelem** lehetőséget.
4. A **BadUSB védelem** jelölőnégyzet használatával engedélyezze vagy tiltsa le az összetevőt.
5. Az **USB-eszközhitelesítés csatlakoztatáskor** részen módosítsa a biztonsági beállításokat hitelesítési kód megadása esetén:
   - **Az USB-készülékhitelesítési kísérletek maximális száma**. Automatikusan blokkolja az USB-eszközt, ha a megadott számú alkalommal helytelenül adják meg a hitelesítési kódot. Az érvényes értékek 1 és 10 között vannak. Ha például 5 kísérletet engedélyez a hitelesítési kód megadására, az alkalmazás az ötödik sikertelen kísérlet után blokkolja az USB-eszközt. A Kaspersky Endpoint Security megjeleníti az USB-eszköz blokkolásának időtartamát. Ezen idő letelte után ismét öt alkalommal próbálkozhat a hitelesítési kód megadásával.
   - **A próbálkozások maximális számának időkorlátja (perc)**. Az USB-eszköz letiltásának időtartama a megadott számú sikertelen engedélyezési kísérlet után. Az érvényes értékek 1 és 180 (perc) között vannak.
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A BadUSB védelem összetevő engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **BadUSB Attack Prevention** elemet.
5. A **BadUSB Attack Prevention ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Az **Authorization of USB devices** részen módosítsa a biztonsági beállításokat a hitelesítő kód megadásához:

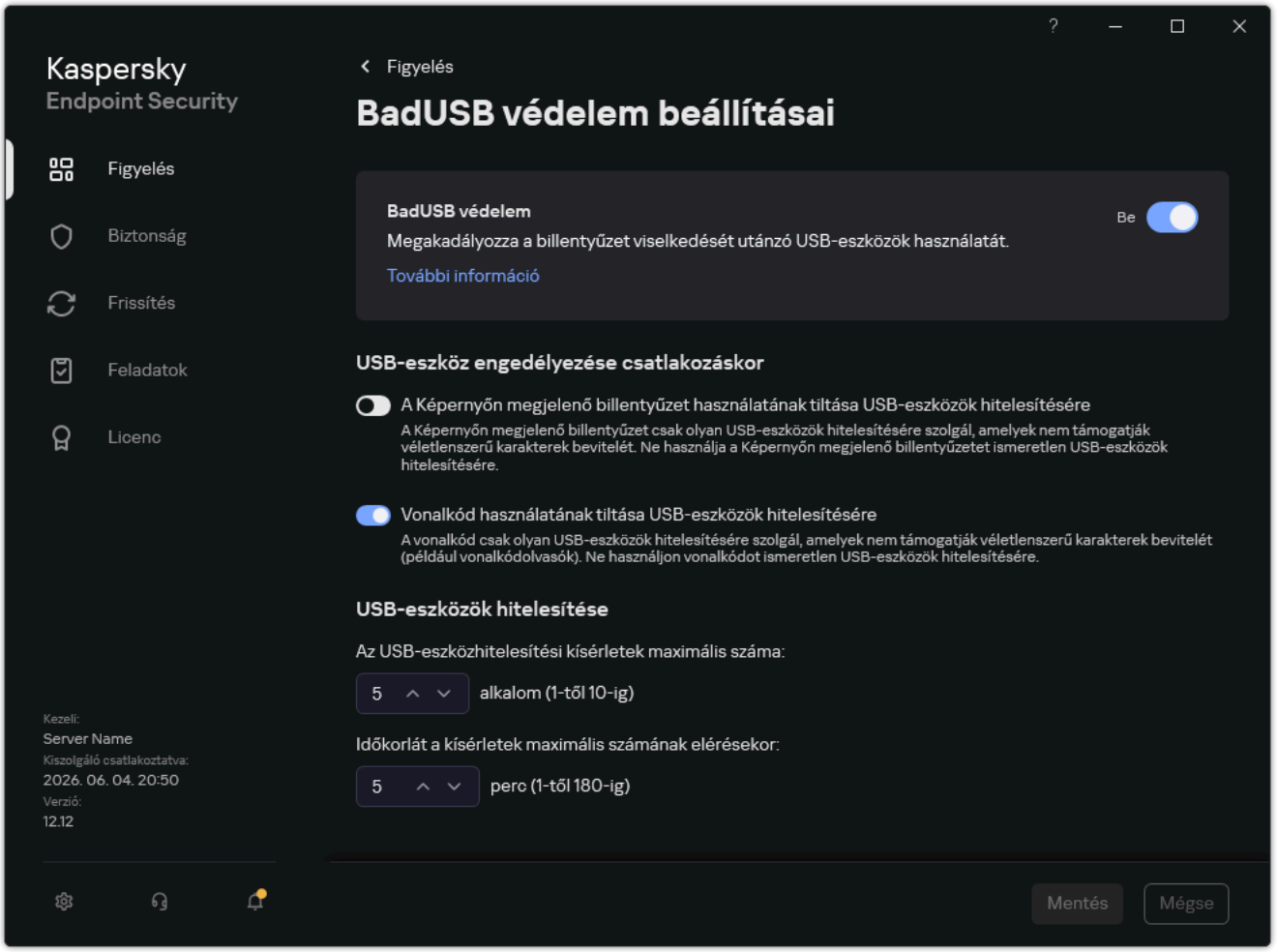
   - **Maximum number of USB device authorization attempts**. Automatikusan blokkolja az USB-eszközt, ha a megadott számú alkalommal helytelenül adják meg a hitelesítési kódot. Az érvényes értékek 1 és 10 között vannak. Ha például 5 kísérletet engedélyez a hitelesítési kód megadására, az alkalmazás az ötödik sikertelen kísérlet után blokkolja az USB-eszközt. A Kaspersky Endpoint Security megjeleníti az USB-eszköz blokkolásának időtartamát. Ezen idő letelte után ismét öt alkalommal próbálkozhat a hitelesítési kód megadásával.

   - **Timeout when reaching the maximum number of attempts (min)**. Az USB-eszköz letiltásának időtartama a megadott számú sikertelen engedélyezési kísérlet után. Az érvényes értékek 1 és 180 (perc) között vannak.
7. Mentse el a módosításokat.

A BadUSB védelem összetevő engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni alapvető védelem → BadUSB védelem** lehetőséget.



A BadUSB Védelem összetevő beállításai

3. A **BadUSB védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Az **USB-eszközhitelesítés csatlakoztatáskor** részen módosítsa a biztonsági beállításokat hitelesítési kód megadása esetén:

   - **Az USB-készülékhitelesítési kísérletek maximális száma**. Automatikusan blokkolja az USB-eszközt, ha a megadott számú alkalommal helytelenül adják meg a hitelesítési kódot. Az érvényes értékek 1 és 10 között vannak. Ha például 5 kísérletet engedélyez a hitelesítési kód megadására, az alkalmazás az ötödik sikertelen kísérlet után blokkolja az USB-eszközt. A Kaspersky Endpoint Security megjeleníti az USB-eszköz blokkolásának időtartamát. Ezen idő letelte után ismét öt alkalommal próbálkozhat a hitelesítési kód megadásával.

   - **Időkorlát a kísérletek maximális számának elérésekor**. Az USB-eszköz letiltásának időtartama a megadott számú sikertelen engedélyezési kísérlet után. Az érvényes értékek 1 és 180 (perc) között vannak.

5. Mentse el a módosításokat.

Ennek eredményeképpen, ha a BadUSB védelem engedélyezve van, a Kaspersky Endpoint Security megköveteli az operációs rendszer által billentyűzetként azonosított csatlakoztatott USB-eszköz engedélyezését. A felhasználó a hitelesítés megtörténtéig nem használhat hitelesítetlen billentyűzetet.

Virtuális billentyűzet használata az USB-eszközök hitelesítésére

A képernyőn megjelenő billentyűzetet csak olyan USB eszközök engedélyezésére szabad használni, amelyek nem támogatják véletlenszerű karakterek bevitelét (például vonalkódolvasók). Ismeretlen USB eszközök hitelesítéséhez nem javasoljuk a képernyőn megjelenő billentyűzet használatát.

A Képernyőn megjelenő billentyűzet engedélyezése vagy tiltása a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → BadUSB védelem** lehetőséget.
4. **Virtuális billentyűzet használatának tiltása az USB-eszközök hitelesítésére** jelölőnégyzettel engedélyezze vagy tiltsa le a képernyőn megjelenő billentyűzet engedélyezésre történő használatát.
5. Mentse el a módosításokat.

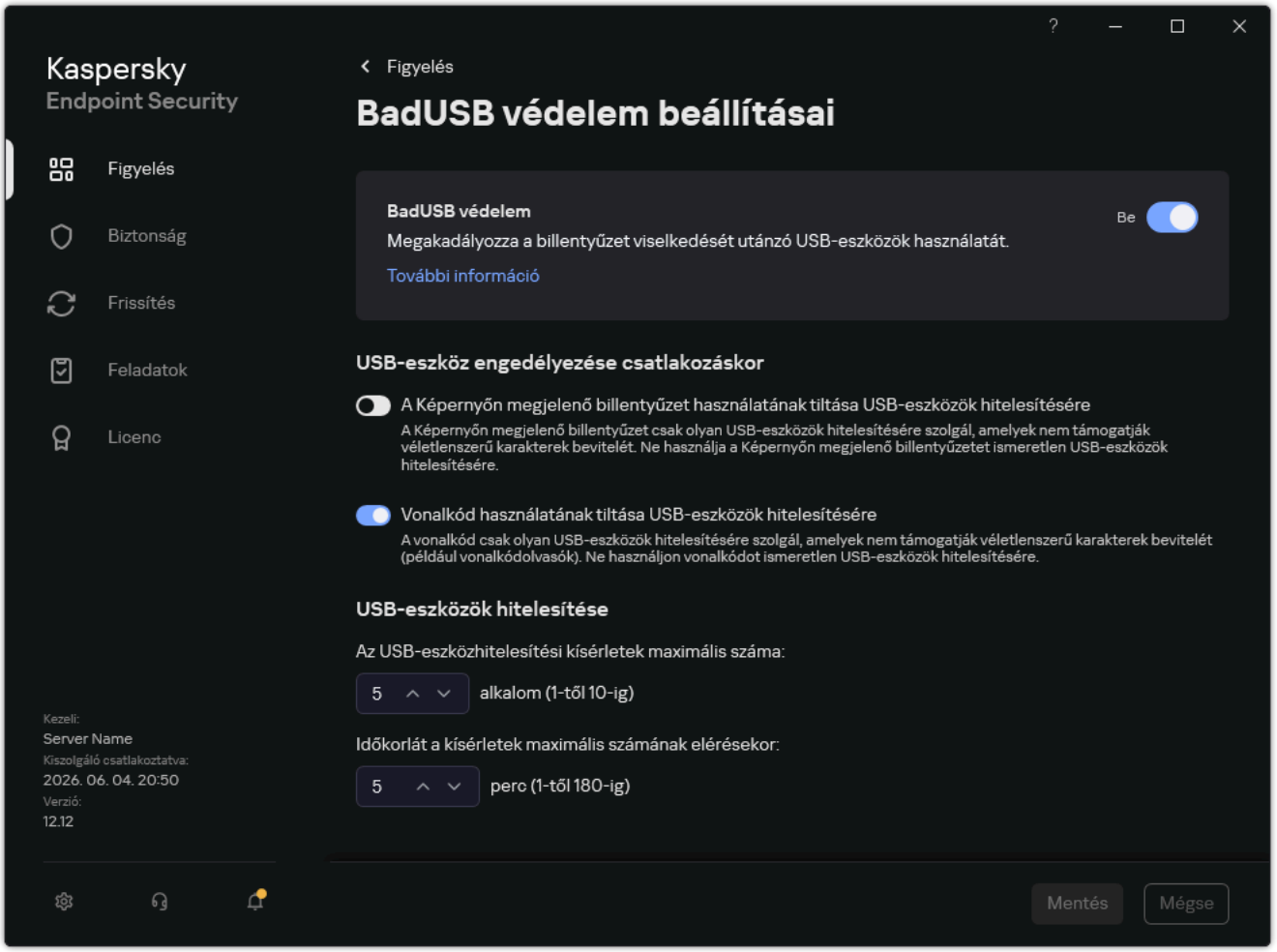
A Képernyőn megjelenő billentyűzet engedélyezése vagy tiltása hitelesítésre a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection → BadUSB Attack Prevention** elemet.
5. Használja a **Prohibit use of On-Screen Keyboard for authorization of USB devices** kapcsolót a képernyőn megjelenő billentyűzet használatának engedélyezésére vagy letiltására.
6. Mentse el a módosításokat.

A Képernyőn megjelenő billentyűzet engedélyezése vagy tiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni alapvető védelem → BadUSB védelem** lehetőséget.



A BadUSB Védelem összetevő beállításai

3. **A Képernyőn megjelenő billentyűzet használatának tiltása USB-eszközök hitelesítésére** kapcsolóval engedélyezze vagy tiltsa le a képernyőn megjelenő billentyűzet engedélyezésre történő használatát.

4. Mentse el a módosításokat.



USB-eszközök hitelesítése

Vonalkódolvasó engedélyezése

Amikor vonalkódolvasót csatlakoztat a számítógéphez, a BadUSB védelem összetevő bemeneti eszközként azonosítja ezt az eszközt, és engedélyezést kér. A vonalkódolvasó engedélyezéséhez be kell olvasnia a képernyőn megjelenő vonalkódot. Az alkalmazás egy Code39 formátumú vonalkódot generál, amelyet a legtöbb vonalkód- és QR-kódolvasó támogat.

A Kaspersky Endpoint Security egy másik vonalkódolvasó-hitelesítési módszert is támogat. Ha érintőképernyős eszközt használ, a kód beírásához használhatja a képernyőn megjelenő billentyűzetet. Ehhez engedélyeznie kell a képernyőn megjelenő billentyűzetet. Ez a módszer például a pénztárgépekbe beépített, helyhez kötött vonalkódolvasók esetében kényelmes. Más vonalkódolvasó-hitelesítési módszerek használata tilos.

Alapértelmezés szerint az alkalmazás nem használ vonalkódot az USB-eszközök hitelesítésére.

USB-eszközök vonalkóddal való hitelesítésének engedélyezése a felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Policies** lehetőséget.

3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

4. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → BadUSB védelem** lehetőséget.

5. A **Vonalkód használatának tiltása az USB-eszközök hitelesítésére** jelölőnégyzettel engedélyezze vagy tiltsa le a vonalkódok engedélyezésre történő használatát.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

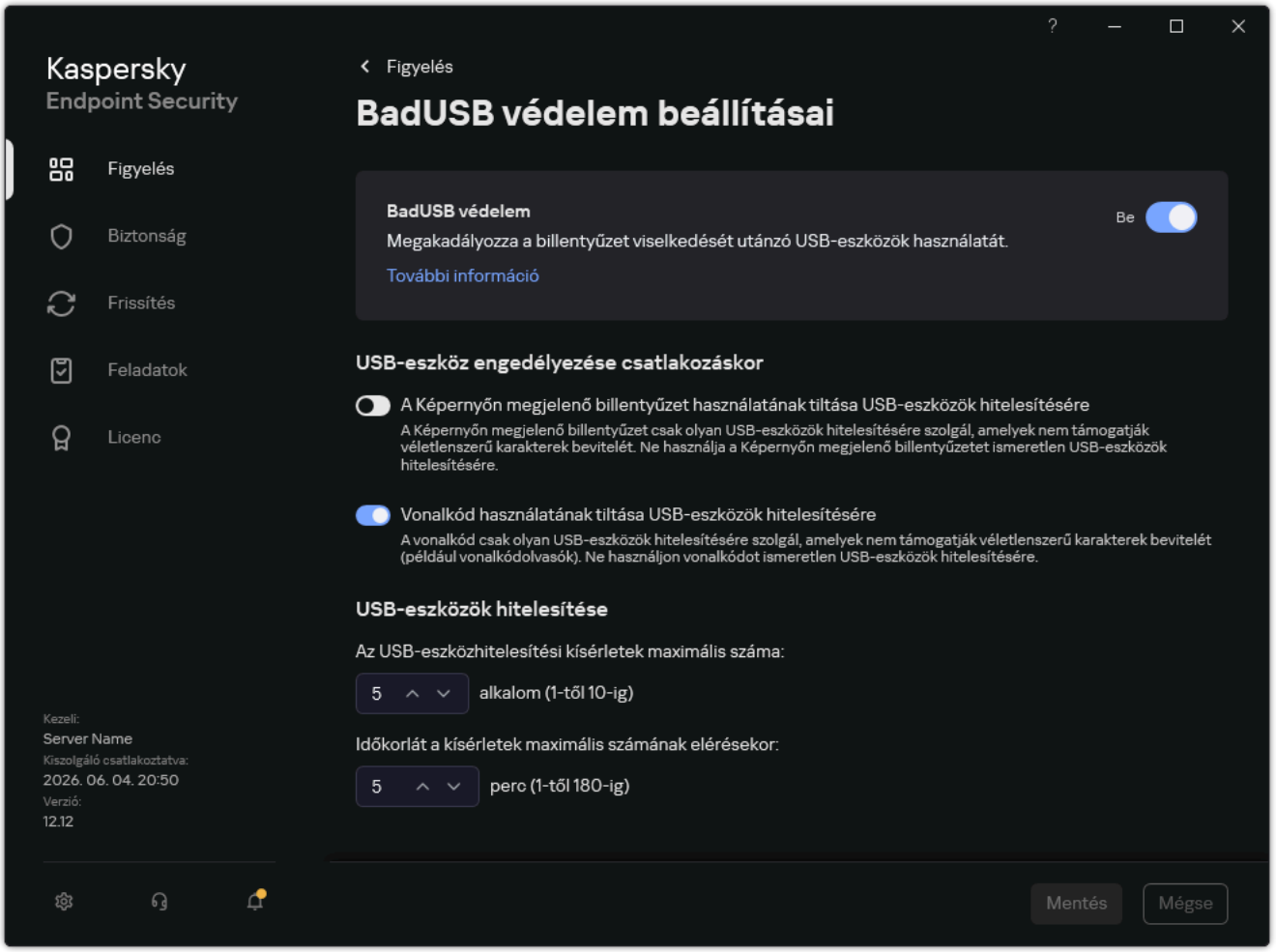
USB-eszközök vonalkóddal való hitelesítésének engedélyezése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **BadUSB Attack Prevention** elemet.
5. Használja a **Prohibit use of a barcode for authorization of USB devices** kapcsolót a vonalkódok hitelesítéshez való használatának engedélyezésére vagy letiltására.
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

USB-eszközök vonalkóddal való hitelesítésének engedélyezése az alkalmazás felületén

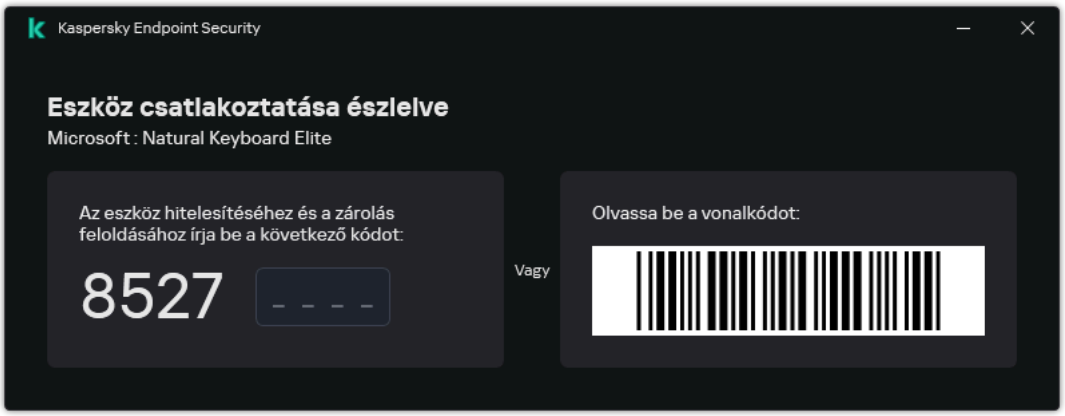
1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni alapvető védelem** → **BadUSB védelem** lehetőséget.



A BadUSB Védelem összetevő beállításai

3. A **Vonalkód használatának tiltása az USB-eszközök hitelesítésére** kapcsolóval engedélyezze vagy tiltsa le a vonalkódok engedélyezésre történő használatát.

4. Mentse el a módosításokat.

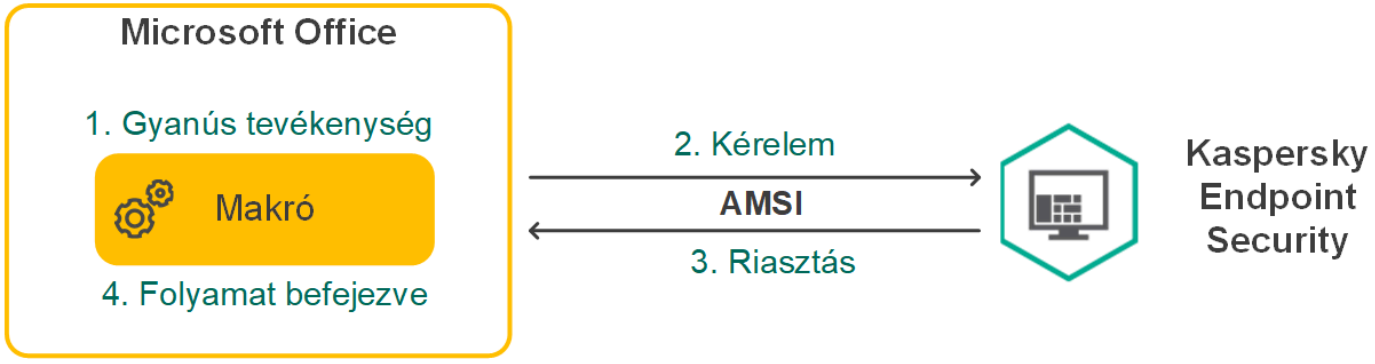


Vonalkódolvasó engedélyezése

AMSI védelem

Az AMSI védelmi összetevő a Microsoft által az Antimalware Scan Interface számára nyújtott támogatás. Az *Antimalware Scan Interface (AMSI)* engedélyezi a harmadik féltől származó, AMSI támogatással rendelkező alkalmazásoknak, hogy objektumokat küldjenek (például PowerShell szkripteket) a Kaspersky Endpoint Security számára további vizsgálat érdekében, valamint azt, hogy vizsgálati eredményeket kapjanak ezen objektumokról. Harmadik féltől származó alkalmazások közé tartozhatnak például a Microsoft Office alkalmazások (lásd az alábbi ábrát). Az AMSI részleteiért lásd a Microsoft dokumentációt.

Az AMSI védelem a fenyegetéseket csak észlelni tudja, valamint értesíteni a harmadik féltől származó alkalmazásokat ezekről. A harmadik féltől származó alkalmazás, miután értesítést kap a fenyegetésről, nem engedi a rosszindulatú tevékenységek végrehajtását (például leállítja a műveletet).



AMSI művelet – példa

Az AMSI védelmi összetevő elutasíthatja a harmadik féltől származó szolgáltató kérelmét, például akkor, ha az alkalmazás túllépte a megadott időtartamra meghatározott maximális kérelmek számát. A Kaspersky Endpoint Security információkat küld a harmadik féltől származó alkalmazások elutasított kérelmeiről az adminisztrációs kiszolgálónak. Az AMSI védelmi összetevő nem tagadja meg azoktól a külső alkalmazásoktól származó kéréseket, amelyekhez a folyamatos integráció az AMSI védelmi összetevővel engedélyezve van.

Az AMSI védelem a következő – munkaállomásokon, illetve kiszolgálókon futó – operációs rendszereken érhető el:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / több munkamenetes Enterprise
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2019 Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (beleértve a Server Core mode megoldást is)
- Windows Server 2025 Standard / Datacenter

Az AMSI védelem engedélyezése és letiltása

Alapértelmezés szerint az AMSI védelem engedélyezve van, és a Kaspersky által ajánlott módban működik (lásd az alábbi táblázatot).

Az AMSI védelem engedélyezése vagy letiltása a Felügyeleti konzolon (MMC)

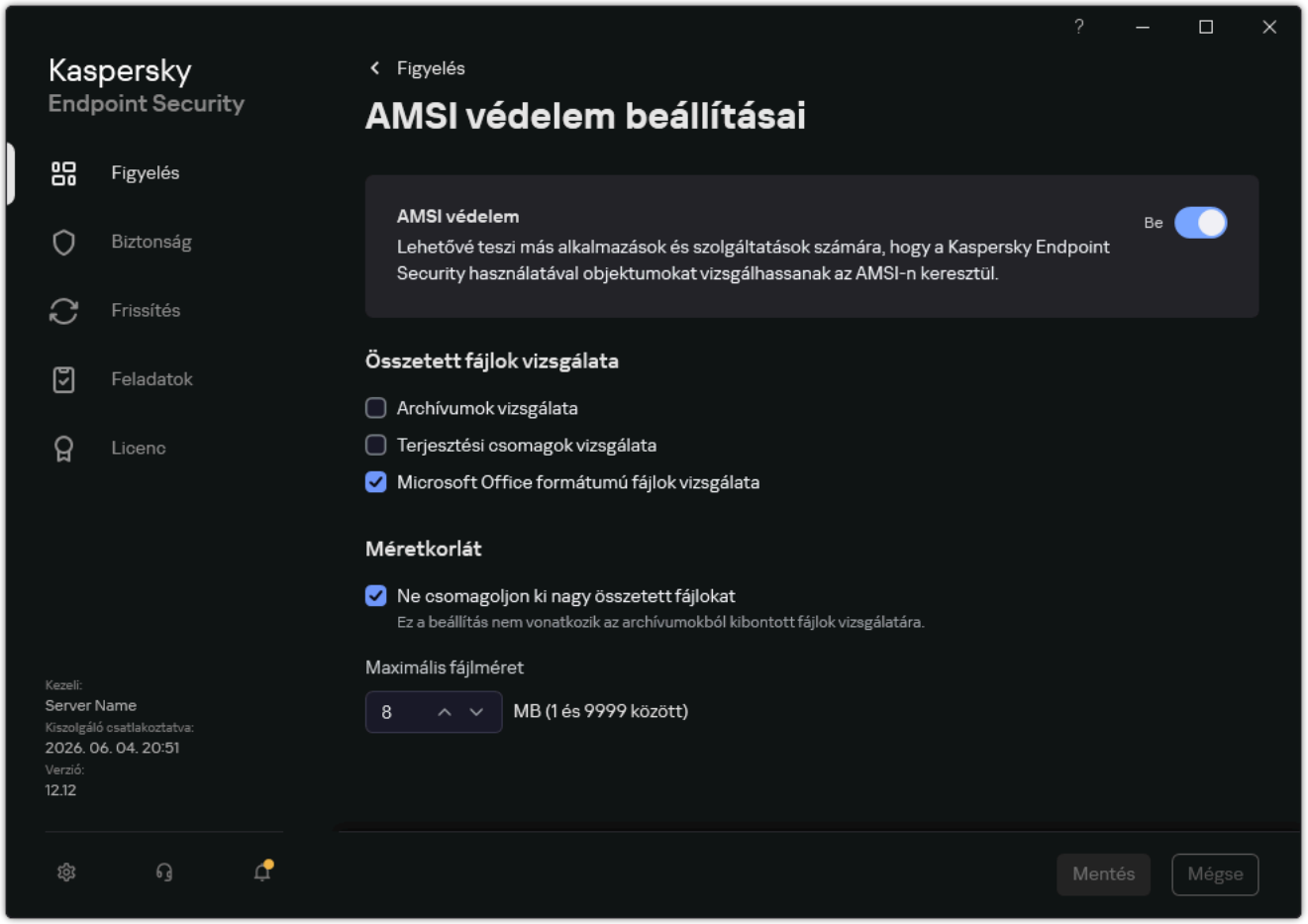
1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Fenyegetések elleni alapvető védelem** → **AMSI kereső** opciót.
4. Az **AMSI kereső** jelölőnégyzettel engedélyezheti vagy letilthatja az összetevőt.
5. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az AMSI védelem engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **AMSI Protection** elemet.
5. A **AMSI Protection ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Mentse el a módosításokat. A házirend számítógépeken való alkalmazásához zárolja a lakatokat .

Az AMSI védelem engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → AMSI védelem** opciót.



AMSI védelem beállításai

3. Az **AMSI védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

A Kaspersky szakértői által ajánlott AMSI védelem beállításai

Paraméter	Érték	Leírás
Archívumok vizsgálata	**Ki**	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.
Terjesztési csomagok vizsgálata	**Ki**	Harmadik féltől származó alkalmazások terjesztőcsomagjainak vizsgálata.
Microsoft Office formátumú fájlok vizsgálata	**Be**	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.
Ne csomagoljon ki nagy összetett fájlokat	**Maximális fájlméret 8 MB**	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás minden összetett fájlt megvizsgál. Az alkalmazás megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.

A fájlvizsgálat optimalizálása az AMSI védelemmel

Optimalizálhatja a fájlvizsgálatot: csökkentheti a vizsgálat idejét, és növelheti a Kaspersky Endpoint Security működési sebességét. Kiválaszthatja a vizsgálandó összetett fájlokat: archívumok, terjesztőcsomagok vagy Office formátumú fájlok. Korlátozhatja a vizsgálandó összetett fájlok méretét is. Az AMSI védelem összetevő nem csomagolja ki a megadott értéknél nagyobb méretű összetett fájlokat.

A vírusok és egyéb rosszindulatú programok álcázásának gyakori módja az összetett fájlokba, pl. archívumokba történő beágyazás. Az ilyen módon elrejtett vírusok és rosszindulatú programok felismeréséhez az összetett fájlt ki kell csomagolni, ami csökkentheti a vizsgálat sebességét. Korlátozhatja a vizsgálandó összetett fájlok típusát, így felgyorsíthatja a vizsgálatot.

Az AMSI védelem által végzett fájlvizsgálat optimalizálása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Fenyegetések elleni alapvető védelem** → **AMSI kereső** opciót.
4. Adja meg az **Összetett fájlok vizsgálata** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, terjesztőcsomagok, illetve Office formátumú fájlok.
5. A **Méretkorlát** blokkban végezze el az alábbiak egyikét:
   - Ha meg szeretné akadályozni, hogy az AMSI védelem összetevő kicsomagolja a nagy méretű összetett fájlokat, jelölje be az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet, és adja meg a szükséges értéket. Az AMSI védelem összetevő nem csomagolja ki a megadott értéknél nagyobb méretű összetett fájlokat.
   - Ha engedélyezni szeretné, hogy az AMSI védelem összetevő kicsomagolja a nagy méretű összetett fájlokat, törölje az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet.

   Az AMSI védelem összetevő az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzet be van-e jelölve.
6. Mentse el a módosításokat. A házirend számítógépeken való alkalmazásához zárolja a lakatokat .

Az AMSI védelem által végzett fájlvizsgálat optimalizálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **AMSI Protection** elemet.
5. Adja meg az **Scan of compound files** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, terjesztőcsomagok, illetve Office formátumú fájlok.

6. A **Scan optimization** részen hajtsa végre a következő műveletek valamelyikét:

   - Ha nem szeretné, hogy az AMSI védelem összetevő kicsomagolja a nagy összetett fájlokat, jelölje be a(z) **Size limits enabled** négyzetet, és adja meg a szükséges értéket. Az AMSI védelem összetevő nem csomagolja ki a megadott értéknél nagyobb méretű összetett fájlokat.

   - Ha engedélyezni szeretné, hogy az AMSI védelem összetevő kicsomagolja a nagy méretű összetett fájlokat, törölje az **Size limits enabled** jelölőnégyzetet.

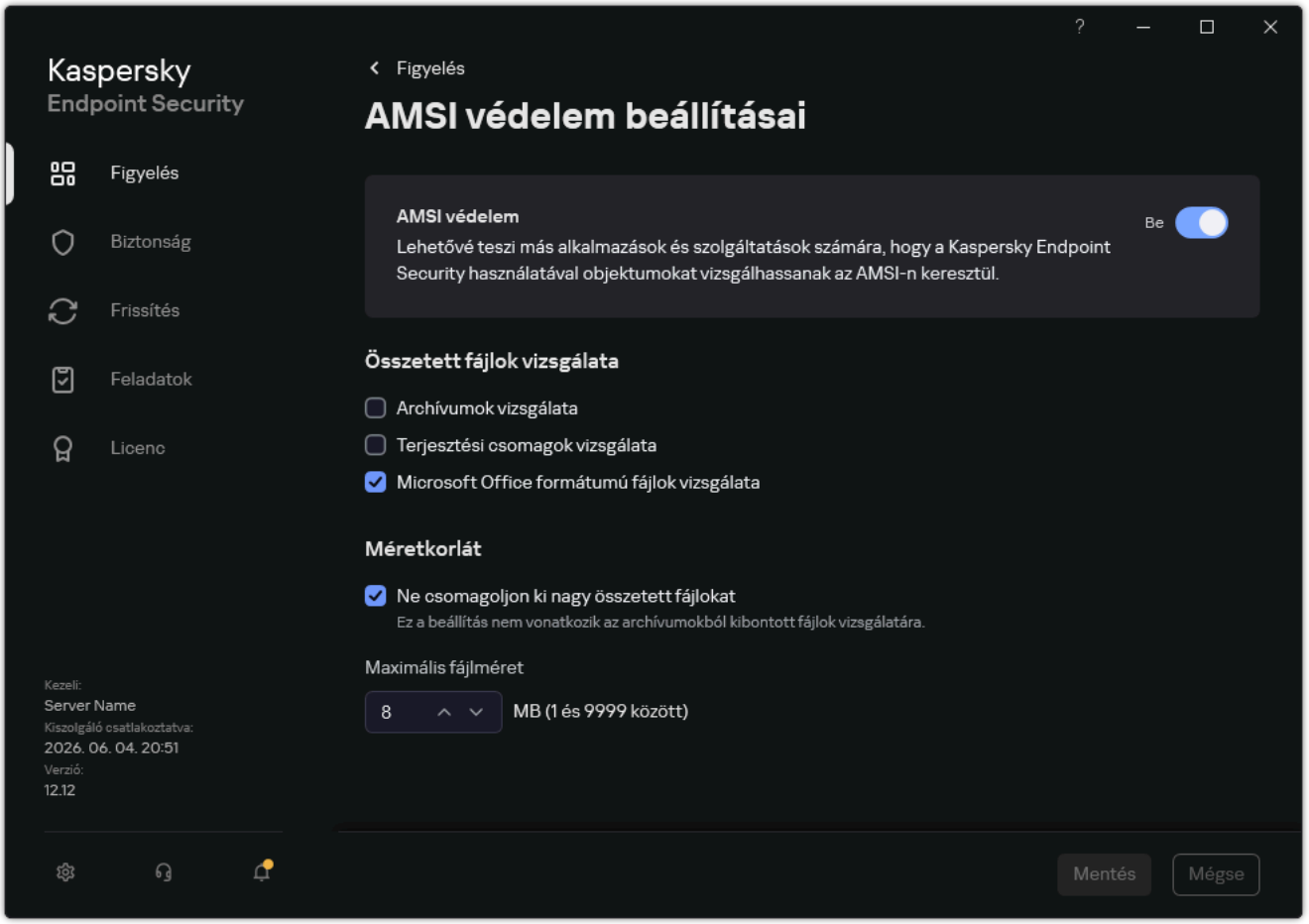
   Az AMSI Védelmi összetevő az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a(z) **Size limits enabled** jelölőnégyzet be van-e jelölve.

7. Mentse el a módosításokat. A házirend számítógépeken való alkalmazásához zárolja a lakatokat.

Az AMSI védelem által végzett fájlvizsgálat optimalizálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → AMSI védelem** opciót.



AMSI védelem beállításai

3. Adja meg az **Összetett fájlok vizsgálata** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, terjesztőcsomagok, illetve Office formátumú fájlok.

4. A **Méretkorlát** blokkban végezze el az alábbiak egyikét:

   - Ha meg szeretné akadályozni, hogy az AMSI védelem összetevő kicsomagolja a nagy méretű összetett fájlokat, jelölje be az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet, és adja meg a szükséges értéket. Az AMSI védelem összetevő nem csomagolja ki a megadott értéknél nagyobb méretű összetett fájlokat.

   - Ha engedélyezni szeretné, hogy az AMSI védelem összetevő kicsomagolja a nagy méretű összetett fájlokat, törölje az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet.

   Az AMSI védelem összetevő az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzet be van-e jelölve.

5. Mentse el a módosításokat.

Web védelem

A Web védelem összetevő megelőzi, hogy rosszindulatú fájlok legyenek letöltve az internetről, valamint blokkolja a rosszindulatú és az adathalász weboldalakat. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

A Kaspersky Endpoint Security csak a HTTP, HTTPS és az FTP forgalmat figyeli meg. A Kaspersky Endpoint Security vizsgálja az URL-eket és az IP-címeket.

A Webfelügyelő használatához el kell végeznie az alkalmazás kezdeti konfigurálását:

- A HTTPS forgalom figyeléséhez, engedélyezze a titkosított kapcsolatok vizsgálatát (alapértelmezés szerint engedélyezve van).

- Válassza ki azokat a portokat, amelyeket a Kaspersky Endpoint Security megoldásnak figyelnie kell (alapértelmezés szerint az alkalmazás az összes portot figyeli).

- Válassza ki azokat az alkalmazásokat, amelyeknek a forgalmát a Kaspersky Endpoint Securityvel meg szeretné figyelni. A legtöbb böngésző már szerepel a Kaspersky által ajánlott alkalmazások listáján. Ha a böngészője hiányzik a listáról, adja hozzá manuálisan.

- Javasoljuk, hogy illesszen be egy weboldal-interakciós parancsfájlt a webes forgalomba (alapértelmezés szerint a parancsfájl beillesztése le van tiltva). Ez a parancsfájl lehetővé teszi a Web védelem eseményeinek regisztrációját az alkalmazás eseménynaplójában, az operációs rendszer eseménynaplójában és a jelentésekben.

Ha a felhasználó rosszindulatú vagy adathalász weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést és figyelmeztetést jelenít meg.

A Web védelem engedélyezése és letiltása

A Web védelem összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. A Web védelemhez az alkalmazás különböző beállításcsoportokat alkalmazhat. Ezeket az alkalmazásban mentett beállításcsoportokat *biztonsági szinteknek* nevezzük: **magas**, **ajánlott**, **alacsony**. Az **Ajánlott** webes forgalom biztonsági szint beállításai tekinthetők optimálisnak, és a Kaspersky szakértői is ezeket ajánlják (lásd az alábbi táblázatot). Választhat a HTTP és FTP protokollokon keresztül fogadott és továbbított webes forgalom előtelepített biztonsági szintjei közül, illetve egyéni webes forgalmi biztonsági szintet állathat be. Ha módosítja a webes forgalom biztonsági szintjének beállításait, bármikor visszatérhet az ajánlott biztonsági szintbeállításokhoz.

A biztonsági szintet csak az Adminisztrációs konzolon (MMC) vagy az alkalmazás helyi felületén lehet kiválasztani vagy konfigurálni. Nem választhatja ki vagy konfigurálhatja a biztonsági szintet a Web Console-ban vagy a Cloud Console-ban.

A Web védelem összetevő engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** lehetőséget.
4. A **Web védelem** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
5. Ha engedélyezte az összetevőt, tegye az alábbiak egyikét a **Biztonsági szint** részben:
   - Ha valamelyik előtelepített biztonsági szintet szeretné alkalmazni, válassza ki a csúszkával:
     - **Magas**. Az a biztonsági szint, amely mellett a Web védelem a számítógépre HTTP-n és FTP-n keresztül érkező webes forgalom maximális vizsgálatát végzi. A Web védelem átfogó vizsgálatot végez minden objektumon az összes alkalmazás-adatbázis használatával, és elvégzi a lehető legalaposabb heurisztikus elemzést.
     - **Ajánlott**. Az alkalmazás teljesítménye és a webes forgalom biztonsága közti optimális egyensúlyt garantáló biztonsági szint. A Web védelem összetevő heurisztikus elemzése közepes vizsgálat szinten üzemel. A Kaspersky szakemberei ezt a webes forgalmi biztonsági szintet ajánlják. Az ajánlott biztonsági szint beállításainak értékeit az alábbi táblázat tartalmazza.
     - **Alacsony**. A webes forgalom biztonsági szintjének ezen beállításai biztosítják a webes forgalom vizsgálatának maximális sebességét. A Web védelem összetevő heurisztikus elemzése egyszerű vizsgálat szinten üzemel.
   - Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, és adja meg a saját összetevőbeállításait.

     Az előre beállított biztonsági szintek értékeit az **Alapértelmezett** gombra kattintva állíthatja vissza.

6. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a webes forgalomban észlelt rosszindulatú objektumokon végez:

   - **Blokkolás**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Web védelem blokkolja az objektumhoz való hozzáférést, és üzenetet jelenít meg a böngészőben.

   - **Tájékoztatás**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Kaspersky Endpoint Security engedélyezi az objektum letöltését a számítógépre, de a fertőzött objektumra vonatkozó információt fűz hozzá az aktív fenyegetések felsorolásához.

7. Mentse el a módosításokat.

A Web védelem összetevő engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Communication & Web Protection** → **Web Threat Protection** elemet.

5. A **Web Threat Protection ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Válassza ki a(z) **Action on threat detection** területen azt a műveletet, amelyet a Kaspersky Endpoint Security a webes forgalomban észlelt rosszindulatú objektumokon végez:

   - **Block**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Web védelem blokkolja az objektumhoz való hozzáférést, és üzenetet jelenít meg a böngészőben.

   - **Allow, inform, or prompt for action (depends on OS)**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Kaspersky Endpoint Security engedélyezi az objektum letöltését a számítógépre, de a fertőzött objektumra vonatkozó információt fűz hozzá az aktív fenyegetések felsorolásához.

7. Ha szükséges, készítse el a megbízható webcímek listáját.

8. Mentse el a módosításokat.

A Web védelem összetevő be- és kikapcsolása

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** opciót.

3. A **Web védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Ha engedélyezte az összetevőt, tegye az alábbiak egyikét a **Biztonsági szint** részben:

   - Ha valamelyik előtelepített biztonsági szintet szeretné alkalmazni, válassza ki a csúszkával:

     - **Magas**. Az a biztonsági szint, amely mellett a Web védelem a számítógépre HTTP-n és FTP-n keresztül érkező webes forgalom maximális vizsgálatát végzi. A Web védelem átfogó vizsgálatot végez minden objektumon az összes alkalmazás-adatbázis használatával, és elvégzi a lehető legalaposabb heurisztikus elemzést.

     - **Ajánlott**. Az alkalmazás teljesítménye és a webes forgalom biztonsága közti optimális egyensúlyt garantáló biztonsági szint. A Web védelem összetevő heurisztikus elemzése közepes vizsgálat szinten üzemel. A Kaspersky szakemberei ezt a webes forgalmi biztonsági szintet ajánlják. Az ajánlott biztonsági szint beállításainak értékeit az alábbi táblázat tartalmazza.

     - **Alacsony**. A webes forgalom biztonsági szintjének ezen beállításai biztosítják a webes forgalom vizsgálatának maximális sebességét. A Web védelem összetevő heurisztikus elemzése egyszerű vizsgálat szinten üzemel.

   - Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Speciális beállítások** gombra, és adja meg a saját összetevői beállításokat.

     Az előre beállított biztonsági szintek értékeit az **Ajánlott biztonsági szint visszaállítása** gombra kattintva állíthatja vissza.

5. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a webes forgalomban észlelt rosszindulatú objektumokon végez:

   - **Blokkolás**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Web védelem blokkolja az objektumhoz való hozzáférést, és üzenetet jelenít meg a böngészőben.

   - **Tájékoztatás**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Kaspersky Endpoint Security engedélyezi az objektum letöltését a számítógépre, de a fertőzött objektumra vonatkozó információt fűz hozzá az aktív fenyegetések felsorolásához.

6. Mentse el a módosításokat.

A Kaspersky szakértői által ajánlott Web védelem beállítások (ajánlott biztonsági szint)

Paraméter	Érték	Leírás
A webcím ellenőrzése a rosszindulatú webcímek adatbázisában	**Be**	A webes címek rosszindulatú URL-ek adatbázisában való ellenőrzésével nyomon követheti az elutasítási listához hozzáadott webhelyeket. A rosszindulatú webcímek adatbázisát a Kaspersky tartja karban, és az megtalálható az alkalmazás telepítőcsomagjában, továbbá a Kaspersky Endpoint Security adatbázisainak frissítésekor frissül.
A webcím ellenőrzése az adathalász webcímek adatbázisában	**Be**	Az adathalász webcímek adatbázisában megtalálhatók az adathalász támadások indítására használt, jelenleg ismert webhelyek webcímei. A Kaspersky az adathalász hivatkozások ezen adatbázisát egy az Anti-Phishing Working Groupként ismert nemzetközi szervezettől származó címekkel egészíti ki. Az adathalász webcímek adatbázisa megtalálható az alkalmazás telepítőcsomagjában, és a Kaspersky Endpoint Security adatbázisainak frissítésekor kiegészül.
Heurisztikus elemzés használata (Web védelem)	**Közepes vizsgálat**	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor a heurisztikus elemző vírusokat és más, fenyegetést jelentő alkalmazásokat keres a webes forgalomban, utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.

Paraméter	Érték	Leírás
Heurisztikus elemzés használata (Adathalászat elleni védelem)	**Be**	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve.
Művelet fenyegetés észlelésekor	**Blokkolás**	Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Web védelem blokkolja az objektumhoz való hozzáférést, és üzenetet jelenít meg a böngészőben.

A rosszindulatú webcím-észlelési módszerek konfigurálása

A Web védelem víruskeresői adatbázisok, a Kaspersky Security Network felhőszolgáltatás és a heurisztikus elemzés segítségével észleli a rosszindulatú webcímeket.

A rosszindulatú webcím-észlelési módszereket csak az Adminisztrációs konzolban (MMC) vagy az alkalmazás helyi felületén választhatja ki. Nem választhat ki rosszindulatú webcím-észlelési módszereket a Web Console-ban vagy a Cloud Console-ban. Az alapértelmezett beállítás a webcímek összehasonlítása a rosszindulatú címek adatbázisával heurisztikus elemzéssel (közepes vizsgálat).

Vizsgálat a rosszindulatú címek adatbázisának használatával

A webes címek rosszindulatú URL-ek adatbázisában való ellenőrzésével nyomon követheti az elutasítási listához hozzáadott webhelyeket. A rosszindulatú webcímek adatbázisát a Kaspersky tartja karban, és az megtalálható az alkalmazás telepítőcsomagjában, továbbá a Kaspersky Endpoint Security adatbázisainak frissítésekor frissül.

A Kaspersky Endpoint Security megvizsgálja az összes hivatkozást, hogy megállapítsa, hogy azok szerepelnek-e a rosszindulatú webcímek adatbázisaiban. Az alkalmazás biztonságos kapcsolatok vizsgálatára vonatkozó beállításai nincsenek hatással a hivatkozásvizsgálati funkcióra. Más szóval, ha a titkosított kapcsolatok vizsgálata le is van tiltva, a Kaspersky Endpoint Security a rosszindulatú webcímek adatbázisával akkor is ellenőrzi a hivatkozásokat, ha a forgalom titkosított kapcsolaton zajlik.

A webcímek rosszindulatú webcímek adatbázisával való összehasonlításának engedélyezése vagy letiltása az Adminisztrációs Konzol (MMC) használatával

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** lehetőséget.
4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
5. A megnyíló ablakban a hivatkozások rosszindulatú webcímek adatbázisai alapján történő ellenőrzésének engedélyezéséhez vagy letiltásához a **Vizsgálatmódok** részben jelölje be **A webcím ellenőrzése a rosszindulatú webcímek adatbázisában** jelölőnégyzetet, vagy törölje annak bejelölését.
6. Mentse el a módosításokat.

A címek rosszindulatú címadatbázissal való ellenőrzésének engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. A hivatkozások rosszindulatú webcímek adatbázisai alapján történő ellenőrzésének engedélyezéséhez vagy letiltásához a **Vizsgálatmódok** részben jelölje be **A webcím ellenőrzése a rosszindulatú webcímek adatbázisában** jelölőnégyzetet, vagy törölje annak bejelölését.
5. Mentse el a módosításokat.

Heurisztikus elemzés

A heurisztikus elemzés során a Kaspersky Endpoint Security elemzi az alkalmazások tevékenységét az operációs rendszerben. A heurisztikus elemzés képes az olyan fenyegetéseket észlelni, amelyeknek még nem szerepel bejegyzése a Kaspersky Endpoint Security adatbázisaiban.

Amikor a heurisztikus elemző vírusokat és más, fenyegetést jelentő alkalmazásokat keres a webes forgalomban, utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alaposságát, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.

A heurisztikus elemzés engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** lehetőséget.
4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
5. A megnyíló ablakban a **Vizsgálatmódok** részben jelölje be a **Heurisztikus elemzés használata** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás heurisztikus elemzést használjon a webes forgalom vírusokra és egyéb rosszindulatú programokra való vizsgálatakor.
6. Állítsa be a csúszkával a heurisztikus elemzés szintjét: **egyszerű vizsgálat**, **közepes vizsgálat** vagy **alapos vizsgálat**.

   Amikor a heurisztikus elemző vírusokat és más, fenyegetést jelentő alkalmazásokat keres a webes forgalomban, utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alaposságát, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
7. Mentse el a módosításokat.

A heurisztikus elemzés használatának engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. A **Vizsgálatmódok** blokkban jelölje be a **Heurisztikus elemzés használata** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás heurisztikus elemzést használjon a webes forgalom vírusokra és egyéb rosszindulatú programokra való vizsgálatakor.

   Amikor a heurisztikus elemző vírusokat és más, fenyegetést jelentő alkalmazásokat keres a webes forgalomban, utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alaposságát, az operációs rendszer erőforrásinak terhelését, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
5. Mentse el a módosításokat.

Adathalászat elleni védelem

A Web védelem ellenőrzi a hivatkozásokat, hogy megbizonyosodjon arról, hogy azok adathalász webcímekhez tartoznak-e. Ezzel segít megelőzni az *adathalász támadásokat*. Az adathalász támadás álcázható például egy e-mail üzenetként is, mely állítólag a banktól érkezett, és a bank hivatalos webhelyére mutató hivatkozást tartalmaz. Ha a hivatkozásra kattint, a bank webhelyének pontos másolatára jut. A böngésző címsorában a valódi webcímet fogja látni még akkor is, ha ténylegesen egy hamisított webhelyen tartózkodik. Ettől a ponttól kezdve a webhelyen végzett minden műveletét rögzítik, és felhasználhatják a pénze megszerzéséhez.

Mivel adathalász webhelyekre mutató hivatkozást nem csupán e-mail üzenetben kaphat, hanem más módokon, például üzenetküldő alkalmazásban is, a Web védelem összetevő a webes forgalom szintjén követi nyomon az adathalász helyek elérésének kísérletét, és blokkolja az ilyen helyekhez való hozzáférést. A Kaspersky Endpoint Security terjesztőkészletében megtalálhatók az adathalász URL-ek listái.

Az adathalászat elleni védelem csak az Adminisztrációs konzolon (MMC) vagy az alkalmazás helyi felületén konfigurálható. Az adathalászat elleni védelem nem konfigurálható a Web Console-ban vagy a Cloud Console-ban. Alapértelmezés szerint a heurisztikus elemzéssel végzett adathalászat elleni védelem engedélyezve van.

Az adathalászat elleni védelem engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** lehetőséget.
4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

5. Az adathalászat elleni védelem engedélyezéséhez vagy letiltásához a megnyíló ablak **Adathalászat elleni védelem beállításai** részében jelölje be **A webcím ellenőrzése az adathalász webcímek adatbázisában** jelölőnégyzetet, vagy törölje annak bejelölését.

   Az adathalász webcímek adatbázisában megtalálhatók az adathalász támadások indítására használt, jelenleg ismert webhelyek webcímei. A Kaspersky az adathalász hivatkozások ezen adatbázisát egy az Anti-Phishing Working Groupként ismert nemzetközi szervezettől származó címekkel egészíti ki. Az adathalász webcímek adatbázisa megtalálható az alkalmazás telepítőcsomagjában, és a Kaspersky Endpoint Security adatbázisainak frissítésekor kiegészül.

6. Jelölje be a **Heurisztikus elemzés használata** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás heurisztikus elemzést használjon a weboldalak adathalászati hivatkozásokra való vizsgálatakor.

   A heurisztikus elemzés során a Kaspersky Endpoint Security elemzi az alkalmazások tevékenységét az operációs rendszerben. A heurisztikus elemzés képes az olyan fenyegetéseket észlelni, amelyeknek még nem szerepel bejegyzése a Kaspersky Endpoint Security adatbázisaiban.

   A hivatkozások vizsgálatához a víruskereső adatbázison és a heurisztikus elemzésen kívül használhatja a Kaspersky Security Network reputációs adatbázisait.

7. Mentse el a módosításokat.

Az Adathalászat elleni védelem engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Web védelem** opciót.

3. Kattintson a **Speciális beállítások** elemre.

4. Ha azt szeretné, hogy a Web védelem összetevő ellenőrizze a hivatkozásokat az adathalász webcímek adatbázisaiban, jelölje be **A webcím ellenőrzése az adathalász webcímek adatbázisában** jelölőnégyzetet az **Adathalászat elleni védelem** blokkban. Az adathalász webcímek adatbázisában megtalálhatók az adathalász támadások indítására használt, jelenleg ismert webhelyek webcímei. A Kaspersky az adathalász hivatkozások ezen adatbázisát egy az Anti-Phishing Working Groupként ismert nemzetközi szervezettől származó címekkel egészíti ki. Az adathalász webcímek adatbázisa megtalálható az alkalmazás telepítőcsomagjában, és a Kaspersky Endpoint Security adatbázisainak frissítésekor kiegészül.

5. Jelölje be a **Heurisztikus elemzés használata** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás heurisztikus elemzést használjon a weboldalak adathalászati hivatkozásokra való vizsgálatakor.

   A heurisztikus elemzés során a Kaspersky Endpoint Security elemzi az alkalmazások tevékenységét az operációs rendszerben. A heurisztikus elemzés képes az olyan fenyegetéseket észlelni, amelyeknek még nem szerepel bejegyzése a Kaspersky Endpoint Security adatbázisaiban.

   A hivatkozások vizsgálatához a víruskereső adatbázison és a heurisztikus elemzésen kívül használhatja a Kaspersky Security Network reputációs adatbázisait.

6. Mentse el a módosításokat.

Megbízható webcímek listájának létrehozása

A rosszindulatú és adathalász webhelyek mellett a Web védelem más webhelyeket is blokkolhat. A Web védelem például blokkolja az RFC-szabványoknak nem megfelelő HTTP-forgalmat. Létrehozhatja azon URL-ek listáját, amelyeknek a tartalmában megbízik. A Web védelem nem elemzi a megbízható webcímekről érkező információkban a vírusok és egyéb fenyegetések jelenlétét. Ez a lehetőség akkor lehet hasznos például, ha a Web védelem összetevő zavarja egy fájl letöltését egy ismert webhelyről.

Az URL egy adott weboldal vagy egy webhely címe lehet.

A szabályzatban szereplő megbízható webcímek listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Védett webcím hozzáadásának menete az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** lehetőséget.
4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
5. A megnyíló ablakban válassza a **Megbízható webcímek** lapfület.
6. Jelölje be a **Ne vizsgálja a megbízható webcímekről érkező webes forgalmat** jelölőnégyzetet.

   Ha az opció be van jelölve, a Web védelem összetevő nem vizsgálja az olyan weboldalak/webhelyek tartalmát, amelyek címe szerepel a megbízható webcímek listáján. A megbízható webcímek listájára a megadott weboldal/webhely címét, illetve címmaszkját egyaránt felveheti.
7. Hozzon létre egy listát olyan URL-ekről/weboldalakról, amelyek tartalmában megbízik.

   A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

   A megbízható webcímek listáját XML-fájlból is importálhatja.
8. Mentse el a módosításokat.

Megbízható webcím hozzáadásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Communication & Web Protection** → **Web Threat Protection** elemet.
5. Kattintson az **Trusted web addresses** gombra.
6. Hozzon létre egy listát olyan URL-ekről/weboldalakról, amelyek tartalmában megbízik.

   A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

   A megbízható webcímek listáját egy JSON fájlból is importálhatja.
7. Mentse el a módosításokat.

Megbízható webcím hozzáadásának menete az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.
4. Jelölje be a **Ne vizsgálja a megbízható URL-ek** jelölőnégyzetet.

   Ha az opció be van jelölve, a Web védelem összetevő nem vizsgálja az olyan weboldalak/webhelyek tartalmát, amelyek címe szerepel a megbízható webcímek listáján. A megbízható webcímek listájára a megadott weboldal/webhely címét, illetve címmaszkját egyaránt felveheti.
5. Hozzon létre egy listát olyan URL-ekről/weboldalakról, amelyek tartalmában megbízik.

   A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

   A megbízható webcímek listáját XML-fájlból is importálhatja.
6. Mentse el a módosításokat.

Ennek eredményeként a Web védelem nem vizsgálja a megbízható webcímek forgalmát. A felhasználó mindig megnyithat egy megbízható webhelyet, és letölthet egy fájlt arról. Ha nem tud hozzáférni a webhelyhez, ellenőrizze a Titkosított kapcsolatok vizsgálata, a Webfelügyelő és Hálózati portok figyelése összetevők beállításait. Ha a Kaspersky Endpoint Security rosszindulatúként észlel egy megbízható webhelyről letöltött fájlt, felveheti a fájlt a kizárásokhoz.

A titkosított kapcsolatokra vonatkozó kizárások általános listáját is létrehozhatja. Ebben az esetben a Kaspersky Endpoint Security nem vizsgálja a megbízható webcímek HTTPS-forgalmát, amikor a Web védelem, a Levelezés védelem és a Webfelügyelő összetevők végzik a munkájukat.

Megbízható webcímek listájának exportálása és importálása

A megbízható webcímek listáját exportálhatja egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú webcím hozzáadásával. Használhatja az exportálás/importálás funkciót a megbízható webcímek biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A megbízható webcímek listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Web védelem** lehetőséget.
4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
5. A megnyíló ablakban válassza a **Megbízható webcímek** lapfület.
6. A megbízható webcímek listájának exportálása:
   a. Jelölje ki az exportálni kívánt megbízható webcímeket. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
      Ha nem jelölt ki egy megbízható webcímet sem, a Kaspersky Endpoint Security az összes webcímet exportálja.
   b. Kattintson az **Exportálás** hivatkozásra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a megbízható webcímek listáját, és válassza a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security a megbízható webcímek teljes listáját exportálja az XML-fájlba.
7. Megbízható címek listájának importálása:
   a. Kattintson az **Import** hivatkozásra.
      A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a megbízható címek listáját.
   b. Nyissa meg a fájlt.
      Ha a számítógépen már létezik egy lista a megbízható címekről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba az XML-fájlból.
8. Mentse el a módosításokat.

A megbízható webcímek listájának exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Communication & Web Protection** → **Web Threat Protection** elemet.

5. A kizárások listájának exportálása a(z) **Rules list** területen:

   a. Jelölje ki az exportálni kívánt megbízható webcímeket.

   b. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a megbízható webcímek listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

6. A kizárások listájának importálása a **Rules list** területen:

   a. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a megbízható címek listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a megbízható címekről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba az JSON-fájlból.

7. Mentse el a módosításokat.

Levelezés védelem

A „Levelezés védelem" összetevő a bejövő és kimenő e-mail üzenetek mellékleteiben vizsgálja a vírusok és egyéb fenyegetések jelenlétét. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

A Levelezés védelem a bejövő és a kimenő üzeneteket is képes megvizsgálni. Az alkalmazás támogatja a POP3, SMTP, IMAP és NNTP protokollokat a következő levelezőprogramokban:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

A Mozilla Thunderbird, MyOffice Mail és R7-Office Organizer levelezőprogramok forgalmának vizsgálatához hozzá kell adnia a Kaspersky tanúsítványt a tanúsítványtárolóhoz, és ki kell választania a saját tanúsítványtárolót.

A Levelezés védelem nem támogat más protokollokat és levelezőprogramokat.

A Levelezés védelem nem mindig képes *protokollszintű* hozzáférést biztosítani az üzenetekhez (például a Microsoft Exchange megoldás használata esetén). Emiatt a Levelezés védelem tartalmaz egy bővítményt a Microsoft Office Outlookhoz. A bővítmény lehetővé teszi az üzenetek vizsgálatát a *levelezőprogram szintjén*. A Levelezés védelem bővítmény az Outlook 2010, 2013, 2016, 2019, 2021, 2024 és 365 32 bites és 64 bites verzióit támogatja. Az ARM-alapú számítógépeken a Levelezés védelem bővítmény az Outlook 2016, az Outlook 2021, az Outlook 2024 és az Outlook 365 for Arm64 32 bites és 64 bites verzióit támogatja.

A „Levelezés védelem" összetevő nem vizsgálja az üzeneteket, ha a levelezési ügyfélprogram böngészőben van megnyitva.

Egy rosszindulatú fájl csatolmányban történő észlelése esetén a Kaspersky Endpoint Security egy, a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Az üzenet feldolgozása megtörtént] <üzenet tárgysora>*.

A Levelezés védelem engedélyezése és letiltása

A Levelezés védelem összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. A Levelezés védelemhez az alkalmazás különböző beállításcsoportokat alkalmazhat. Ezeket az alkalmazásban mentett beállításcsoportokat *biztonsági szinteknek* nevezzük: **magas**, **ajánlott**, **alacsony**. Az **Ajánlott** levelezési biztonsági szint beállításai tekinthetők optimálisnak, és a Kaspersky szakértői is ezeket ajánlják (lásd az alábbi táblázatot). Kiválaszthatja az előre beállított e-mail-biztonsági szintek egyikét, de egyéni beállításokat is megadhat. Ha módosította az e-mail-biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.

A Mozilla Thunderbird levelezőprogram használata esetén a Levelezés védelem összetevő nem vizsgálja az IMAP protokollon keresztül továbbított üzenetekben a vírusok és egyéb fenyegetések jelenlétét, ha az üzenetek szűrők segítségével vannak áthelyezve a Beérkezett üzenetek mappából.

A Levelezés védelem összetevő engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Fenyegetések elleni alapvető védelem** → **Levelezés védelem** lehetőséget.
4. A **Levelezés védelem** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.

5. Ha engedélyezte az összetevőt, tegye az alábbiak egyikét a **Biztonsági szint** részben:

   - Ha valamelyik előtelepített biztonsági szintet szeretné alkalmazni, válassza ki a csúszkával:

     - **Magas**. Ha ez az e-mail-biztonsági szint van kiválasztva, a Levelezés védelem összetevő a legalaposabban vizsgálja meg az e-mail-üzeneteket. A Levelezés védelem összetevő megvizsgálja a bejövő és kimenő e-mail-üzeneteket, és mély heurisztikus elemzést végez. A Magas levelezés biztonsági szint a magas kockázatú környezetekhez ajánlott. Például ilyen környezet egy ingyenes e-mail szolgáltatáshoz történő csatlakozás központi e-mail védelemmel nem rendelkező otthoni hálózatból.

     - **Ajánlott**. Az alkalmazás teljesítménye és az e-mail-biztonság közti optimális egyensúlyt garantáló biztonsági szint. A Levelezés védelem összetevő megvizsgálja a bejövő és kimenő e-mail-üzeneteket, és közepes szintű heurisztikus elemzést végez. Ezt a levélforgalmi biztonsági szintet ajánlják a Kaspersky szakemberei. Az ajánlott biztonsági szint beállításainak értékeit az alábbi táblázat tartalmazza.

     - **Alacsony**. Ennél az e-mail-biztonsági szintnél a Levelezés védelem összetevő csak a bejövő e-mail üzeneteket vizsgálja, egyszerű heurisztikus elemzést végez, és nem vizsgálja az e-mail üzenetekhez mellékelt archívumokat. Ennél az e-mail-biztonsági szintnél a Levelezés védelem összetevő az e-mail üzenetek elemzését maximális sebességgel, az operációs rendszer erőforrásainak minimális kihasználása mellett végzi. Jól védett környezetben Alacsony e-mail-biztonsági szint ajánlott. Ilyen környezet lehet például a központi e-mail védelemmel rendelkező vállalati helyi hálózat.

   - Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, és adja meg a saját összetevőbeállításait.

     Az előre beállított biztonsági szintek értékeit az **Alapértelmezett** gombra kattintva állíthatja vissza.

6. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a rosszindulatú objektumokon végez:

   - **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás törli a fertőzött objektumot. Az alkalmazás a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Üzenet fel lett dolgozva] <üzenet tárgysora>*.

   - **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel egy bejövő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel egy kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

   - **Blokkolás**. Ha fertőzött objektumot észlel valamely bejövő üzenetben, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Levelezés védelem összetevő engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Communication & Web Protection** → **Mail Threat Protection** elemet.

5. A **Mail Threat Protection ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Válassza ki a **Action on threat detection** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a rosszindulatú objektumokon végez:

   - **Disinfect, delete if disinfection fails**. Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás törli a fertőzött objektumot. Az alkalmazás a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Üzenet fel lett dolgozva] <üzenet tárgysora>*.

   - **Disinfect, block if disinfection fails**. Ha fertőzött objektumot észlel egy bejövő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel egy kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

   - **Block**. Ha fertőzött objektumot észlel valamely bejövő üzenetben, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

7. Ha szükséges, szerkessze a Levelezés védelem speciális beállításait.

8. Mentse el a módosításokat.

A Levelezés védelem összetevő engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Levelezés védelem** opciót.

3. A **Levelezés védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Ha engedélyezte az összetevőt, tegye az alábbiak egyikét a **Biztonsági szint** részben:

   - Ha valamelyik előtelepített biztonsági szintet szeretné alkalmazni, válassza ki a csúszkával:

     - **Magas**. Ha ez az e-mail-biztonsági szint van kiválasztva, a Levelezés védelem összetevő a legalaposabban vizsgálja meg az e-mail-üzeneteket. A Levelezés védelem összetevő megvizsgálja a bejövő és kimenő e-mail-üzeneteket, és mély heurisztikus elemzést végez. A Magas levelezés biztonsági szint a magas kockázatú környezetekhez ajánlott. Például ilyen környezet egy ingyenes e-mail szolgáltatáshoz történő csatlakozás központi e-mail védelemmel nem rendelkező otthoni hálózatból.

     - **Ajánlott**. Az alkalmazás teljesítménye és az e-mail-biztonság közti optimális egyensúlyt garantáló biztonsági szint. A Levelezés védelem összetevő megvizsgálja a bejövő és kimenő e-mail-üzeneteket, és közepes szintű heurisztikus elemzést végez. Ezt a levélforgalmi biztonsági szintet ajánlják a Kaspersky szakemberei. Az ajánlott biztonsági szint beállításainak értékeit az alábbi táblázat tartalmazza.

     - **Alacsony**. Ennél az e-mail-biztonsági szintnél a Levelezés védelem összetevő csak a bejövő e-mail üzeneteket vizsgálja, egyszerű heurisztikus elemzést végez, és nem vizsgálja az e-mail üzenetekhez mellékelt archívumokat. Ennél az e-mail-biztonsági szintnél a Levelezés védelem összetevő az e-mail üzenetek elemzését maximális sebességgel, az operációs rendszer erőforrásainak minimális kihasználása mellett végzi. Jól védett környezetben Alacsony e-mail-biztonsági szint ajánlott. Ilyen környezet lehet például a központi e-mail védelemmel rendelkező vállalati helyi hálózat.

   - Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Speciális beállítások** gombra, és adja meg a saját összetevői beállításokat.

     Az előre beállított biztonsági szintek értékeit az **Ajánlott biztonsági szint visszaállítása** gombra kattintva állíthatja vissza.

5. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a rosszindulatú objektumokon végez:

   - **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás törli a fertőzött objektumot. Az alkalmazás a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Üzenet fel lett dolgozva] <üzenet tárgysora>*.

   - **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel egy bejövő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel egy kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

   - **Blokkolás**. Ha fertőzött objektumot észlel valamely bejövő üzenetben, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

6. Mentse el a módosításokat.

A Levelezés védelem Kaspersky szakértői által ajánlott beállításai (ajánlott biztonsági szint)

Paraméter	Érték	Leírás
Védelem hatóköre	**Bejövő és kimenő üzenetek**	A *védelem hatóköre* magában foglalja azokat az objektumokat, amelyeket az összetevő a futtatáskor ellenőriz: bejövő és kimenő üzenetek vagy csak bejövő üzenetek. A számítógép védelméhez csak a bejövő üzeneteket kell megvizsgálni. Bekapcsolhatja a kimenő üzenetek vizsgálatát is, hogy megakadályozza a fertőzött fájlok archívumokban történő továbbítását. A kimenő üzenetek vizsgálatát akkor is bekapcsolhatja, ha meg akarja akadályozni, hogy bizonyos formátumú fájlok – például hang- és videofájlok – kerüljenek küldésre.
Microsoft Outlook-bővítmény csatlakoztatása	**Be**	Ha a jelölőnégyzetben van jelölés, a POP3, az SMTP, az NNTP és az IMAP protokollal továbbított e-mail üzenetek vizsgálata a Microsoft Outlookba beépített bővítmény oldalán van engedélyezve. Ha az e-mailek vizsgálata a Microsoft Outlook bővítményével történik, akkor javasoljuk a Cached Exchange Mode használatát. A gyorsítótáras Exchange móddal kapcsolatban további információ, valamint a használatára vonatkozó ajánlások a Microsoft Tudásbázisban találhatók.
Csatolt archívumok vizsgálata	**Be**	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.
Microsoft Office formátumú csatolt fájlok vizsgálata	**Be**	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.
Mellékletszűrő	**Kiválasztott típusú mellékletek átnevezése**	Ha ezt a lehetőséget választja, a Levelezés védelem összetevő a megadott típusú csatolt fájlok kiterjesztésének utolsó karakterét aláhúzásjellel helyettesíti (például melléklet.doc_). Így a fájl megnyitásához a felhasználónak át kell neveznie a fájlt.
Heurisztikus elemzés	**Közepes vizsgálat**	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
Művelet fenyegetés észlelésekor	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**	Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás törli a fertőzött objektumot. Az alkalmazás a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Üzenet fel lett dolgozva] <üzenet tárgysora>*.

A fertőzött e-mail üzeneteken végrehajtandó művelet módosítása

Alapértelmezett esetben a Levelezés védelem összetevő automatikusan megpróbálja az összes észlelt fertőzött e-mail üzenetet vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Levelezés védelem összetevő törli a fertőzött e-mail üzeneteket.

A fertőzött e-mail üzeneteken végrehajtandó művelet módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Levelezés védelem** opciót.

3. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security fertőzött üzenet észlelése esetén végez:

   - **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás törli a fertőzött objektumot. Az alkalmazás a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Üzenet fel lett dolgozva] <üzenet tárgysora>*.

   - **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel egy bejövő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel egy kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

   - **Blokkolás**. Ha fertőzött objektumot észlel valamely bejövő üzenetben, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.

4. Mentse el a módosításokat.

A Levelezés védelem összetevő védelmi hatókörének kialakítása

A *védelem hatóköre* azon objektumok körére utal, amelyeket az összetevő aktív állapotában vizsgál. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak. A Levelezés védelem összetevő védelmi hatókörének tulajdonságai közé a Levelezés védelem levelezőprogramokba való integrációjának beállításai, valamint az e-mail üzenetek típusainak és azon e-mail protokolloknak a beállításai tartoznak, amelyeknek forgalmát a Levelezés védelem összetevő vizsgálja. A Kaspersky Endpoint Security alapértelmezés szerint vizsgálja a bejövő és kimenő e-maileket, valamint a POP3, SMTP, NNTP és IMAP protokollok forgalmát, és integrálva van a Microsoft Office Outlook levelezőprogramba.

A Levelezés védelem összetevő védelmi hatókörének kialakítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Levelezés védelem** opciót.

3. Kattintson a **Speciális beállítások** elemre.

4. A **Védelem hatóköre** blokkban válassza ki a vizsgálandó üzenetet:

   - **Bejövő és kimenő üzenetek**.

   - **Csak bejövő üzenetek**.

   A számítógép védelméhez csak a bejövő üzeneteket kell megvizsgálni. Bekapcsolhatja a kimenő üzenetek vizsgálatát is, hogy megakadályozza a fertőzött fájlok archívumokban történő továbbítását. A kimenő üzenetek vizsgálatát akkor is bekapcsolhatja, ha meg akarja akadályozni, hogy bizonyos formátumú fájlok – például hang- és videofájlok – kerüljenek küldésre.

Ha úgy fönt, hogy csak a bejövő üzeneteket vizsgálja, javasoljuk, hogy egyszer vizsgálja meg az összes kimenő üzenetet is, mivel fennáll a veszélye, hogy a számítógépen e-mail férgek találhatók, melyek e-mailben terjednek. Ezzel elkerülheti az olyan problémákat, amelyeket az Ön számítógépéről érkező ellenőrizetlen tömeges fertőzött üzenetek okozhatnak.

5. A **Kapcsolat** részben végezze el az alábbiak egyikét:

   - Ha azt szeretné, hogy a Levelezés védelem összetevő megvizsgálja a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzeneteket, mielőtt azokat fogadja a felhasználó számítógépe, jelölje be a **POP3-, SMTP-, NNTP- és IMAP-forgalom vizsgálata** jelölőnégyzetet.

     Ha nem szeretné, hogy a Levelezés védelem összetevő megvizsgálja a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzeneteket, mielőtt azok megérkeznek a felhasználó számítógépére, törölje a **POP3 / SMTP / NNTP és IMAP forgalom vizsgálata** jelölőnégyzetet. Ilyenkor a Levelezés védelem Microsoft Office Outlook levelezőprogramba beépült kiterjesztése azután vizsgálja az e-mail üzeneteket, hogy azok a felhasználó számítógépére letöltődtek, ha be van jelölve a **Microsoft Outlook-bővítmény csatlakoztatása** jelölőnégyzetet.

     Ha nem Microsoft Office Outlook levelezőprogramot használ, a Levelezés védelem összetevő nem vizsgálja a POP3, SMTP, NNTP és IMAP protokollon keresztül továbbított üzeneteket, amikor a **POP3, SMTP, NNTP és IMAP forgalom vizsgálata** jelölőnégyzet bejelölése törölve van.

   - Ha a Microsoft Office Outlookból hozzá szeretne férni a Levelezés védelem összetevő beállításaihoz, és be szeretné kapcsolni a POP3, SMTP, NNTP és IMAP és MAPI protokollokon keresztül továbbított üzenetek vizsgálatát a Microsoft Office Outlookba beépülő kiterjesztéssel, miután megérkeztek a számítógépre, jelölje be a **Microsoft Outlook-bővítmény csatlakoztatása** jelölőnégyzetet.

     Ha a Microsoft Office Outlookból blokkolni szeretné a Levelezés védelem összetevő beállításait, és ki szeretné kapcsolni a POP3, SMTP, NNTP és IMAP és MAPI protokollokon keresztül továbbított üzenetek vizsgálatát a Microsoft Office Outlookba beépülő kiterjesztéssel, miután megérkeztek a számítógépre, törölje a **Microsoft Outlook-bővítmény csatlakoztatása** jelölőnégyzet kijelölését.

     A Levelezés védelem kiterjesztés beágyazása a Microsoft Office Outlook levelezőprogramba a Kaspersky Endpoint Security telepítése során történik.

6. Mentse el a módosításokat.

Az e-mail üzenetekhez mellékelt összetett fájlok vizsgálata

Bekapcsolhatja vagy kikapcsolhatja az üzenetek mellékleteinek vizsgálatát, és beállíthat egy maximális mérethatárt az üzenetek mellékleteinek vizsgálatához, és korlátozhatja az üzenetek mellékletei vizsgálatának maximális időtartamát.

Az e-mail üzenetekhez mellékelt összetett fájlok vizsgálatának beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Levelezés védelem** opciót.
3. Kattintson a **Speciális beállítások** elemre.

4. Az **Összetett fájlok vizsgálata** részen konfigurálja a vizsgálati beállításokat:

   - **Microsoft Office formátumú csatolt fájlok vizsgálata**. Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.

   - **Csatolt archívumok vizsgálata**. ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.

     Ha a vizsgálat során az alkalmazás egy archívum jelszavát észleli az üzenet szövegében, ezt a jelszót használja fel, hogy az archívumban rosszindulatú alkalmazásokat keressen. Ebben az esetben a jelszó nem kerül mentésre. A vizsgálat során az archívum ki lett csomagolva. Ha a kicsomagolási folyamat során alkalmazáshiba lép fel, manuálisan törölheti a kicsomagolt fájlokat, amelyek mentése a következő elérési útvonalon történik: %systemroot%\temp. A fájlok PR előtaggal rendelkeznek.

   - **Ne legyen archívumok vizsgálata, ha a méret nagyobb, mint N MB (1 és 9999 között)**. Ha ez a jelölőnégyzet be van jelölve, a Levelezés védelem összetevő a vizsgálatból kizárja azokat az e-mail üzenetekhez mellékelt archívumokat, melyeknek a mérete meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, a Levelezés védelem összetevő minden méretű e-mailhez mellékelt archívumot megvizsgál.

   - **Archívumok ellenőrzésének korlátozása N másodpercre (1 és 9999 között)**. Ha a jelölőnégyzet be van jelölve, akkor az e-mail üzenetekhez mellékelt archívumok vizsgálatára kijelölt időtartam a megadott időre korlátozódik.

5. Mentse el a módosításokat.

E-mail-üzenetek mellékletének szűrése

A mellékletszűrő nincs alkalmazva a kimenő e-mail-üzenetekre.

A rosszindulatú alkalmazások az e-mailek mellékleteiben is terjedhetnek. A szűrést az e-mail üzenetek mellékleteinek típusa alapján is beállíthatja, így az adott típusú fájlokat az alkalmazás automatikusan átnevezi vagy törli. Adott típusú melléklet átnevezésével a Kaspersky Endpoint Security védelmet tud nyújtani a számítógép számára a rosszindulatú alkalmazások automatikus végrehajtása ellen.

A mellékletek szűrésének beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Levelezés védelem** opciót.

3. Kattintson a **Speciális beállítások** elemre.

4. A **Mellékletszűrő** részen hajtsa végre a következő műveletek valamelyikét:

   - **Szűrés letiltása**. Ha ez az opció van kiválasztva, a Levelezés védelem összetevő nem szűri az e-mail üzenetekhez csatolt fájlokat.

   - **Kiválasztott típusú mellékletek átnevezése**. Ha ezt a lehetőséget választja, a Levelezés védelem összetevő a megadott típusú csatolt fájlok kiterjesztésének utolsó karakterét aláhúzásjellel helyettesíti (például melléklet.doc_). Így a fájl megnyitásához a felhasználónak át kell neveznie a fájlt.

   - **Kiválasztott típusú mellékletek törlése**. Ha ez az opció van kiválasztva, a Levelezés védelem összetevő törli az e-mail üzenetekből a megadott típusú mellékelt fájlokat.

5. Ha az előző lépésben az **Kiválasztott típusú mellékletek átnevezése** vagy **Kiválasztott típusú mellékletek törlése** lehetőséget választotta, jelölje be a kívánt fájltípusokkal szemben lévő jelölőnégyzeteket.

6. Mentse el a módosításokat.

Mellékletszűrő kiterjesztések exportálása és importálása

A mellékletszűrő kiterjesztések listáját exportálhatja egy XML-fájlba. Használhatja az exportálás/importálás funkciót a kiterjesztések listája biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A mellékletszűrő kiterjesztések listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Communication & Web Protection** → **Mail Threat Protection** elemet.

5. A bővítmények listájának exportálása a **Attachment filter** területen:

   a. Jelölje ki az exportálni kívánt kiterjesztéseket.

   b. Kattintson a **Export** hivatkozásra.

   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe a kiterjesztések listáját exportálni szeretné, és válassza a fájl mentésére kiszemelt mappát.

   d. Mentse a fájlt.

      A Kaspersky Endpoint Security a kiterjesztések teljes listáját exportálja az XML-fájlba.

6. A bővítmények listájának importálása a **Attachment filter** területen:

   a. Kattintson a **Import** hivatkozásra.

   b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kiterjesztések listáját.

c. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a kiterjesztésekről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

7. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabályablakban válassza az **Fenyegetések elleni alapvető védelem → Levelezés védelem** lehetőséget.

4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

5. A megnyíló ablakban válassza ki a **Mellékletszűrő** lapot.

6. A kiterjesztések listájának exportálása:

a. Jelölje ki az exportálni kívánt kiterjesztéseket. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.

b. Kattintson az **Exportálás** hivatkozásra.

c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe a kiterjesztések listáját exportálni szeretné, és válassza a fájl mentésére kiszemelt mappát.

d. Mentse a fájlt.

A Kaspersky Endpoint Security a kiterjesztések teljes listáját exportálja az XML-fájlba.

7. A kiterjesztések listájának importálása:

a. Kattintson az **Import** hivatkozásra.

b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kiterjesztések listáját.

c. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a kiterjesztésekről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

8. Mentse el a módosításokat.

E-mailek vizsgálata a Microsoft Office Outlookban

A Kaspersky Endpoint Security telepítése során a Levelezés védelem kiterjesztése beágyazódik a Microsoft Office Outlookba (a továbbiakban: Outlook is). A kiterjesztés lehetővé teszi az üzenetek vizsgálatát a levelezőprogram szintjén a protokollszint helyett. Az üzeneteken kívül a kiterjesztés lehetővé teszi a Microsoft Exchange-tárhelyekről a MAPI-felületen keresztül kapott objektumok (például a Naptárban lévő objektumok) vizsgálatát is. Ez a vizsgálat a levelezőprogramban történik.

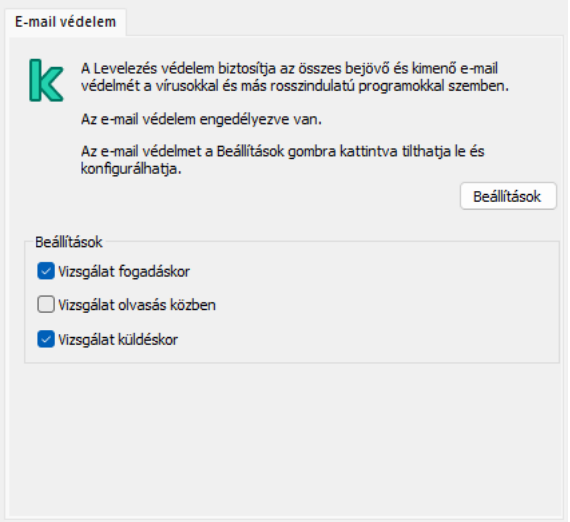
Az Outlookból megnyithatja a Levelezés védelem összetevő beállításait, és megadhatja, hogy keressen-e az e-mail üzenetekben vírusokat és más fenyegetéseket.

A Levelezés védelem bővítmény az Outlook 2010, 2013, 2016, 2019, 2021, 2024 és 365 32 bites és 64 bites verzióit támogatja.

Az ARM-alapú számítógépeken a Levelezés védelem bővítmény az Outlook 2016, az Outlook 2021, az Outlook 2024 és az Outlook 365 for Arm64 32 bites és 64 bites verzióit támogatja.

Az Outlookban a bejövő üzeneteket először a Levelezés védelem összetevő (ha be van jelölve a POP3-, SMTP-, NNTP- és IMAP-forgalom vizsgálata jelölőnégyzet a Kaspersky Endpoint Security felületén), majd az Outlook Levelezés védelem kiterjesztése vizsgálja. Ha a Levelezés védelem összetevő egy üzenetben rosszindulatú objektumot észlel, értesítést jelenít meg erről.

A Levelezés védelem összetevő beállításait akkor lehet közvetlenül az Outlookban megadni, ha a Microsoft Office Outlook bővítmény csatlakoztatva van a Kaspersky Endpoint Security felületén (lásd az alábbi ábrát).



A Levelezés védelem összetevő beállításai az Outlookban

A kimenő üzeneteket először az Outlook Levelezés védelem kiterjesztése, majd a Levelezés védelem összetevő vizsgálja meg.

Ha az e-mailek vizsgálata az Outlook Levelezés védelem kiterjesztésével történik, akkor javasoljuk a Gyorsítótárazott Exchange-mód használatát. A gyorsítótáras Exchange móddal kapcsolatban további információ, valamint a használatára vonatkozó ajánlások a Microsoft Tudásbázisban találhatók.

Az Outlook Levelezés védelem kiterjesztés üzemmódjának beállításai:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Fenyegetések elleni alapvető védelem → Levelezés védelem** lehetőséget.
4. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
5. A megnyíló ablakban a **Kapcsolat** részben kattintson a **Beállítások** gombra.

6. Az **E-mail védelem** ablakban végezze el az alábbiak egyikét:

   - Jelölje be a **Vizsgálat fogadáskor** jelölőnégyzetet, ha azt szeretné, hogy az Outlook Levelezés védelem kiterjesztés a bejövő üzeneteket megvizsgálja, amint a postaládába megérkeznek.
   - Jelölje be a **Vizsgálat olvasás közben** jelölőnégyzetet, ha azt szeretné, hogy az Outlook Levelezés védelem kiterjesztés a bejövő üzeneteket akkor vizsgálja meg, amikor a felhasználó megnyitja őket.
   - Jelölje be a **Vizsgálat küldéskor** jelölőnégyzetet, ha azt szeretné, hogy az Outlook Levelezés védelem kiterjesztés a kimenő üzeneteket megvizsgálja, amint elküldésre kerülnek.

7. Mentse el a módosításokat.

E-mailek vizsgálata a Thunderbird, a MyOffice és az R7-Office alkalmazásban

A „Levelezés védelem" összetevő a bejövő és kimenő e-mail üzenetek mellékleteiben vizsgálja a vírusok és egyéb fenyegetések jelenlétét. A Mozilla Thunderbird, a MyOffice Mail és az R7-Office Organizer levelezőkliensek esetében az alkalmazás csak *protokoll szinten* (POP3, SMTP, IMAP, NNTP) fér hozzá az üzenetekhez.

A Mozilla Thunderbird, MyOffice Mail és R7-Office Organizer levelezőprogramok forgalmának vizsgálatához hozzá kell adnia a Kaspersky tanúsítványt a tanúsítványtárolóhoz, és ki kell választania a saját tanúsítványtárolót.

A „Levelezés védelem" összetevő nem vizsgálja az üzeneteket, ha a levelezési ügyfélprogram böngészőben van megnyitva.

Valós idejű levelezés védelem

A Levelezés védelem a bejövő és a kimenő üzeneteket is képes megvizsgálni. Alapértelmezett esetben a Levelezés védelem összetevő automatikusan megpróbálja az összes észlelt fertőzött e-mail üzenetet vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Levelezés védelem összetevő törli a fertőzött e-mail üzeneteket. Egy rosszindulatú fájl csatolmányban történő észlelése esetén a Kaspersky Endpoint Security egy, a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Az üzenet feldolgozása megtörtént] <üzenet tárgysora>*.

A Mozilla Thunderbird levelezőprogram használata esetén a Levelezés védelem összetevő nem vizsgálja az IMAP protokollon keresztül továbbított üzenetekben a vírusok és egyéb fenyegetések jelenlétét, ha az üzenetek szűrők segítségével vannak áthelyezve a Beérkezett üzenetek mappából.

Kártevők azonosítása a levelező adatbázisokban

A *Kártevő vizsgálata* feladat lehetővé teszi levél formátumú fájlok vizsgálatát. Ha ezeknek a levelezőprogramoknak a fájljaiban rosszindulatú objektumot észlel, a Kaspersky Endpoint Security csak az észlelt objektumokra vonatkozó információkat adja hozzá az aktív fenyegetések listájához. Az alkalmazás a feladat beállításaitól függetlenül nem vírusmentesíti és nem törli a levelezési adatbázisokban lévő fertőzött fájlokat.

Aktív fenyegetések megszüntetése

A Levelezés védelem protokoll szinten akadályozza meg a számítógép megfertőződését, de ha a számítógép a Kaspersky Endpoint Security telepítése előtt már fertőzött volt, előfordulhat, hogy az alkalmazás csak a levelezési adatbázisokban észleli a fenyegetést. A Levelezés védelem nem tartalmaz olyan összetevőket, amelyek kifejezetten lehetővé teszik az üzenetek részekre (fejléc, törzs, mellékletek) bontását, mint a Microsoft Office Outlook esetében. Ezért az alkalmazás nem tudja törölni vagy vírusmentesíteni az észlelt objektumokat. A Kaspersky Endpoint Security csak az észlelt objektumokra vonatkozó információkat adja hozzá az aktív fenyegetések listájához.

Aktív fenyegetések megszüntetése:

1. Manuálisan kell megkeresnie és törölnie az észlelt objektumot tartalmazó üzenetet a levelezőkliens felületén.

   Az alkalmazás megjeleníti az aktív fenyegetések listájában szereplő észlelt objektumokra fájlokra vonatkozó információkat.

   Példa az észlelt objektum kártyára:

   HEUR:Trojan.PDF.Phish.gen
   Objektum: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Hajtsa végre az adatbázis-tömörítési műveletet.

   Ha töröl egy üzenetet a felhasználói felületen, a levelezőprogram csak egy törlésjelet ad hozzá. A levelezőprogram valójában csak az adatbázis-tömörítés után törli az üzenetet. Az adatbázis-tömörítés részleteiért lásd a levelezőkliens súgóját (például Mozilla Thunderbird).

3. Futtassa megint a *Kártevő vizsgálata* feladatot, és győződjön meg arról, hogy a fenyegetés már nincs jelen.

Hálózati védelem

A *Hálózati védelem* összetevő (más néven Intrusion Detection System, IDS) figyeli a bejövő hálózati forgalmat a hálózati támadásokra jellemző tevékenységek szempontjából. Ha az alkalmazás hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában. Az alkalmazás-adatbázisok tartalmazzák a már ismert hálózati támadások típusainak és az elhárításuk módszereinek leírását. A Hálózati védelem összetevő által észlelhető hálózati támadások listája az alkalmazás adatbázisainak és alkalmazásmoduljainak frissítésekor frissül.

A Hálózati védelem engedélyezése és letiltása

Alapértelmezés szerint a Hálózati védelem be van kapcsolva és optimális módban működik. A Kaspersky Endpoint Security figyeli a bejövő hálózati forgalmat a hálózati támadásokra jellemző tevékenységek szempontjából, és blokkolja a támadásokat.

A Hálózati védelem összetevő engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

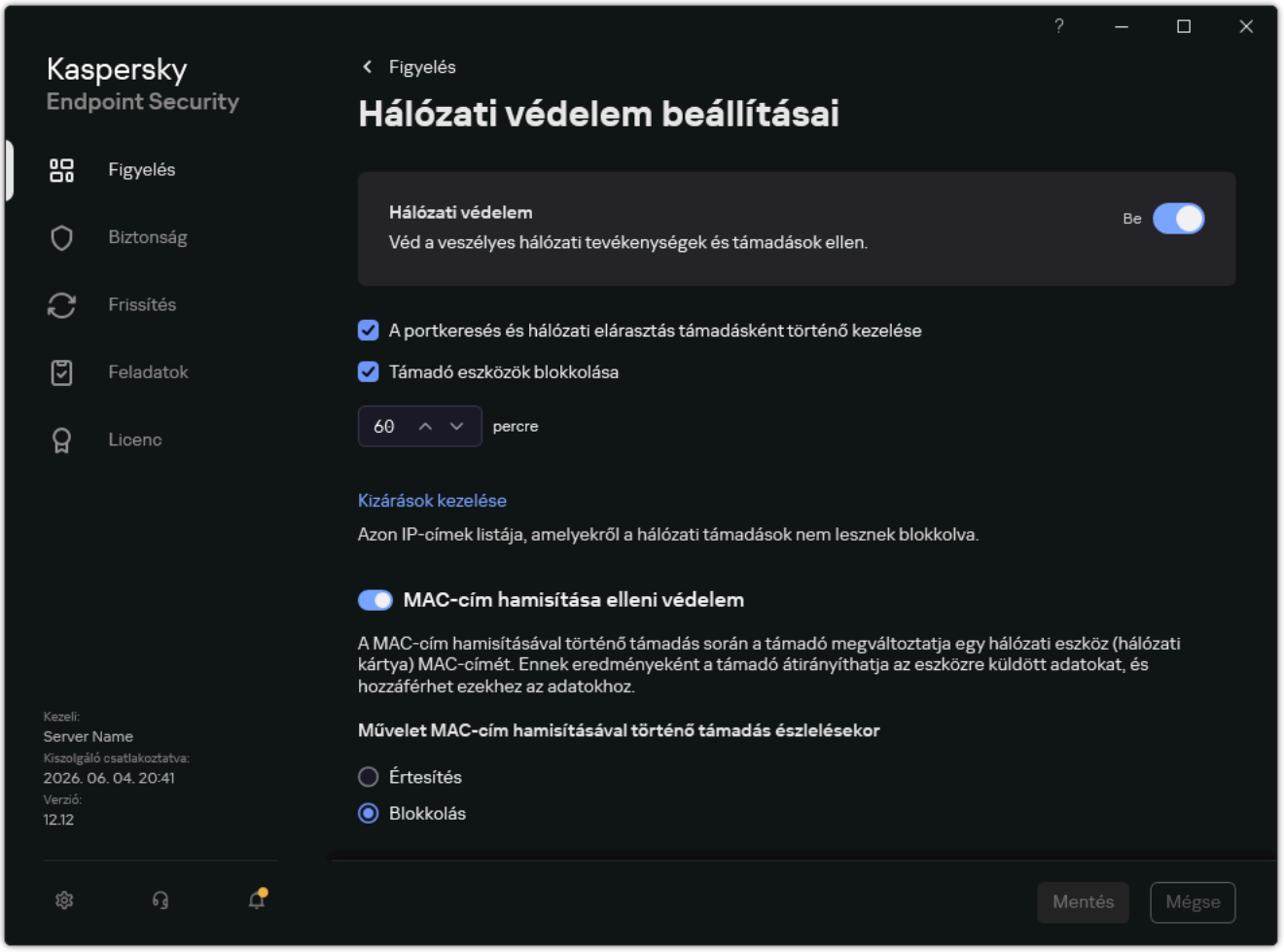
1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** lehetőséget.
4. A **Hálózati védelem** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
5. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Hálózati védelem engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Communication & Web Protection → Network Threat Protection** elemet.
5. A **Network Threat Protection ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Mentse el a módosításokat.

A Hálózati védelem engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** opciót.



A Hálózati védelem beállításai

3. A **Hálózati védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Támadó számítógép blokkolása

Ha a Hálózati védelem összetevő engedélyezve van, a Kaspersky Endpoint Security automatikusan blokkolja a hálózati fenyegetéseket. Ezenkívül az alkalmazás blokkolhatja a támadó számítógépet, és bizonyos ideig korlátozhatja a hálózati csomagok küldését. Alapértelmezés szerint a Kaspersky Endpoint Security egy óráig blokkolja a számítógépet.

A támadó számítógép blokkolása az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** lehetőséget.

4. A **Hálózati védelem beállításaiban** jelölje be a **Támadó eszközök blokkolása N percre** jelölőnégyzetet.

   Ha a funkció engedélyezve van, a Hálózati védelem összetevő a támadó számítógépet felveszi a blokkolási listára. Ez azt jelenti, hogy a Hálózati védelem összetevő az első hálózati támadási próbálkozást követően a megadott ideig blokkolja a támadó számítógép hálózati kapcsolatát. A blokkolás automatikusan védi a felhasználó számítógépét az ugyanerről a címről érkező lehetséges további hálózati támadásoktól. A támadó számítógépnek legalább egy percet kell eltöltenie a blokkoltak listáján. A maximális időtartam 999 perc.

5. Állítson be egy másik blokkolási időtartamot a támadó számítógép számára a **Támadó eszközök blokkolása N percre** jelölőnégyzettől jobbra lévő mezőben.

6. Mentse el a módosításokat.

A támadó számítógép blokkolása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Communication & Web Protection** → **Network Threat Protection** elemet.

5. A **Action on threat detection** részen jelölje be az **Block attack and attacking device for (min)** jelölőnégyzetet.

   Ha a funkció engedélyezve van, a Hálózati védelem összetevő a támadó számítógépet felveszi a blokkolási listára. Ez azt jelenti, hogy a Hálózati védelem összetevő az első hálózati támadási próbálkozást követően a megadott ideig blokkolja a támadó számítógép hálózati kapcsolatát. A blokkolás automatikusan védi a felhasználó számítógépét az ugyanerről a címről érkező lehetséges további hálózati támadásoktól. A támadó számítógépnek legalább egy percet kell eltöltenie a blokkoltak listáján. A maximális időtartam 999 perc.

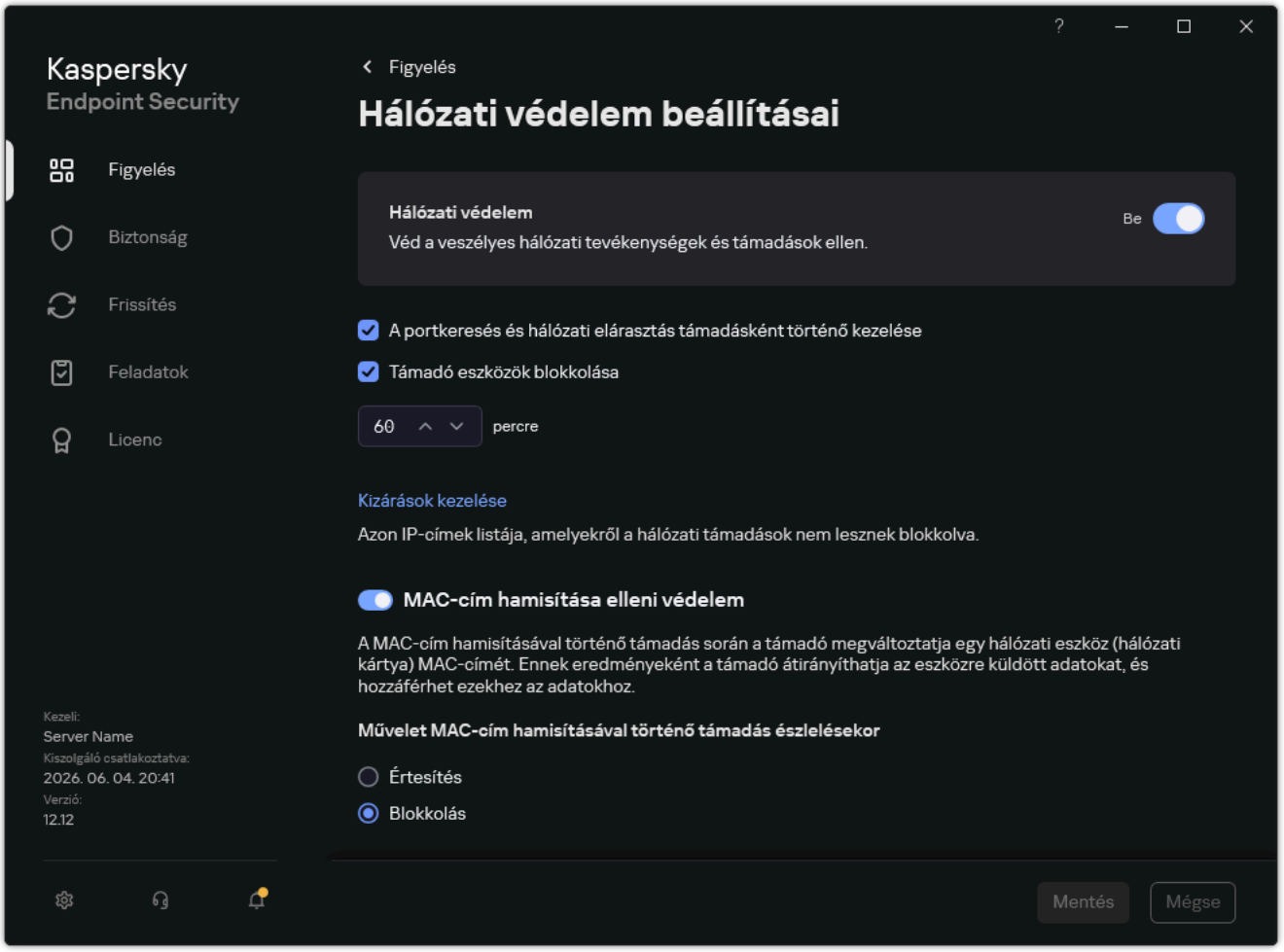
6. Módosíthatja a támadó számítógép blokkolásának időtartamát.

7. Mentse el a módosításokat.

A támadó számítógép blokkolása az alkalmazás felhasználói felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** opciót.



A Hálózati védelem beállításai

3. Kapcsolja be a **Támadó eszközök blokkolása N percre** kapcsolót.

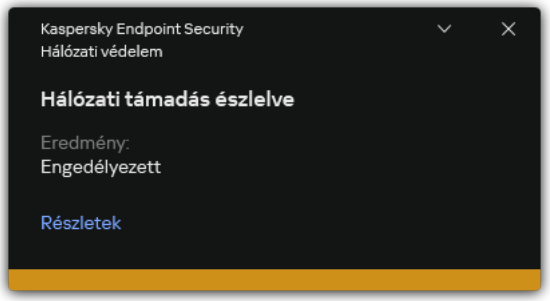
   Ha a funkció engedélyezve van, a Hálózati védelem összetevő a támadó számítógépet felveszi a blokkolási listára. Ez azt jelenti, hogy a Hálózati védelem összetevő az első hálózati támadási próbálkozást követően a megadott ideig blokkolja a támadó számítógép hálózati kapcsolatát. A blokkolás automatikusan védi a felhasználó számítógépét az ugyanerről a címről érkező lehetséges további hálózati támadásoktól. A támadó számítógépnek legalább egy percet kell eltöltenie a blokkoltak listáján. A maximális időtartam 999 perc.

4. Állítson be egy másik blokkolási időtartamot a támadó számítógép számára a **Támadó eszközök blokkolása N percre** kapcsoló alatti mezőben.

5. Mentse el a módosításokat.

Ennek eredményeként, amikor a Kaspersky Endpoint Security a felhasználó számítógépe ellen indított hálózati támadási kísérletet észlel, blokkolni fogja az összes kapcsolatot a támadást indító számítógéppel. A Kaspersky Endpoint Security létrehozza a *Network attack detected* eseményt. Az esemény információkat tartalmaz a támadó számítógépről: IP- és MAC-címek.

A támadó számítógép MAC-címe az alkalmazás felhasználói felületén vagy a Kaspersky Security Center konzol 15.1-es vagy újabb verziójában tekinthető meg.



Értesítés hálózati támadás észleléséről

A Kaspersky Endpoint Security feloldja a számítógép blokkolását, amikor a megadott idő lejár. A Kaspersky Security Center konzol nem biztosít más eszközöket a blokkolt számítógépek megfigyelésére, kivéve a *Network attack detected* eseményeket a jelentésben. Az alkalmazás felületén csak a blokkolt számítógépek listáját tekintheti meg. Ezt a funkciót a *Hálózatfigyelő* eszköz biztosítja. A Hálózatfigyelő eszközt is használhatja egy számítógép blokkolásának feloldására.

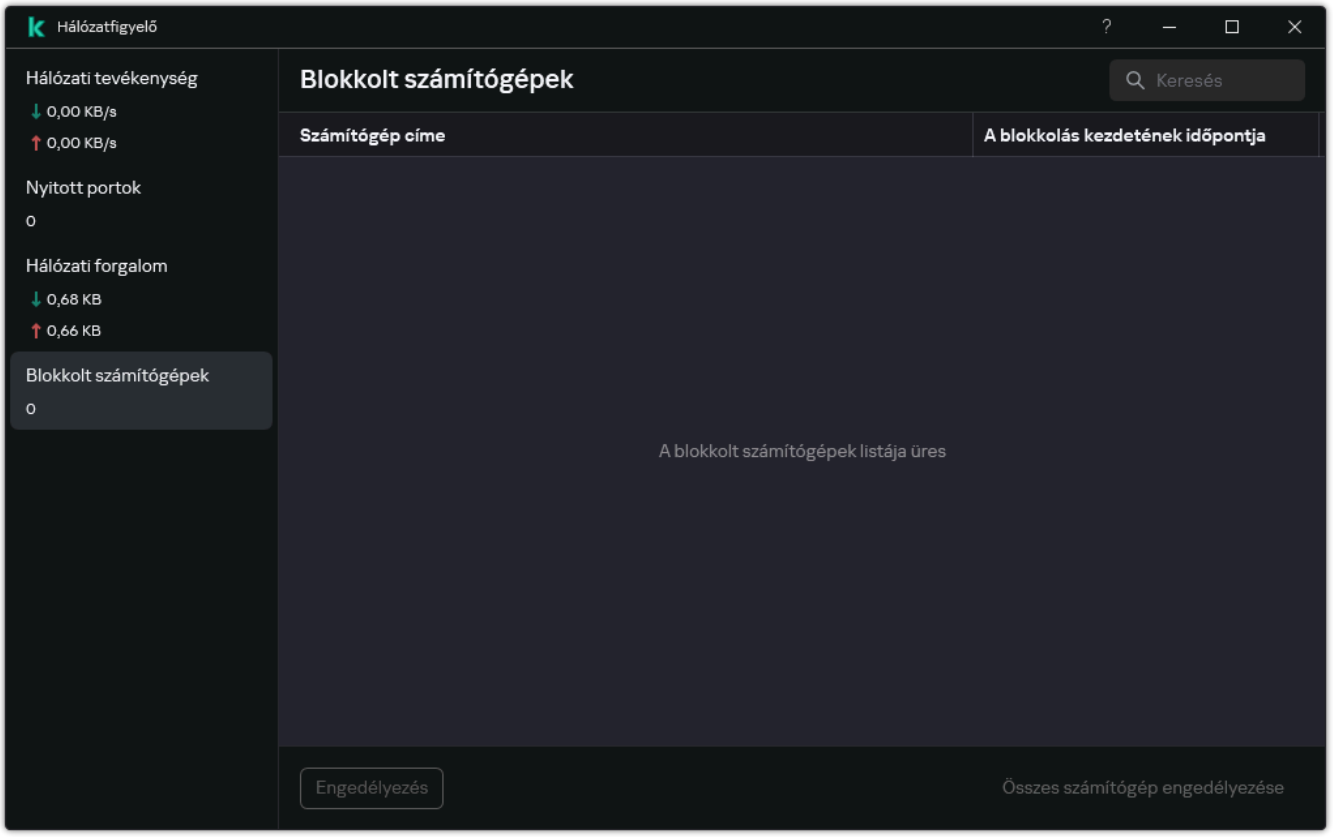
Számítógép blokkolásának feloldása:

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Hálózatfigyelő** csempére.
2. Nyissa meg a **Blokkolt számítógépek** lapot.

   Ez megnyitja a blokkolt számítógépek listáját (lásd az alábbi ábrát).

   A Kaspersky Endpoint Security törli a tiltólistát az alkalmazás újraindításakor és a Hálózati védelem beállításainak megváltoztatásakor.

3. Válassza ki a feloldani kívánt számítógépet, és kattintson az **Engedélyezés** elemre.



A blokkolt számítógépek listája

A blokkolásból kizárt címek beállítása

A Kaspersky Endpoint Security fel tudja ismerni a hálózati támadásokat, és blokkolni tudja a nagyszámú csomagot továbbító nem védett hálózati kapcsolatot (például a térfigyelő kameráktól). A megbízható eszközökkel való munkához hozzáadhatja ezeknek az eszközöknek az IP-címét a kizárások listájához. Kiválaszthatja a kommunikációhoz használt protokollt és portot is, és engedélyezhet bizonyos hálózati tevékenységeket.

A Kaspersky Endpoint Security 12.2 kiegészült a kizárásokhoz szükséges protokollok és portok kiválasztásának lehetőségével. Győződjön meg arról, hogy az alkalmazás és a felügyeleti bővítmény frissült a 12.2 vagy újabb verzióra. Ha az alkalmazás vagy a felügyeleti bővítmény egy korábbi verzióját használja, a Kaspersky Endpoint Security csak IP-cím alapján engedélyezheti a hálózati tevékenységeket.

A blokkolási kizárások listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat” nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok” használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot” az alapértelmezett állapotra.

A blokkolásból kizárt címek konfigurálása az Adminisztrációs konzolban (MMC)

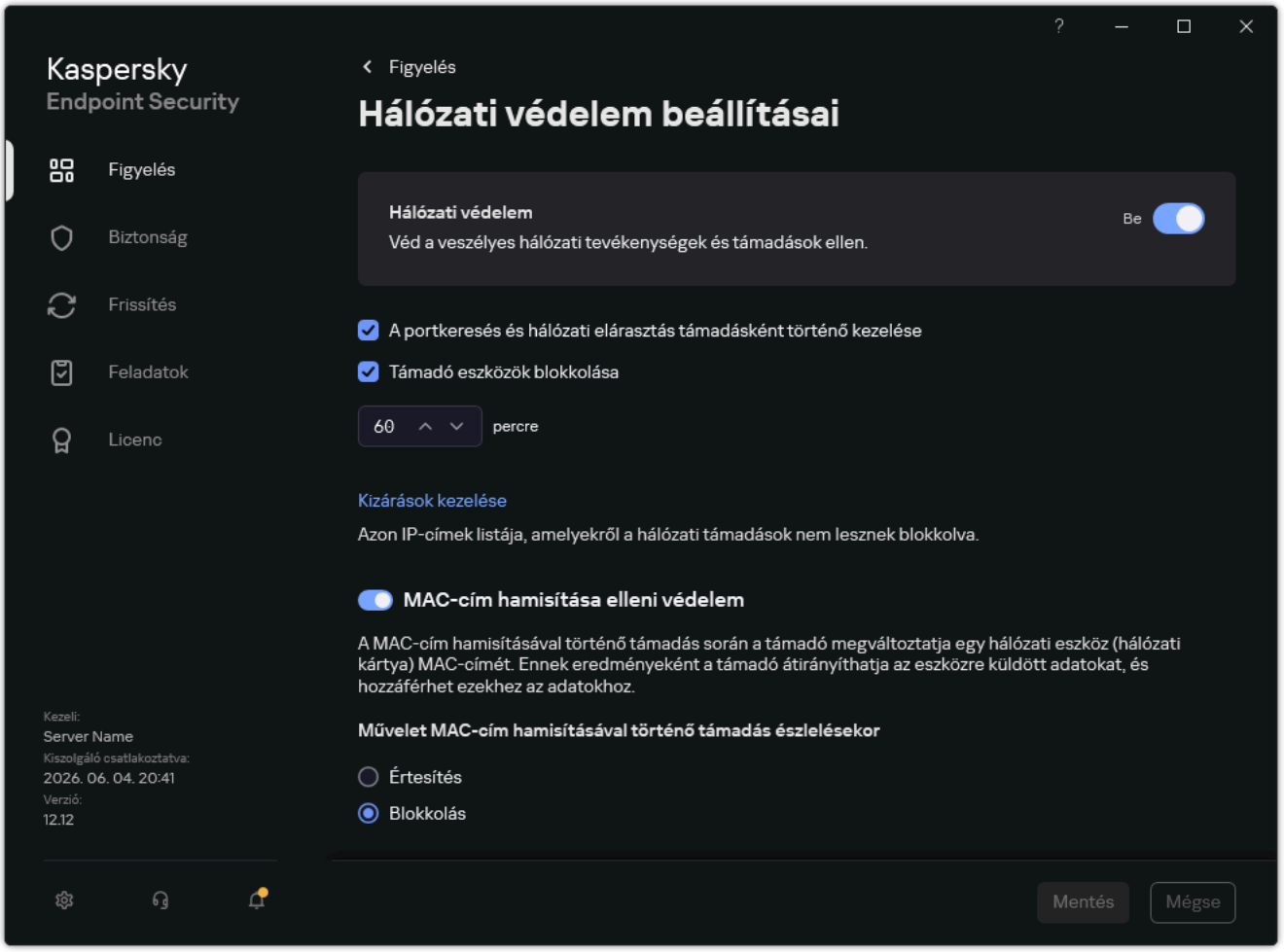
1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** lehetőséget.
4. A **Hálózati védelem beállításai** blokkban kattintson a **Kizárások** gombra.
5. Az ablakban kattintson a **Hozzáadás** gombra.
6. Adja meg annak a számítógépnek az IP-címét, amelyről a hálózati támadásokat nem szabad blokkolni.
   Ha szükséges, válassza ki azt a protokollt és portokat, amelyeken keresztül az adatok továbbításra kerülnek.
7. Mentse el a módosításokat.

A blokkolásból kizárt címek konfigurálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Communication & Web Protection → Network Threat Protection** elemet.
5. Az ablak felső részében kattintson a **Trusted IP addresses** hivatkozásra.
6. Az ablakban kattintson a **Add** gombra.
7. Adja meg annak a számítógépnek az IP-címét, amelyről a hálózati támadásokat nem szabad blokkolni.
   Szükség esetén adja meg az alhálózatot.
8. Mentse el a módosításokat.

A blokkolásból kizárt címek konfigurálása az alkalmazás felhasználói felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** opciót.



A Hálózati védelem beállításai

3. Kattintson a **Kizárások kezelése** hivatkozásra.
4. Az ablakban kattintson a **Hozzáadás** gombra.
5. Adja meg annak a számítógépnek az IP-címét, amelyről a hálózati támadásokat nem szabad blokkolni.

   Ha szükséges, válassza ki azt a protokollt és portokat, amelyeken keresztül az adatok továbbításra kerülnek.
6. Mentse el a módosításokat.

Blokkolásból való kizárások listájának exportálása és importálása

A kizárások listáját exportálhatja egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú cím hozzáadásával. Használhatja az exportálás/importálás funkciót a kizárások biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A kizárások listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** lehetőséget.
4. A **Hálózati védelem beállításai** blokkban kattintson a **Kizárások** gombra.
5. A szabályok listájának exportálása:
   a. Jelölje ki az exportálni kívánt kizárásokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
      Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.
   b. Kattintson a → **Hozzáadás** gombra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba.
6. A kizárások listájának importálása:
   a. Kattintson a → **Hozzáadás** gombra.
   b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kizárások listáját.
   c. Nyissa meg a fájlt.
      Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
7. Mentse el a módosításokat.

A kizárások listájának exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Communication & Web Protection → Network Threat Protection** elemet.
5. Az ablak felső részében kattintson a **Trusted IP addresses** hivatkozásra.
   Megnyílik a kizárások listája.

6. A szabályok listájának exportálása:

   a. Jelölje ki az exportálni kívánt kizárásokat.

   b. Kattintson az → **Export** gombra.

      A Kaspersky Endpoint Security a kizárások listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

7. A kizárások listájának importálása:

   a. Kattintson az → **Import** gombra.

      A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a kizárások listáját.

   b. Nyissa meg a fájlt.

      Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.

8. Mentse el a módosításokat.

A Hálózati védelem konfigurálása típus szerint

A Kaspersky Endpoint Security a következő típusú hálózati támadások elleni védelem felügyeletét teszi lehetővé:

- A *hálózati elárasztás* a vállalat hálózati erőforrásainak (például webkiszolgálók) megtámadását jelenti. A támadás abból áll, hogy nagyszámú kérésekkel túlterhelik a hálózati erőforrások sávszélességét. Ilyenkor a felhasználók nem tudnak hozzáférni a vállalat hálózati erőforrásaihoz.

- A *portkereséses támadás* az UDP-portok, a TCP-portok és a számítógép hálózati szolgáltatásainak vizsgálatából áll. Lehetővé teszi a támadónak, hogy azonosítsa a számítógép sebezhetőségének mértékét, mielőtt veszélyesebb hálózati támadásokat hajtana végre. A portkereséssel a támadó a számítógépen lévő operációs rendszert is képes azonosítani, és kiválaszthatja az adott operációs rendszernek megfelelő hálózati támadásokat.

- A *MAC-hamisítási támadás* a hálózati eszköz (hálózati kártya) MAC-címének megváltoztatásával történik. Ennek eredményeképpen a támadó átirányíthatja az eszköznek küldött adatokat másik eszközre, és hozzáférhet ezekhez az adatokhoz. A Kaspersky Endpoint Security segítségével blokkolhatja a MAC-hamisítási támadásokat, valamint értesítést kaphat a támadásokról.

Letilthatja az ilyen típusú támadások észlelését, ha az engedélyezett alkalmazások egy része ilyen típusú támadásokra jellemző műveleteket hajt végre. Ez segít elkerülni a téves riasztásokat.

Alapértelmezés szerint a Kaspersky Endpoint Security nem figyeli a hálózati elárasztást, a portkeresést és a MAC-hamisítási támadásokat.

Nem javasoljuk a MAC-hamisítása elleni védelem engedélyezését virtuális gépeken a Microsoft Hyper-V infrastruktúrájában. A Microsoft Hyper-V platform sajátosságai miatt a Kaspersky Industrial CyberSecurity for Nodes vakriasztási eredmény esetén blokkolhatja a hipervizort.

A Hálózati védelem konfigurálása típus szerint az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** lehetőséget.
4. Használja **A portkeresés és hálózati elárasztás támadásként történő kezelése** jelölőnégyzetet az ilyen támadások észlelésének engedélyezéséhez vagy letiltásához.

   Ha ez a funkció engedélyezve van, a Kaspersky Endpoint Security figyeli a hálózati forgalmat portkeresés és hálózati elárasztás szempontjából. Ha ilyen viselkedést észlel, az alkalmazás értesíti a felhasználót, és elküldi a megfelelő eseményt a Kaspersky Security Center számára. Az alkalmazás információt szolgáltat a kéréseket küldő számítógépről. Ez az információ az időben történő válaszadáshoz szükséges. Azonban a Kaspersky Endpoint Security nem blokkolja a kéréseket küldő számítógépet, mivel az ilyen forgalom normális esemény lehet a vállalati hálózaton.
5. Válassza ki a következő lehetőségek egyikét a **MAC-cím hamisítása elleni védelmi mód** részen:
   - **Ne kövesse a MAC-cím hamisításán alapuló támadásokat**.
   - **Tájékoztatás**.
   - **Blokkolás**.
6. Mentse el a módosításokat.

A Hálózati védelem konfigurálása típus szerint a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Communication & Web Protection → Network Threat Protection** elemet.
5. Használja a(z) **Treat port scanning and network flooding as attacks** jelölőnégyzetet az ilyen támadások észlelésének engedélyezésére vagy letiltására.

   Ha ez a funkció engedélyezve van, a Kaspersky Endpoint Security figyeli a hálózati forgalmat portkeresés és hálózati elárasztás szempontjából. Ha ilyen viselkedést észlel, az alkalmazás értesíti a felhasználót, és elküldi a megfelelő eseményt a Kaspersky Security Center számára. Az alkalmazás információt szolgáltat a kéréseket küldő számítógépről. Ez az információ az időben történő válaszadáshoz szükséges. Azonban a Kaspersky Endpoint Security nem blokkolja a kéréseket küldő számítógépet, mivel az ilyen forgalom normális esemény lehet a vállalati hálózaton.

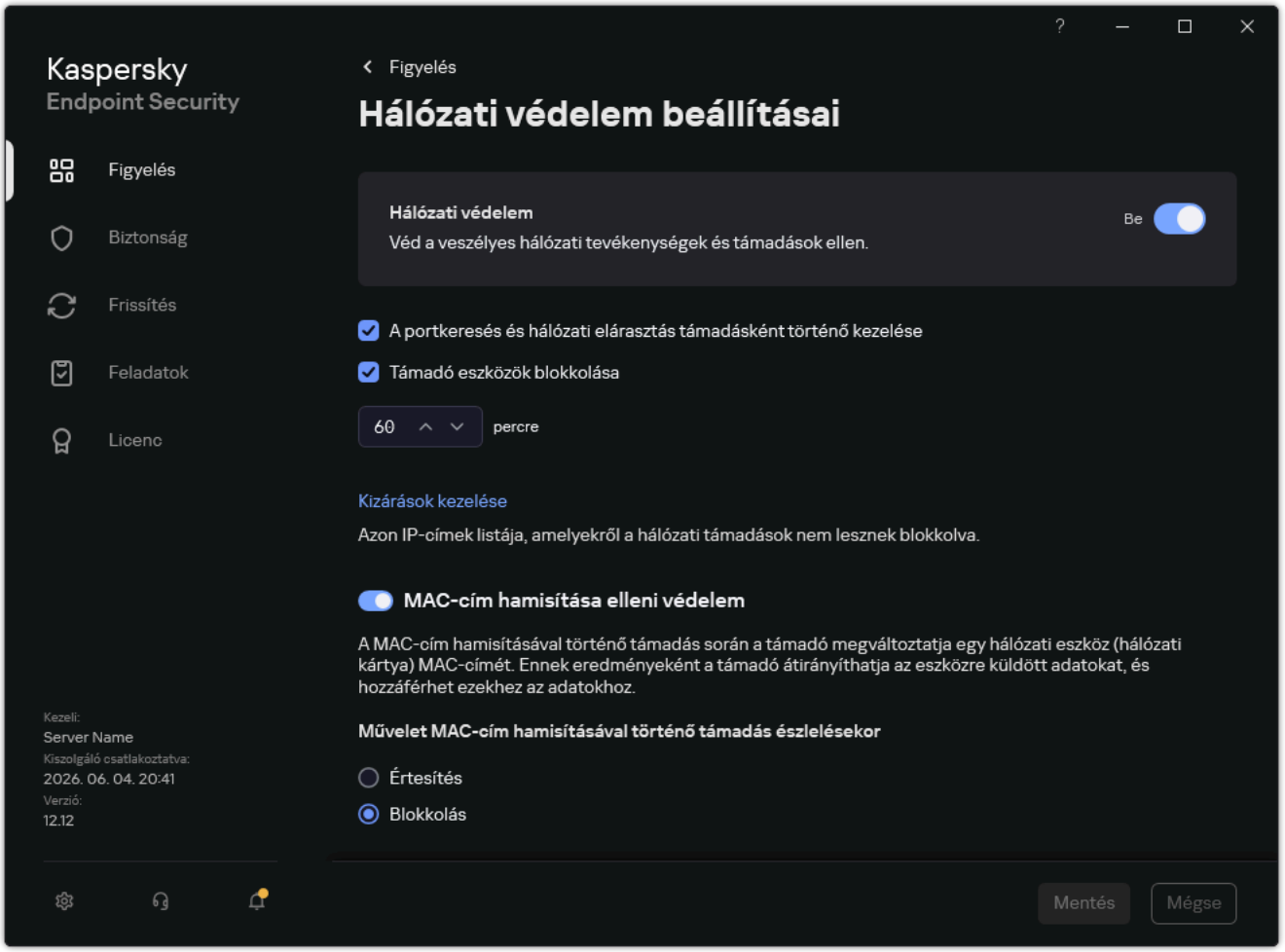
6. A **MAC Spoofing Protection** blokkban válassza ki a következő opciók egyikét:

   - **MAC Spoofing Protection ENABLED**.
   - **Inform**.
   - **Block**.

7. Mentse el a módosításokat.

A Hálózati védelem konfigurálása típus szerint az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem → Hálózati védelem** opciót.



A Hálózati védelem beállításai

3. Használja **A portkeresés és hálózati elárasztás támadásként történő kezelése** kapcsolót az ilyen támadások észlelésének engedélyezéséhez vagy letiltásához.

   Ha ez a funkció engedélyezve van, a Kaspersky Endpoint Security figyeli a hálózati forgalmat portkeresés és hálózati elárasztás szempontjából. Ha ilyen viselkedést észlel, az alkalmazás értesíti a felhasználót, és elküldi a megfelelő eseményt a Kaspersky Security Center számára. Az alkalmazás információt szolgáltat a kéréseket küldő számítógépről. Ez az információ az időben történő válaszadáshoz szükséges. Azonban a Kaspersky Endpoint Security nem blokkolja a kéréseket küldő számítógépet, mivel az ilyen forgalom normális esemény lehet a vállalati hálózaton.

4. Használja a **MAC-cím hamisítása elleni védelem** kapcsolót az ilyen támadások észlelésének engedélyezésére vagy letiltására.

5. A **MAC-cím hamisításával történő támadás észlelésekor végrehajtandó művelet** részen válassza ki a következő opciók egyikét:

   - **Tájékoztatás**.
   - **Blokkolás**.

6. Mentse el a módosításokat.

Tűzfal

A Tűzfal blokkolja a jogosulatlan kapcsolódási kísérleteket a számítógépen az interneten vagy a helyi hálózaton végzett munka során. A Tűzfal felügyeli a számítógépen futó alkalmazások hálózati tevékenységét is. Ez lehetővé teszi, hogy védje a vállalat helyi hálózatát a személyes adatok ellopásával és más támadásokkal szemben. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és előre definiált *hálózati szabályok.* segítségével biztosít védelmet a számítógépnek.

A Hálózati ügynök a Kaspersky Security Centerrel való kommunikációra szolgál. A Tűzfal automatikusan létrehozza az alkalmazás és a hálózati ügynök működéséhez szükséges hálózati szabályokat. Ennek eredményeként a Tűzfal több portot nyit meg a számítógépen. A megnyitott portok a számítógép szerepkörétől függenek (például terjesztési pont). Ha többet szeretne megtudni a számítógépen megnyíló portokról, olvassa el a Kaspersky Security Center súgóját.

Hálózati szabályok

A hálózati szabályokat a következő szinteken konfigurálhatja:

- *Hálózati csomagszabályok.* A hálózati csomagszabályok a hálózati csomagokat alkalmazástól függetlenül korlátozzák. Ezek a szabályok korlátozzák a bejövő és kimenő hálózati forgalmat a kiválasztott adatprotokoll adott portjain. A Kaspersky Endpoint Security alkalmazásban előre definiált hálózatiadatcsomag-szabályok érhetők el, a Kaspersky szakértői által javasolt jogosultságokkal.
- *Alkalmazás hálózati szabályai.* Az alkalmazások hálózati szabályai adott alkalmazások hálózati tevékenységét korlátozzák. Nem csupán a hálózati csomag jellemzőit veszik figyelembe, hanem azt a konkrét alkalmazást is, amelynek a hálózati csomag címezve van, illetve amely a hálózati csomagot elküldte.

Az alkalmazások szabályozott hozzáférést kapnak az operációs rendszer erőforrásaihoz, a folyamatokhoz és a személyes adatokhoz, amit a Behatolásmegelőző rendszer összetevő biztosít *alkalmazásjogok* használatával.

Az alkalmazás első indítása során a Tűzfal a következő műveleteket hajtja végre:

1. Ellenőrzi az alkalmazás biztonságát letöltött antivírus adatbázisok segítségével.
2. Ellenőrzi az alkalmazás biztonságát a Kaspersky Security Networkben.

   Javasoljuk, hogy vegyen részt a Kaspersky Security Networkben, amivel segíthet hatékonyabbá tenni a Tűzfal működését.

3. Az alkalmazást a megbízhatósági csoportok valamelyikébe helyezi: *Megbízható*, *Alacsony korlátozás*, *Magas korlátozás*, *Nem megbízható*.

   A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére használ. A Kaspersky Endpoint Security egy alkalmazást az alapján helyez megbízhatósági csoportba, hogy az alkalmazás milyen veszélyességi szintet képvisel a számítógép szempontjából.

   A Kaspersky Endpoint Security az alkalmazásokat a Tűzfal és a Behatolásmegelőző rendszer összetevő számára helyezi megbízhatósági csoportba. Nem lehet módosítani a megbízhatósági csoportot kizárólag a Tűzfal vagy a Behatolásmegelőző rendszer esetében.

   Ha nem vesz részt a KSN rendszerében vagy nincs hálózat, a Kaspersky Endpoint Security a Behatolásmegelőző rendszer összetevő beállításai alapján helyezi az alkalmazást megbízhatósági csoportba. Miután megérkezett az alkalmazás megítélése a KSN hálózattól, a rendszer automatikusan módosíthatja az alkalmazás megbízhatósági csoportját.

4. Blokkolja az alkalmazás hálózati tevékenységét a megbízhatósági csoportba tartozása alapján. Például a *Magas korlátozás* megbízhatósági csoportba tartozó alkalmazások egyáltalán nem használhatnak hálózati kapcsolatot.

Az alkalmazás következő indításakor a Kaspersky Endpoint Security ellenőrzi annak integritását. Amennyiben az alkalmazás nem változott meg, az összetevő az aktuális hálózati szabályokat alkalmazza. Ha az alkalmazás módosult, a Kaspersky Endpoint Security ugyanúgy végigelemzi, mintha az első elindítására kerülne sor.

A hálózati szabályok fontossági sorrendje

Minden szabálynak van valamilyen prioritása. Minél magasabban helyezkedik el egy szabály a szabályok listáján, annál magasabb a prioritása. Ha egy hálózati tevékenység több szabályhoz is társítva van, a Tűzfal a legmagasabb prioritású szabálynak megfelelően szabályozza a hálózati tevékenységet.

A hálózati csomagszabályok prioritása magasabb, mint az alkalmazások hálózati szabályaié. Ha ugyanazon típusú hálózati tevékenységre csomagszabályok és alkalmazásszabályok is meg vannak adva, a hálózati tevékenységet a csomagszabályok fogják szabályozni.

Az alkalmazások hálózati szabályai meghatározott módon működnek. Az alkalmazásokhoz tartozó hálózati szabály a hálózati állapot alapján foglal magában hozzáférési szabályokat: *nyilvános hálózat*, *helyi hálózat* vagy *megbízható hálózat*. Például a *Magas korlátozás* megbízhatósági csoportban lévő alkalmazások esetében alapértelmezetten minden hálózati állapotban le van tiltva a hálózati tevékenység. Ha egy hálózati szabály meg van adva egy egyéni alkalmazásra (szülőalkalmazásra) vonatkozóan, akkor az egyéb alkalmazások gyermekfolyamatai a szülőalkalmazás hálózati szabálya szerint fognak futni. Ha az alkalmazásnak nincs hálózati szabálya, az utódfolyamatok az alkalmazás megbízhatósági csoportjának hálózati szabálya szerint fognak futni.

Példa: Ön az alkalmazások számára az összes hálózati állapotban letiltotta a hálózati tevékenységet, kivéve az X böngésző számára. Ha az X böngészőből (szülőalkalmazás) elindítja az Y böngésző telepítését (gyermekfolyamat), az Y böngésző telepítője hozzáfér az internethez, és letölti a szükséges fájlokat. A telepítés után az Y böngésző a Tűzfal beállításai miatt nem fogja tudni elérni a hálózati kapcsolatokat. Ahhoz, hogy Ön az Y böngésző telepítője (gyermekfolyamat) számára megtiltsa a hálózati tevékenységet, hozzá kell adnia egy hálózati szabályt az Y böngésző telepítőjéhez.

Hálózati kapcsolati típusok

A Tűzfal lehetővé teszi Önnek a hálózat tevékenység felügyeletét a hálózati kapcsolat típusától függően. A Kaspersky Endpoint Security a számítógép operációs rendszerétől kapja meg a hálózati kapcsolatok típusát. Az operációs rendszerben a hálózati kapcsolat típusát a felhasználó szabhatja meg a kapcsolat létrehozásakor. Lehetősége van megváltoztatni a hálózati kapcsolat típusát a Kaspersky Endpoint Security beállításai között. A Tűzfal a Kaspersky Endpoint Security beállításaiban, és nem az operációs rendszerben megadott hálózattípustól függően figyeli a hálózati tevékenységet.

A következő hálózati kapcsolattípusok érhetők el:

- **Nyilvános hálózat**. A hálózatot nem védi víruskereső alkalmazás, tűzfal és szűrő (például wifi egy kávézóban). Az ilyen hálózathoz kapcsolódó számítógép felhasználója számára a Tűzfal blokkolja a számítógép fájljaihoz és nyomtatóihoz való hozzáférést. A külső felhasználók megosztott mappákon keresztül sem férhetnek hozzá adatokhoz, illetve a számítógép asztalához sincs távoli hozzáférésük. A Tűzfal az egyes alkalmazások hálózati tevékenységét az azokhoz beállított hálózati szabályok alapján szűri ki.

  A Tűzfal alapértelmezés szerint az internetnek *Nyilvános hálózat* típust oszt ki. Az internet típusa nem módosítható.

- **Helyi hálózat**. Hálózat olyan felhasználóknak, akik korlátozott hozzáféréssel rendelkeznek a jelen számítógép fájljaihoz és nyomtatóihoz (például vállalati LAN vagy otthoni hálózat).

- **Megbízható hálózat**. Biztonságos hálózat, amelyen a számítógép nincs kitéve támadásoknak, sem az adatok illetéktelen elérésére irányuló próbálkozásoknak. A Tűzfal az ilyen állapotú hálózaton belül minden hálózati tevékenységet engedélyez.

A Tűzfal be- és kikapcsolása

Alapértelmezés szerint a Tűzfal be van kapcsolva és optimális módban működik.

A Tűzfal funkció engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem → Tűzfal** lehetőséget.
4. A **Tűzfal** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
5. Mentse el a módosításokat.

A Tűzfal funkció engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.

4. Válassza az **Communication & Web Protection** → **Firewall** lehetőséget.
5. A **Firewall ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Mentse el a módosításokat.

A Tűzfal funkció engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. A **Tűzfal** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ha a Tűzfal engedélyezve van, a Kaspersky Endpoint Security felügyeli a hálózati tevékenységeket, és blokkolja a számítógép illetéktelen hálózati kapcsolatait, illetve a számítógépén található alkalmazások illetéktelen hálózati tevékenységeit. A hálózati tevékenységeket a Hálózati védelem összetevő is felügyeli. A Hálózati védelem összetevő (más néven behatolásérzékelő rendszer, IDS) figyeli a bejövő hálózati forgalmat a hálózati támadásokra jellemző tevékenységek szempontjából.

A Kaspersky Endpoint Security a jelentésében naplózza a hálózati támadási eseményeket, függetlenül a Tűzfal beállításaitól. Még ha a Tűzfal blokkolja is a hálózati kapcsolatot a szabályok használatával és megakadályozza a hálózati támadásokat, a Hálózati védelem összetevő akkor is regisztrálja a hálózati támadási eseményeket. Erre azért van szükség, hogy a rendszer statisztikai adatokat tudjon összegyűjteni a cég vagy szervezet számítógépeit ért hálózati támadásokról.

A hálózati kapcsolat típusának módosítása

A Tűzfal alapértelmezés szerint az internetnek *Nyilvános hálózat* típust oszt ki. Az internet típusa nem módosítható.

A hálózati kapcsolat típusának módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson az **Elérhető hálózatok** elemre.
4. Válassza ki azt a hálózati kapcsolatot, amelynek módosítani szeretné a típusát.

5. A **Hálózat típusa** oszlopban válassza ki a hálózati kapcsolat típusát:

   - **Nyilvános hálózat**. A hálózatot nem védi víruskereső alkalmazás, tűzfal és szűrő (például wifi egy kávézóban). Az ilyen hálózathoz kapcsolódó számítógép felhasználója számára a Tűzfal blokkolja a számítógép fájljaihoz és nyomtatóihoz való hozzáférést. A külső felhasználók megosztott mappákon keresztül sem férhetnek hozzá adatokhoz, illetve a számítógép asztalához sincs távoli hozzáférésük. A Tűzfal az egyes alkalmazások hálózati tevékenységét az azokhoz beállított hálózati szabályok alapján szűri ki.

   - **Helyi hálózat**. Hálózat olyan felhasználóknak, akik korlátozott hozzáféréssel rendelkeznek a jelen számítógép fájljaihoz és nyomtatóihoz (például vállalati LAN vagy otthoni hálózat).

   - **Megbízható hálózat**. Biztonságos hálózat, amelyen a számítógép nincs kitéve támadásoknak, sem az adatok illetéktelen elérésére irányuló próbálkozásoknak. A Tűzfal az ilyen állapotú hálózaton belül minden hálózati tevékenységet engedélyez.

6. Mentse el a módosításokat.

A hálózati csomagszabályok kezelése

A hálózati csomagszabályok kezelése során a következő műveleteket végezheti el:

- Új hálózati csomagszabály létrehozása.

  Új hálózati csomagszabályt úgy állíthat elő, hogy létrehozza a hálózati csomagokra és adatfolyamokra alkalmazandó feltételek és műveletek készletét.

- Hálózati csomagszabály be- és kikapcsolása.

  A Tűzfal által létrehozott összes hálózati csomagszabály alapértelmezett állapota *Engedélyezve*. Ha egy hálózati csomagszabály engedélyezve van, a Tűzfal alkalmazza a szabályt.

  A hálózati csomagszabályok listáján bármelyik hálózati csomagszabály kikapcsolható. Ha egy hálózati csomagszabály ki van kapcsolva, a Tűzfal átmenetileg nem alkalmazza a szabályt.

  > Az új egyéni hálózati csomagszabály alapértelmezés szerint *Engedélyezve* állapottal kerül a hálózati csomagszabályok listájára.

- Meglévő hálózati csomagszabály beállításainak szerkesztése.

  Az új hálózati csomagszabály előállítását követően mindig visszatérhet a beállításai szerkesztéséhez és igény szerinti módosításához.

- A Tűzfal műveletének módosítása hálózati csomagszabálynál.

  A hálózati csomagszabályok listáján szerkesztheti azt a műveletet, amelyet a Tűzfal egy adott hálózati csomagszabállyal egyező hálózati tevékenység észlelésekor végez.

- Hálózati csomagszabály prioritásának módosítása.

  A listán kijelölt hálózati csomagszabály prioritását növelheti vagy csökkentheti.

- Hálózati csomagszabály eltávolítása.

  A hálózati csomagszabályok eltávolításával a Tűzfal többé nem alkalmazza a szabályokat hálózati tevékenység észlelésekor, és a szabályok többé nem jelennek meg a hálózati csomagszabályok listáján *Kikapcsolt* állapottal.

Hálózati csomagszabály létrehozása

A Tűzfal a hálózati csomagszabályoknak megfelelően szűr minden hálózati tevékenységet a számítógépen. A hálózati csomagszabályok olyan feltételeket (például irány, protokoll) tartalmaznak, amelyeket a Tűzfal a számítógép hálózati kapcsolatainak felügyeletéhez alkalmaz. A hálózati csomagszabályok azt is meghatározzák, hogy a Tűzfal milyen műveletet hajtson végre a szabálynak megfelelő kapcsolattal (a kapcsolat engedélyezése vagy blokkolása).

Javaslatok a hálózati csomagszabályok létrehozásához

Megadhat egy IP-címet vagy IP-címtartományt a hálózati tevékenység szűréséhez. DNS-nevet is megadhat, de javasoljuk az IP-címek és IP-címtartományok használatát. Előfordulhat, hogy a DNS-nevek használata a hálózati csomagnevekben nem biztonságos, mert a DNS-kiszolgáló tulajdonosa módosíthatja a DNS-rekord paramétereit. A rosszindulatú szereplők a DNS-üzeneteket is meghamisíthatják, és a tűzfalszabályokat megkerülhetik.

A hálózati kapcsolatokat DNS-nevek alapján felügyelheti a Webfelügyelő szabályaival. Ha meg kell adnia egy DNS-nevet a tűzfalszabályokban:

- Gondoskodjon a vállalati LAN biztonságáról.
- Biztosítsa a gyorsítótárazás és a hiteles DNS-kiszolgálók biztonságát.
- Engedélyezze a DNS-rekord módosítása elleni védelmét.

Hálózati csomagszabályok létrehozásakor ne feledje, hogy azok az alkalmazások hálózati szabályai felett állnak.

A hálózati csomagszabályok létrehozásának módszerei

Hálózati csomagszabályt az alábbi módokon hozhat létre:

- Használja a Hálózatfigyelő eszközt.

  A *Hálózatfigyelő* eszközzel valós időben tekinthetők meg a felhasználó számítógépének hálózati tevékenységével kapcsolatos információk. Ez kényelmes, mert nem kell konfigurálnia az összes szabálybeállítást. A rendszer egyes tűzfalbeállításokat automatikusan beilleszt a Hálózatfigyelő adataiból. A Hálózatfigyelő csak az alkalmazás felületén érhető el.

- Konfigurálja a Tűzfal beállításait.

  Lehetővé teszi a Tűzfal beállításainak finomhangolását. Bármely hálózati tevékenységhez szabályokat hozhat létre, még akkor is, ha az adott pillanatban nincs hálózati tevékenység.

Hálózati csomagszabály létrehozása a Hálózatfigyelő eszközzel az alkalmazás felületén

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Hálózatfigyelő** csempére.
2. Nyissa meg a **Hálózati tevékenység** lapot.

   A **Hálózati tevékenység** lapon az összes, a számítógépen jelenleg aktív hálózati kapcsolat látható. A kimenő és bejövő hálózati kapcsolatok egyaránt megjelennek.
3. A hálózati kapcsolat helyi menüjében válassza ki a **Hálózati csomagszabály létrehozása** lehetőséget.

   Ezután megjelennek a hálózati szabály tulajdonságai.
4. Állítsa be a csomagszabály **Aktív** állapotát.
5. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.
6. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

   Kiválaszthat egy előre meghatározott szabálysablont a **Hálózati szabály sablonja** hivatkozásra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

   A hálózati szabály összes beállítása automatikusan kitöltődik.
7. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.
8. Kattintson a **Mentés** gombra.

   Az új hálózati szabály felkerül a listára.
9. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.
10. Mentse el a módosításokat.

Hálózati csomagszabály létrehozása a Tűzfal beállításainak használatával az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson a **Csomagszabályok** gombra.

   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
4. A **Hozzáadás** legördülő listában válassza ki a szabály helyét a listában: a lista tetején, a lista alján vagy a kiválasztott szabály mellett.

   A szabály listán elfoglalt helye határozza meg a szabály prioritását. A lista tetején lévő szabálynak van a legmagasabb prioritása.
5. Állítsa be a csomagszabály **Aktív** állapotát.
6. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.
7. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

   Kiválaszthat egy előre meghatározott szabálysablont a **Hálózati szabály sablonja** hivatkozásra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

   A hálózati szabály összes beállítása automatikusan kitöltődik.

8. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.

9. Kattintson a **Mentés** gombra.

   Az új hálózati szabály felkerül a listára.

10. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.

11. Mentse el a módosításokat.

Hálózati csomagszabály létrehozása az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** lehetőséget.

4. A **A Tűzfal beállításai** részen kattintson a **Beállítások** gombra.

   Ez megnyitja a hálózati csomagszabályok és az alkalmazás hálózati szabályainak listáját.

5. Nyissa meg a **Hálózati csomagszabályok** lapot.

   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.

6. A **Hozzáadás** legördülő listában válassza ki a szabály helyét a listában: a lista tetején, a lista alján vagy a kiválasztott szabály mellett.

   A szabály listán elfoglalt helye határozza meg a szabály prioritását. A lista tetején lévő szabálynak van a legmagasabb prioritása.

7. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.

8. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

   Kiválaszthat egy előre meghatározott szabálysablont a gombra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

   A hálózati szabály összes beállítása automatikusan kitöltődik.

9. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.

10. Mentse az új hálózati szabályt.

11. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.

12. Mentse el a módosításokat.

A Tűzfal a szabály szerint kezeli a hálózati csomagokat. Letilthatja a csomagszabály Tűzfalon belüli kezelését anélkül, hogy törölné azt a listáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

Hálózati csomagszabály létrehozása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.
4. Válassza az **Communication & Web Protection → Firewall** lehetőséget.
5. Válassza ki az **Network packet rules** lapot.

   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
6. Kattintson az **Add** gombra.

   Ezzel megnyílik az új hálózati szabály űrlapja.
7. Adja meg manuálisan a hálózati szolgáltatás nevét a **Rule name** mezőben.
8. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

   Kiválaszthat egy előre meghatározott szabálysablont a **Select rule template** hivatkozásra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

   A hálózati szabály összes beállítása automatikusan kitöltődik.
9. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Log events** jelölőnégyzetet.
10. Mentse a hálózati szabályt.

    Az új hálózati szabály felkerül a listára.
11. A **Move** gombbal állíthatja be a hálózati szabály prioritását.
12. Mentse el a módosításokat.

A Tűzfal a szabály szerint kezeli a hálózati csomagokat. Letilthatja a csomagszabály Tűzfalon belüli kezelését anélkül, hogy törölné azt a listáról. A **Status** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le a csomagszabályt.

Hálózati csomagszabály beállításai

Paraméter	Leírás
Művelet	**Engedélyezés**. **Blokkolás**. **Alkalmazásszabályok szerint**. Ha ezt az opciót választja, a Tűzfal az alkalmazás hálózati szabályait alkalmazza a hálózati kapcsolatra.
Protokoll	Hálózati tevékenység felügyelete a kiválasztott protokollon: TCP, UDP, ICMP, ICMPv6, IGMP és GRE. Ha az ICMP vagy ICMPv6 protokollt választotta, meghatározhatja az ICMP csomag típusát és a kódját. Ha a TCP vagy az UDP protokolltípust választotta, megadhatja a helyi és a távoli számítógépek portszámait, amelyek között a kapcsolatot figyelni kell. A portszámok lehetséges értéktartománya: 0–65535. Minden mezőbe több értéket is megadhat `,` karakterekkel elválasztva, vagy megadhat egy értéktartományt `-` karakterekkel. Például: • `100,101` • `100-130` • `100,110-130`
Direction	**Bejövő (csomag)**. A Tűzfal az összes bejövő hálózati csomagra alkalmazza a hálózati szabályt. **Bejövő**. A Tűzfal a távoli számítógép által kezdeményezett kapcsolaton keresztül küldött összes hálózati csomagra alkalmazza a hálózati szabályt. **Bejövő / kimenő**. A Tűzfal a hálózati szabályt minden bejövő és kimenő hálózati csomagra alkalmazza. **Kimenő (csomag)**. A Tűzfal az összes kimenő hálózati csomagra alkalmazza a hálózati szabályt. **Kimenő**. A Tűzfal a felhasználó számítógépe által kezdeményezett kapcsolaton keresztül küldött összes hálózati csomagra alkalmazza a hálózati szabályt.
Hálózati adapterek	Hálózati adapterek, amelyek hálózati csomagokat küldhetnek és/vagy fogadhatnak. A hálózati adapterek beállításainak megadásával különbséget lehet tenni az azonos IP-című hálózati adapterek által küldött, illetve fogadott hálózati csomagok között.
Élettartam (TTL)	A hálózati csomagok felügyeletének korlátozása élettartamukra (Time to Live, TTL).

Paraméter	Leírás
Távoli címek	Távoli számítógépek hálózati címei, amelyek hálózati csomagokat küldhetnek és/vagy fogadhatnak. A Tűzfal a távoli hálózati címek megadott tartományára alkalmazza a hálózati szabályt. Felveheti az összes IP-címet egy hálózati szabályba, létrehozhat egy külön IP-címlistát, meghatározhat egy IP-címtartományt, vagy kiválaszthat egy alhálózatot (Megbízható hálózatok, Helyi hálózatok, Nyilvános hálózatok). A számítógép DNS-nevét is megadhatja az IP-címe helyett. A DNS-neveket csak LAN-hálózaton lévő számítógépekhez vagy belső szolgáltatásokhoz használja. A felhőszolgáltatásokkal (például Microsoft Azure) és más internetes erőforrásokkal való interakciót a Web Control összetevőnek kell kezelnie. Ha a hálózati csomagszabályban olyan DNS-nevet adott meg, amelynek IP-címe nem határozható meg, a Kaspersky Endpoint Security figyelmeztetést jelenít meg. A Web Console-ban a hálózati csomagszabályok listája kiegészül egy oszloppal, amely tartalmazza a hiba leírását. Az adminisztrációs konzolon (MMC) a hibaleírás nem érhető el. Az ilyen csomagszabályok színnel vannak kiemelve.
Helyi címek	Számítógépek hálózati címei, amelyek hálózati csomagokat küldhetnek és/vagy fogadhatnak. A Tűzfal a hálózati szabályt a helyi hálózati címek megadott tartományára alkalmazza. Felveheti az összes IP-címet egy hálózati szabályba, létrehozhat egy külön IP-címlistát, vagy meghatározhat egy IP-címtartományt. Az alkalmazás csak akkor tárolja a helyi címeket, ha távoli címek listája meg van adva. Ez azt jelenti, hogy a **Címek a listából** érték lett kiválasztva a **Távoli címek** esetében, és legalább egy cím hozzá lett adva. Néha a helyi címet alkalmazásoknál nem lehet beszerezni. Ebben az esetben ez a paraméter figyelmen kívül marad.

Hálózati csomagszabály be- és kikapcsolása

Hálózati csomagszabály be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson a **Csomagszabályok** gombra.
   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati csomagszabályok listáját.
4. A listán válassza ki a szükséges hálózati csomagszabályt.
5. A **Státusz** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le a szabályt.
6. Mentse el a módosításokat.

A Tűzfal műveletének módosítása hálózati csomagszabálynál

A Tűzfal hálózati csomagszabályra alkalmazott műveletének módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson a **Csomagszabályok** gombra.
   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati csomagszabályok listáját.

4. Válassza ki a hálózati csomagszabályok listáról, és kattintson a **Szerkesztés** gombra.

5. Válassza ki a **Művelet** legördülő listán a Tűzfal által az adott típusú hálózati tevékenység észlelésekor végrehajtandó műveletet:

   - **Engedélyezés**.
   - **Blokkolás**.
   - **Alkalmazásszabályok szerint**. Ha ezt az opciót választja, a Tűzfal az alkalmazás hálózati szabályait alkalmazza a hálózati kapcsolatra.

6. Mentse el a módosításokat.

Hálózati csomagszabály prioritásának módosítása

Egy hálózati csomagszabály prioritását a hálózati csomagszabályok listáján elfoglalt helye határozza meg. A lista legfelső hálózati csomagszabálya a legmagasabb prioritású.

Minden kézileg létrehozott hálózati csomagszabály a lista végére kerül, és a legalacsonyabb lesz a prioritása.

A Tűzfal a szabályokat abban a sorrendben hajtja végre, ahogy fentről lefelé a hálózati csomagszabályok listáján elhelyezkednek. Az adott hálózati kapcsolatra vonatkozó egyes feldolgozott hálózati csomagszabályoknak megfelelően a Tűzfal vagy engedélyezi, vagy blokkolja a hálózati hozzáférést a hálózati kapcsolat beállításaiban megadott címhez és porthoz.

Hálózati csomagszabály prioritásának módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson a **Csomagszabályok** gombra.

   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati csomagszabályok listáját.

4. Válassza ki a listán azt a hálózati csomagszabályt, amelynek módosítani szeretné a prioritását.
5. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.
6. Mentse el a módosításokat.

Hálózati csomagszabályok exportálása és importálása

A hálózati csomagszabályok listáját exportálhatja egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú szabály hozzáadásával. Használhatja az exportálás/importálás funkciót a hálózati csomagszabályok biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A hálózati csomagszabályok listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** lehetőséget.
4. A **A Tűzfal beállításai** részen kattintson a **Beállítások** gombra.

   Ez megnyitja a hálózati csomagszabályok és az alkalmazás hálózati szabályainak listáját.
5. Nyissa meg a **Hálózati csomagszabályok** lapot.
6. Hálózati csomagszabályok listájának exportálása:

   a. Jelölje ki az exportálni kívánt szabályokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.

   Ha nem jelölt ki szabályt, a Kaspersky Endpoint Security az összes szabályt exportálja.

   b. Kattintson az **Exportálás** hivatkozásra.

   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a szabályok listáját, és válassza a fájl mentésére kiszemelt mappát.

   d. Mentse a fájlt.

   A Kaspersky Endpoint Security exportálja a szabályok listáját az XML-fájlba.
7. Hálózati csomagszabályok listájának importálása:

   a. Kattintson az **Import** hivatkozásra.

   A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
8. Mentse el a módosításokat.

A hálózati csomagszabályok listájának exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Válassza az **Communication & Web Protection** → **Firewall** lehetőséget.

5. A szabályok listájának exportálása a **Network packet rules** területen:

   a. Jelölje ki az exportálni kívánt szabályokat.

   b. Kattintson az → **Export** gombra.

      A Kaspersky Endpoint Security a szabályok listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

6. A szabályok listájának importálása a **Network packet rules** területen:

   a. Kattintson az → **Import** gombra.

      A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a szabályok listáját.

   b. Nyissa meg a fájlt.

      Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.

7. Mentse el a módosításokat.

Hálózati csomagszabályok definiálása XML-ben

A Tűzfal lehetővé teszi a hálózati csomagszabályok XML-formátumban történő exportálását. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú szabály hozzáadásával.

Az XML-fájl két fő csomópontot tartalmaz: `Rules` és `Resources`. A `Rules` csomópont listázza a hálózati csomagszabályokat. Ez a csomópont tartalmazza az alapértelmezetten konfigurált szabályokat (*előre meghatározott szabályok*), valamint a felhasználó által hozzáadott szabályokat (*egyéni szabályok*).

Hálózati csomagszabályok jelölése

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Paraméter	Leírás	Érték
`<key name="0000">`	A szabály prioritása. Minél alacsonyabb az érték, annál magasabb a prioritás.	Egész szám A prioritási értéknek 4 számjegyből kell állnia. Az XML-fájlban a csomópontokat prioritási érték szerint kell elrendezni, `0000` értékkel kezdve.
`RuleId`	A szabály azonosítója.	**Előre definiált szabályok** `100` –**Kérések a DNS kiszolgáló számára TCP protokollon keresztül**. `101` –**Kérések a DNS kiszolgáló számára UDP protokollon keresztül**. `102` – **E-mailek küldése**. `110` – **Bármiféle hálózati tevékenység** (Megbízható hálózatok). `125` – **Bármiféle hálózati tevékenység** (Helyi hálózatok). `130` – **Távoli asztal hálózati tevékenysége**. `131` – **TCP kapcsolatok helyi portokon keresztül**. `132` – **UDP kapcsolatok helyi portokon keresztül**. `133` – **Bejövő TCP adatfolyam**. `134` – **Bejövő UDP adatfolyam**. `137` – **ICMP Cél elérhetetlen bejövő válaszok**. `138` – **Bejövő ICMP visszhangválasz csomagok**. `140` – **Bejövő ICMP időtúllépés válaszok**. `142` – **Bejövő ICMP adatfolyam**. `266` – **Bejövő ICMPv6 visszhangkérés csomagok**.
`RuleState`	A szabály állapota.	`0` – az előre meghatározott szabály le van tiltva `1` – az előre meghatározott szabály engedélyezve van `2` – az egyéni szabály le van tiltva `3` – az egyéni szabály engedélyezve van
`RuleTypeId`	A szabálytípus azonosítója.	`4` – hálózati csomagszabály.
`AppIdEx`	Annak az alkalmazásnak az azonosítója, amelyhez a hálózati csomagszabály tartozik.	Ha a szabály nem tartozik egyetlen alkalmazáshoz sem, az érték `0`.
`ResIdEx`	A szabálybeállításokat tartalmazó erőforrás fő azonosítója. Ezzel az azonosítóval kereshet meg egy blokkot a szabálybeállításokkal az `Resources` csomópontban.	Egész szám
`ResIdEx2`	A hálózati típus azonosítója.	`0` – **Bármely cím**. `50` – **Megbízható hálózatok**. `51` – **Helyi hálózatok**. `52` – **Nyilvános hálózatok**. `<Network Identifier>` – **Címek a listából** (a címek meghatározása manuálisan történik).
`AccessFlag`	A **Művelet** paraméter értéke.	`0` – **Engedélyezés**. `2` – **Alkalmazásszabályokkal**. `3` – **Blokkolás**. `4` – **Engedélyezés** és **Események naplózása**. `6` – **Alkalmazásszabályokkal** és **Események naplózása**. `7` – **Blokkolás** és **Események naplózása**.
`</key>`		

Az `Resources` csomópont tartalmazza a hálózati csomagszabályok beállításait. Az egyéni hálózati csomagszabály beállításai a `<key name="0004">` blokkban találhatók.

Egyéni hálózati csomagszabály jelölése

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Egyéni hálózati csomagszabály beállításai

Paraméter	Leírás	Érték
`<key name="Data">`	A paraméterblokk azonosítója.	Egész szám
`RemotePorts`	A **Távoli portok** paraméter értéke.	A távoli porttartományok listája.
`LocalPorts`	A **Helyi portok** paraméter értéke.	A helyi porttartományok listája.

Paraméter	Leírás	Érték
`AdapterBindings`	A **Hálózati adapterek** paraméter értéke.	`IpAddresses` – a **IP-címek** paraméter értéke. `MacAddresses` – a **MAC-címek** paraméter értéke. `AdapterName` – a hálózati adapter neve. `InterfaceType` – a **Felület típusa** paraméter értéke: • `0` – **Egyéb**. • `1` – **LoopBack**. • `2` – **Vezetékes hálózat (Ethernet)**. • `3` – **Vezeték nélküli hálózat (Wi-Fi)**. • `4` – **Alagút**. • `5` – **PPP-kapcsolat**. • `6` – **PPPoE-kapcsolat**. • `7` – **VPN-kapcsolat**. • `8` – **Modemes kapcsolat**.
`unique`	A struktúra belső azonosítója.	Egész szám Ajánlott ezt a paramétert változatlanul hagyni.
`Proto`	A **Protokoll** paraméter értéke.	`0` – letiltva. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Az **Irány** paraméter értéke.	`1` – **Bejövő (csomag)**. `2` – **Kimenő (csomag)**. `3` – **Bejövő / kimenő**. `4` – **Bejövő**. `5` – **Kimenő**.

Paraméter	Leírás	Érték
`IcmpType`	Az **ICMP típus** paraméter értéke.	**ICMP protokoll** `0` – **Visszhangválasz** (ICMP) vagy letiltva. `3` – **A cél nem elérhető** (ICMP). `4` – **Forráselnyomás**. `5` – **Átirányítás**. `6` – **Alternatív gazdagép cím**. `8` – **Visszhangkérés**. `9` – **Útválasztói hirdetmény**. `10` – **Útválasztói megszólítás**. `11` – **Időtúllépés**. `12` – **Paraméterprobléma**. `13` – **Időbélyeg**. `14` – **Időbélyeg válasz**. `15` – **Információkérés**. `16` – **Információválasz**. `17` – **Címmaszkkérés**. `18` – **Címmaszkválasz**. `30` – **Nyomkövetés útvonala**. `31` – **Datagram-konverziós hiba**. `32` – **Mobil gazdagép átirányítása**. `33` – **IPv6 Hol-vagy**. `34` – **IPv6 Itt-vagyok**. `35` – **Mobilregisztrációs kérés**. `36` – **Mobilregisztrációs válasz**. `37` – **Tartománynév-kérelem**. `38` – **Tartománynév-válasz**. `40` – **Photuris**. **ICMPv6 protokoll** `1` – **A cél nem elérhető**. `2` – **Túl nagy csomag**. `3` – **Időtúllépés**. `4` – **Paraméterprobléma**. `128` – **Visszhangkérés**. `129` – **Visszhangválasz**. `130` – **Csoportos küldési figyelő lekérdezés**. `131` – **Csoportos küldési figyelő jelentés**. `132` – **Csoportos küldési figyelő kész**. `133` – **Útválasztói megszólítás**. `134` – **Útválasztói hirdetmény**. `135` – **Szomszédmegszólítás**. `136` – **Szomszédhirdetmény**. `137` – **Üzenet átirányítása**. `138` – **Útválasztó újraszámozása**. `139` – **ICMP csomópont-információk lekérdezése**. `141` – **Inverz szomszéd-felderítési megszólítási üzenet**. `142` – **Inverz szomszéd-felderítési hirdetményüzenet**. `143` – **Csoportos küldési figyelő jelentés, 2. verzió**.

Paraméter	Leírás	Érték
		`144` – **Honállomás címfelderítés kérési üzenet**. `145` – **Honállomás címfelderítési válaszüzenet**. `146` – **Mobil előtag megszólítás**. `147` – **Mobil előtag hirdetmény**. `148` – **Tanúsítványlánc megszólítási üzenet**. `149` – **Tanúsítványlánc hirdetményüzenet**. `151` – **Csoportos küldésű útválasztó hirdetmény**. `152` – **Csoportos küldésű útválasztó megszólítás**. `153` – **Csoportos küldésű útválasztó befejezés**.
`IcmpCode`	Az **ICMP kód** paraméter értéke.	`0` – **0. kód** vagy letiltva. `1` – **1. kód**. `2` – **2. kód**.
`Flags`	Szerkezeti attribútum mutatója.	Egész szám Ajánlott ezt a paramétert változatlanul hagyni.
`TTL`	Az **Élettartam (TTL)** paraméter értéke.	Érték másodpercben. Ha le van tiltva, az érték `0`.
`</key>`		
`Id`	Az erőforrás fő azonosítója (lásd a `Rules` csomópontot).	Egész szám
`ParentID`	A szülőcsoport azonosítója.	Egész szám Ajánlott ezt a paramétert változatlanul hagyni.
`Flags`	A szabály állapota.	`6` – a szabály le van tiltva. `38` – a szabály engedélyezve van.
`Name`	A hálózati csomagszabály neve.	Karakterlánc

Az alkalmazások hálózati szabályainak kezelése

A Kaspersky Endpoint Security alapértelmezés szerint a számítógépen telepített összes alkalmazást azon szoftverek forgalmazójának neve alapján csoportosítja, amelyek fájl- vagy hálózati tevékenységét figyeli. Az alkalmazáscsoportok pedig megbízhatósági csoportokba vannak besorolva. Minden alkalmazás és alkalmazáscsoport örökli a tulajdonságokat szülőcsoportjától: az alkalmazásfelügyeleti szabályoktól, az alkalmazások hálózati szabályaitól és végrehajtási prioritásuktól.

A Behatolásmegelőző rendszer összetevőhöz hasonlóan a Tűzfal összetevő alapértelmezés szerint az alkalmazáscsoportok hálózati szabályait akkor alkalmazza, ha a csoporton belüli összes alkalmazás hálózati tevékenységét szűri. Az alkalmazáscsoport hálózati szabályai határozzák meg a csoportba tartozó alkalmazások különféle hálózati kapcsolatokhoz való hozzáféréshez fűződő jogait.

A Tűzfal alapértelmezés szerint a Kaspersky Endpoint Security által a számítógépen észlelt minden alkalmazáscsoport számára egy-egy hálózati szabálykészletet állít elő. Az alkalmazáscsoportok alapértelmezés szerint előállított hálózati szabályaira alkalmazott Tűzfal-műveletet módosíthatja. Az alkalmazáscsoportok alapértelmezés szerint előállított hálózati szabályait nem szerkesztheti, nem távolíthatja el, nem kapcsolhatja ki, és prioritásukat nem módosíthatja.

Hálózati szabályt egyenként is létrehozhat az alkalmazásokhoz. Az ilyen szabályok prioritása magasabb, mint azoké a szabályoké, amely az adott alkalmazást tartalmazó csoportra vonatkozik.

Alkalmazás hálózati szabályának létrehozása

Alapértelmezés szerint az alkalmazás tevékenységét olyan hálózati szabályok felügyelik, amelyek olyan megbízhatósági csoporthoz tartoznak, amelybe a Kaspersky Endpoint Security az alkalmazást annak első indításakor besorolta. Szükség esetén létrehozhat hálózati szabályokat egy teljes megbízhatósági csoporthoz, egy egyedi alkalmazáshoz vagy egy megbízhatósági csoporton belüli alkalmazások adott csoportjához.

A manuálisan definiált hálózati szabályok a megbízhatósági csoporthoz meghatározott hálózati szabályoknál magasabb prioritással rendelkeznek. Más szóval, ha a manuálisan definiált alkalmazásszabályok eltérnek a megbízhatósági csoporthoz meghatározott alkalmazásszabályoktól, a Tűzfal az alkalmazás manuálisan definiált szabályai szerint felügyeli az alkalmazás tevékenységét.

Alapértelmezés szerint a Tűzfal az alábbi hálózati szabályokat hozza létre minden egyes alkalmazáshoz:

- Bármely hálózati tevékenység megbízható hálózatokon.
- Bármilyen hálózati tevékenység helyi hálózatokon.
- Bármilyen hálózati tevékenység nyilvános hálózatokon.

A Kaspersky Endpoint Security az alábbiak alapján felügyeli az alkalmazások hálózati tevékenységét az előre meghatározott hálózati szabályok szerint:

- Megbízható és alacsony korlátozású: minden hálózati tevékenység engedélyezve van.
- Magas korlátozású és nem megbízható: minden hálózati tevékenység blokkolva van.

Az előre definiált alkalmazásszabályokat nem lehet szerkeszteni vagy törölni.

Egy alkalmazás hálózati szabályát az alábbi módokon hozhatja létre:

- Használja a Hálózatfigyelő eszközt.

  A *Hálózatfigyelő* eszközzel valós időben tekinthetők meg a felhasználó számítógépének hálózati tevékenységével kapcsolatos információk. Ez kényelmes, mert nem kell konfigurálnia az összes szabálybeállítást. A rendszer egyes tűzfalbeállításokat automatikusan beilleszt a Hálózatfigyelő adataiból. A Hálózatfigyelő csak az alkalmazás felületén érhető el.

- Konfigurálja a Tűzfal beállításait.

  Lehetővé teszi a Tűzfal beállításainak finomhangolását. Bármely hálózati tevékenységhez szabályokat hozhat létre, még akkor is, ha az adott pillanatban nincs hálózati tevékenység.

Az alkalmazások hálózati szabályainak létrehozásakor ne feledje, hogy a hálózati csomagszabályok elsőbbséget élveznek az alkalmazás hálózati szabályaival szemben.

Alkalmazás hálózati szabályának létrehozása a Hálózatfigyelő eszközzel az alkalmazás felületén

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Hálózatfigyelő** csempére.
2. Nyissa meg a **Hálózati tevékenység** vagy a **Nyitott portok** lapot.

   A **Hálózati tevékenység** lapon az összes, a számítógépen jelenleg aktív hálózati kapcsolat látható. A kimenő és bejövő hálózati kapcsolatok egyaránt megjelennek.

   A **Nyitott portok** lapon látható a számítógép összes nyitott portja.
3. A hálózati kapcsolat helyi menüjében válassza ki az **Alkalmazáshoz tartozó hálózati szabály létrehozása** lehetőséget.

   Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.
4. Válassza ki a **Hálózati szabályok** lapot.

   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
5. Kattintson **Hozzáadás** gombra.

   Ezután megjelennek a hálózati szabály tulajdonságai.
6. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.
7. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

   Kiválaszthat egy előre meghatározott szabálysablont a **Hálózati szabály sablonja** hivatkozásra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

   A hálózati szabály összes beállítása automatikusan kitöltődik.
8. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.
9. Kattintson a **Mentés** gombra.

   Az új hálózati szabály felkerül a listára.
10. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.
11. Mentse el a módosításokat.

Alkalmazás hálózati szabályának létrehozása a Tűzfal beállításainak használatával az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson az **Alkalmazások szabályai** gombra.

   Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.

4. Az alkalmazások listáján kiválaszthatja azt az alkalmazást vagy alkalmazáscsoportot, amelynél hálózati szabályt szeretne létrehozni.

5. Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Részletek és szabályok** lehetőséget.

   Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.

6. Válassza ki a **Hálózati szabályok** lapot.

7. Kattintson **Hozzáadás** gombra.

   Ezután megjelennek a hálózati szabály tulajdonságai.

8. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.

9. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

   Kiválaszthat egy előre meghatározott szabálysablont a **Hálózati szabály sablonja** hivatkozásra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

   A hálózati szabály összes beállítása automatikusan kitöltődik.

10. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.

11. Kattintson a **Mentés** gombra.

    Az új hálózati szabály felkerül a listára.

12. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.

13. Mentse el a módosításokat.

Alkalmazás hálózati szabályának létrehozása az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** lehetőséget.

4. A **A Tűzfal beállításai** részen kattintson a **Beállítások** gombra.

   Ez megnyitja a hálózati csomagszabályok és az alkalmazás hálózati szabályainak listáját.

5. Nyissa meg az **Alkalmazás hálózati szabályai** lapot.

6. Kattintson **Hozzáadás** gombra.

7. A megnyíló ablakban adja meg azon alkalmazás keresési feltételeit, amelyhez hálózati szabályt szeretne létrehozni.

   Megadhatja az alkalmazás nevét vagy a gyártó nevét is. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

8. Kattintson a **Frissítés**.

   A Kaspersky Endpoint Security megkeresi az alkalmazást a felügyelt számítógépekre telepített alkalmazások összesített listáján. A Kaspersky Endpoint Security megjeleníti azon alkalmazások listáját, amelyek megfelelnek a keresési feltételeknek.

9. Válassza ki a szükséges alkalmazást.

10. A **Kijelölt alkalmazás hozzáadása a megbízhatósági csoporthoz** legördülő listában válassza ki az **Alapértelmezett csoportok** lehetőséget, majd kattintson az **OK** gombra.

    A rendszer hozzáadja az alkalmazást az alapértelmezett csoporthoz.

11. Válassza ki a megfelelő alkalmazást, majd válassza az **Alkalmazásjogok** lehetőséget az alkalmazás helyi menüjében.

    Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.

12. Válassza ki a **Hálózati szabályok** lapot.

    Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.

13. Kattintson **Hozzáadás** gombra.

    Ezután megjelennek a hálózati szabály tulajdonságai.

14. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.

15. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

    Kiválaszthat egy előre meghatározott szabálysablont a gombra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

    A hálózati szabály összes beállítása automatikusan kitöltődik.

16. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.

17. Mentse az új hálózati szabályt.

18. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.

19. Mentse el a módosításokat.

Alkalmazás hálózati szabályának létrehozása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Válassza az **Communication & Web Protection** → **Firewall** lehetőséget.

5. A **Application rights and protected resources** részen kattintson a **Application rights** hivatkozásra.

   Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.

6. Nyissa meg a **Application rights** lapot.

   Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.

7. A **Applications** részen kattintson a **Add** gombra.

   Ezután elindul a varázsló, amellyel hozzáadhat egy alkalmazást egy megbízhatósági csoporthoz.

8. Válassza ki az alkalmazás megfelelő megbízhatósági csoportját.

9. Válassza ki az **Application** típust. Lépjen a következő lépésre.

   Ha több alkalmazáshoz szeretne létrehozni hálózati szabályt, válassza ki a **Group** típust, és adjon egy nevet az alkalmazáscsoportnak.

10. Az alkalmazások megnyílt listájában kiválaszthatja azokat az alkalmazásokat, amelyekhez hálózati szabályt szeretne létrehozni.

    Használjon szűrőt. Megadhatja az alkalmazás nevét vagy a gyártó nevét is. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

11. Lépjen ki a varázslóból.

    A rendszer hozzáadja az alkalmazást a megbízhatósági csoporthoz.

12. Az ablak bal oldalán válassza ki a megfelelő alkalmazást.

13. Az ablak jobb oldalán válassza ki a **Network rules** elemet a legördülő listából.

    Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.

14. Kattintson az **Add** gombra.

    Ez megnyitja az alkalmazásszabályok tulajdonságait.

15. Adja meg manuálisan a hálózati szolgáltatás nevét a **Rule name** mezőben.

16. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).

    Kiválaszthat egy előre meghatározott szabálysablont a **Select rule template** hivatkozásra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.

    A hálózati szabály összes beállítása automatikusan kitöltődik.

17. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Log events** jelölőnégyzetet.

18. Mentse a hálózati szabályt.

    Az új hálózati szabály felkerül a listára.

19. A **Move** gombbal állíthatja be a hálózati szabály prioritását.

20. Mentse el a módosításokat.

Alkalmazás hálózati szabályának beállításai

Paraméter	Leírás
Művelet	**Engedélyezés**. **Blokkolás**.
Protokoll	Hálózati tevékenység felügyelete a kiválasztott protokollon: TCP, UDP, ICMP, ICMPv6, IGMP és GRE. Ha az ICMP vagy ICMPv6 protokollt választotta, meghatározhatja az ICMP csomag típusát és a kódját. Ha a TCP vagy az UDP protokolltípust választotta, megadhatja a helyi és a távoli számítógépek portszámait, amelyek között a kapcsolatot figyelni kell. A portszámok lehetséges értéktartománya: 0–65535. Minden mezőbe több értéket is megadhat `,` karakterekkel elválasztva, vagy megadhat egy értéktartományt `-` karakterekkel. Például: • `100,101` • `100-130` • `100,110-130`
Direction	**Bejövő**. **Bejövő / kimenő**. **Kimenő**.

Paraméter	Leírás
Távoli címek	Távoli számítógépek hálózati címei, amelyek hálózati csomagokat küldhetnek és/vagy fogadhatnak. A Tűzfal a távoli hálózati címek megadott tartományára alkalmazza a hálózati szabályt. Felveheti az összes IP-címet egy hálózati szabályba, létrehozhat egy külön IP-címlistát, meghatározhat egy IP-címtartományt, vagy kiválaszthat egy alhálózatot (Megbízható hálózatok, Helyi hálózatok, Nyilvános hálózatok). A számítógép DNS-nevét is megadhatja az IP-címe helyett. A DNS-neveket csak LAN-hálózaton lévő számítógépekhez vagy belső szolgáltatásokhoz használja. A felhőszolgáltatásokkal (például Microsoft Azure) és más internetes erőforrásokkal való interakciót a Web Control összetevőnek kell kezelnie. Ha a hálózati csomagszabályban olyan DNS-nevet adott meg, amelynek IP-címe nem határozható meg, a Kaspersky Endpoint Security figyelmeztetést jelenít meg. A Web Console-ban a hálózati csomagszabályok listája kiegészül egy oszloppal, amely tartalmazza a hiba leírását. Az adminisztrációs konzolon (MMC) a hibaleírás nem érhető el. Az ilyen csomagszabályok színnel vannak kiemelve.
Helyi címek	Számítógépek hálózati címei, amelyek hálózati csomagokat küldhetnek és/vagy fogadhatnak. A Tűzfal a hálózati szabályt a helyi hálózati címek megadott tartományára alkalmazza. Felveheti az összes IP-címet egy hálózati szabályba, létrehozhat egy külön IP-címlistát, vagy meghatározhat egy IP-címtartományt. Az alkalmazás csak akkor tárolja a helyi címeket, ha távoli címek listája meg van adva. Ez azt jelenti, hogy a **Címek a listából** érték lett kiválasztva a **Távoli címek** esetében, és legalább egy cím hozzá lett adva. Néha a helyi címet alkalmazásoknál nem lehet beszerezni. Ebben az esetben ez a paraméter figyelmen kívül marad.

Alkalmazás hálózati szabályának be- és kikapcsolása

Alkalmazás hálózati szabályának be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson az **Alkalmazások szabályai** gombra.

   Ez megnyitja az alkalmazásszabályok listát.
4. Az alkalmazások listáján kiválaszthatja azt az alkalmazást vagy alkalmazások csoportját, amely(ek)nél hálózati szabályt szeretne létrehozni vagy szerkeszteni.
5. Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Részletek és szabályok** lehetőséget.

   Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.
6. Válassza ki a **Hálózati szabályok** lapot.
7. Válassza ki az alkalmazáscsoport hálózati szabályainak listáján a kívánt hálózati szabályt.

   Megnyílik a hálózati szabály tulajdonságai ablak.
8. Állítsa be a hálózati szabály **Aktív** vagy **Inaktív** állapotát.

   Az alkalmazáscsoportoknak a Tűzfal által alapértelmezés szerint létrehozott hálózati szabályai nem kapcsolhatók ki.
9. Mentse el a módosításokat.

A Tűzfal műveletének módosítása alkalmazás hálózati szabályánál

Az alkalmazások vagy alkalmazáscsoportok alapértelmezés szerint előállított hálózati szabályaira alkalmazott Tűzfal-műveletet módosíthatja, továbbá módosíthatja az alkalmazások vagy alkalmazáscsoportok egyedi hálózati szabályaihoz tartozó Tűzfal-műveletet is.

Alkalmazás vagy alkalmazások csoportja összes hálózati szabályához tartozó Tűzfal-művelet módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson az **Alkalmazások szabályai** gombra.

   Ez megnyitja az alkalmazásszabályok listát.
4. Ha módosítani szeretné azt a Tűzfal-műveletet, amely alapértelmezés szerint létrehozott összes hálózati szabályra vonatkozik, válasszon ki egy alkalmazást vagy alkalmazáscsoportot a listán. A kézileg létrehozott hálózati szabályok változatlanul maradnak.
5. Kattintson a jobb egérgombbal a helyi menü megnyitásához, válassza ki a **Hálózati szabályok** lehetőséget, majd válassza ki a társítani kívánt műveletet:
   - **Öröklés**.
   - **Engedélyezés**.
   - **Blokkolás**.
6. Mentse el a módosításokat.

Alkalmazás vagy alkalmazások csoportja egyetlen hálózati szabályához tartozó Tűzfal-reakció módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson az **Alkalmazások szabályai** gombra.

   Ez megnyitja az alkalmazásszabályok listát.
4. A listán kiválaszthatja azt az alkalmazást vagy alkalmazások csoportját, amely(ek)nél egyetlen hálózati szabályhoz tartozó műveletet módosítani szeretne.
5. Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Részletek és szabályok** lehetőséget.

   Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.
6. Válassza ki a **Hálózati szabályok** lapot.
7. Válassza ki azt a hálózati szabályt, amelynél módosítani szeretné a Tűzfal műveletét.

8. Kattintson a **Engedély** oszlopban a jobb egérgombbal a helyi menü megjelenítéséhez, majd válassza ki a kiosztani kívánt műveletet:
   - **Öröklés**.
   - **Engedélyezés**.
   - **Tiltás**.
   - **Események naplózása**.
9. Mentse el a módosításokat.

Alkalmazás hálózati szabálya prioritásának módosítása

Egy hálózati szabály prioritását a hálózati szabályok listáján elfoglalt helye határozza meg. A Tűzfal a szabályokat abban a sorrendben hajtja végre, ahogy fentről lefelé a hálózati szabályok listáján elhelyezkednek. Az adott hálózati kapcsolatra vonatkozó egyes feldolgozott hálózati szabályoknak megfelelően a Tűzfal vagy engedélyezi, vagy blokkolja a hálózati hozzáférést a hálózati kapcsolat beállításaiban jelzett címhez és porthoz.

A kézileg létrehozott hálózati szabályok prioritása magasabb, mint az alapértelmezett hálózati szabályokéi.

Az alkalmazáscsoportok alapértelmezés szerint létrehozott hálózati szabályainak prioritását nem lehet megváltoztatni.

Hálózati szabály prioritásának módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson az **Alkalmazások szabályai** gombra.

   Ez megnyitja az alkalmazásszabályok listát.
4. Az alkalmazások listáján kiválaszthatja azt az alkalmazást vagy alkalmazások csoportját, amely(ek)nél hálózati szabály prioritását szeretné módosítani.
5. Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Részletek és szabályok** lehetőséget.

   Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.
6. Válassza ki a **Hálózati szabályok** lapot.
7. Válassza ki azt a hálózati szabályt, amelynek módosítani szeretné a prioritását.
8. Állítsa be a **Fel** / **Le** gombokkal a hálózati szabály prioritását.
9. Mentse el a módosításokat.

Hálózatfigyelő

A *Hálózatfigyelő* eszközzel valós időben tekinthetők meg a felhasználó számítógépének hálózati tevékenységével kapcsolatos információk.

A Hálózatfigyelő elindítása:

Az alkalmazás főablakában a **Figyelés** részen kattintson a **Hálózatfigyelő** csempére.

Megnyílik a Hálózatfigyelő ablak. Ebben az ablakban a számítógép hálózati tevékenysége négy lapon látható:

- A **Hálózati tevékenység** lapon az összes, a számítógépen jelenleg aktív hálózati kapcsolat látható. A kimenő és bejövő hálózati kapcsolatok egyaránt megjelennek. Ezen a lapon hálózati csomagszabályokat is létrehozhat a Tűzfal működéséhez.
- A **Nyitott portok** lapon látható a számítógép összes nyitott portja. Ezen a lapon hálózati csomagszabályokat és alkalmazásjogokat is létrehozhat a Tűzfal működéséhez.
- A **Hálózati forgalom** lapon a felhasználó számítógépe és a hálózaton lévő jelenleg kapcsolódó egyéb számítógépek közti bejövő és kimenő hálózati forgalom mennyisége látható.
- A **Blokkolt számítógépek** lapon azon távoli számítógépek IP-címei láthatók, amelyek hálózati tevékenységét a Hálózati védelem összetevő blokkolta, miután onnan érkező hálózati támadási próbálkozásokat észlelt.

Biztonsági rések kihasználásának megelőzése

A Biztonsági rések kihasználásának megelőzése összetevő észleli azon programkódokat, amik a számítógép sebezhetőségeinek segítségével kihasználják a rendszergazda jogait vagy rosszindulatú tevékenységeket hajtanak végre. Például, ezek a kihasználások puffertúlcsordulást eredményezhetnek. Ennek eléréséhez a kihasználás nagy mennyiségű adatot küld a sebezhető alkalmazásnak. Az adatok feldolgozásakor a sebezhető alkalmazás végrehajtja a rosszindulatú kódot. A támadás eredményeképp a kihasználás engedély nélkül indíthatja el a rosszindulatú program telepítését. Ha a Kaspersky Endpoint Security egy sebezhető alkalmazásból származó végrehajtható fájl futtatására irányuló olyan kísérletet észlel, amelyet nem a felhasználó végzett el, akkor blokkolja a fájl indítását vagy értesíti a felhasználót.

A Biztonsági rések kihasználásának megelőzése összetevő emellett a hálózati portokat is figyeli az olyan alkalmazások folyamatai után, amelyek veszélyt jelenthetnek a számítógép biztonságára. Az alkalmazás vírusadatbázisok segítségével szerez információt az ilyen folyamatokról.

A Biztonsági rések kihasználásának megelőzése összetevő be- és kikapcsolása

Alapértelmezés szerint a Biztonsági rések kihasználásának megelőzése be van kapcsolva és optimális módban működik. A Kaspersky Endpoint Security figyeli a sebezhető alkalmazások által futtatott végrehajtható fájlokat. Ha a Kaspersky Endpoint Security azt észleli, hogy egy sebezhető alkalmazáshoz tartozó futtatható fájlt a felhasználótól eltérő entitás indított el, akkor a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet (például blokkolni fogja a műveletet).

A Biztonsági rések kihasználásának megelőzése funkció engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Biztonsági rések kihasználásának megelőzése** lehetőséget.
4. A **Biztonsági rések kihasználásának megelőzése** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
5. Válassza ki a vonatkozó műveletet a **Sebezhetőség kihasználásának észlelésekor** blokkban:
   - **Blokkolás**. Ha a kihasználás észlelése során ez az elem van kiválasztva, a Kaspersky Endpoint Security blokkolja a kihasználás műveleteit és egy naplóbejegyzést készít, benne a kihasználás adataival.
   - **Tájékoztatás**. Ha ez az elem van kiválasztva, amikor a Kaspersky Endpoint Security észlel egy kihasználást, egy naplóbejegyzést készít, benne a kihasználás adataival, majd hozzáadja az adatokat az aktív fenyegetések listához.
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Biztonsági rések kihasználásának megelőzése funkció engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection → Behavior Analysis → Exploit Prevention** elemet.
5. A **Exploit Prevention** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Válassza ki a vonatkozó műveletet a **Action on threat detection** területen:

   - **Block**. Ha a kihasználás észlelése során ez az elem van kiválasztva, a Kaspersky Endpoint Security blokkolja a kihasználás műveleteit és egy naplóbejegyzést készít, benne a kihasználás adataival.

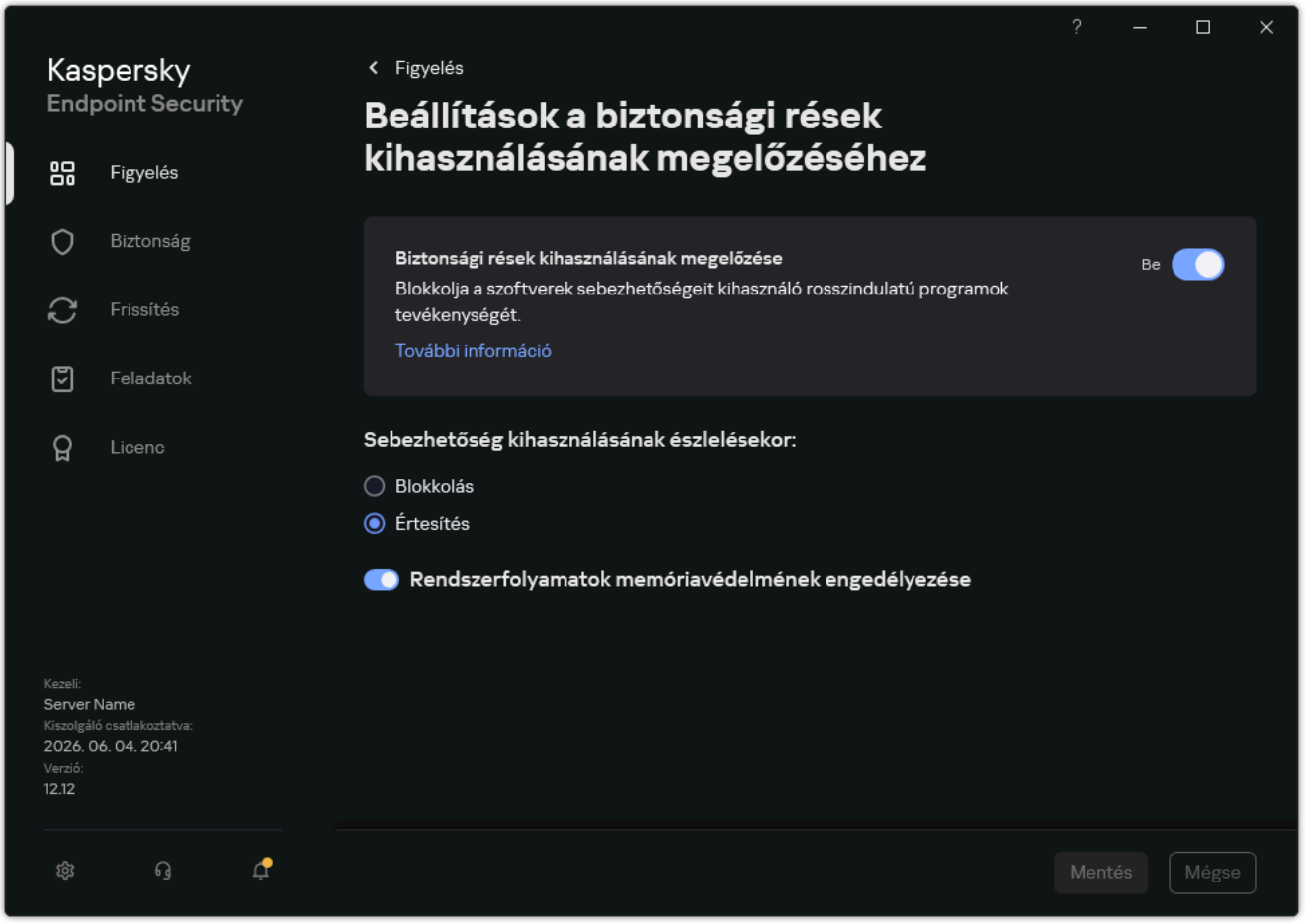
   - **Inform**. Ha ez az elem van kiválasztva, amikor a Kaspersky Endpoint Security észlel egy kihasználást, egy naplóbejegyzést készít, benne a kihasználás adataival, majd hozzáadja az adatokat az aktív fenyegetések listához.

7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Biztonsági rések kihasználásának megelőzése funkció engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem → Biztonsági rések kihasználásának megelőzése** lehetőséget.



Exploit Prevention beállításai

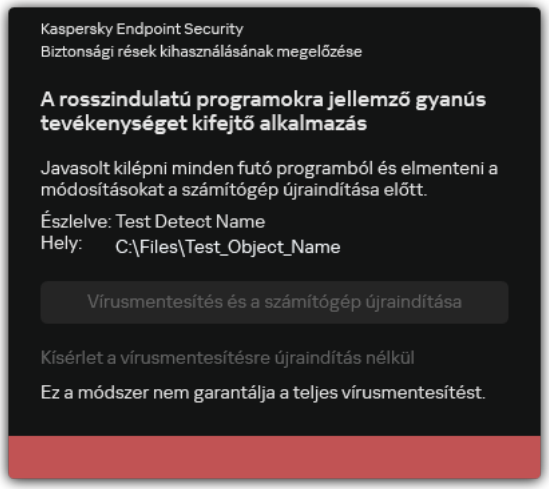
3. A **Biztonsági rések kihasználásának megelőzése** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Válassza ki a vonatkozó műveletet a **Sebezhetőség kihasználásának észlelésekor** blokkban:

   - **Blokkolás**. Ha a kihasználás észlelése során ez az elem van kiválasztva, a Kaspersky Endpoint Security blokkolja a kihasználás műveleteit és egy naplóbejegyzést készít, benne a kihasználás adataival.

   - **Tájékoztatás**. Ha ez az elem van kiválasztva, amikor a Kaspersky Endpoint Security észlel egy kihasználást, egy naplóbejegyzést készít, benne a kihasználás adataival, majd hozzáadja az adatokat az aktív fenyegetések listához.

5. Mentse el a módosításokat.



Értesítés aktív fenyegetésről

Rendszerfolyamatok memóriavédelme

Alapértelmezés szerint a rendszerfolyamatok memóriavédelme be van kapcsolva. A Kaspersky Endpoint Security blokkolja a külső folyamatokat, amelyek megpróbálnak hozzáférni a rendszerfolyamatokhoz.

A rendszerfolyamatok memóriavédelmének engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Biztonsági rések kihasználásának megelőzése** lehetőséget.

4. A **Rendszerfolyamatok memóriavédelmének engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le a funkciót.

5. Mentse el a módosításokat.

A rendszerfolyamatok memóriavédelmének engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention** elemet.

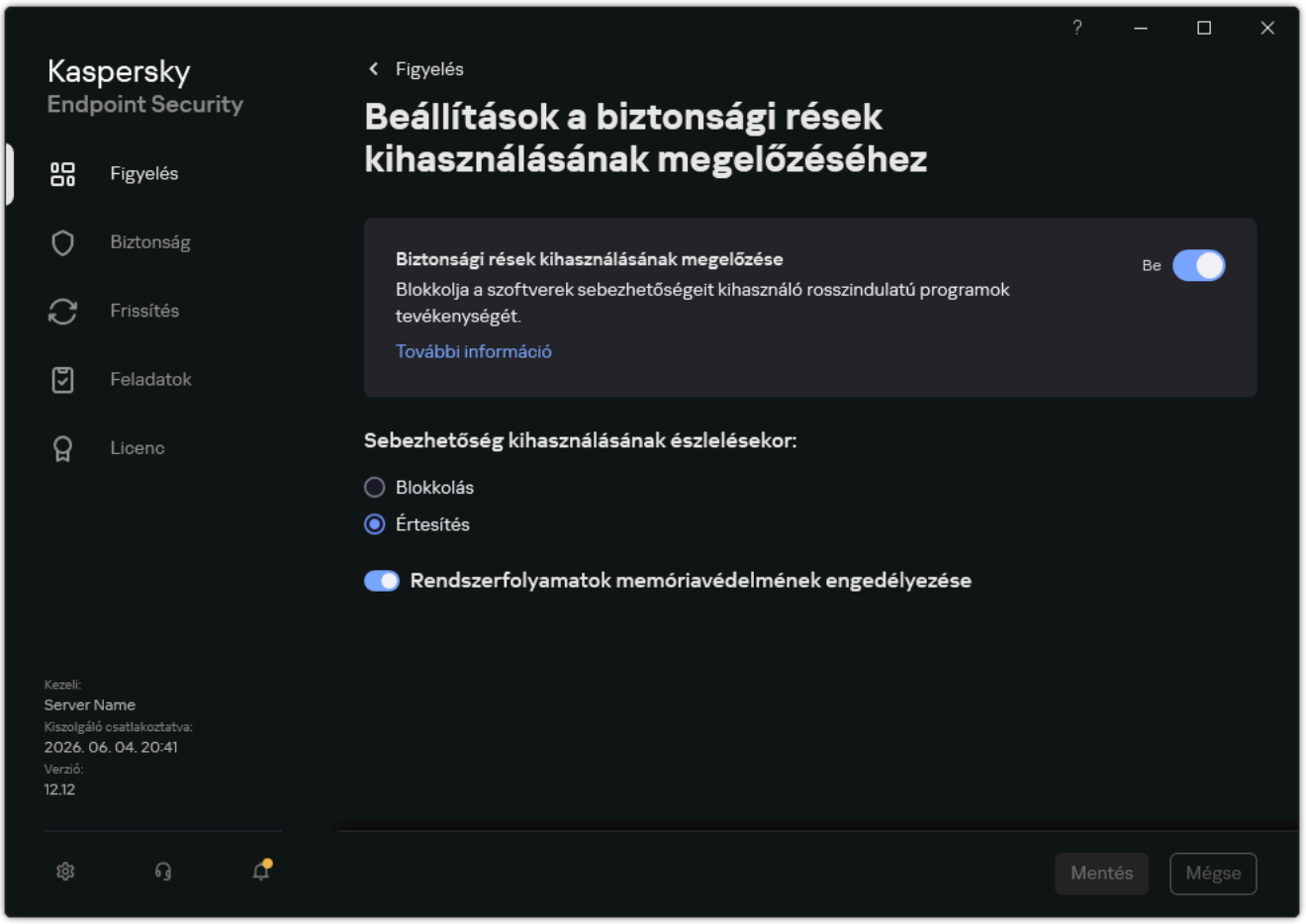
5. A(z) **System process memory protection ENABLED** kapcsolóval engedélyezheti vagy letilthatja ezt a funkciót.

6. Mentse el a módosításokat.

A rendszerfolyamatok memóriavédelmének engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Biztonsági rések kihasználásának megelőzése** lehetőséget.



Exploit Prevention beállításai

3. A **Rendszerfolyamatok memóriavédelmének engedélyezése** kapcsolóval engedélyezze vagy tiltsa le a funkciót.

4. Mentse el a módosításokat.

Viselkedésészlelés

A Viselkedésészlelés összetevő a számítógépen futó alkalmazások műveleteiről fogad adatokat, és a teljesítmény növelése érdekében átadja ezeket az információkat a többi védelmem összetevőinek. A Viselkedésészlelés összetevő Viselkedésfolyam-aláírásokat (BSS) alkalmaz az alkalmazásokhoz. Ha egy alkalmazás aktivitása megegyezik egy viselkedésfolyam-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet. A Kaspersky Endpoint Security funkciói viselkedésfolyam-aláíráson alapulnak, és a számítógép számára proaktív védelmet nyújtanak.

A Viselkedésészlelés összetevő emellett a hálózati portokat is figyeli az olyan alkalmazások folyamatait illetően, amelyek veszélyt jelenthetnek a számítógép biztonságára nézve. Az alkalmazás vírusadatbázisok segítségével szerez információt az ilyen folyamatokról.

A Viselkedésészlelés alapértelmezés szerint be van kapcsolva, és a Kaspersky által javasolt módban működik. Ha rosszindulatú tevékenységet észlel, a Kaspersky Endpoint Security törli a rosszindulatú alkalmazás futtatható fájlját.

Ha nem feltétlenül szükséges, nem javasolt kikapcsolni a Viselkedésészlelést, mivel kihat a védelmi összetevők eredményességére. A védelmi összetevők a Viselkedésészlelés által gyűjtött adatokat kikérhetik, hogy segítségükkel észleljék a fenyegetéseket.

A Viselkedéselemzés engedélyezése vagy letiltása a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Viselkedésészlelés** lehetőséget.
5. A **Viselkedéselemzés** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
6. Válassza ki a vonatkozó műveletet a **Művelet kártevő tevékenységének észlelésekor** blokkban:
   - **Törlés**. Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security törli az alkalmazás végrehajtható fájlját, miközben a fájlról biztonsági másolatot készít a Biztonsági mentésben.
   - **Blokkolás**. Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security az érintett alkalmazást bezárja.
   - **Tájékoztatás**. Ha ez az elem be van jelölve, és egy alkalmazás rosszindulatú programként viselkedik, akkor a Kaspersky Endpoint Security információkat ad hozzá az aktív fenyegetések listájához az alkalmazás rosszindulatú tevékenységeiről.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Viselkedéselemzés engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

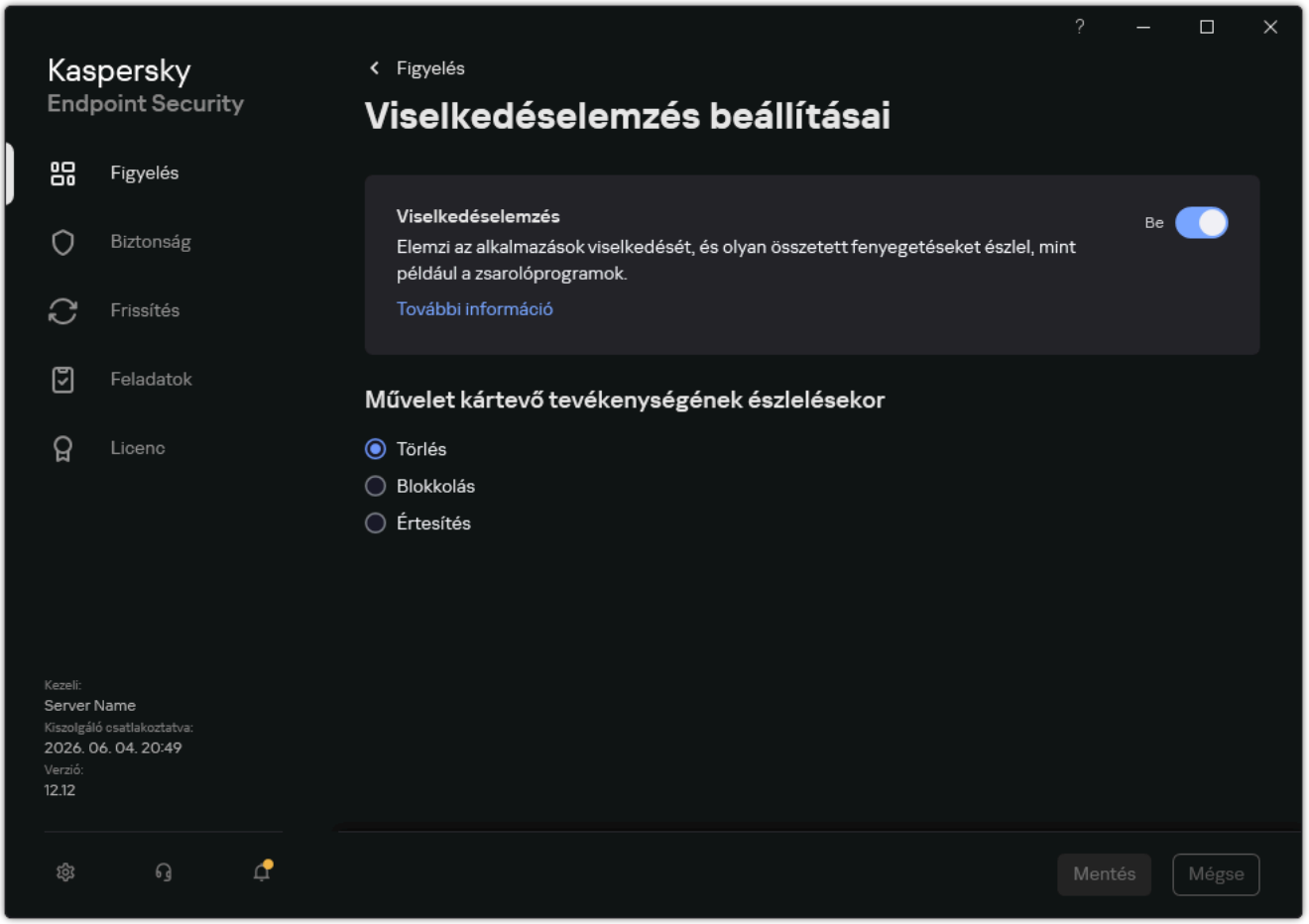
1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Behavior Detection** elemet
5. A **Behavior Detection ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Válassza ki a vonatkozó műveletet a **Action on threat detection** területen:

   - **Delete**. Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security törli az alkalmazás végrehajtható fájlját, miközben a fájlról biztonsági másolatot készít a Biztonsági mentésben.
   - **Block**. Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security az érintett alkalmazást bezárja.
   - **Inform**. Ha ez az elem be van jelölve, és egy alkalmazás rosszindulatú programként viselkedik, akkor a Kaspersky Endpoint Security információkat ad hozzá az aktív fenyegetések listájához az alkalmazás rosszindulatú tevékenységeiről.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Viselkedéselemzés engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem → Viselkedésészlelés** lehetőséget.



Viselkedésészlelés beállításai

3. A **Viselkedésészlelés** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Válassza ki a vonatkozó műveletet a **Művelet kártevő tevékenységének észlelésekor** blokkban:

   - **Törlés**. Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security törli az alkalmazás végrehajtható fájlját, miközben a fájlról biztonsági másolatot készít a Biztonsági mentésben.
   - **Blokkolás**. Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security az érintett alkalmazást bezárja.
   - **Tájékoztatás**. Ha ez az elem be van jelölve, és egy alkalmazás rosszindulatú programként viselkedik, akkor a Kaspersky Endpoint Security információkat ad hozzá az aktív fenyegetések listájához az alkalmazás rosszindulatú tevékenységeiről.

5. Mentse el a módosításokat.

Ennek eredményeképpen, ha a Viselkedésészlelés engedélyezve van, a Kaspersky Endpoint Security viselkedésfolyam-aláírásokat fog használni az alkalmazások operációs rendszerben végzett tevékenységének elemzéséhez.

Anti-Cryptor

A Kaspersky Endpoint Security 12.12 for Windows verziótól kezdve a megosztott mappák külső titkosítás elleni védelme, amely korábban a Viselkedéselemzés összetevő részét képezte, ma már külön összetevő. Ez az Anti-Cryptor.

Az összetevő csak az NTFS fájlrendszerű tárolóeszközökön tárolt, EFS-titkosítással nem rendelkező fájlokon történő műveleteket figyeli.

Az Anti-Cryptor összetevő a megosztott mappákban végzett tevékenységeket elemzi. Ha ez a tevékenység megegyezik a külső titkosításra jellemző viselkedésfolyamat-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet.

Az Anti-Cryptor összetevő működéséhez engedélyeznie kell a Viselkedéselemzés összetevőt.

Ha a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észleli, a következőt teszi:

- Blokkolja a fájlmódosítási hozzáférést a rosszindulatú tevékenységet kiváltó munkamenet számára (a fájl írásvédett lesz).
- Másolatot hoz létre a fájlokról, amik módosítva vannak.
- Hozzáad egy bejegyzést a helyi alkalmazásfelületi jelentésekhez, és információt küld az észlelt rosszindulatú tevékenységről a Kaspersky Security Center számára.
- Továbbá, ha a Kármentesítő motor összetevő be van kapcsolva, a módosított fájlok vissza lesznek állítva a biztonsági mentésből.

Megosztott mappák külső titkosítás elleni védelmének be- és kikapcsolása

Alapértelmezés szerint a megosztott mappák külső titkosítás elleni védelme engedélyezve van, és a Kaspersky szakértői által javasolt módon működik. A funkció beállításához szükség esetén létrehozhat egy védelmi hatókört, és konfigurálhat kizárásokat. Alapértelmezés szerint az alkalmazás automatikusan azonosítja a megosztott mappákat, és minden mappában figyeli a fájltevékenységet. Ha a megosztott mappákban lévő fájlok külső titkosítására irányuló kísérletet észlel, a Kaspersky Endpoint Security egy órára blokkolja (alapértelmezés szerint) a távoli felhasználó munkamenetét.

A Kaspersky Endpoint Security telepítése után a megosztott mappák külső titkosítás elleni védelme korlátozva lesz a számítógép újraindításáig.

A megosztott mappák külső titkosítás elleni védelmének engedélyezése vagy letiltása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.
4. Az **Anti-Cryptor** jelölőnégyzet segítségével engedélyezheti vagy letilthatja a külső titkosításra jellemző tevékenységek észlelését.
5. Válassza ki az alkalmazás által végrehajtandó műveletet, ha az megosztott mappákban lévő fájlok módosítására irányuló kísérletet észlel:
   - **Kapcsolódás blokkolása N percig**. Ha ez az opció be van jelölve, a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észlelve blokkolja a fájlmódosításhoz való hozzáférést a rosszindulatú tevékenységet kezdeményező munkamenet számára, és biztonsági másolatokat készít a módosított fájlokról.

     Ha a Kármentesítő motor összetevő engedélyezve van, és a **Kapcsolat blokkolása N percig** lehetőség ki van választva, a módosított fájlok a biztonsági mentésekből kerülnek visszaállításra.

   - **Tájékoztatás**. Ha ez a beállítás be van jelölve, a megosztott mappákban lévő fájlok módosítási kísérletének észlelésekor a Kaspersky Endpoint Security a módosítási kísérletről szóló információkat hozzáadja az aktív fenyegetések listájához, bejegyzést add hozzá a helyi alkalmazásfelület jelentéseibe, és az észlelt rosszindulatú tevékenységről információt küld a Kaspersky Security Center számára.
6. Ha szükséges, szerkessze a védelmi hatókört, és határozza meg a kizárásokat.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A megosztott mappák külső titkosítás elleni védelmének engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor** elemet.
5. A(z) **Anti-Cryptor ENABLED** jelölőnégyzet segítségével engedélyezheti vagy letilthatja a külső titkosításra jellemző tevékenységek észlelését.

6. Válassza ki az alkalmazás által végrehajtandó műveletet, ha az megosztott mappákban lévő fájlok módosítására irányuló kísérletet észlel:

   - **Block connection for (min) N percig**. Ha ez az opció be van jelölve, a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észlelve blokkolja a fájlmódosításhoz való hozzáférést a rosszindulatú tevékenységet kezdeményező munkamenet számára, és biztonsági másolatokat készít a módosított fájlokról.

     Ha a Kármentesítő motor összetevő engedélyezve van, és a(z) **Block connection for (min) N percig** lehetőség ki van választva, a módosított fájlok a biztonsági mentésekből kerülnek visszaállításra.

   - **Inform**. Ha ez a beállítás be van jelölve, a megosztott mappákban lévő fájlok módosítási kísérletének észlelésekor a Kaspersky Endpoint Security a módosítási kísérletről szóló információkat hozzáadja az aktív fenyegetések listájához, bejegyzést add hozzá a helyi alkalmazásfelület jelentéseibe, és az észlelt rosszindulatú tevékenységről információt küld a Kaspersky Security Center számára.

7. Ha szükséges, szerkessze a védelmi hatókört, és határozza meg a kizárásokat.

8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A megosztott mappák külső titkosítás elleni védelmének engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem → Anti-Cryptor** lehetőséget.

3. **A megosztott mappák védelme a külső titkosítás ellen** jelölőnégyzet segítségével engedélyezheti vagy letilthatja a külső titkosításra jellemző tevékenységek észlelését.

4. **A megosztott mappák védelme a külső titkosítás ellen** jelölőnégyzet segítségével engedélyezheti vagy letilthatja a külső titkosításra jellemző tevékenységek észlelését.

5. Válassza ki az alkalmazás által végrehajtandó műveletet, ha az megosztott mappákban lévő fájlok módosítására irányuló kísérletet észlel:

   - **Kapcsolódás blokkolása (perc) N percig**. Ha ez az opció be van jelölve, a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észlelve blokkolja a fájlmódosításhoz való hozzáférést a rosszindulatú tevékenységet kezdeményező munkamenet számára, és biztonsági másolatokat készít a módosított fájlokról.

     Ha a Kármentesítő motor összetevő engedélyezve van, és a **Kapcsolat blokkolása (perc) N percig** lehetőség ki van választva, a módosított fájlok a biztonsági mentésekből kerülnek visszaállításra.

   - **Tájékoztatás**. Ha ez a beállítás be van jelölve, a megosztott mappákban lévő fájlok módosítási kísérletének észlelésekor a Kaspersky Endpoint Security a módosítási kísérletről szóló információkat hozzáadja az aktív fenyegetések listájához, bejegyzést add hozzá a helyi alkalmazásfelület jelentéseibe, és az észlelt rosszindulatú tevékenységről információt küld a Kaspersky Security Center számára.

6. Ha szükséges, szerkessze a védelmi hatókört, és határozza meg a kizárásokat.

7. Mentse el a módosításokat.

Nem megbízható számítógépek blokkolási időszakának konfigurálása

A *nem megbízható számítógép* egy olyan távoli számítógép, amely rosszindulatú tevékenységet folytat vagy adattitkosítást végez. Alapértelmezés szerint a Kaspersky Endpoint Security egy órára blokkolja a távoli felhasználó munkamenetét. A blokkolási időszak lejártakor a Kaspersky Endpoint Security eltávolítja a számítógépet a tiltólistáról, és visszaállítja a hozzáférést a megosztott mappához.

Nem megbízható számítógépek blokkolási időszakának konfigurálása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.
4. A **Művelet fenyegetés észlelésekor** területen válassza a **Kapcsolódás blokkolása N percig** lehetőséget.
5. Konfigurálhatja a rosszindulatú tevékenységet folytató vagy adattitkosítást végző, nem megbízható számítógépek blokkolási idejét.
6. Mentse el a módosításokat.

Nem megbízható számítógépek blokkolási időszakának konfigurálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor** elemet.
5. A(z) **Action on threat detection**, területen konfigurálhatja a rosszindulatú tevékenységet folytató vagy adattitkosítást végző, nem megbízható számítógépek blokkolási idejét.
6. Mentse el a módosításokat.

Nem megbízható számítógépek blokkolási időszakának konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.
3. A **Művelet fenyegetés észlelésekor** területen válassza a **Kapcsolódás blokkolása ennyi percig (perc):** lehetőséget.

4. Konfigurálhatja a rosszindulatú tevékenységet folytató vagy adattitkosítást végző, nem megbízható számítógépek blokkolási idejét.

5. Mentse el a módosításokat.

Ennek eredményeként a távoli számítógép zárolásra kerül. A távoli számítógép zárolásának feloldásához indítsa újra a Kaspersky Endpoint Security alkalmazást.

A védelem hatókörének szerkesztése

A *védelem hatóköre* azon megosztott mappák elérési útvonalainak listája, amelyekben a Kaspersky Endpoint Security figyeli a fájltevékenységet. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. Alapértelmezés szerint az alkalmazás automatikusan azonosítja a megosztott mappákat, és minden mappában figyeli a fájltevékenységet.

Egy mappa kizárása a védelem hatóköréből csökkentheti az álpozitív találatok számát, ha a cég adattitkosítást használ a megosztott mappák segítségével történő fájlcsere során. A Viselkedelemzés például vakriasztást okozhat, ha a felhasználó ENC kiterjesztésű fájlokkal dolgozik egy megosztott mappában. Ez a tevékenység megfelel a külső titkosításra jellemző viselkedési mintának. Ha az adatok védelme céljából titkosított fájlokat tárol egy megosztott mappában, vegye fel a mappát a kizárások közé.

> Továbbá kizárhatja azokat a számítógépeket, amelyekről a külső titkosítási kísérleteket nem szabad kezelni.

Védelem hatókörének szerkesztése a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.

4. A **Védelem hatóköre** területen válassza a **Csak megadott megosztott mappák** lehetőséget.

5. A mappák listájában kattintson a **Hozzáadás** elemre.

6. A megnyíló ablakban adja meg annak a megosztott mappának az elérési útját, amelyet be akar vonni a védelmi hatókörbe (például `C:\Share`).

   > Ha megosztott mappát szeretne hozzáadni a védelmi hatókörhöz, használjon helyi elérési utat.

7. Kattintson az **OK** gombra.

8. Ha szükséges, adja meg a védelmi hatókör kizárásait:

   a. A **Kizárások a vizsgálatból** területen kattintson a **Maszk alapján** gombra.

   b. Az ablakban kattintson a **Hozzáadás** gombra.

c. A megjelenő ablakban adja meg a fájlkiterjesztést `*.<file extension>` formátumban, illetve a mappa elérési útvonalát. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

Az alkalmazás nem támogat egyes kizárási fájlkiterjesztéseket. Így kizárást `*.docx` vagy `**\Folder\**` feltétellel is megadhat.

Egy objektumot anélkül is kizárhat a vizsgálatokból, hogy eltávolítaná azt a védelem hatókörébe tartozó objektumok listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

9. Mentse el a módosításokat.

Védelem hatókörének szerkesztése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor** elemet.
5. A **Protection scope** területen válassza az **Only specified shared folders** opciót.
6. A mappalistában kattintson a **Add** elemre.
7. A megnyíló ablakban adja meg annak a megosztott mappának az elérési útját, amelyet be akar vonni a védelmi hatókörbe (például `C:\Share`).

   Ha megosztott mappát szeretne hozzáadni a védelmi hatókörhöz, használjon helyi elérési utat.
8. Kattintson az **OK** gombra.
9. Ha szükséges, adja meg a védelmi hatókör kizárásait:

   a. Az ablak felső részében kattintson a **Scan exclusions** hivatkozásra.

   b. Az ablakban kattintson a **Add** gombra.

   c. A megjelenő ablakban adja meg a fájlkiterjesztést `*.<file extension>` formátumban, illetve a mappa elérési útvonalát. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

   Az alkalmazás nem támogat egyes kizárási fájlkiterjesztéseket. Így kizárást `*.docx` vagy `**\Folder\**` feltétellel is megadhat.

   Egy objektumot anélkül is kizárhat a vizsgálatokból, hogy eltávolítaná azt a védelem hatókörébe tartozó objektumok listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.
10. Mentse el a módosításokat.

Védelem hatókörének szerkesztése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.

3. A **Védelem hatóköre** területen válassza a **Csak megadott megosztott mappák** lehetőséget.

4. A mappák listájában kattintson a **Hozzáadás** elemre.

5. A megnyíló ablakban adja meg annak a megosztott mappának az elérési útját, amelyet be akar vonni a védelmi hatókörbe (például `C:\Share`).

   > Ha megosztott mappát szeretne hozzáadni a védelmi hatókörhöz, használjon helyi elérési utat.

6. Kattintson az **OK** gombra.

7. Ha szükséges, adja meg a védelmi hatókör kizárásait:

   a. Az ablak felső részében kattintson a **Kizárások maszk szerint** hivatkozásra.

   b. Az ablakban kattintson a **Hozzáadás** gombra.

   c. A megjelenő ablakban adja meg a fájlkiterjesztést `*.<file extension>` formátumban, illetve a mappa elérési útvonalát. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

      Az alkalmazás nem támogat egyes kizárási fájlkiterjesztéseket. Így kizárást `*.docx` vagy `**\Folder\**` feltétellel is megadhat.

   Egy objektumot anélkül is kizárhat a vizsgálatokból, hogy eltávolítaná azt a védelem hatókörébe tartozó objektumok listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

8. Mentse el a módosításokat.

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.

3. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

4. Kattintson **Hozzáadás** gombra.

5. Kattintson a **Tallózás** gombra, és válassza ki a megosztott mappát.

Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `?:\Users\*\Folder\` maszkot.

6. A **Védelmi összetevők** részen válassza ki a **Viselkedésészlelés** összetevőt.

7. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

8. Válassza ki az **Aktív** állapotot a kizáráshoz.

   Bármikor használhatja a kapcsolót egy kizárás megszüntetéséhez.

9. Mentse el a módosításokat.

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Trusted Zone** szakaszt.

5. Az ablakban kattintson a **Malware Scan exclusions** hivatkozásra.

6. Válassza a **Merge values when inheriting** jelölőnégyzetet, ha egy összesített listát szeretne létrehozni a vállalat összes számítógépén lévő kizárásokról. A szülő és gyermek házirendjeiben lévő kizárási listák egyesítve lesznek. A lista egyesítve lesz, ha öröklésкor az értékek egyesítése öröklésкor engedélyezve van. A szülő házirendjében lévő kizárások a gyermek házirendjében csak olvasható nézetben jelennek meg. A szülő házirendjében lévő kizárásokat nem lehet módosítani vagy törölni.

7. Jelölje be a **Allow use of local exclusions** jelölőnégyzetet, ha szeretné engedélyezni a felhasználó számára a kizárások helyi listájának létrehozását. Így a felhasználó létrehozhatja a kizárások saját listáját, a házirendben létrehozott kizárások általános listája mellett. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.

   Ha a jelölőnégyzet nincs bejelölve, a felhasználó a kizárásoknak csak a házirendben létrehozott általános listájához férhet hozzá. Ezenkívül, ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security elrejti a vizsgálati kizárások összevont listáját az alkalmazás felhasználói felületén.

8. Kattintson a **Add** gombra, és válasszon ki egy műveletet:

   - **Category**. A vizsgálati kizárásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy vizsgálati kizárást a kategóriához.
   - **New exclusion**. A Kaspersky Endpoint Security egy új vizsgálati kizárást ad hozzá a lista gyökeréhez.
   - **Select exclusion from list**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált vizsgálati kizárásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált vizsgálati kizárások is hozzá lettek adva. Előre definiált vizsgálati kizárásokat kell kiválasztania a védett kiszolgáló céljától függően.

9. Válassza ki, hogyan kívánja hozzáadni a **Path to the file or folder** kizárást.

10. Adja meg a megosztott mappa elérési útját.

    Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor:

    - A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
    - Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
    - A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

    Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `C:\Users\*\Folder\` maszkot.

11. A(z) **Apply exclusion to** területen válassza ki a **Behavior Detection** összetevőt.

12. Szükség esetén adjon meg rövid megjegyzést a **Comment** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

13. Válassza ki a **Add to exclusions** állapotot a kizáráshoz.

    Bármikor használhatja a kapcsolót egy kizárás megszüntetéséhez.

14. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.

4. A **Kizárások a vizsgálatból és megbízható alkalmazások → Kizárások a vizsgálatból** részen kattintson a **Beállítások** gombra.

   Ez megnyitja a kizárások listáját tartalmazó ablakot.

5. Válassza az **Merge values when inheriting** jelölőnégyzetet, ha egy összesített listát szeretne létrehozni a vállalat összes számítógépén lévő kizárásokról. A szülő és gyermek házirendjeiben lévő kizárási listák egyesítve lesznek. A lista egyesítve lesz, ha örökléskor az értékek egyesítése örökléskor engedélyezve van. A szülő házirendjében lévő kizárások a gyermek házirendjében csak olvasható nézetben jelennek meg. A szülő házirendjében lévő kizárásokat nem lehet módosítani vagy törölni.

6. Jelölje be a **Allow use of local exclusions** jelölőnégyzetet, ha szeretné engedélyezni a felhasználó számára a kizárások helyi listájának létrehozását. Így a felhasználó létrehozhatja a kizárások saját listáját, a házirendben létrehozott kizárások általános listája mellett. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.

   Ha a jelölőnégyzet nincs bejelölve, a felhasználó a kizárásoknak csak a házirendben létrehozott általános listájához férhet hozzá. Ezenkívül, ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security elrejti a vizsgálati kizárások összevont listáját az alkalmazás felhasználói felületén.

7. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

   - **Kategória**. A vizsgálati kizárásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy vizsgálati kizárást a kategóriához.

   - **Új kizárás**. A Kaspersky Endpoint Security egy új vizsgálati kizárást ad hozzá a lista gyökeréhez.

   - **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált vizsgálati kizárásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált vizsgálati kizárások is hozzá lettek adva. Előre definiált vizsgálati kizárásokat kell kiválasztania a védett kiszolgáló céljától függően.

8. Kattintson **Hozzáadás** gombra.

9. A **Properties** részben jelölje be a **File or folder** jelölőnégyzetet.

10. Kattintson a **Válasszon fájlt vagy mappát** hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben a **Fájl vagy mappa neve** ablak megnyitásához.

11. Kattintson a **Tallózás** gombra, és válassza ki a megosztott mappát.

Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `?:\Users\*\Folder\` maszkot.

12. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

13. Kattintson a hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben a **Védelem összetevők** ablak megnyitásához.

14. Jelölje be a **Viselkedésészlelés** összetevő melletti jelölőnégyzetet.

15. Mentse el a módosításokat.

Megbízható számítógépek hozzáadása külső adattitkosításhoz

Ha a vállalat külső adattitkosítást használ a fájlcsere-munkafolyamatban, létre kell hoznia a megbízható számítógépek listáját. A Kaspersky Endpoint Security nem figyeli a megbízható számítógépek adattitkosítását.

A megosztott mappák külső titkosítás elleni védelme alóli címkizáráshoz be kell kapcsolni a Bejelentkezés hitelesítése szolgáltatást. Alapértelmezésben a Bejelentkezés felülvizsgálata szolgáltatás le van tiltva. (A Bejelentkezés felülvizsgálata szolgáltatás engedélyezéséről a Microsoft webhelyén talál részletes információkat.)

A megosztott mappák külső titkosítás elleni védelme alóli címkizárás funkció nem működik olyan távoli számítógépen, mely a Kaspersky Endpoint Security elindítása előtt lett bekapcsolva. A megosztott mappák külső titkosítás elleni védelme alóli címkizárás funkció működése érdekében a Kaspersky Endpoint Security elindítása után újraindíthatja a távoli számítógépet.

A megbízható számítógépek listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Megbízható számítógép hozzáadása külső adattitkosításhoz a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.
4. A **Kizárások a vizsgálatból** részen kattintson a **Név vagy IP-cím alapján** gombra.
5. A megnyíló ablakban kattintson a **Név vagy IP-cím alapján** gombra.
6. Adja meg azon IP-címeket, IP-címtartományt vagy számítógépek nevét, amelyekről a külső titkosítási kísérleteket nem szabad kezelni.

   Példák:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

7. Mentse el a módosításokat.

Megbízható számítógép hozzáadása külső adattitkosításhoz a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor** elemet.
5. Az ablak felső részében kattintson a **Exclusions by name or IP address** hivatkozásra.
6. Az ablakban kattintson a **Add** gombra.
7. Adja meg azon IP-címeket, IP-címtartományt vagy számítógépek nevét, amelyekről a külső titkosítási kísérleteket nem szabad kezelni.
   Példák:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Mentse el a módosításokat.

Megbízható számítógép hozzáadása külső adattitkosításhoz az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.
3. Az ablak felső részén kattintson a **Kizárások név vagy IP-cím alapján** hivatkozásra.
4. Az ablakban kattintson a **Hozzáadás** gombra.
5. Adja meg azon IP-címeket, IP-címtartományt vagy számítógépek nevét, amelyekről a külső titkosítási kísérleteket nem szabad kezelni.
   Példák:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. Mentse el a módosításokat.

A megosztott mappák külső titkosítással szembeni védelméből származó kizárások listájának exportálása és importálása

A kizárások listáját exportálhatja egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú cím hozzáadásával. Használhatja az exportálás/importálás funkciót a kizárások biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A kizárások listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza a **Fenyegetések elleni fejlett védelem** → **Anti-Cryptor** lehetőséget.
4. A **Kizárások a vizsgálatból** részen kattintson a **Név vagy IP-cím alapján** gombra.
5. A szabályok listájának exportálása:
   a. Jelölje ki az exportálni kívánt kizárásokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
      Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.
   b. Kattintson a → **Hozzáadás** gombra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba.
6. A kizárások listájának importálása:
   a. Kattintson a → **Hozzáadás** gombra.
   b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kizárások listáját.
   c. Nyissa meg a fájlt.
      Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
7. Mentse el a módosításokat.

A kizárások listájának exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor** elemet.
5. Kattintson a **Exclusions by name or IP address** hivatkozásra.
6. A szabályok listájának exportálása:

   a. Jelölje ki az exportálni kívánt kizárásokat.

   b. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a kizárások listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.
7. A kizárások listájának importálása:

   a. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a kizárások listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.
8. Mentse el a módosításokat.

Kármentesítő motor

A Kármentesítő motor összetevő révén a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben végrehajtott műveleteket visszagörgetni.

A rosszindulatú programok operációs rendszerben végzett tevékenységeinek visszagörgetésekor a Kaspersky Endpoint Security a rosszindulatú programok alábbi típusú tevékenységeit kezeli:

- **Fájl tevékenysége**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Törli a rosszindulatú program által létrehozott végrehajtható fájlokat (minden médián, kivéve a hálózati meghajtókon).
  - Törli az olyan végrehajtható fájlokat, amiket a rosszindulatú programokkal fertőzött fájlok hoztak létre.
  - Visszaállítja a rosszindulatú program által módosított vagy törölt fájlokat.

  A fájlvisszaállítás funkciónak számos korlátozása van.

- **Beállításjegyzék-tevékenység**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Törli a rosszindulatú program által létrehozott beállításkulcsokat.
  - Nem állítja vissza a rosszindulatú program által módosított vagy törölt beállításkulcsokat.

- **Rendszertevékenység**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Megszűnteti a rosszindulatú program által kezdeményezett folyamatokat.
  - Megszakítja azokat a folyamatokat, amelyekbe a rosszindulatú alkalmazás bejutott.
  - Nem folytatja a rosszindulatú program által megállított folyamatokat.

- **Hálózati tevékenység**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Blokkolja a rosszindulatú program hálózati tevékenységét.
  - Blokkolja a rosszindulatú programok által fertőzött folyamatok hálózati tevékenységét.

A rosszindulatú tevékenységek utáni visszagörgetés elindítható a Fájl védelem vagy Viselkedésészlelés összetevővel, illetve a Kártevő vizsgálata során.

A rosszindulatú programok műveleteinek visszagörgetése szigorúan meghatározott adatkészletet érint. A visszagörgetés semmilyen negatív következménnyel nem jár az operációs rendszerre és a számítógép adatainak integritására nézve.

A Kármentesítő motor rendszer összetevő engedélyezése vagy letiltása az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza ki a **Fenyegetések elleni fejlett védelem → Kármentesítő motor** lehetőséget.
4. A **Kármentesítő motor** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
5. Mentse el a módosításokat.

A Kármentesítő motor összetevő engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Host Threat Protection → Behavior Analysis → Remediation Engine** elemet.

5. A **Remediation Engine ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Mentse el a módosításokat.

A Kármentesítő motor összetevő engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem → Kármentesítő motor** lehetőséget.

3. A **Kármentesítő motor** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Mentse el a módosításokat.

Ennek eredményeképpen, ha a Kármentesítő motor engedélyezve van, a Kaspersky Endpoint Security visszagörgeti a rosszindulatú alkalmazások által az operációs rendszerben végrehajtott műveleteket.

Kaspersky Security Network

A számítógép védelmének fokozása érdekében a Kaspersky Endpoint Security a felhasználóktól a világ minden tájáról kapott adatokat használja. A Kaspersky Security Network feladata ezen adatok fogadása.

A KSN-funkciók nem lesznek elérhetők a szoftverben az Egyesült Államok területén.

A *Kaspersky Security Network (KSN)* felhőalapú szolgáltatások egy olyan infrastruktúrája, amely hozzáférést nyújt a Kaspersky online tudásbázisához, ahonnan információkat kaphat fájlok, webes erőforrások és szoftverek megbízhatóságáról. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban reagál az új típusú fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken. Ha tagja a Kaspersky Security Networknek, a KSN szolgáltatások a Kaspersky Endpoint Security számára információkat nyújtanak a vizsgált webcímek megbízhatóságáról, valamint a vizsgált fájlok kategóriájáról és megbízhatóságáról. A KSN-hez való hozzáférés konfigurálásával kapcsolatos további részletekért lásd a Kaspersky Security Center súgóját.

A Kaspersky Security Network használata önkéntes. Az alkalmazás a kezdeti beállítás során kéri a felhasználót, hogy használja a KSN szolgáltatást. A felhasználók bármikor megszüntethetik részvételüket a KSN-ben.

A KSN-ben való részvétel során keletkező statisztikai adatok Kaspersky részére történő elküldésével és az ilyen adatok tárolásával és megsemmisítésével kapcsolatos részletes információk a Kaspersky Security Network nyilatkozatában és a Kaspersky webhelyén találhatók. A Kaspersky Security Network nyilatkozatának szövegét tartalmazó ksn_<nyelv azonosítója>.txt fájl megtalálható az alkalmazás terjesztőkészletében.

A Kaspersky megbízhatósági adatbázisainak infrastruktúrája

A Kaspersky Endpoint Security a következő infrastrukturális megoldásokat támogatja a Kaspersky megbízhatósági adatbázisaival való együttműködéshez:

- A *Kaspersky Security Network (KSN)* a legtöbb Kaspersky-alkalmazás által használt megoldás. A KSN-résztvevők információkat kapnak a Kaspersky-től, és elküldik a Kaspersky számára a felhasználó számítógépén észlelt objektumokat, hogy a Kaspersky is elemezze azokat, és belevegye a megbízhatósági és statisztikai adatbázisába.

- A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről. A KPSN vállalati felhasználóknak ajánlott, akik a következő okokból nem tudnak részt venni a Kaspersky Security Networkben:

  - A helyi munkaállomások nem csatlakoznak az internethez.

  - Az adatok vállalati LAN-hálózaton vagy az országon kívüli továbbítását tiltja a törvény vagy a vállalat biztonsági rendszabálya.

A Kaspersky Security Network használatának engedélyezése és letiltása

A Kaspersky Endpoint Security alapértelmezetten a Kiterjesztett KSN módot használja. A *Kiterjesztett KSN mód* egy olyan mód, melyben a Kaspersky Endpoint Security [további adatokat] küld a Kaspersky számára.

A KSN használat engedélyezése vagy letiltása a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A szabályzat ablakában válassza a **Fenyegetések elleni fejlett védelem → Kaspersky Security Network** lehetőséget.

4. A **Kaspersky Security Network** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

   Ha engedélyezte a KSN használatát, a Kaspersky Endpoint Security megjeleníti a Kaspersky Security Network Nyilatkozatot. Olvassa el és fogadja el a Kaspersky Security Network (KSN) használati feltételeit, ha egyetért azokkal.

5. Ha szükséges, törölje a **Kiterjesztett KSN mód engedélyezése** jelölőnégyzetet. Alapértelmezés szerint a kibővített KSN mód engedélyezve van.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A KSN használat engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Kaspersky Security Network** elemet.
5. A **Use of Kaspersky Security Network (KSN) ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

   Ha engedélyezte a KSN használatát, a Kaspersky Endpoint Security megjeleníti a Kaspersky Security Network Nyilatkozatot. Olvassa el és fogadja el a Kaspersky Security Network (KSN) használati feltételeit, ha egyetért azokkal.
6. Ha szükséges, kapcsolja ki a(z) **Use extended KSN mode** kapcsolót. Alapértelmezés szerint a kibővített KSN mód engedélyezve van.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A KSN használat engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Kaspersky Security Network** lehetőséget.
3. A **Kaspersky Security Network** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

   Ha engedélyezte a KSN használatát, a Kaspersky Endpoint Security megjeleníti a Kaspersky Security Network Nyilatkozatot. Olvassa el és fogadja el a Kaspersky Security Network (KSN) használati feltételeit, ha egyetért azokkal.
4. Szükség esetén kapcsolja át a **Kiterjesztett KSN mód engedélyezése** kapcsolót. Alapértelmezés szerint a kibővített KSN mód engedélyezve van.
5. Mentse el a módosításokat.

Ennek eredményeként, ha a KSN használata engedélyezett, a Kaspersky Endpoint Security a Kaspersky Security Networktől kapott információkat használja a fájlok, webes erőforrások és alkalmazások megbízhatóságával kapcsolatban.

A Kaspersky Private Security Network korlátozásai

A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről. A Privát Kaspersky Security Network lehetővé teszi, hogy saját helyi megbízhatósági adatbázissal ellenőrizze az objektumok (fájlok vagy webcímek) megbízhatóságát. A helyi megbízhatósági adatbázisba felvett objektum megbízhatóságának nagyobb prioritása van, mint a KSN/KPSN-hez hozzáadott objektumnak. Képzelje el például, hogy a Kaspersky Endpoint Security egy számítógépet vizsgál, és lekéri egy fájl megbízhatóságát a KSN/KPSN-ben. Ha a fájl *Nem megbízható* a helyi megbízhatósági adatbázisban, de *Megbízható* hírnév van a KSN/KPSN-ben, a Kaspersky Endpoint Security a fájlt *Nem megbízhatóként* fogja felismerni, és végrehajtja az észlelt fenyegetésekre meghatározott műveletet.

Bizonyos esetekben azonban előfordulhat, hogy a Kaspersky Endpoint Security nem kéri le egy objektum megbízhatóságát a KSN/KPSN-ben. Ebben az esetben a Kaspersky Endpoint Security nem kap adatokat a KPSN helyi megbízhatósági adatbázisából. A Kaspersky Endpoint Security egy objektum megbízhatóságát a következő okok miatt nem kéri le a KSN/KPSN-ben:

- A Kaspersky alkalmazások offline megbízhatósági adatbázisokat használnak. Az offline megbízhatósági adatbázisokat úgy tervezték, hogy a Kaspersky alkalmazások működése során optimalizálják az erőforrásokat, és megvédjék a számítógép kritikus fontosságú objektumait. Az offline megbízhatósági adatbázisokat a Kaspersky szakértői hozzák létre a Kaspersky Security Network adatai alapján. A Kaspersky alkalmazások az adott alkalmazás vírusadatbázisával frissítik az offline megbízhatósági adatbázisokat. Ha az offline megbízhatósági adatbázisok információkat tartalmaznak egy vizsgált objektumról, az alkalmazás nem kéri az objektum megbízhatóságát a KSN/KPSN-től.

- A kizárások a vizsgálatból (megbízható zóna) az alkalmazás beállításaiban vannak konfigurálva. Ebben az esetben az alkalmazás nem veszi figyelembe az objektum megbízhatóságát a helyi megbízhatósági adatbázisban.

- Az alkalmazás vizsgálatoptimalizálási technológiákat használ, mint például az iSwift vagy az iChecker, vagy gyorsítótárazza a megbízhatósági kéréseket a KSN/KPSN számára. Ebben az esetben előfordulhat, hogy az alkalmazás nem kéri le a korábban megvizsgált objektumok megbízhatóságát.

- A terhelés optimalizálása érdekében az alkalmazás bizonyos formátumú és méretű fájlokat vizsgál. A releváns formátumok és méretkorlátok listáját a Kaspersky szakértői határozzák meg. Ez a lista az alkalmazás vírusadatbázisaival frissül. Az alkalmazás felületén konfigurálhatja a vizsgálat optimalizálásának beállításait is, például a Fájl védelem összetevőhöz.

- A Kaspersky Endpoint Security Light Agent üzemmódban egy KSN proxykiszolgálón keresztül kommunikál a KSN-kiszolgálókkal. A KSN-nel való közvetlen kommunikáció nem támogatott.

Felhő mód be- és kikapcsolása a védelmi összetevőknél

A *Felhő mód* arra az alkalmazásműveleti módra vonatkozik, amiben a Kaspersky Endpoint Security az antivírus adatbázisok egyszerű verzióját használja. A Kaspersky Security Network támogatja az alkalmazásműveletet, ha az antivírus adatbázisok egyszerű verziója van használva. Az antivírus adatbázisok egyszerű verziójával körülbelül fele annyi RAM-ot használ a számítógépen, amit az átlagos adatbázisokkal használna. Ha nem vesz részt a Kaspersky Security Networkben, vagy ha a felhő mód ki van kapcsolva, a Kaspersky Endpoint Security letölti az antivírus adatbázisok teljes verzióját a Kaspersky szerverekről.

A Kaspersky Private Security Network használata közben a felhő mód funkció, a Kaspersky Private Security Network 3.0 verziótól érhető el.

Ha az alkalmazás Light Agent üzemmódban működik, a Felhő mód nem érhető el.

A védelmi összetevők felhő üzemmódjának engedélyezése vagy letiltása a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A szabályzat ablakában válassza a **Fenyegetések elleni fejlett védelem → Kaspersky Security Network** lehetőséget.

4. A **Felhő mód engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.

5. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A felhő üzemmód engedélyezése vagy letiltása a védelmi összetevők számára a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Kaspersky Security Network** elemet.

5. A **Use cloud mode** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A felhő üzemmód engedélyezése vagy letiltása a védelmi összetevők számára az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Kaspersky Security Network** lehetőséget.

3. A **Felhő mód engedélyezése** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Mentse el a módosításokat.

Ennek eredményeképpen a Kaspersky Endpoint Security a következő frissítés során letölti a vírusadatbázisok könnyített vagy teljes verzióját.

Ha az antivírus adatbázisok egyszerű verziója nem használható, a Kaspersky Endpoint Security automatikusan átvált az antivírus adatbázisok prémium verziójára.

KSN Proxy beállítások

A Kaspersky Security Center Administration Server által kezelt felhasználói számítógépek a KSN-nel közvetlenül vagy a KSN Proxy szolgáltatáson keresztül léphetnek interakcióba.

Ha az alkalmazás Light Agent üzemmódban fut, a KSN-nel való közvetlen kommunikáció nem támogatott. A Kaspersky Endpoint Security egy KSN proxykiszolgálón keresztül kommunikál a KSN-kiszolgálókkal.

A KSN Proxy szolgáltatás az alábbi lehetőségeket kínálja:

- A felhasználó számítógépe lekérdezheti a KSN-t, és információkat küldhet el részére akár közvetlen internetelérés nélkül is.
- A KSN Proxy szolgáltatás a feldolgozott adatokat gyorsítótárba helyezi, ezzel csökkentve a külső hálózati kommunikációs csatorna terhelését és felgyorsítva a felhasználó számítógépe által kért információk fogadását.

Alapértelmezésben a KSN engedélyezése és a KSN nyilatkozat elfogadása után az alkalmazás egy proxy-kiszolgálót használ a Kaspersky Security Networkhöz való csatlakozáshoz. Az alkalmazás által használt proxykiszolgáló a Kaspersky Security Center Felügyeleti Kiszolgáló a TCP 13111 porton keresztül. Ezért, ha a KSN proxykiszolgáló nem elérhető, a következőket kell ellenőrizni:

- A `ksnproxy` szolgáltatás fut a Felügyeleti kiszolgálón.
- A számítógépen lévő Tűzfal nem blokkolja a 13111 portot.

A KSN Proxy használatát a következőképpen konfigurálhatja: engedélyezze vagy tiltsa le a KSN Proxyt és konfigurálja a kapcsolati portot. Ehhez meg kell nyitnia a Felügyeleti kiszolgáló tulajdonságait. A KSN Proxy konfigurációjával kapcsolatos további részletekért olvassa el a Kaspersky Security Center súgóját. Engedélyezheti vagy letilthatja a KSN Proxy szolgáltatást az egyes számítógépeken a Kaspersky Endpoint Security szabályzatban.

A KSN Proxy engedélyezése vagy letiltása a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakában válassza a **Fenyegetések elleni fejlett védelem → Kaspersky Security Network** lehetőséget.
4. A **KSN proxy beállítások** blokkban használja a **Adminisztrációs kiszolgáló használata KSN-proxykiszolgálóként** jelölőnégyzetet KSN Proxy engedélyezéséhez vagy letiltásához.
5. Ha szükséges, válassza ki **A Kaspersky Security Network kiszolgálóinak használata, ha a KSN-proxykiszolgáló nem érhető el** jelölőnégyzetet.

   Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a KSN kiszolgálókat használja, ha a KSN Proxykiszolgáló elérhetetlen. A KSN kiszolgálók egyaránt lehetnek a Kaspersky oldalán és harmadik felek oldalán (a Privát Kaspersky Security Network használata esetén).
6. Mentse el a módosításokat.

Az KSN Proxy engedélyezése vagy letiltása a webkonzolban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings → Kaspersky Security Network** elemet.
5. A **Use Administration Server as a KSN proxy server** jelölőnégyzettel engedélyezheti vagy tilthatja le a KSN Proxy szolgáltatást.

6. Ha szükséges, tegyen jelölést a **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** jelölőnégyzetbe.

   Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a KSN kiszolgálókat használja, ha a KSN Proxykiszolgáló elérhetetlen. A KSN kiszolgálók egyaránt lehetnek a Kaspersky oldalán és harmadik felek oldalán (a Privát Kaspersky Security Network használata esetén). Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.

7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A KSN Proxy címe megegyezik a felügyeleti kiszolgáló címével. Amikor a Felügyeleti kiszolgáló tartományneve megváltozik, manuálisan kell frissítenie a KSN Proxy címét.

A KSN Proxy címének beállítása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki a konzolfán az **Advanced** → **Remote installation** → **Installation packages** mappát.
3. Az **Installation packages** mappa helyi menüjében válassza a **Properties** lehetőséget.
4. A megnyitott ablak **General** lapon adja meg a KSN proxykiszolgáló új nevét.
5. Mentse el a módosításokat.

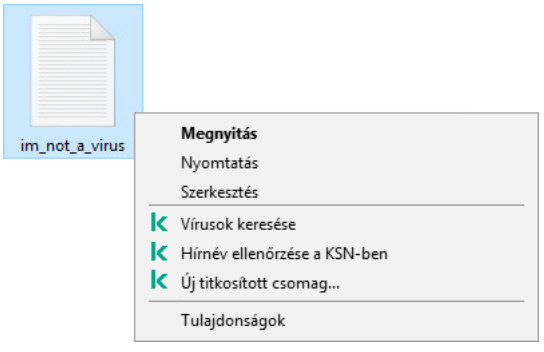
Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével

Ha nem biztos egy adott fájl biztonságosságával kapcsolatban, lehetősége van megtekinteni annak megítélését a Kaspersky Security Network hálózaton.

Egy fájl megítélését akkor tudja megtekinteni, ha elfogadta a Kaspersky Security Network nyilatkozatot.

Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével:

Nyissa meg a fájl helyi menüjét, és válassza a **Megbízhatóság ellenőrzése a KSN-ben** lehetőséget (részletek az alábbi ábrán).



Fájl helyi menüje

A Kaspersky Endpoint Security megjeleníti a fájl megítélését:

Megbízható (Kaspersky Security Network). Az alkalmazás akkor tekint megbízhatónak egy fájlt, ha az alábbi feltételek közül legalább egy teljesül:

- a fájlt egy megbízható gyártó digitálisan aláírta;
- a fájl megbízható hírnévvel rendelkezik a Kaspersky Security Network szolgáltatásban;
- a felhasználó a fájlt a Megbízható csoportba helyezte.

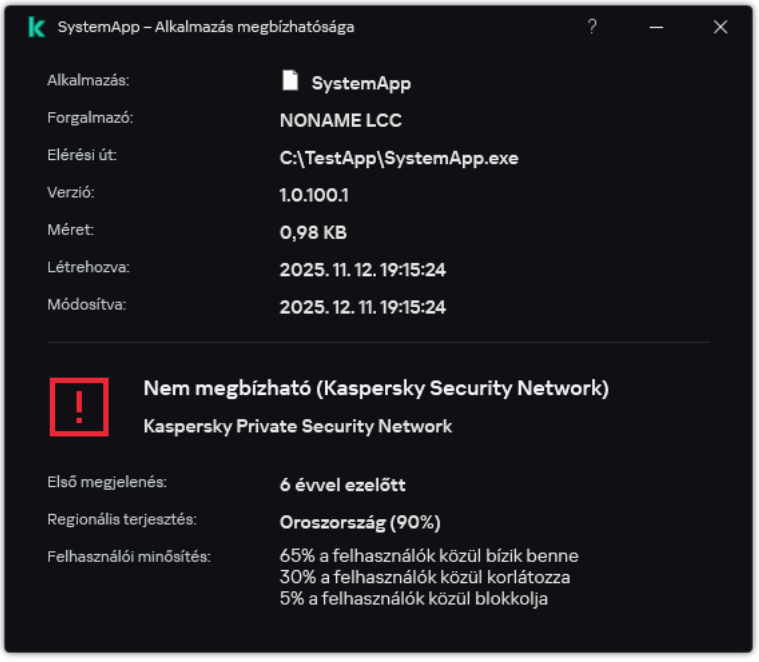
Legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait. Miközben ezeknek az alkalmazásoknak nincs rosszindulatú funkciója, a behatolók felhasználhatják őket rosszindulatú eljárásaik során. A jogszerű szoftverek részleteiért, amelyekkel a bűnözők károsíthatják a számítógépet vagy a személyes adatokat, keresse fel a Kaspersky IT Encyclopedia webhelyet. Lehetősége van felvenni ezeket az alkalmazásokat a megbízható alkalmazások listájára.

Nem megbízható (Kaspersky Security Network). Vírus vagy más alkalmazás, amely fenyegetést jelent.

Ismeretlen (Kaspersky Security Network). A Kaspersky Security Network nem rendelkezik információval az adott fájlra vonatkozóan. Lehetősége van megvizsgálni egy fájlt antivírus adatbázisok segítségével (a helyi menü **Vírusok keresése** elemét választva).

A Kaspersky Endpoint Security megjeleníti a fájl megítélésének meghatározásához használt KSN-megoldást: *Kaspersky Security Network* vagy *Kaspersky Private Security Network*.

A Kaspersky Endpoint Security további információt is megjelenít a fájlról (részletek a lentebbi ábrán).



Fájl megítélése a Kaspersky Security Network hálózaton

Titkosított kapcsolatok vizsgálata

A telepítést követően a Kaspersky Endpoint Security hozzáadja a Kaspersky tanúsítványt a rendszer által tárolt megbízható tanúsítványok közé (Windows tanúsítványtároló). A Kaspersky Endpoint Security ezt a tanúsítványt használja a titkosított kapcsolatok vizsgálatához. A Kaspersky Endpoint Security emellett használja a Firefox és a Thunderbird megbízható tanúsítványainak rendszertárolóját is ezen alkalmazások adatforgalmának vizsgálatához.

A Webfelügyelő, a Levelezés védelem, a Web védelem, a Viselkedésészlelés és a Biztonsági rések kihasználásának megelőzése összetevő képes a következő protokollokon keresztül küldött forgalmat visszafejteni és vizsgálni:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Titkosított kapcsolatok vizsgálatának engedélyezése

Alapértelmezés szerint az alkalmazás nem mindig vizsgálja a titkosított kapcsolatokat, csak akkor, ha a védelmi összetevők kérik.

A titkosított kapcsolatok vizsgálatának engedélyezése a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A házirend ablakban válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
5. A **Titkosított kapcsolatok vizsgálata** részen válassza ki a titkosított kapcsolatok vizsgálatának módját:
   - **Titkosított kapcsolatok vizsgálata**. A Kaspersky Endpoint Security nem fog hozzáférni az olyan webhelyek tartalmához, amelyek címének a kezdete `https://`.
   - **Titkosított kapcsolatok vizsgálata a védelmi összetevők kérésére**. A Kaspersky Endpoint Security csak akkor vizsgálja a titkosított forgalmat, ha a Web védelem, a Levelezés védelem vagy a Webfelügyelő összetevő ezt kéri.
   - **Mindig vizsgálja a titkosított kapcsolatokat**. A Kaspersky Endpoint Security akkor is vizsgálni fogja a titkosított hálózati forgalmat, ha a védelem összetevői nem működnek.

A Kaspersky Endpoint Security nem vizsgálja azokat a titkosított kapcsolatokat, amelyeket olyan megbízható alkalmazások hoztak létre, amelyeknél a forgalomvizsgálat le van tiltva. A Kaspersky Endpoint Security nem vizsgálja a titkosított kapcsolatokat a megbízható webhelyek előre meghatározott listájáról. A megbízható webhelyek előre meghatározott listáját a Kaspersky szakértői hozták létre. Ez a lista az alkalmazás vírusadatbázisaival frissül. A megbízható webhelyek előre meghatározott listáját csak a Kaspersky Endpoint Security felületen tekintheti meg. Nem tudja megtekinteni a listát a Kaspersky Security Center konzolon.

6. Szükség esetén adjon hozzá kizárásokat: megbízható címek és alkalmazások.

7. Konfigurálja a titkosított kapcsolatok vizsgálatának beállításait (lásd az alábbi táblázatban).

8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A titkosított kapcsolatok vizsgálatának engedélyezése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Network Settings** elemet.

5. A(z) **Encrypted Connections Scan** területen kapcsolja be a(z) **Encrypted Connections Scan ENABLED** kapcsolót.

   Ha a kapcsoló ki van kapcsolva, a Kaspersky Endpoint Security nem fog hozzáférni az olyan webhelyek tartalmához, amelyek címének a kezdete `https://`.

6. Kattintson a(z) **Settings** elemre, és válassza ki a titkosított kapcsolat vizsgálati módját:

   - **Scan encrypted connections upon request from protection components**. A Kaspersky Endpoint Security csak akkor vizsgálja a titkosított forgalmat, ha a Web védelem, a Levelezés védelem vagy a Webfelügyelő összetevő ezt kéri.

   - **Always scan encrypted connections**. A Kaspersky Endpoint Security akkor is vizsgálni fogja a titkosított hálózati forgalmat, ha a védelem összetevői nem működnek.

   A Kaspersky Endpoint Security nem vizsgálja azokat a titkosított kapcsolatokat, amelyeket olyan megbízható alkalmazások hoztak létre, amelyeknél a forgalomvizsgálat le van tiltva. A Kaspersky Endpoint Security nem vizsgálja a titkosított kapcsolatokat a megbízható webhelyek előre meghatározott listájáról. A megbízható webhelyek előre meghatározott listáját a Kaspersky szakértői hozták létre. Ez a lista az alkalmazás vírusadatbázisaival frissül. A megbízható webhelyek előre meghatározott listáját csak a Kaspersky Endpoint Security felületen tekintheti meg. Nem tudja megtekinteni a listát a Kaspersky Security Center konzolon.

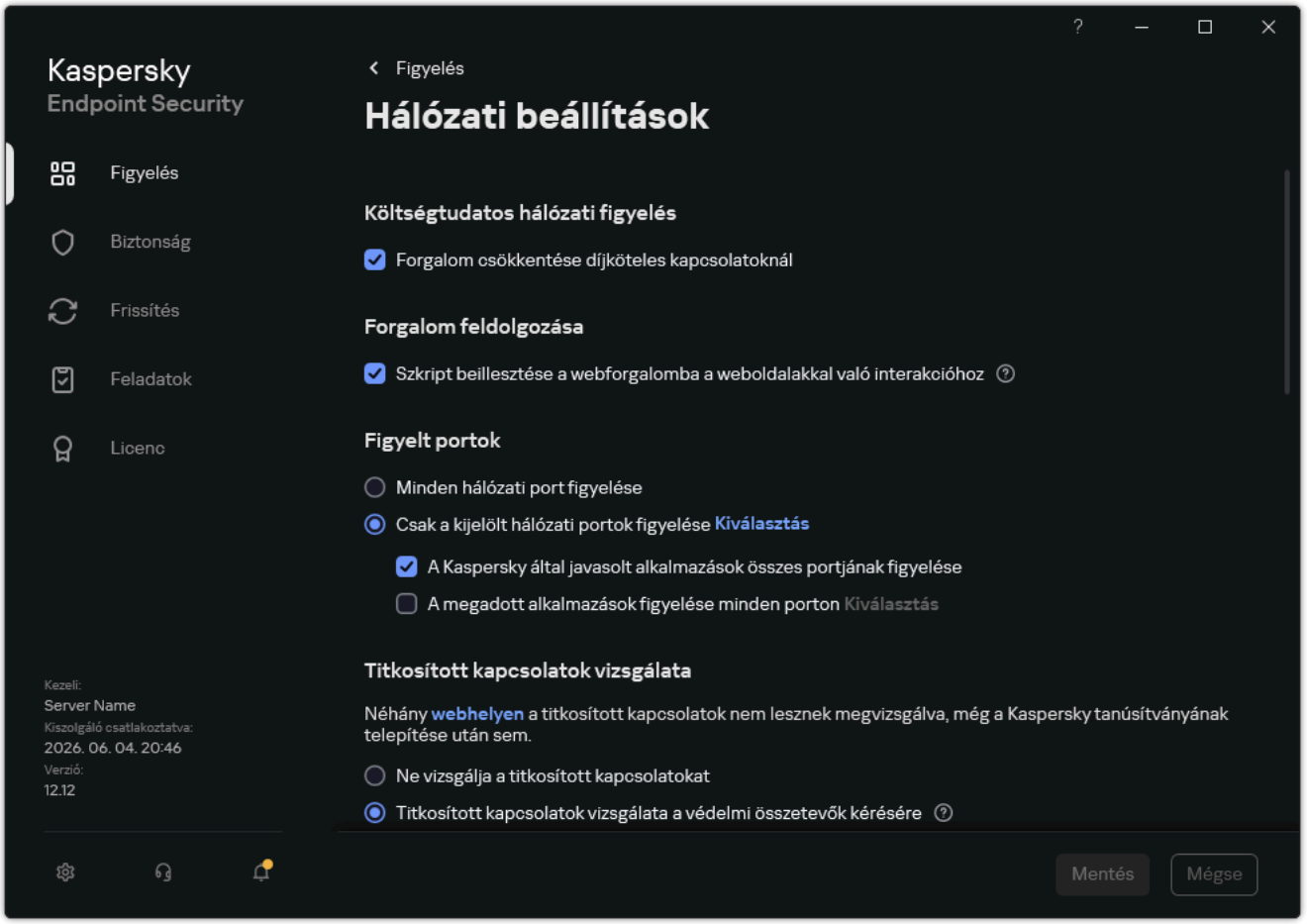
7. Szükség esetén adjon hozzá kizárásokat: megbízható címek és alkalmazások.

8. Konfigurálja a titkosított kapcsolatok vizsgálatának beállításait (lásd az alábbi táblázatban).

9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A titkosított kapcsolatok vizsgálatának engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.



Titkosított kapcsolatok vizsgálatának beállításai

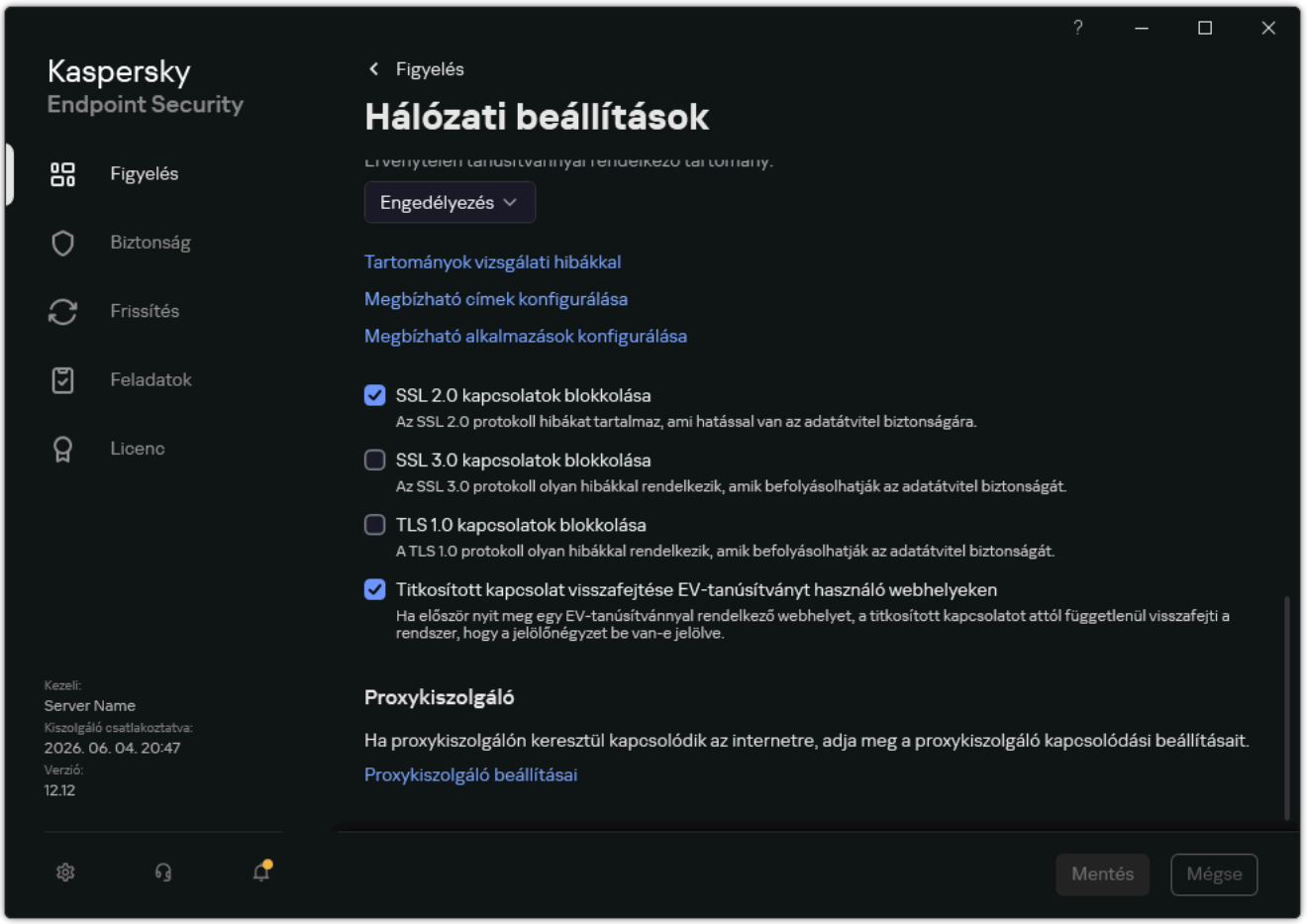
3. A **Titkosított kapcsolatok vizsgálata** részen válassza ki a titkosított kapcsolatok vizsgálatának módját:

   - **Ne vizsgálja a titkosított kapcsolatokat**. A Kaspersky Endpoint Security nem fog hozzáférni az olyan webhelyek tartalmához, amelyek címének a kezdete `https://`.
   - **Titkosított kapcsolatok vizsgálata a védelmi összetevők kérésére**. A Kaspersky Endpoint Security csak akkor vizsgálja a titkosított forgalmat, ha a Web védelem, a Levelezés védelem vagy a Webfelügyelő összetevő ezt kéri.
   - **Mindig vizsgálja a titkosított kapcsolatokat**. A Kaspersky Endpoint Security akkor is vizsgálni fogja a titkosított hálózati forgalmat, ha a védelem összetevői nem működnek.

   A Kaspersky Endpoint Security nem vizsgálja azokat a titkosított kapcsolatokat, amelyeket olyan megbízható alkalmazások hoztak létre, amelyeknél a forgalomvizsgálat le van tiltva. A Kaspersky Endpoint Security nem vizsgálja a titkosított kapcsolatokat a megbízható webhelyek előre meghatározott listájáról. A megbízható webhelyek előre meghatározott listáját a Kaspersky szakértői hozták létre. Ez a lista az alkalmazás vírusadatbázisaival frissül. A megbízható webhelyek előre meghatározott listáját csak a Kaspersky Endpoint Security felületen tekintheti meg. Nem tudja megtekinteni a listát a Kaspersky Security Center konzolon.

4. Szükség esetén adjon hozzá kizárásokat: megbízható címek és alkalmazások.

5. Konfigurálja a titkosított kapcsolatok vizsgálatának beállításait (lásd az alábbi táblázatban).



További beállítások a titkosított kapcsolatok vizsgálatához

6. Mentse el a módosításokat.

Paraméter	Leírás
Megbízható főtanúsítványok	A megbízható főtanúsítványok listája. A Kaspersky Endpoint Security lehetővé teszi, hogy megbízható főtanúsítványokat telepítsen a felhasználói számítógépekre, ha például új tanúsítványközpontot kell telepítenie. Az alkalmazás lehetővé teszi, hogy tanúsítványt adjon hozzá egy speciális Kaspersky Endpoint Security tanúsítványtárolóhoz. Ebben az esetben a tanúsítvány csak a Kaspersky Endpoint Security alkalmazás esetében tekinthető megbízhatónak. Más szóval a felhasználó az új tanúsítvánnyal a böngészőben hozzáférhet egy webhelyhez. Ha egy másik alkalmazás megpróbál hozzáférni a webhelyhez, akkor tanúsítványprobléma miatt kapcsolódási hiba jelentkezhet. A rendszer tanúsítványtárolójához való hozzáadáshoz használhatja az Active Directory csoportházirendjeit.
Nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása	• **Engedélyezés**. A nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása esetén a Kaspersky Endpoint Security engedélyezi a hálózati kapcsolatot. A nem megbízható tanúsítvánnyal rendelkező tartomány böngészővel történő megnyitása esetén a Kaspersky Endpoint Security megjelenít egy HTML-oldalt, ami egy figyelmeztetést mutat, valamint az okot, amiért nem javasolt a tartomány meglátogatása. A felhasználó rákattinthat a hivatkozásra a HTML figyelmeztető oldalon, hogy hozzáférést kapjon a kért webes erőforráshoz. Ha egy harmadik féltől származó alkalmazás vagy szolgáltatás kapcsolatot létesít egy nem megbízható tanúsítványú tartománnyal, a Kaspersky Endpoint Security saját tanúsítványt hoz létre a forgalom vizsgálatához. Az új tanúsítvány *Nem megbízható* állapotot kap. Erre azért van szükség, hogy figyelmeztesse a harmadik féltől származó alkalmazást a nem megbízható kapcsolatra, mert a HTML-oldal ebben az esetben nem jeleníthető meg, és a kapcsolat létrejöhet háttérmódban. • **Blokkolás**. A nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása esetén a Kaspersky Endpoint Security blokkolja a hálózati kapcsolatot. A nem megbízható tanúsítvánnyal rendelkező tartomány böngészővel történő megnyitása esetén a Kaspersky Endpoint Security megjelenít egy HTML-oldalt, ami mutatja az okot, hogy miért van blokkolva a tartomány.
Titkosított kapcsolatok vizsgálati hibájával rendelkező tartomány meglátogatása	• **Blokkolás**. Ha titkosított kapcsolat vizsgálatakor hiba történik, a Kaspersky Endpoint Security blokkolja a hálózati kapcsolatot. • **Engedélyezés és tartomány hozzáadása a kizárásokhoz**. Ha titkosított kapcsolat vizsgálatakor hiba történik, a Kaspersky Endpoint Security hozzáadja a hibát okozó tartományt a vizsgálati hibákat mutató tartományok listájához, és nem figyeli a titkosított hálózati forgalmat, amikor ezt a tartományt meglátogatják. Azoknak a tartományoknak a listáját, amelyeknél a titkosított kapcsolatok vizsgálata során hiba jelentkezett, csak az alkalmazás helyi felületén lehet megtekinteni. A lista tartalmának törléséhez ki kell választania a **Blokkolás** lehetőséget. A Kaspersky Endpoint Security eseményt is generál a titkosított kapcsolat vizsgálati hibájához.
SSL 2.0 kapcsolatok blokkolása	Ha a jelölőnégyzet be van jelölve, akkor az alkalmazás figyeli és blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Az alkalmazás azonban nem figyeli a hálózati forgalmat ezen a protokollon keresztül.
SSL 3.0 kapcsolatok blokkolása	Ha a jelölőnégyzet be van jelölve, akkor az alkalmazás blokkolja az SSL 3.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem blokkolja az SSL 3.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Az alkalmazás ezen a protokollon keresztül figyeli a hálózati forgalmat. Az alkalmazás minden összetevője korlátozások nélkül működik.
TLS 1.0 kapcsolatok blokkolása	Ha a jelölőnégyzet be van jelölve, akkor az alkalmazás blokkolja az TLS 1.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem blokkolja az TLS 1.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Az alkalmazás ezen a protokollon keresztül figyeli a hálózati forgalmat. Az alkalmazás minden összetevője korlátozások nélkül működik.
Titkosított kapcsolat visszafejtése EV-tanúsítványt használó webhelyeken	Az EV-tanúsítványok (Extended Validation Certificate) hitelesítik a weboldalakat és növelik a kapcsolat biztonságát. A Böngészők a zár ikont használják a címsávjukban, hogy jelezzék, hogy a weboldal EV-tanúsítvánnyal rendelkezik. A böngészők részben vagy egészben zöldre is színezhetik a címsávot. Ha ez a jelölőnégyzet be van jelölve, az alkalmazás visszafejti és figyeli az EV-tanúsítványt használó webhelyekkel történő titkosított kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem fér hozzá a HTTPS-forgalom tartalmához. Ezen okokból az alkalmazás csak a webcím alapján figyeli meg a HTTPS-forgalmat, például: `https://bing.com`. Ha először nyit meg egy EV-tanúsítvánnyal rendelkező weboldalt, a titkosított kapcsolat attól függetlenül vissza lesz fejtve, hogy Ön kijelölte-e a jelölőnégyzetet.

Megbízható főtanúsítványok telepítése

A Kaspersky Endpoint Security lehetővé teszi, hogy megbízható főtanúsítványokat telepítsen a felhasználói számítógépekre, ha például új tanúsítványközpontot kell telepítenie. Az alkalmazás lehetővé teszi, hogy tanúsítványt adjon hozzá egy speciális Kaspersky Endpoint Security tanúsítványtárolóhoz. Ebben az esetben a tanúsítvány csak a Kaspersky Endpoint Security alkalmazás esetében tekinthető megbízhatónak. Más szóval a felhasználó az új tanúsítvánnyal a böngészőben hozzáférhet egy webhelyhez. Ha egy másik alkalmazás megpróbál hozzáférni a webhelyhez, akkor tanúsítványprobléma miatt kapcsolódási hiba jelentkezhet. A rendszer tanúsítványtárolójához való hozzáadáshoz használhatja az Active Directory csoportházirendjeit.

A megbízható főtanúsítványok listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Megbízható főtanúsítványok telepítésének menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
4. A **Megbízható főtanúsítványok** részen kattintson a **Hozzáadás** gombra.
5. A megnyíló ablakban válasszon ki egy megbízható főtanúsítványt.
   A Kaspersky Endpoint Security a PEM, DER és CRT kiterjesztésű tanúsítványokat támogatja.
6. Mentse el a módosításokat.

Megbízható főtanúsítványok telepítésének menete a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Network Settings** elemet.
5. Kattintson a **Trusted root certificates** hivatkozásra.

6. A megnyíló ablakban kattintson a **Add** gombra, és válasszon ki egy megbízható főtanúsítványt.

   A Kaspersky Endpoint Security a PEM, DER és CRT kiterjesztésű tanúsítványokat támogatja.

7. Mentse el a módosításokat.

Megbízható főtanúsítványok telepítésének menete az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Titkosított kapcsolatok vizsgálata** részen kattintson a **Tanúsítványok megjelenítése** gombra.
4. A megnyíló ablakban kattintson a **Hozzáadás** gombra, és válasszon ki egy megbízható főtanúsítványt.

   A Kaspersky Endpoint Security a PEM, DER és CRT kiterjesztésű tanúsítványokat támogatja.

5. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Endpoint Security az adatforgalom vizsgálatakor a rendszer tanúsítványtárolóján kívül a saját tanúsítványtárolóját is használja.

Titkosított kapcsolatok vizsgálata nem megbízható tanúsítvánnyal

A telepítést követően a Kaspersky Endpoint Security hozzáadja a Kaspersky tanúsítványt a rendszer által tárolt megbízható tanúsítványok közé (Windows tanúsítványtároló). A Kaspersky Endpoint Security ezt a tanúsítványt használja a titkosított kapcsolatok vizsgálatához. Amikor egy nem megbízható tanúsítvánnyal rendelkező tartományt keres fel, engedélyezheti vagy megtagadhatja a felhasználói hozzáférést az adott tartományhoz (lásd az alábbi utasításokat).

Ha engedélyezte a felhasználó számára, hogy nem megbízható tanúsítvánnyal rendelkező tartományokat keressen fel, a Kaspersky Endpoint Security a következő műveleteket hajtja végre:

- Nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatásakor a *böngészőben* a Kaspersky Endpoint Security a Kaspersky-tanúsítványt használja a forgalom vizsgálatához. A Kaspersky Endpoint Security egy HTML-oldalt jelenít meg figyelmeztetéssel és információval arról, hogy miért nem javasolt a megfelelő tartomány felkeresése (lásd az alábbi ábrát). A felhasználó rákattinthat a hivatkozásra a HTML figyelmeztető oldalon, hogy hozzáférést kapjon a kért webes erőforráshoz. A hivatkozásra való lépés után, a következő órában a Kaspersky Endpoint Security nem fogja megjeleníteni a nem megbízható tanúsítványokról szóló figyelmeztetéseket, ha egyéb erőforrásokat látogat meg ugyanazon tartományon belül. A Kaspersky Endpoint Security eseményt is generál egy nem megbízható tanúsítvánnyal rendelkező titkosított kapcsolat létrehozásáról.

  Bizonyos esetekben a Kaspersky Endpoint Security technikailag nem tudja megjeleníteni a böngészőben a figyelmeztetéssel ellátott HTML-oldalt (lásd az alábbi ábrát). Például, ha egy webes erőforrás egy hálózati protokoll elavult verzióját és egy nem szabványos portot használ. Ezekben az esetekben a Kaspersky Endpoint Security blokkolja a tartományhoz való hozzáférést, és a böngésző a szokásos `ERR_CONNECTION_RESET` ablakot jeleníti meg. Egy webes erőforrás eléréséhez hozzáadhat tartományt a kizárásokhoz, vagy használhat megbízható tanúsítványt.

- Ha *egy harmadik féltől származó alkalmazás vagy szolgáltatás* kapcsolatot létesít egy nem megbízható tanúsítványú tartománnyal, a Kaspersky Endpoint Security saját tanúsítványt hoz létre a forgalom vizsgálatához. Az új tanúsítvány *Nem megbízható* állapotot kap. Erre azért van szükség, hogy figyelmeztesse a harmadik féltől származó alkalmazást a nem megbízható kapcsolatra, mert a HTML-oldal ebben az esetben nem jeleníthető meg, és a kapcsolat létrejöhet háttérmódban. Ezért, ha egy harmadik féltől származó alkalmazás beépített tanúsítvány-ellenőrző eszközökkel rendelkezik, a kapcsolat megszakadhat. Ebben az esetben kapcsolatba kell lépnie a tartomány tulajdonosával, és be kell állítania egy megbízható kapcsolatot. Ha a megbízható kapcsolat létrehozása lehetetlen, hozzáadhatja a harmadik féltől származó alkalmazást a megbízható alkalmazások listájához. A Kaspersky Endpoint Security eseményt is generál egy nem megbízható tanúsítvánnyal rendelkező titkosított kapcsolat létrehozásáról.

A nem megbízható tanúsítvánnyal rendelkező titkosított kapcsolatok ellenőrzésének konfigurálása az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
4. A **Titkosított kapcsolatok vizsgálata** részen kattintson a **Speciális beállítások** gombra.
5. A megnyíló ablakban válassza ki az alkalmazás működési módját, amikor nem megbízható tanúsítvánnyal rendelkező tartományt keres fel: **Engedélyezés** vagy **Blokkolás**.
6. Mentse el a módosításokat.

A nem megbízható tanúsítvánnyal rendelkező titkosított kapcsolatok vizsgálatának konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Network Settings** elemet.

5. A **Encrypted Connections Scan** részen kattintson a **Settings** hivatkozásra.

6. A megnyíló ablakban válassza ki az alkalmazás működési módját, amikor nem megbízható tanúsítvánnyal rendelkező tar tományt keres fel: **Allow connection** or **Block connection**.

7. Mentse el a módosításokat.

A nem megbízható tanúsítvánnyal rendelkező titkosított kapcsolatok vizsgálatának konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.

3. A **Titkosított kapcsolatok vizsgálata** részen válassza ki az alkalmazás működési módját, amikor nem megbízható tanúsítvánnyal rendelkező tartományt keres fel: **Engedélyezés** vagy **Blokkolás**.

4. Mentse el a módosításokat.



Figyelmeztetés nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatásakor

Kaspersky tanúsítvány hozzáadása a saját tanúsítványtárolóhoz

A böngészők és a levelezőprogramok a tanúsítványt a webes erőforrások biztonságának és hitelességének ellenőrzésére használják. A tanúsítvány emellett adattitkosítást is biztosít a webes erőforrások és a felhasználó között. A legtöbb böngésző és levelezőprogram a megbízható tanúsítványtárolót (Windows tanúsítványtároló) használja. Például a Google Chrome. Egyes böngészők és levelezőprogramok alapértelmezés szerint saját tanúsítványtárolójukat használják a Windows tanúsítványtárolója helyett. Például a Firefox és a Thunderbird.

A telepítést követően a Kaspersky Endpoint Security hozzáadja a Kaspersky tanúsítványt a rendszer által tárolt megbízható tanúsítványok közé (Windows tanúsítványtároló). Ha a Kaspersky Security Center telepítve van a szervezetben és házirend van alkalmazva a számítógépre, a Kaspersky Endpoint Security a böngészőkben és levelezőprogramokban automatikusan engedélyezi a Windows tanúsítványtárolójának használatát az alkalmazások forgalmának vizsgálatára. Ha nincs házirend alkalmazva a számítógépen, kiválaszthatja a böngészők és levelezőprogramok által használt tanúsítványtárolót. Ha a saját tanúsítványtárolót választotta, manuálisan adja hozzá a Kaspersky tanúsítványt a tárolóhoz. Ez segít elkerülni a hibákat a HTTPS-forgalommal való munka során.

A Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmának vizsgálatához engedélyeznie kell a Titkosított kapcsolatok vizsgálatát. Ha a Titkosított kapcsolatok vizsgálata le van tiltva, az alkalmazás nem vizsgálja a Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmát. A titkosított kapcsolatok vizsgálatát a MyOffice Mail és az R7-Office Organizer levelezőprogramok forgalmának vizsgálatához is engedélyezni kell.

Mielőtt tanúsítványt adna hozzá a böngésző vagy a levelezőügynök saját tanúsítványtárolójához, exportálja a Kaspersky-tanúsítványt a Windows Vezérlőpultjáról (Internettulajdonságok). A tanúsítványok tárolóhoz való hozzáadásáról többet tudhat meg például a Mozilla technikai támogatási webhelyén.

A tanúsítványtárolót csak az alkalmazás helyi felületén választhatja ki.

Tanúsítványtároló kiválasztása a titkosított kapcsolatok vizsgálatához a böngészőben és levelezőprogramban:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.
3. A **Titkosított kapcsolatok vizsgálata** részen válassza ki **A saját tanúsítványtárolóval rendelkező alkalmazások titkosított kapcsolatainak vizsgálatához használja** jelölőnégyzetet.
4. Válasszon egy tanúsítványtárolót:
   - **Windows tanúsítványtároló (ajánlott)**. A Kaspersky főtanúsítvány bekerül ebbe a tárolóba a Kaspersky Endpoint Security telepítése során.
   - **Saját tanúsítványtároló**. A Mozilla Firefox és a Thunderbird saját tanúsítványtárolóját használja. Ha a Mozilla tanúsítványtároló van kiválasztva, manuálisan kell hozzáadnia a Kaspersky főtanúsítványt ehhez a tárolóhoz a böngésző beállításaiban.

     A MyOffice Mail és az R7-Office Organizer levelezőprogramok szintén saját tanúsítványtárolót használnak.
5. Mentse el a módosításokat.

Titkosított kapcsolatok kizárása a vizsgálat alól

A legtöbb webes erőforrás titkosított kapcsolatokat használ. A Kaspersky szakértők a következő engedélyezését ajánlják: Titkosított kapcsolatok vizsgálata. Ha a titkosított kapcsolatok vizsgálata munkával kapcsolatos tevékenységgel ütközik, hozzáadhat egy webhelyet a kizárásokhoz, más néven *megbízható címekhez*. Ebben az esetben a Kaspersky Endpoint Security nem vizsgálja a megbízható webcímek HTTPS-forgalmát, amikor a Web védelem, a Levelezés védelem és a Webfelügyelő összetevők végzik a munkájukat.

Ha egy megbízható alkalmazás titkosított kapcsolatot használ, kikapcsolhatja a titkosított kapcsolatok vizsgálatát az alkalmazás esetében. Például kikapcsolhatja a titkosított kapcsolatos vizsgálatát olyan cloud-tárhelyalkalmazásoknál, melyek kétlépéses hitelesítést használnak a saját tanúsítványukkal.

A megbízható címek listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Webcím kizárása a titkosított kapcsolatok vizsgálatából az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
4. A **Titkosított kapcsolatok vizsgálata** részen kattintson a **Megbízható címek konfigurálása** gombra.
5. Kattintson **Hozzáadás** gombra.
6. Adjon meg egy tartománynevet vagy IP-címet, ha szeretné, hogy a Kaspersky Endpoint Security ne vizsgálja az adott tartomány felkeresésekor létrehozott titkosított kapcsolatokat.

   A Kaspersky Endpoint Security támogatja a `*` karaktert maszk megadásához a tartománynévben.

   A Kaspersky Endpoint Security nem támogatja a `*` szimbólumot IP-címek esetén. Az IP-címek tartományát alhálózati maszk segítségével választhatja ki (például 198.51.100.0/24).

   Példák:

   - `domain.com` – a rekord a következő címeket tartalmazza: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. A rekord nem tartalmaz altartományt (pl. `subdomain.domain.com`).
   - `subdomain.domain.com` – a rekord a következő címeket tartalmazza: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.
   - `*.domain.com` – a rekord a következő címeket tartalmazza: `https://movies.domain.com`, `https://images.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.
7. Mentse el a módosításokat.

Webcím kizárása a titkosított kapcsolatok vizsgálatából a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Network Settings** elemet.
5. A **Encrypted Connections Scan** részen kattintson a **Trusted domains** gombra.
6. Kattintson az **Add** gombra.
7. Adjon meg egy tartománynevet vagy IP-címet, ha szeretné, hogy a Kaspersky Endpoint Security ne vizsgálja az adott tartomány felkeresésekor létrehozott titkosított kapcsolatokat.

   A Kaspersky Endpoint Security támogatja a `*` karaktert maszk megadásához a tartománynévben.

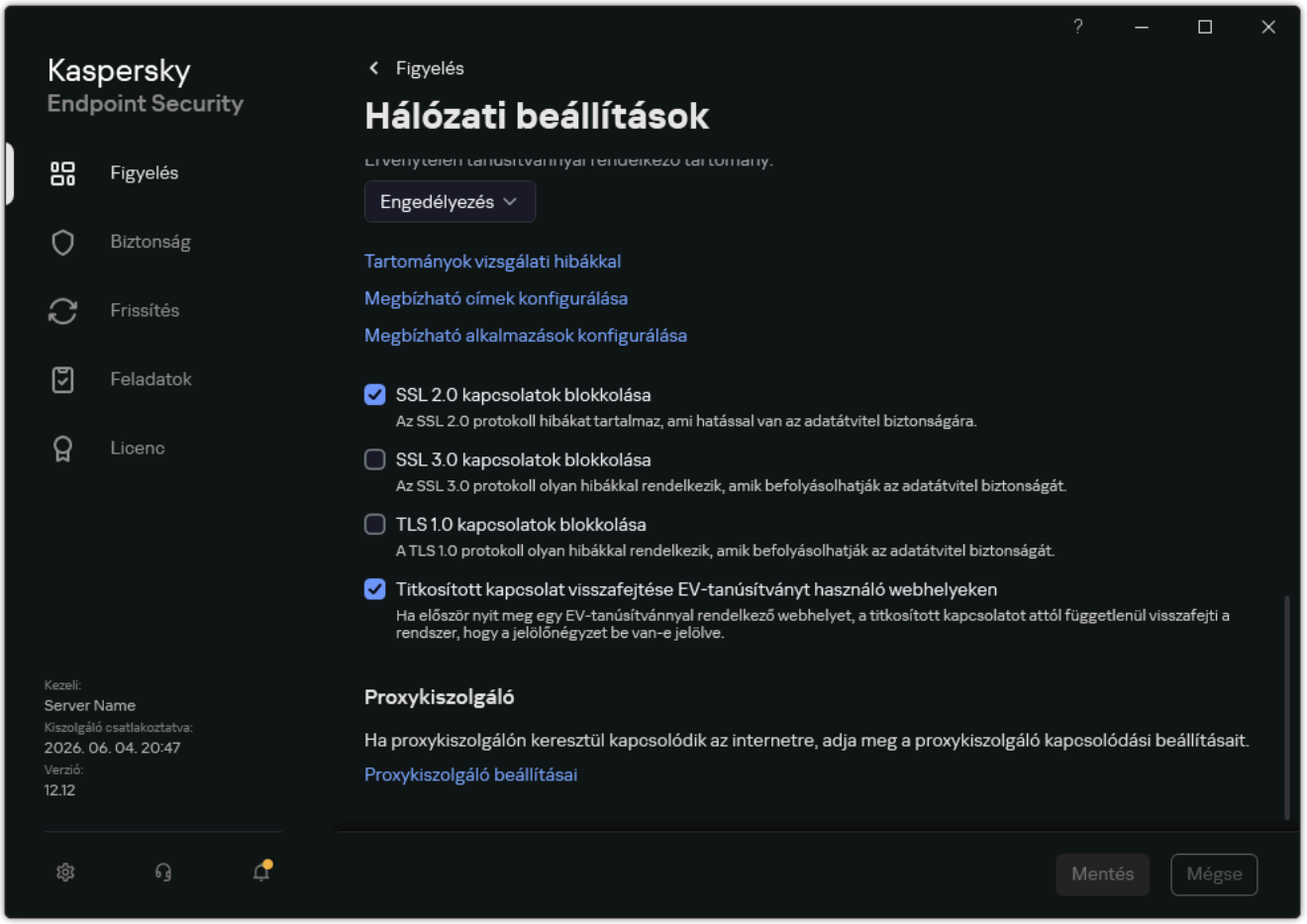
   > A Kaspersky Endpoint Security nem támogatja a `*` szimbólumot IP-címek esetén. Az IP-címek tartományát alhálózati maszk segítségével választhatja ki (például 198.51.100.0/24).

   Példák:

   - `domain.com` – a rekord a következő címeket tartalmazza: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. A rekord nem tartalmaz altartományt (pl. `subdomain.domain.com`).
   - `subdomain.domain.com` – a rekord a következő címeket tartalmazza: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.
   - `*.domain.com` – a rekord a következő címeket tartalmazza: `https://movies.domain.com`, `https://images.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.
8. Mentse el a módosításokat.

Webcím kizárása a titkosított kapcsolatok vizsgálatából az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.



Alkalmazások hálózati beállításai

3. A **Titkosított kapcsolatok vizsgálata** részen kattintson a **Megbízható címek konfigurálása** gombra.
4. Kattintson **Hozzáadás** gombra.
5. Adjon meg egy tartománynevet vagy IP-címet, ha szeretné, hogy a Kaspersky Endpoint Security ne vizsgálja az adott tartomány felkeresésekor létrehozott titkosított kapcsolatokat.

   A Kaspersky Endpoint Security támogatja a `*` karaktert maszk megadásához a tartománynévben.

   > A Kaspersky Endpoint Security nem támogatja a `*` szimbólumot IP-címek esetén. Az IP-címek tartományát alhálózati maszk segítségével választhatja ki (például 198.51.100.0/24).

Példák:

- `domain.com` – a rekord a következő címeket tartalmazza: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. A rekord nem tartalmaz altartományt (pl. `subdomain.domain.com`).
- `subdomain.domain.com` – a rekord a következő címeket tartalmazza: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.
- `*.domain.com` – a rekord a következő címeket tartalmazza: `https://movies.domain.com`, `https://images.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.

6. Mentse el a módosításokat.

Alapértelmezés szerint a Kaspersky Endpoint Security hiba fellépése esetén nem vizsgálja a titkosított kapcsolatokat, és hozzáadja azokat a *Tartományok vizsgálati hibákkal* nevű speciális listához. A Kaspersky Endpoint Security minden felhasználó esetében külön listának felel meg, nem küld adatokat a Kaspersky Security Center számára. Ön engedélyezheti a kapcsolatok blokkolását, ha vizsgálati hiba lép fel. Azoknak a tartományoknak a listáját, amelyeknél a titkosított kapcsolatok vizsgálata során hiba jelentkezett, csak az alkalmazás helyi felületén lehet megtekinteni.

A vizsgálati hibákkal rendelkező tartományok megtekintéséhez:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.
3. A **Titkosított kapcsolatok vizsgálata** részben kattintson a **Tartományok vizsgálati hibákkal** gombra.

Megnyílik a vizsgálati hibákkal rendelkező tartományok listája. A lista visszaállításához engedélyezze a kapcsolatok blokkolását, ha hiba lép fel a rendszabályban, majd alkalmazza a rendszabályt, végül pedig állítsa vissza a paraméterét a kezdeti értékre, és alkalmazza újra.

A Kaspersky specialists egy listát készít a *globális kivételekről* — olyan, megbízható weboldalak, melyeket a Kaspersky Endpoint Security az alkalmazásbeállításoktól függetlenül nem ellenőriz.

A globális kivételek megtekintéséhez a titkosított forgalomvizsgálat alól

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.
3. A **Titkosított kapcsolatok vizsgálata** részben kattintson a megbízható webhelyek hivatkozásra.

Ez megnyitja a Kaspersky szakértői által összeállított webhelyek listáját. A Kaspersky Endpoint Security nem vizsgálja a védett kapcsolatokat a listán szereplő webhelyek esetében. A lista frissülhet, ha a Kaspersky Endpoint Security adatbázisai és moduljai frissülnek.

Adatok törlése

A Kaspersky Endpoint Security segítségével egy feladattal távolról törölhet adatokat a felhasználó számítógépéről.

A Kaspersky Endpoint Security a következőképp törli az adatokat:

- Csendes módban;
- Merevlemezeken és cserélhető meghajtókon;
- A számítógépen lévő összes felhasználói fiókon.

A Kaspersky Endpoint Security végrehajtja az *Adatok törlése* feladatot, függetlenül attól, hogy melyik licenctípus van használatban, még akkor is, miután a licenc lejárt.

Adattörlési módok

Ezzel a feladattal adatokat törölhet a következő módokban:

- Azonnali adattörlés.

  Ebben a módban többek között törölhet elavult adatokat, hogy tárhelyet szabadítson fel.

- Eltolt adattörlés.

  Ezzel a móddal többet között megvédheti a laptop adatait, ha az elveszett vagy ellopták. Beállíthatja az automatikus adattörlést, ha a laptop a vállalati hálózaton kívülre kerül, és régóta nem volt szinkronizálva a Kaspersky Security Centerrel.

A feladat tulajdonságaiban nem lehet ütemtervet megadni az adatok törlésére. Az adatokat csak azonnal a feladat manuális indítása után törölheti, vagy konfigurálhatja a késleltetett adattörlést, ha nincs kapcsolat a Kaspersky Security Center alkalmazással.

Korlátozások

Az Adatok törlése a következő korlátozásokkal rendelkezik:

- Csak egy Kaspersky Security Center rendszergazda kezelheti az *Adatok törlése* feladatot. A Kaspersky Endpoint Security helyi felületén nem konfigurálhat és nem indíthat el feladatot.
- Az NTFS fájlrendszereknél a Kaspersky Endpoint Security csak a fő adatfolyamok neveit törli. Az alternatív adatfolyamok nevei nem törlődnek.
- Ha szimbolikus linkfájlokat töröl, a Kaspersky Endpoint Security azokat a fájlokat is törli, amelyek elérési útvonala meg van adva a szimbolikus linkben.

Adatok törlése feladat létrehozása

A felhasználók számítógépen lévő adatok törléséhez:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Wipe data** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *Adatok törlése (Anti-Theft)*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

   Ha a feladat hatókörén belül új számítógép lesz hozzáadva az adminisztrációs csoporthoz, akkor az azonnali adattörlés csak akkor lesz futtatva az új számítógépeken, ha a feladat az új számítógépek hozzáadását követő 5 percben teljesül.

5. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

6. Kattintson a Kaspersky Endpoint Security **Wipe data** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

7. Válassza ki az **Application settings** lapot.

8. Válassza ki az adattörlés módszerét:

   - **Delete by means of the operating system**. A Kaspersky Endpoint Security az operációs rendszer erőforrásait használja arra, hogy törölje a fájlokat anélkül, hogy a lomtárba küldené azokat.

   - **Delete completely, no recovery possible**. A Kaspersky Endpoint Security véletlenszerű adatokkal felülírja a fájlokat. A törlés után gyakorlatilag lehetetlen visszaállítani az adatokat.

9. Ha el szeretné halasztani az adatok törlését, jelölje be az **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days** jelölőnégyzetet. Adja meg a napok számát.

   Az adattörlés eltolása feladat minden alkalommal el lesz végezve, ha a megadott ideig nincs kapcsolat a Kaspersky Security Centerrel.

Az elhalasztott adattörlés konfigurálásakor vegye figyelembe, hogy az alkalmazottak munkabeosztása eltérő lehet. Vegye figyelembe az offline felhasználók munkarendjét is. Az offline számítógépekkel és az irodán kívüli felhasználókkal való együttműködéssel kapcsolatos további tudnivalókért lásd a Kaspersky Security Center súgót.

Ha a számítógép ki van kapcsolva, és a kapcsolat a beállított időtartamnál hosszabb ideig nem áll fenn, a számítógép bekapcsolása után a Kaspersky Endpoint Security nem törli azonnal az adatokat. Az alkalmazás egy órán át várja a szinkronizálást a Kaspersky Security Centerrel. Erre azért van szükség, hogy megelőzhető legyen az adatok illetéktelen törlése azon felhasználók számítógépein, akik például nyaralásuk előtt kikapcsolták a számítógépüket.

Ha a jelölőnégyzet törölve van, a feladat a Kaspersky Security Centerrel való szinkronizálás után azonnal végre lesz hajtva.

10. A törlendő objektumok listájának elkészítése:

- **Mappák**. A Kaspersky Endpoint Security törli a mappában és az almappákban lévő összes fájlt. A Kaspersky Endpoint Security nem támogatja a maszkok és a környezeti változók használatát a mappa elérési útvonalának megadásakor.
- **Fájlok kiterjesztés alapján**. A Kaspersky Endpoint Security csak a megadott kiterjesztésű fájlokat keresi a számítógép meghajtóin, köztük a cserélhető meghajtókon. Használja a „`;`” vagy a „`,`” karaktert több kiterjesztés megadásához.
- **Előre megadott hatókör**. A Kaspersky Endpoint Security törli a fájlokat a következő területekről:
  - **Documents**. Az operációs rendszer szokványos *Dokumentumok* mappájában, valamint az azon belüli almappákban található fájlok.
  - **Cookies**. Fájlok, amelyekben a böngésző elmenti a felhasználó által meglátogatott weboldalak adatait (például a hitelesítő adatokat).
  - **Desktop**. Az operációs rendszer szokványos *Asztal* mappájában, valamint az azon belüli almappákban található fájlok.
  - **Temporary Internet Explorer files**. Az Internet Explorer működéséhez kapcsolódó ideiglenes fájlok, például a weboldalak, képek és médiafájlok másolata.
  - **Temporary files**. A számítógépre telepített alkalmazások működéséhez kapcsolódó ideiglenes fájlok. Például a Microsoft Office alkalmazások olyan ideiglenes fájlokat hoznak létre, amelyek a dokumentumok biztonsági mentését tartalmazzák.
  - **Outlook files**. Az Outlook levelezőprogram működéséhez kapcsolódó fájlok: adatfájlok (PST), offline adatfájlok (OST), offline címjegyzékfájlok (OAB) és személyes címjegyzékfájlok (PAB).
  - **User profile**. Fájlok vagy mappák, amik az operációs rendszer beállításait tárolják a helyi felhasználói fiókon.

Az egyes füleken létrehozhatja a törlendő objektumok listáját. A Kaspersky Endpoint Security létrehoz egy összesített listát, a feladat végrehajtása után pedig törli a listán lévő fájlokat.

Nem lehet törölni a Kaspersky Endpoint Security működéséhez szükséges fájlokat.

11. Mentse el a módosításokat.

12. Válassza ki a feladat melletti jelölőnégyzetet.

13. Kattintson az **Start** gombra.

    Ennek eredményeképpen a felhasználók számítógépein lévő adatok a kiválasztott módnak megfelelően törlődnek: azonnal, vagy a kapcsolat hiánya esetén. Ha a Kaspersky Endpoint Security nem tud törölni egy fájlt, vagy ha a felhasználó jelenleg használ egy fájlt, akkor az alkalmazás nem próbálja meg újra törölni. Az adattörlés befejezéséhez futtassa újra a feladatot.

Számítógépvezérlés

Webfelügyelő

A Webfelügyelő kezeli a felhasználók hozzáférését a webes erőforrásokhoz. Ez csökkenti a forgalmat és a munkaidő nem megfelelő használatát. Ha a felhasználó a Webfelügyelő által korlátozott weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést vagy figyelmeztetést jelenít meg (lásd az alábbi ábrát).

A Webfelügyelő használatához el kell végeznie az alkalmazás kezdeti konfigurációját:

- A HTTPS forgalom figyeléséhez, engedélyezze a titkosított kapcsolatok vizsgálatát (alapértelmezés szerint engedélyezve van).
- Válassza ki azokat a portokat, amelyeket a Kaspersky Endpoint Security megoldásnak figyelnie kell (alapértelmezés szerint az alkalmazás az összes portot figyeli).
- Válassza ki azokat az alkalmazásokat, amelyeknek a forgalmát a Kaspersky Endpoint Securityvel meg szeretné figyelni. A legtöbb böngésző már szerepel a Kaspersky által ajánlott alkalmazások listáján. Ha a böngészője hiányzik a listáról, adja hozzá manuálisan.
- Javasoljuk, hogy illesszen be egy weboldal-interakciós parancsfájlt a webes forgalomba (alapértelmezés szerint a parancsfájl beillesztése le van tiltva). Ez a parancsfájl lehetővé teszi a Webfelügyelő események regisztrációját az alkalmazás eseménynaplójában, az operációs rendszer eseménynaplójában és a jelentésekben.

A weboldalak elérésének kezelési módszerei

A Webfelügyelővel a következő módszerekkel konfigurálhatja a weboldalak elérését:

- **Weboldalkategória**. A weboldalak a Kaspersky Security Network felhőszolgáltatás, a heurisztikus elemzés és az ismert weboldalak adatbázisai (köztük az alkalmazás-adatbázisok) alapján vannak besorolva. Például korlátozhatja a felhasználói hozzáférést a *Közösségi hálózatok* kategóriához vagy más kategóriákhoz.
- **Adattípus**. Például korlátozhatja egy felhasználó hozzáférését a webhely adataihoz, elrejthet képeket. A Kaspersky Endpoint Security a fájl formátuma alapján határozza meg az adattípust, nem pedig a kiterjesztése alapján.

  > A Kaspersky Endpoint Security nem vizsgálja a fájlokat az archívumokban. Például, ha képfájlok vannak egy archívumban, a Kaspersky Endpoint Security *Archívumok* adattípusként azonosítja azokat, nem pedig *Grafika*.

- **Egyedi címek**. Megadhat webcímet vagy használhat maszkokat.

Egyszerre több módszert is használhat a weboldalak elérésének szabályozására. Például korlátozhatja az *Office-alkalmazások fájljai* adattípus elérést a *Webalapú e-mail* webhely-kategória számára.

Weboldalhozzáférési szabályok

A Webfelügyelő szabályozza a weboldalakhoz történő hozzáférést a *hozzáférési szabályokkal*. A következő speciális beállításokat alkalmazhatja a weboldal hozzáférési szabályához:

- A felhasználók, akikre a szabály vonatkozik.

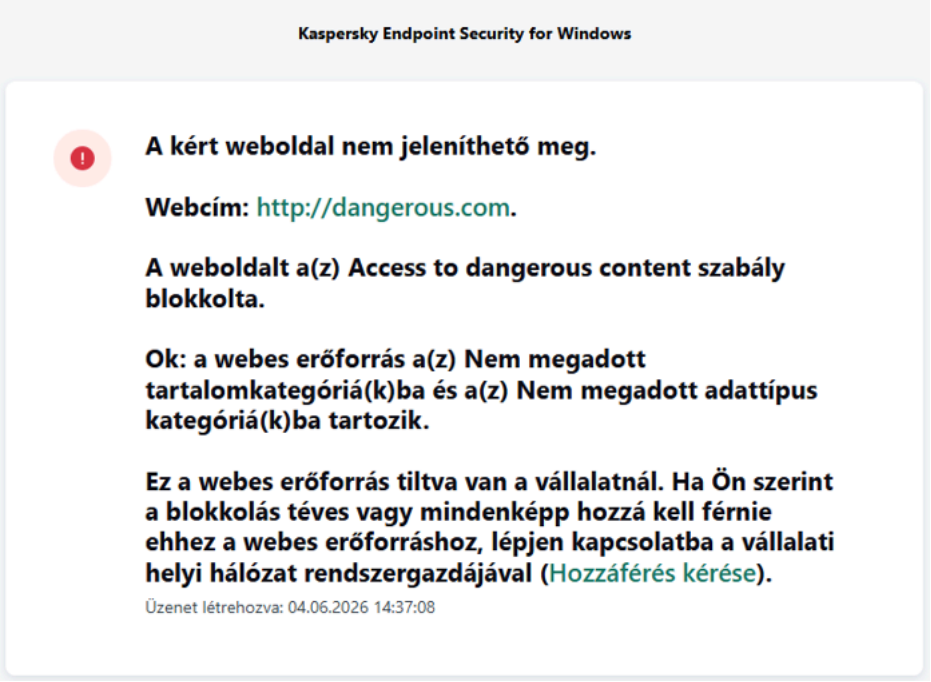
  Például korlátozhatja minden olyan felhasználó számára a böngészőn keresztül történő internetelérést, akik nem az IT osztályon vannak.

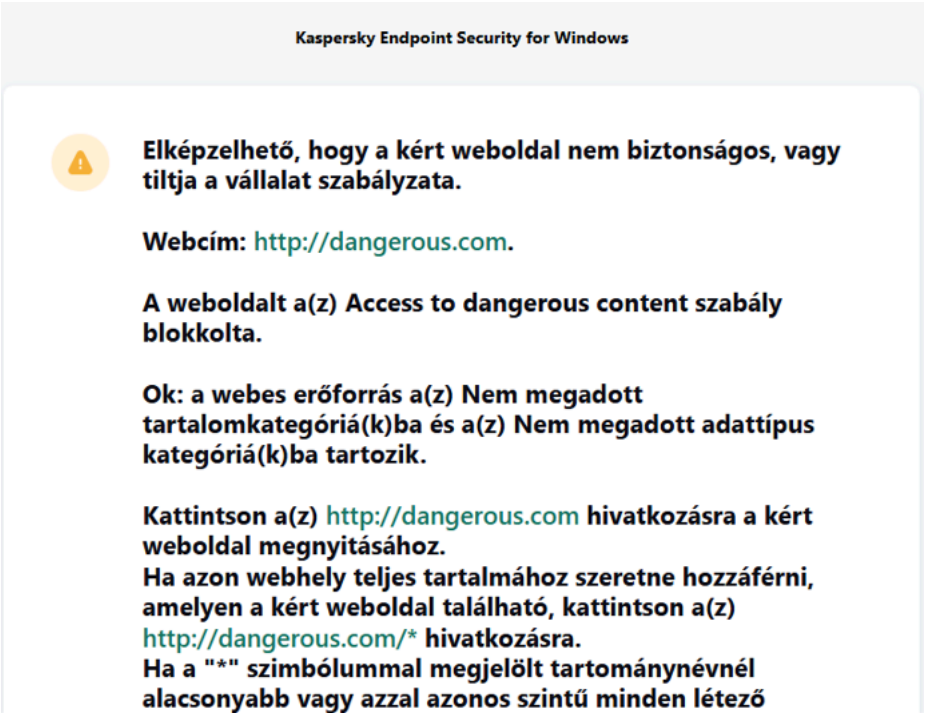
- Szabályütemezés.

  Korlátozhatja a böngészőn keresztül történő internetelérést a munkaidő alatt.

Hozzáférési szabály prioritásai

Minden szabálynak van valamilyen prioritása. Minél magasabban helyezkedik el egy szabály a szabályok listáján, annál magasabb a prioritása. Ha egy weboldal számos szabályhoz lett hozzáadva, a Webfelügyelő a legmagasabb prioritású szabály alapján szabályozza a weboldal elérését. Például, a Kaspersky Endpoint Security a vállalati portált közösségi hálózatként azonosíthatja. A közösségi hálózatok elérésének korlátozásához és a vállalati webportál elérésének biztosításához hozzon létre két szabályt: egy blokkoló szabályt, ami a *Közösségi hálózatok* weboldalkategóriára vonatkozik, és egy engedélyező szabályt, ami a vállalat webportáljára vonatkozik. A vállalati webportál hozzáférési szabályának magasabb prioritásúnak kell lennie, mint a közösségi hálózatok hozzáférési szabályának.





Webfelügyelő üzenet

Webes erőforrás hozzáférési szabályainak megadása

A *webes erőforrás hozzáférési szabálya* olyan szűrők és műveletek készlete, amelyeket a Kaspersky Endpoint Security akkor alkalmaz, amikor a felhasználók webes erőforrásokat keresnek fel. A hozzáférési szabályok tartalmazhatnak szabályütemezést.

Nem javasoljuk 1000-nél több szabály létrehozását webes erőforrások hozzáférésére vonatkozóan, mivel ekkor a rendszer instabillá válhat.

A webes erőforrások hozzáférési szabályai szűrők és olyan műveletek készletét adják meg, amelyeket a Kaspersky Endpoint Security akkor végez, ha a felhasználó a szabályban leírt webes erőforrásokat keres fel a szabály ütemezésében jelzett időszak folyamán. A szűrők révén pontosan megadhatja azon webes erőforrások készletét, amelyeknél a hozzáférést a Webfelügyelő összetevő szabályozza.

A következő szűrők állnak rendelkezésre:

- **Szűrés tartalom szerint**. A Webfelügyelő a webes erőforrásokat tartalom és adattípus szerint kategorizálja. A kategóriák által meghatározott típusokba tartozó tartalmú, illetve adattípusú webes erőforrásokhoz való felhasználói hozzáférés szabályozható. Ha a felhasználó a kiválasztott tartalmi és / vagy adattípus-kategóriába tartozó webes erőforrásokat keres fel, a Kaspersky Endpoint Security elvégzi a szabályban megadott műveletet.

- **Szűrés webes erőforrás címei szerint**. A felhasználó hozzáférése szabályozható az összes webes erőforrás, illetve egyes webes erőforrások és / vagy webes erőforrások csoportjai tekintetében.

  Ha tartalom szerinti és webes erőforrások címei szerinti szűrés van megadva, és a megadott webes erőforrások címei és / vagy webes erőforrások csoportjainak címei a kiválasztott tartalmi kategóriákhoz vagy adattípus-kategóriákhoz tartoznak, a Kaspersky Endpoint Security nem szabályozza a hozzáférést a kiválasztott tartalmi kategóriákban és / vagy adattípus-kategóriákban lévő összes webes erőforráshoz. Ehelyett az alkalmazás kizárólag a megadott webes erőforrás címeihez és / vagy webes erőforrások csoportjainak címeihez való hozzáférést szabályozza.

- **Szűrés felhasználók vagy felhasználói csoportok nevei szerint**. Megadhatja azoknak a felhasználóknak és / vagy felhasználócsoportoknak a neveit, akiknél a szabálynak megfelelően sor kerül a webes erőforrások szabályozására.

- **Szabályütemezés**. Megadhatja a szabály ütemezését. A szabály ütemezése szabja meg azt az időszakot, melynek során a Kaspersky Endpoint Security figyelemmel kíséri a szabály által lefedett webes erőforrásokhoz való hozzáférést.

A Kaspersky Endpoint Security telepítését követően a Webfelügyelő összetevő szabályainak listája nem üres. Az *Alapértelmezett szabály* előre be van állítva. Ez a szabály minden olyan webes erőforrásra alkalmazva lesz, amiket nem fed más szabály, és engedélyezi vagy letiltja ezeket az erőforrásokat a felhasználók számára.

Minden szabálynak van valamilyen prioritása. Minél magasabban helyezkedik el egy szabály a szabályok listáján, annál magasabb a prioritása. Ha egy weboldal számos szabályhoz lett hozzáadva, a Webfelügyelő a legmagasabb prioritású szabály alapján szabályozza a weboldal elérését. Például, a Kaspersky Endpoint Security a vállalati portált közösségi hálózatként azonosíthatja. A közösségi hálózatok elérésének korlátozásához és a vállalati webportál elérésének biztosításához hozzon létre két szabályt: egy blokkoló szabályt, ami a *Közösségi hálózatok* weboldalkategóriára vonatkozik, és egy engedélyező szabályt, ami a vállalat webportáljára vonatkozik. A vállalati webportál hozzáférési szabályának magasabb prioritásúnak kell lennie, mint a közösségi hálózatok hozzáférési szabályának.

Webes erőforrás hozzáférési szabályának hozzáadása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.

4. Jelölje be a **Webfelügyelő** jelölőnégyzetet.

5. A **Webfelügyelői beállítások** részen kattintson a **Hozzáadás** gombra.

   Megnyílik a **Szabály a webes erőforrásokhoz való hozzáféréshez** ablak.

6. Állítsa be a webes erőforrás hozzáférési szabályát (lásd az alábbi táblázatot).

7. Ha azt szeretné, hogy a Webfelügyelő a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Az aktív felhasználói munkamenetek megszüntetése a szabály alkalmazása után** jelölőnégyzetet.

   > A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

   Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

8. Mentse el a módosításokat.

Webes erőforrás hozzáférési szabályának hozzáadása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **Web Control** elemet.

5. Kapcsolja be az **Web Control ENABLED** kapcsolót.

6. A **Rules list** részen kattintson a **Add** gombra.

7. Állítsa be a webes erőforrás hozzáférési szabályát (lásd az alábbi táblázatot).

8. Ha azt szeretné, hogy a Webes felügyelet a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Terminate active user browser sessions after the rule is applied** jelölőnégyzetet.

   A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

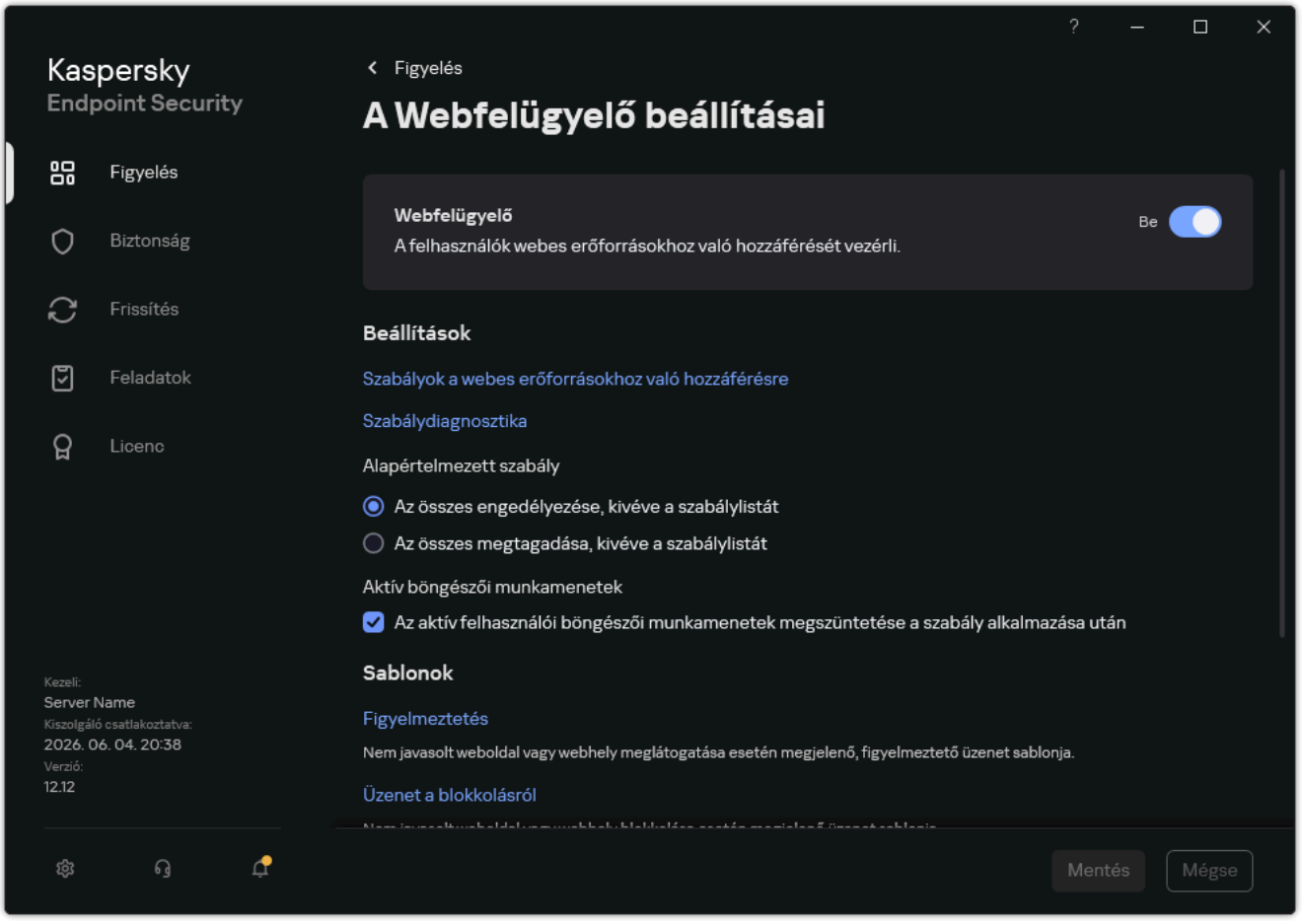
   Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

9. Mentse el a módosításokat.

Webes erőforrás hozzáférési szabályának hozzáadása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. Kapcsolja be a **Webfelügyelő** kapcsolót.

4. A **Beállítások** részen kattintson a **Szabályok a webes erőforrásokhoz való hozzáférésre** gombra.

5. Az ablakban kattintson a **Hozzáadás** gombra.

   Megnyílik a **Szabály a webes erőforrásokhoz való hozzáféréshez** ablak.

6. Állítsa be a webes erőforrás hozzáférési szabályát (lásd az alábbi táblázatot).

7. Ha azt szeretné, hogy a Webfelügyelő a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Az aktív felhasználói munkamenetek megszüntetése a szabály alkalmazása után** jelölőnégyzetet.

   > A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

   Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

8. Mentse el a módosításokat.

Ennek eredményeképpen az új webfelügyelői szabály bekerül a listába. Szükség esetén módosítsa a webfelügyelői szabály prioritását. Továbbá a kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát anélkül, hogy eltávolítaná azt a listáról.

Webfelügyelői szabályparaméterek

Paraméter	Leírás
Szabály neve	Webfelügyelői szabály neve.
Állapot	• **Be**. • **Ki**. A kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát.
Művelet	• **Engedélyezés**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést. • **Blokkolás**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet. • **Figyelmeztetés**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.
A szűrő tartalma	• **Tartalomkategória alapján**. Kategória (például *Közösségi hálózatok* kategória) szerint szabályozhatja a felhasználók hozzáférését a webes erőforrásokhoz. • **Adattípus alapján**. A webes erőforrásokhoz való felhasználói hozzáférést a közzétett adatok meghatározott adattípusa (például *Grafika*) alapján szabályozhatja.
Címek	• **Minden címre**. A Webfelügyelet nem fogja cím szerint szűrni a webes erőforrásokat. • **Egyedi címekre**. A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata. Ha a Titkosított kapcsolatok vizsgálata ki van kapcsolva, a HTTPS protokollnál csak kiszolgálónév szerint szűrhet.
Felhasználók	• **Minden felhasználónak**. A Webfelügyelet nem fogja szűrni a webes erőforrásokat az adott felhasználókhoz. • **Egyéni felhasználóknak és/vagy csoportoknak**. A Webfelügyelet csak az adott felhasználóknak fogja szűrni a webes erőforrásokat. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.
Szabályütemezés	A szabály ütemezése szabja meg azt az időszakot, melynek során a Kaspersky Endpoint Security figyelemmel kíséri a szabály által lefedett webes erőforrásokhoz való hozzáférést. Korlátozhatja a böngészőn keresztül történő internetelérést a munkaidő alatt.

Szűrés webes erőforrás címei szerint

Az egyes webes erőforrásokhoz való hozzáférés szabályozásához létre kell hoznia egy webfelügyeleti szabályt, létre kell hoznia a webcímek listáját, és ki kell választania egy webfelügyeleti műveletet. A webcímlista létrehozásakor megadhatja az URL-címeket, vagy használhat maszkokat.

A szabályok tartalmazhatnak egy szabályütemezést és azon felhasználók listáját, akikre a szabály vonatkozik. Például korlátozhatja a webhelyekhez való hozzáférést csak munkaidőben, vagy engedélyezheti a webhelyek látogatását bizonyos csoportok felhasználói számára.

Webes erőforrás címszűrőjének engedélyezése a felügyeleti konzolbon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.
4. Jelölje be a **Webfelügyelő** jelölőnégyzetet.
5. A **Webfelügyelői beállítások** részen kattintson a **Hozzáadás** gombra.

   Megnyílik a **Szabály a webes erőforrásokhoz való hozzáféréshez** ablak.

6. A webes erőforrások hozzáférési szabályának konfigurálása:

   a. A **Név** mezőben adja meg a szabály nevét.

   b. Az **Alkalmazás címekre** legördülő listában válassza az **Egyedi címekre** lehetőséget.

   c. Hozza létre a webes erőforrások címeinek listáját. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja.

      Ha a Titkosított kapcsolatok vizsgálata ki van kapcsolva, a HTTPS protokollnál csak kiszolgálónév szerint szűrhet.

   d. A **Felhasználókra való alkalmazás** legördülő listában válassza ki a felhasználókra vonatkozó szűrőt:

      - **Minden felhasználónak**. A Webfelügyelet nem fogja cím szerint szűrni a webes erőforrásokat.
      - **Egyéni felhasználóknak vagy csoportoknak**. A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   e. A **Művelet** legördülő listában válasszon egy lehetőséget:

      - **Engedélyezés**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
      - **Blokkolás**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet.
      - **Figyelmeztetés**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.

   f. A **Szabályütemezés** legördülő listában válasszon ki egy ütemezést, vagy hozzon létre egy új ütemezést.

7. Ha azt szeretné, hogy a Webfelügyelő a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Az aktív felhasználói munkamenetek megszüntetése a szabály alkalmazása után** jelölőnégyzetet.

   A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

   Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

8. Mentse el a módosításokat.

Webes erőforrás címszűrőjének engedélyezése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Web Control** elemet.
5. Kapcsolja be az **Web Control ENABLED** kapcsolót.
6. A **Rules list** részen kattintson a **Add** gombra.
7. A webes erőforrások hozzáférési szabályának konfigurálása:

   a. A **Rule name** mezőben adja meg a szabály nevét.

   b. A webes erőforrás hozzáférési szabályánál válassza a **Enabled** állapotot.

   A kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát anélkül, hogy eltávolítaná azt a listáról.

   c. A **Action** részen válassza ki a releváns opciót:

   - **Allow**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
   - **Block**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet.
   - **Inform**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.

   d. A **Scope** részen válassza a **Individual websites** elemet.

   e. A tartalomszűrő konfigurálása:

   - **Individual address**. Hozza létre a webes erőforrások címeinek listáját. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja.

     Ha a Titkosított kapcsolatok vizsgálata ki van kapcsolva, a HTTPS protokollnál csak kiszolgálónév szerint szűrhet.

   - **Data type**. A webes erőforrásokhoz való felhasználói hozzáférést a közzétett adatok meghatározott adattípusa (például *Grafika*) alapján szabályozhatja.

f. A(z) **User or group** területen válassza ki a felhasználókat, akikre azt szeretné, hogy a Webfelügyelő alkalmazza a szabályt.

A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

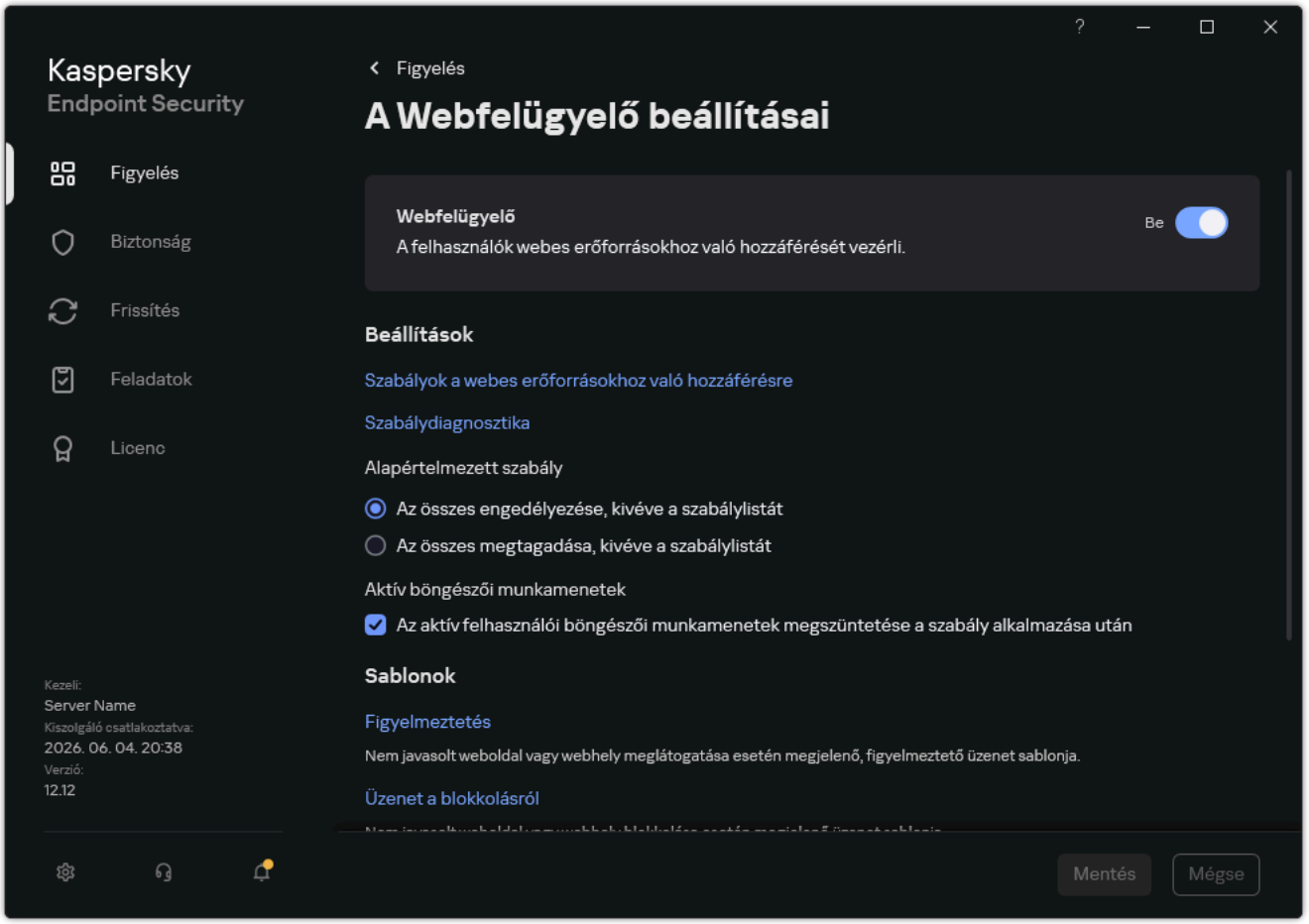
g. A **Access schedule** részen válasszon ki egy ütemezést, vagy hozzon létre egy új ütemezést.

8. Mentse el a módosításokat.

Webes erőforrás címszűrőjének engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. A **Beállítások** részen kattintson a **Szabályok a webes erőforrásokhoz való hozzáférésre** gombra.

4. Az ablakban kattintson a **Hozzáadás** gombra.

Megnyílik a **Szabály a webes erőforrásokhoz való hozzáféréshez** ablak.

5. A **Szabály neve** mezőben adja meg a szabály nevét.

6. A webes erőforrás hozzáférési szabályánál válassza a **Be** állapotot.

A kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát.

7. A **Művelet** blokkban válassza ki a releváns opciót:

   - **Engedélyezés**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
   - **Blokkolás**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet.
   - **Figyelmeztetés**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.

8. A **Címek** alatt válassza az **Egyedi címekre** lehetőséget.

   Hozza létre a webes erőforrások címeinek listáját. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja.

   > Ha a Titkosított kapcsolatok vizsgálata ki van kapcsolva, a HTTPS protokollnál csak kiszolgálónév szerint szűrhet.

9. A **Felhasználók** blokkban válassza ki a felhasználókra releváns szűrőt:

   - **Minden felhasználónak**. A Webfelügyelet nem fogja szűrni a webes erőforrásokat az adott felhasználókhoz.
   - **Egyéni felhasználóknak és/vagy csoportoknak**. A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

10. A **Szabályütemezés** legördülő listában válasszon ki egy ütemezést, vagy hozzon létre egy új ütemezést.

11. Ha azt szeretné, hogy a Webfelügyelő a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Az aktív felhasználói munkamenetek megszüntetése a szabály alkalmazása után** jelölőnégyzetet.

    > A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

    Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

12. Mentse el a módosításokat.

Ennek eredményeképpen az új webfelügyelői szabály bekerül a listába. Szükség esetén módosítsa a webfelügyelői szabály prioritását. Továbbá a kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát anélkül, hogy eltávolítaná azt a listáról.

Szűrés webes erőforrás tartalma szerint

A webes erőforrás tartalma szerinti hozzáférés szabályozásához a Webfelügyelő kategóriaszűrőt és adattípus-szűrőt biztosít.

A weboldalak a Kaspersky Security Network felhőszolgáltatás, a heurisztikus elemzés és az ismert weboldalak adatbázisai (köztük az alkalmazás-adatbázisok) alapján vannak besorolva. Például korlátozhatja a felhasználói hozzáférést a *Közösségi hálózatok* kategóriához vagy más kategóriákhoz.

Korlátozhatja a felhasználók hozzáférését egy webhelyhez az adatok típusa alapján, például képek elrejtése céljából. A Kaspersky Endpoint Security a fájl formátuma alapján határozza meg az adattípust, nem pedig a kiterjesztése alapján. A Webfelügyelő a következő adattípusokat különbözteti meg:

- Videó
- Hang
- Office-alkalmazások fájljai
- Végrehajtható fájlok
- Archívumok
- Grafika
- Parancsfájlok

A Kaspersky Endpoint Security nem vizsgálja a fájlokat az archívumokban. Például, ha képfájlok vannak egy archívumban, a Kaspersky Endpoint Security *Archívumok* adattípusként azonosítja azokat, nem pedig *Grafika*.

A szabályok tartalmazhatnak egy szabályütemezést és azon felhasználók listáját, akikre a szabály vonatkozik. Például korlátozhatja a webhelyekhez való hozzáférést csak munkaidőben, vagy engedélyezheti a webhelyek látogatását bizonyos csoportok felhasználói számára.

Webes erőforrás tartalomszűrőjének engedélyezése a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
4. Jelölje be a **Webfelügyelő** jelölőnégyzetet.
5. A **Webfelügyelői beállítások** részen kattintson a **Hozzáadás** gombra.

   Megnyílik a **Szabály a webes erőforrásokhoz való hozzáféréshez** ablak.

6. A webes erőforrások hozzáférési szabályának konfigurálása:

   a. A **Név** mezőben adja meg a szabály nevét.

   b. A **Tartalomszűrés** legördülő listában válassza ki a megfelelő tartalomszűrőt:

   - **Tartalomkategória alapján**. Kategória (például *Közösségi hálózatok* kategória) szerint szabályozhatja a felhasználók hozzáférését a webes erőforrásokhoz.
   - **Adattípus alapján**. A webes erőforrásokhoz való felhasználói hozzáférést a közzétett adatok meghatározott adattípusa (például *Grafika*) alapján szabályozhatja.
   - **Tartalomkategória és adattípus alapján**. A tartalomkategória és adattípus szerinti szűrők engedélyezve vannak.

   A szűrők kiválasztása után konfigurálja a szűrő paramétereit.

   c. A **Felhasználókra való alkalmazás** legördülő listában válassza ki a felhasználókra vonatkozó szűrőt:

   - **Minden felhasználónak**. A Webfelügyelet nem fogja cím szerint szűrni a webes erőforrásokat.
   - **Egyéni felhasználóknak vagy csoportoknak**. A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   d. A **Művelet** legördülő listában válasszon egy lehetőséget:

   - **Engedélyezés**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
   - **Blokkolás**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet.
   - **Figyelmeztetés**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.

   e. A **Szabályütemezés** legördülő listában válasszon ki egy ütemezést, vagy hozzon létre egy új ütemezést.

7. Ha azt szeretné, hogy a Webfelügyelő a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Az aktív felhasználói munkamenetek megszüntetése a szabály alkalmazása után** jelölőnégyzetet.

   A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

   Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

8. Mentse el a módosításokat.

Webes erőforrás tartalomszűrőjének engedélyezése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Web Control** elemet.
5. Kapcsolja be az **Web Control ENABLED** kapcsolót.
6. A **Rules list** részen kattintson a **Add** gombra.
7. A webes erőforrások hozzáférési szabályának konfigurálása:

   a. A **Rule name** mezőben adja meg a szabály nevét.

   b. A webes erőforrás hozzáférési szabályánál válassza a **Enabled** állapotot.

   A kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát.

   c. A **Action** részen válassza ki a releváns opciót:

   - **Allow**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
   - **Block**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet.
   - **Inform**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.

   d. A **Scope** részen válassza a **Content category** elemet.

   e. A tartalomszűrő konfigurálása:

   - **Content category**. Kategória (például *Közösségi hálózatok* kategória) szerint szabályozhatja a felhasználók hozzáférését a webes erőforrásokhoz.
   - **Data type**. A webes erőforrásokhoz való felhasználói hozzáférést a közzétett adatok meghatározott adattípusa (például *Grafika*) alapján szabályozhatja.

f. A(z) **User or group** területen válassza ki a felhasználókat, akikre azt szeretné, hogy a Webfelügyelő alkalmazza a szabályt.

A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

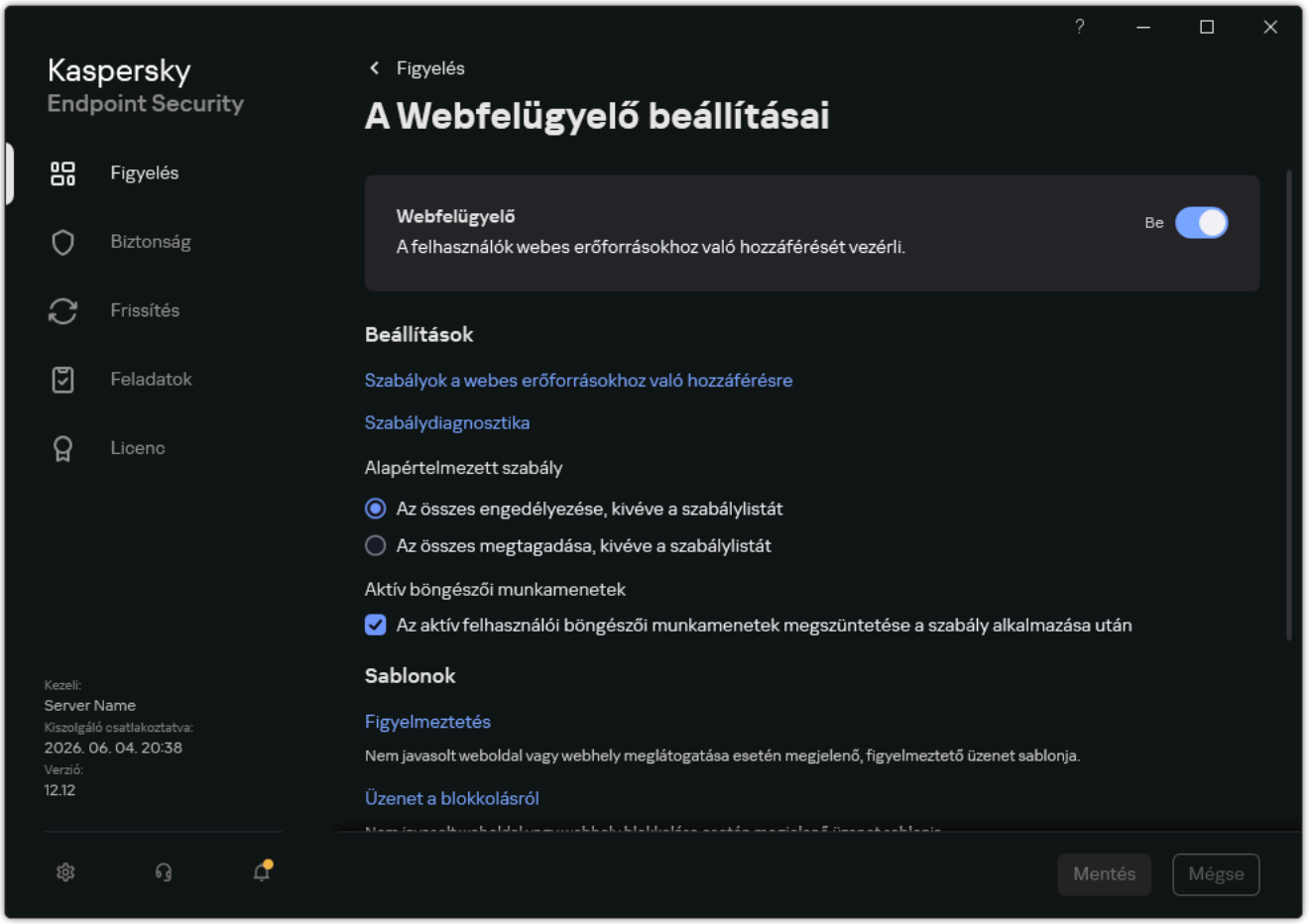
g. A **Access schedule** részen válasszon ki egy ütemezést, vagy hozzon létre egy új ütemezést.

8. Mentse el a módosításokat.

Webes erőforrás tartalomszűrőjének engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. A **Beállítások** részen kattintson a **Szabályok a webes erőforrásokhoz való hozzáférésre** gombra.

4. Az ablakban kattintson a **Hozzáadás** gombra.

Megnyílik a **Szabály a webes erőforrásokhoz való hozzáféréshez** ablak.

5. A **Szabály neve** mezőben adja meg a szabály nevét.

6. A webes erőforrás hozzáférési szabályánál válassza a **Be** állapotot.

A kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát.

7. A **Művelet** blokkban válassza ki a releváns opciót:

   - **Engedélyezés**. A Webfelügyelő engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
   - **Blokkolás**. A Webfelügyelő blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést, és megjeleníti a webhelyhez való hozzáférés megtagadása üzenetet.
   - **Figyelmeztetés**. Amikor a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely megfelel a szabálynak, a Webfelügyelő figyelmeztetést jelenít meg, hogy a webes erőforrás felkeresése nem ajánlott. A figyelmeztető üzenetben lévő hivatkozások segítségével a felhasználó hozzáférhet a kért webes erőforráshoz.

8. **A szűrő tartalma** részen válassza ki a kapcsolódó tartalomszűrőt:

   - **Tartalomkategória alapján**. Kategória (például *Közösségi hálózatok* kategória) szerint szabályozhatja a felhasználók hozzáférését a webes erőforrásokhoz.
   - **Adattípus alapján**. A webes erőforrásokhoz való felhasználói hozzáférést a közzétett adatok meghatározott adattípusa (például *Grafika*) alapján szabályozhatja.

   A tartalomszűrő konfigurálásához:

   a. Kattintson a **Beállítások** hivatkozásra.

   b. Jelölje be a jelölőnégyzeteket a kívánt tartalmi kategóriák és / vagy adattípusok nevei mellett.

   Ha egy tartalmi kategória és / vagy adattípus neve mellett lévő jelölőnégyzetet bejelöli, a Kaspersky Endpoint Security alkalmazza az adott tartalmi kategóriába és / vagy adattípushoz tartozó webes erőforrásokhoz való hozzáférést vezérlő szabályt.

   c. Térjen vissza az ablakhoz a webes erőforrás hozzáférési szabályának konfigurálásához.

9. A **Felhasználók** blokkban válassza ki a felhasználókra releváns szűrőt:

   - **Minden felhasználónak**. A Webfelügyelet nem fogja cím szerint szűrni a webes erőforrásokat.
   - **Egyéni felhasználóknak és/vagy csoportoknak**. A Webfelügyelet csak a listáról fogja szűrni a webes erőforrások címeit. Megadhat webcímet vagy használhat maszkokat. A webes erőforrás címek listáját TXT fájlból is exportálhatja. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata. Lista létrehozása azokról a felhasználókról, akikre alkalmazni szeretné a szabályt:

     a. Kattintson **Hozzáadás** gombra.

     b. A megnyíló ablakban jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, amelyekre alkalmazni szeretné a webes erőforrás hozzáférési szabályt.

     c. Térjen vissza az ablakhoz a webes erőforrás hozzáférési szabályának konfigurálásához.

10. Válassza ki a **Szabályütemezés** legördülő listán a szükséges ütemezés nevét, illetve állítson elő új ütemezést a kiválasztott szabályütemezés alapján. Ehhez:

    a. Kattintson **Szerkesztés vagy új hozzáadása** gombra.

    b. Az ablakban kattintson a **Hozzáadás** gombra.

c. A megnyíló ablakban írja be a szabályütemezés nevét.

d. Konfigurálja a webes erőforrások hozzáférési ütemezését a felhasználók számára.

e. Térjen vissza az ablakhoz a webes erőforrás hozzáférési szabályának konfigurálásához.

11. Ha azt szeretné, hogy a Webfelügyelő a házirend alkalmazása után azonnal megszakítsa a kapcsolatot a tiltott webes erőforrással, jelölje be **Az aktív felhasználói munkamenetek megszüntetése a szabály alkalmazása után** jelölőnégyzetet.

   A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza.

   Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.

12. Mentse el a módosításokat.

Ennek eredményeképpen az új webfelügyelői szabály bekerül a listába. Szükség esetén módosítsa a webfelügyelői szabály prioritását. Továbbá a kapcsolóval bármikor letilthatja a webes erőforrás hozzáférési szabályát anélkül, hogy eltávolítaná azt a listáról.

A webes erőforrások hozzáférési szabályainak tesztelése

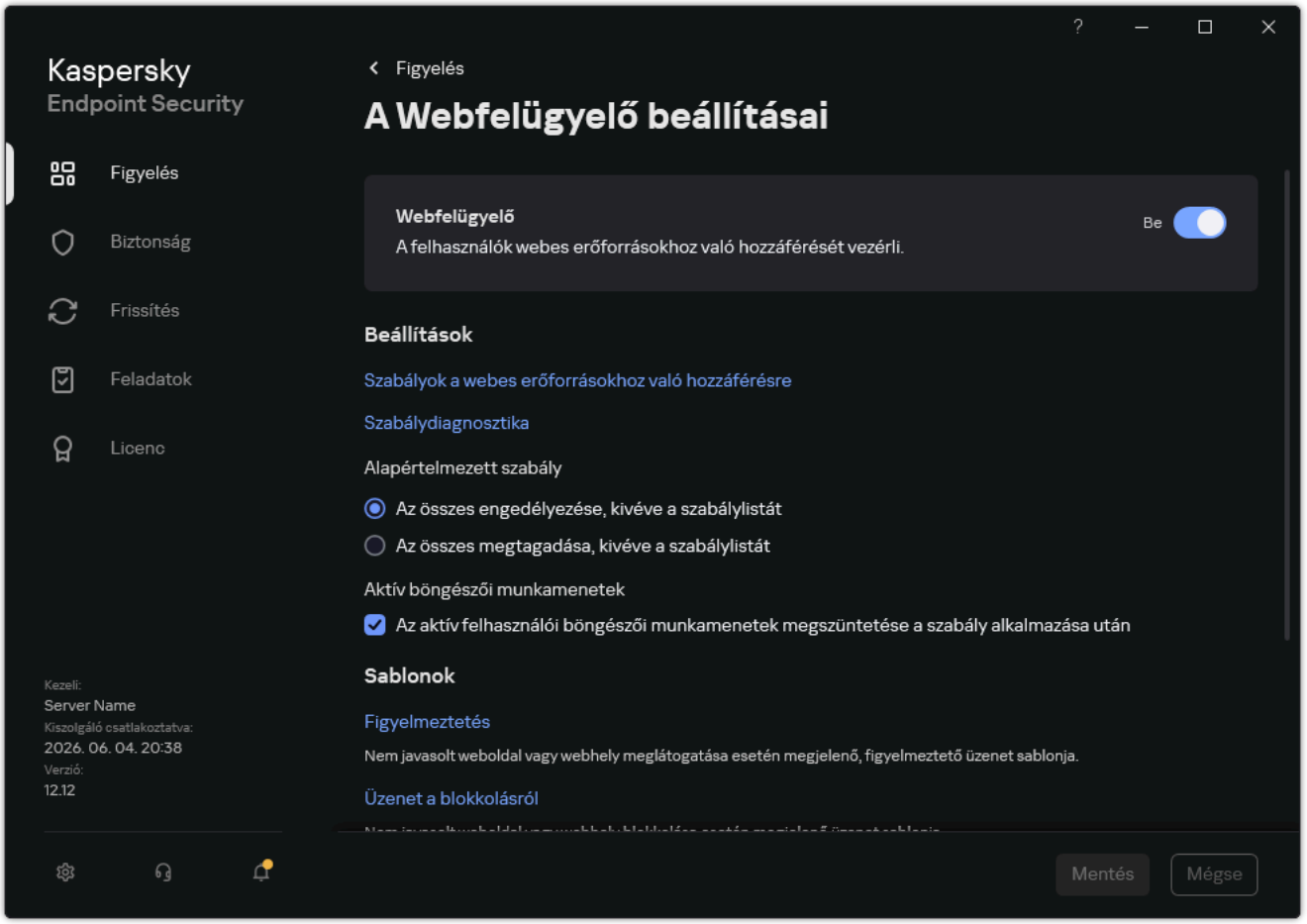
A Webfelügyelő konfigurálásakor előfordulhat, hogy Ön véletlenül blokkolja a felhasználóknak a munkájukhoz szükséges webes erőforrásokhoz való hozzáférést. Annak megállapításához, hogy melyik webfelügyelői szabály blokkolja a webes erőforrásokhoz való hozzáférést, használhatja a *Webfelügyelői szabálydiagnosztika* eszközt. A Webfelügyelői szabálydiagnosztika csak a Kaspersky Endpoint Security felületén érhető el. A Kaspersky Security Center konzolon nem lehet kideríteni, hogy egy adott erőforrást melyik webfelügyelői szabály tartalmaz.

Ha a felhasználó úgy véli, hogy a webes erőforrás tévedésből van blokkolva, akkor a blokkolásról szóló üzenet szövegében lévő hivatkozásra kattintva egy előre generált üzenetet küldhet a helyi vállalati hálózati rendszergazdának.

A webes erőforrások hozzáférési szabályainak tesztelése:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. A **Beállítások** blokkban kattintson a **Szabálydiagnosztika** hivatkozásra.

   Megnyílik a **Szabálydiagnosztika** ablak.

4. Ha tesztelni szeretné a Kaspersky Endpoint Security által egy adott webes erőforráshoz való hozzáférés vezérlésére használt szabályt, jelölje be a **Cím megadása** jelölőnégyzetet. Adja meg a webes erőforrás címét a lenti mezőben.

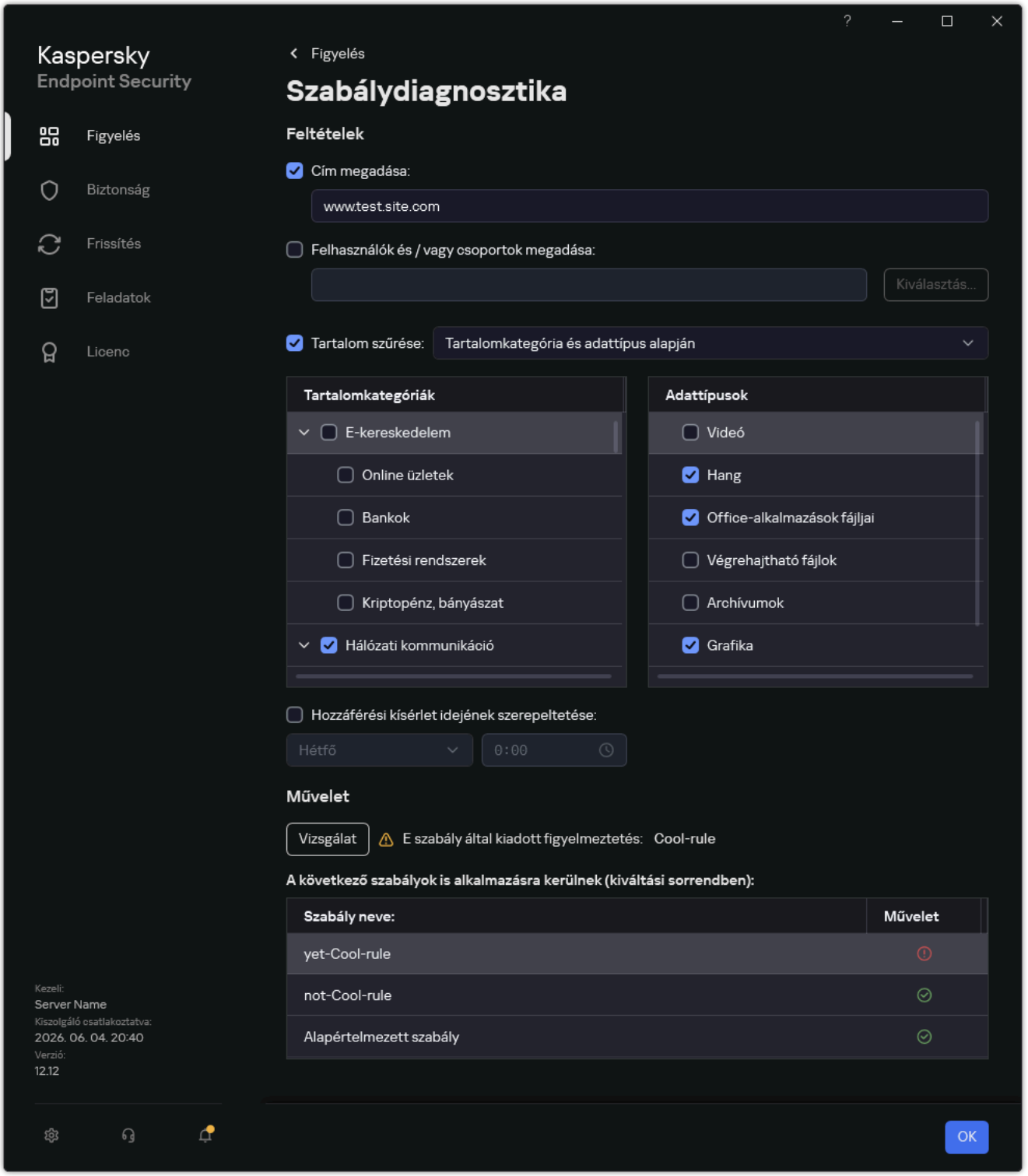
5. Ha azokat a szabályokat szeretné tesztelni, amelyeket a Kaspersky Endpoint Security a webes erőforrásokhoz való hozzáférés vezérlésére használ adott felhasználók és / vagy felhasználócsoportok esetén, adja meg a felhasználók és / vagy felhasználócsoportok listáját.

6. Ha azokat a szabályokat szeretné tesztelni, amelyeket a Kaspersky Endpoint Security bizonyos tartalomkategóriákba és/vagy adattípus-kategóriákba tartozó webes erőforrásokhoz való hozzáférés vezérlésére használ, jelölje be a **Tartalomszűrés** jelölőnégyzetet, és válassza ki a releváns opciót a legördülő listán (**Tartalomkategória alapján**, **Adattípus alapján**, illetve **Tartalomkategória és adattípus alapján**).

7. Ha a szabályokat úgy szeretné tesztelni, hogy a szabálydiagnosztikai feltételekben megadott webes erőforrásokhoz való hozzáférési kísérlet időpontja és a hét napja is rögzítésre kerüljön, akkor jelölje be a **Hozzáférési kísérlet idejének szerepeltetése** jelölőnégyzetet. Ezután adja meg a hét napját és az időt.

8. Kattintson a **Vizsgálat** gombra.

A teszt elvégzését követően megjelenik egy üzenet a Kaspersky Endpoint Security által végzett műveletről a megadott webes erőforráshoz való hozzáférési kísérlet által kiváltott első szabálynak megfelelően (engedélyezés, blokkolás vagy figyelmeztetés). Az első kiváltott szabály az a szabály, amely a Webfelügyelő szabályainak listáján magasabb helyen áll, mint a diagnosztikai feltételeknek megfelelő egyéb szabályok. Az üzenet a **Vizsgálat** gombtól jobbra jelenik meg. Az alábbi táblázat a fennmaradó kiváltott szabályokat sorolja fel, és megadja a Kaspersky Endpoint Security által végzett műveletet. A szabályok fordított prioritási sorrendben vannak felsorolva.



Webes erőforrás hozzáférési tesztjének eredménye

Web Control szabályok exportálása és importálása

A Webfelügyelő szabályainak listáját egy XML- vagy JSON-fájlba exportálhatja. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú cím hozzáadásával. Használhatja az exportálás/importálás funkciót a Webfelügyelő-szabályok biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A Webfelügyelő-szabályok listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
4. A Webfelügyelő-szabályok listájának exportálása:
   a. Jelölje ki az exportálni kívánt szabályokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
      Ha nem jelölt ki szabályt, a Kaspersky Endpoint Security az összes szabályt exportálja.
   b. Kattintson az **Exportálás** hivatkozásra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a szabályok listáját, és válassza a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security exportálja a szabályok listáját az XML-fájlba.
5. A Webfelügyelő-szabályok listájának importálása:
   a. Kattintson az **Import** hivatkozásra.
      A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.
   b. Nyissa meg a fájlt.
      Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
6. Mentse el a módosításokat.

A Webfelügyelő-szabályok listájának exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Web Control** elemet.

5. A szabályok listájának exportálása a **Rules list** területen:

   a. Jelölje ki az exportálni kívánt szabályokat.

   b. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a szabályok listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

6. A szabályok listájának importálása a **Rules list** területen:

   a. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a szabályok listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.

7. Mentse el a módosításokat.

A webfelügyelői szabályhoz tartozó webes erőforrás címeinek exportálása és importálása

Ha webes erőforrások hozzáférési szabályában elkészítette a webes erőforrások címeinek listáját, a listát exportálhatja fájlba:

- TXT formátumban a felügyeleti konzolon (MMC)
- CSV formátumban az alkalmazás felületén

Ezután ebből a fájlból importálhatja a listát, hogy ne kelljen kézileg új listát készítenie a webes erőforrások címeiről, amikor hozzáférési szabályt állít be. A webes erőforrások címeit tartalmazó lista exportálási és importálási lehetősége például akkor jöhet jól, ha hasonló paraméterekkel rendelkező hozzáférési szabályokat készít.

Az összes webfelügyelői szabály exportálható/importálható, nem csak az egyes szabályok webes erőforráscímei.

A webfelügyelői szabály webes erőforráscímei nem exportálhatók/importálhatók a Web Console-on vagy a Cloud Console-on.

A webfelügyelői szabály webes erőforráscímeinek exportálása/importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
4. A **Webfelügyelői beállítások** részen válassza ki azt a szabályt, amelynél a webes erőforrások címlistáját szeretné exportálni vagy importálni.

   Megjelennek a webfelügyelői szabály tulajdonságai.

5. A webes erőforrások listájának exportálásához tegye a következőket a címlistában:

   a. Jelölje ki az exportálni kívánt címeket.

      Ha nem jelölt ki címet, a Kaspersky Endpoint Security az összes címet exportálja.

   b. Kattintson az gombra.

   c. A megnyíló ablakban adja meg a TXT-fájl nevét, amelybe exportálni szeretné a webes erőforráscímek listáját, és válassza ki a fájl mentésére kiszemelt mappát.

   d. Mentse a fájlt.

      A Kaspersky Endpoint Security egy TXT-fájlba exportálja a webes erőforráscímek listáját.

6. A webes erőforrások listájának importálásához tegye a következőket a címlistában:

   a. Kattintson az gombra.

      A megnyíló ablakban válassza ki azt a TXT-fájlt, amelyből importálni szeretné a webes erőforrások listáját.

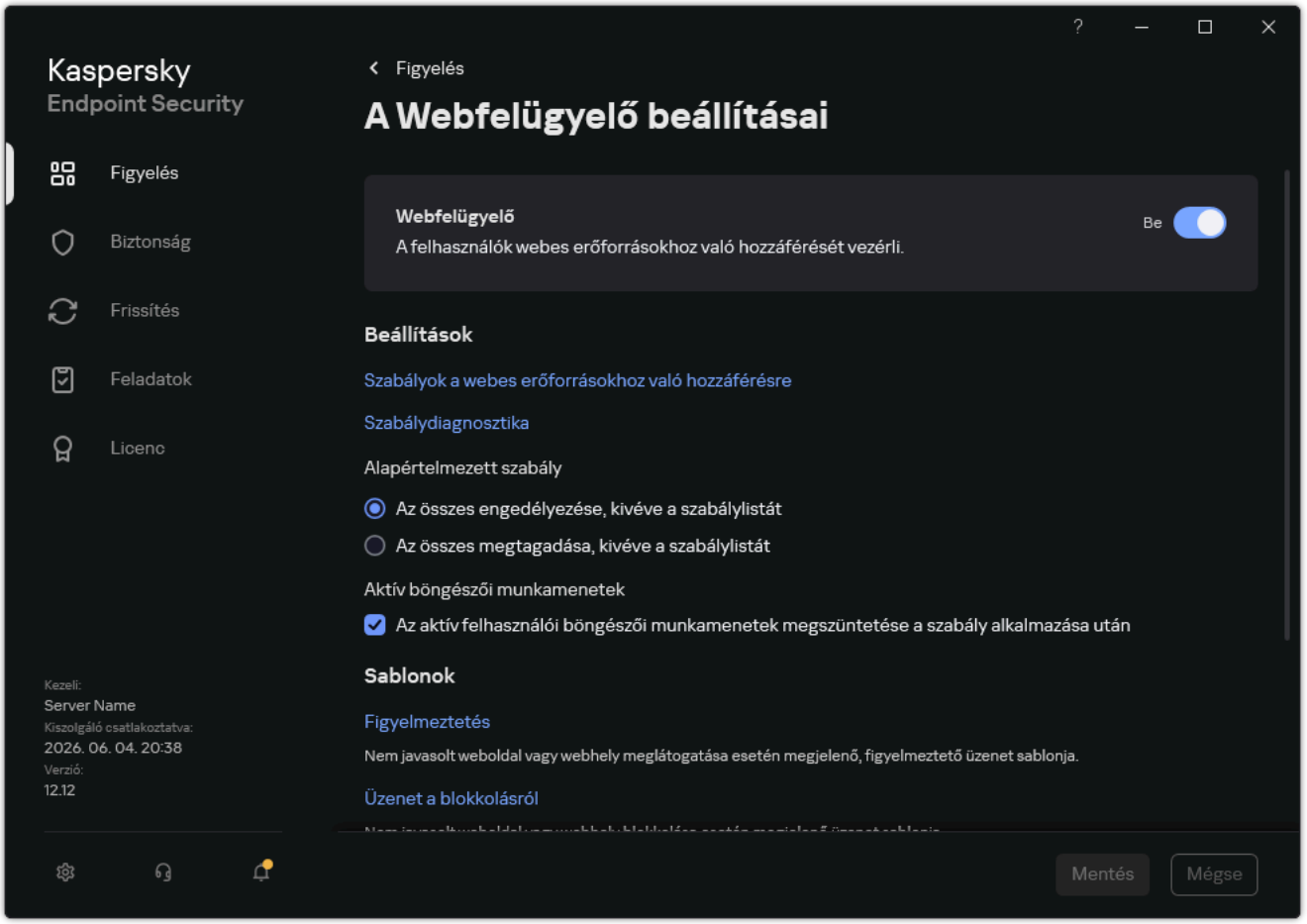
   b. Nyissa meg a fájlt.

      Ha a számítógépen már létezik egy lista a címekről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a TXT-fájlból.

7. Mentse el a módosításokat.

A webfelügyelői szabály webes erőforráscímeinek exportálása/importálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. A **Beállítások** részen kattintson a **Szabályok a webes erőforrásokhoz való hozzáférésre** gombra.
4. Válassza ki azt a szabályt, amelynél a webes erőforrások címlistáját szeretné exportálni vagy importálni.
5. A megbízható webcímek listájának exportálásához tegye a következőket a **Címek** blokkban:
   a. Jelölje ki az exportálni kívánt címeket.
      Ha nem jelölt ki címet, a Kaspersky Endpoint Security az összes címet exportálja.
   b. Kattintson az **Export** gombra.
   c. A megnyíló ablakban adja meg a CSV-fájl nevét, amelybe exportálni szeretné a webes erőforráscímek listáját, és válassza ki a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security egy CSV-fájlba exportálja a webes erőforráscímek listáját.
6. A webes erőforrások listájának importálásához tegye a következőket a **Címek** blokkban:
   a. Kattintson az **Import** gombra.
      A megnyíló ablakban válassza ki azt a CSV-fájlt, amelyből importálni szeretné a webes erőforrások listáját.

b. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a címekről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a CSV-fájlból.

7. Mentse el a módosításokat.

A felhasználó internetes tevékenységének megfigyelése

A Kaspersky Endpoint Security segítségével naplózhatja a weboldalak látogatását, köztük az engedélyezett weboldalakét is. Ezzel a böngészőben a megtekintések teljes előzményét láthatja. A Kaspersky Endpoint Security felhasználói tevékenység-eseményeket küld a Kaspersky Security Center, a Kaspersky Endpoint Security helyi naplója és a Windows eseménynapló számára. Ahhoz, hogy eseményeket kapjon a Kaspersky Security Centerben, először meg kell adnia az események beállításait az Adminisztrációs konzol vagy a Webfelügyelő rendszabályaiban. Beállíthatja a Webfelügyelő eseményeinek e-mailben történő átvitelét is, valamint a felhasználó számítógépén, a képernyőn lévő értesítések megjelenítését is.

A figyelési funkciót támogató böngészők: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. A felhasználói tevékenység figyelése más böngészőkben nem működik.

A Kaspersky Endpoint Security a következő internetes felhasználói tevékenységeket hozza létre:

- Weboldal blokkolása (*Critical* állapot ⓘ).
- Látogasson meg egy nem javasolt weboldalt (*Warning* állapot ⚠).
- Engedélyezett weboldal meglátogatása (*Info* állapot ⓘ).

A felhasználó internetes tevékenysége figyelésének engedélyezése előtt a következőket kell tennie:

- Injektáljon be egy weboldal-interakciós parancsfájlt a webes forgalomba (lásd az alábbi utasításokat). A parancsfájl lehetővé teszi a Webfelügyelő események regisztrációját.
- A HTTPS forgalom megfigyeléséhez engedélyeznie kell a titkosított kapcsolatok vizsgálatát.

Weboldal interakciós parancsfájl beillesztése

Weboldal interakciós parancsfájl beillesztése a webes forgalomba a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
4. A **Titkosított kapcsolatok vizsgálata** szakaszban jelölje be a **Szkript beillesztése a webforgalomba a weboldalakkal való interakcióhoz** jelölőnégyzetet.
5. Mentse el a módosításokat.

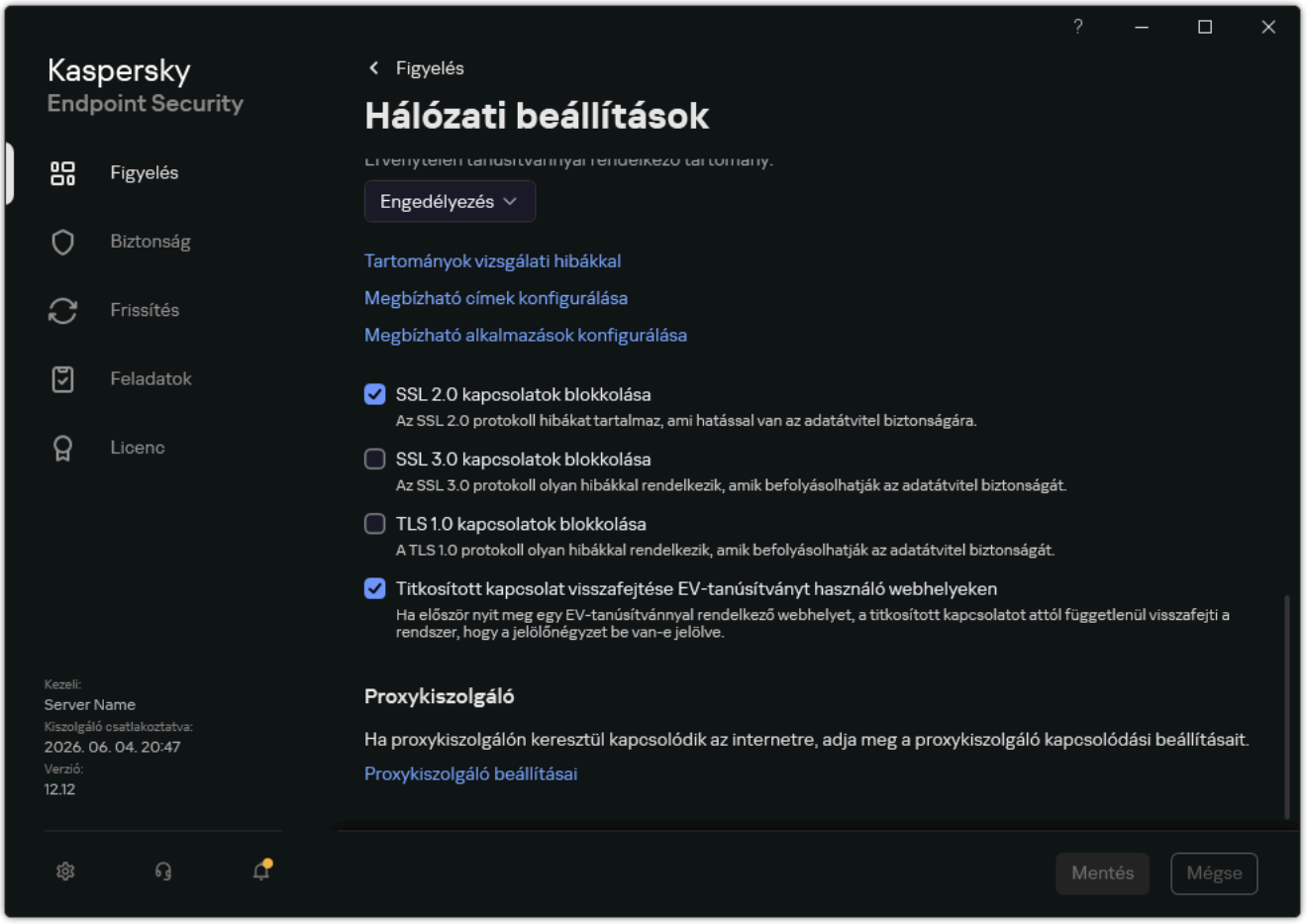
Weboldal interakciós parancsfájl beillesztése a webes forgalomba a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. A házirend ablakban válassza ki az **General Settings** → **Network Settings** lehetőséget.
5. A(z) **Monitoring of internet connections** területen kapcsolja be a(z) **Monitoring of internet connections ENABLED** kapcsolót.
6. Mentse el a módosításokat.

Weboldal interakciós parancsfájl beillesztése a webes forgalomba az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.



Alkalmazások hálózati beállításai

3. A **Forgalom feldolgozása** szakaszban jelölje be a **Szkript beillesztése a webforgalomba a weboldalakkal való interakcióhoz** jelölőnégyzetet.
4. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Endpoint Security beinjektál egy weboldal-interakciós parancsfájlt a webes forgalomba. Ez a parancsfájl lehetővé teszi a Webfelügyelő események regisztrációját az alkalmazás eseménynaplójában, az operációs rendszer eseménynaplójában és a jelentésekben.

A Web Control-események naplózásának konfigurálása

A Webfelügyelő eseményeinek naplózásához a felhasználók számítógépein:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
3. Az **Értesítések** részen kattintson az **Értesítések konfigurálása** gombra.
4. A megnyíló ablakban válassza a **Webfelügyelő** részt.

   Ez megnyitja a Webfelügyelő eseményeinek és az értesítési módszereknek a táblázatát.
5. Adjon meg értesítési módszert az egyes eseményekhez: **Mentés a helyi jelentésbe** vagy **Mentés a Windows eseménynaplóba**.

   Az engedélyezett weboldalak látogatásainak naplózásához a Webfelügyelőt is be kell állítania (lásd az alábbi utasítást).

   Az események táblázatban engedélyezheti a képernyőn lévő értesítést és az e-mail értesítést is. Ahhoz, hogy e-mailben küldjön értesítéseket, meg kell adnia az SMTP szerver beállításait. Az e-mailben történő értesítésküldéssel kapcsolatban lásd: Kaspersky Security Center Súgó.
6. Mentse el a módosításokat.

Ennek eredményeképp a Kaspersky Endpoint Security naplózni kezdi a felhasználó internetes tevékenységeit.

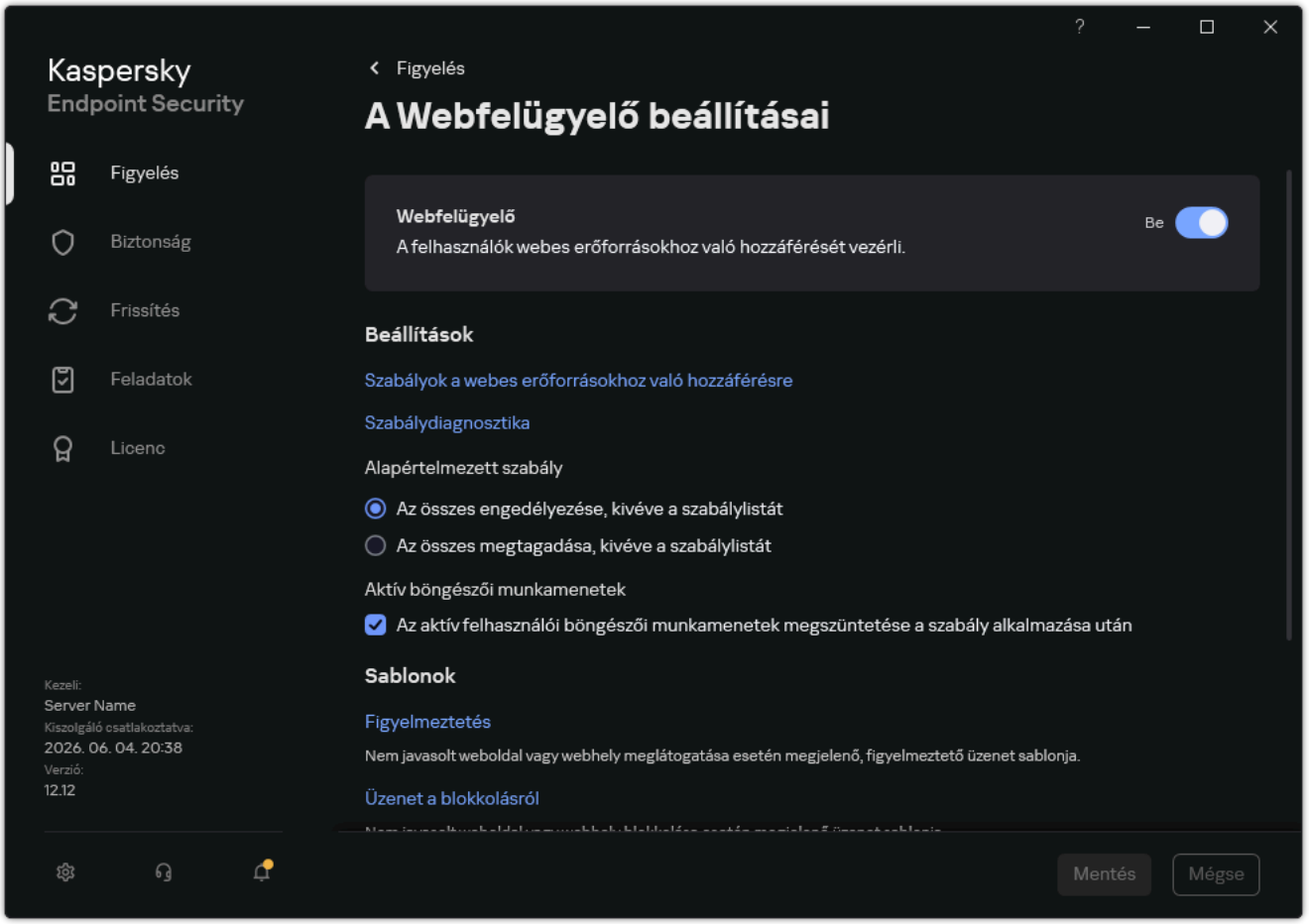
A Webfelügyelő felhasználói tevékenységi eseményeket küld a Kaspersky Security Centernek a következőknek megfelelően:

- Ha Ön a Kaspersky Security Centert használja, a Webfelügyelő eseményt küld minden olyan objektumhoz, amelyből a weblap áll. Ezért számos esemény is létre lehet hozva, amikor egy weboldal blokkolva volt. Például a http://www.example.com weboldal blokkolása esetén a Kaspersky Endpoint Security továbbíthat eseményeket a következő objektumoknak: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js stb.
- Ha Ön a Kaspersky Security Center Cloud Console-t használja, a Webfelügyelő csoportba rendezi az eseményeket, és csak a webhely protokollját és tartományát küldi el. Ha például egy felhasználó megnyitja a http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery nemkívánatos weboldalt, a Kaspersky Endpoint Security csak egy eseményt küld, a http://www.example.com objektummal.

Események naplózása engedélyezett webhelyek meglátogatásakor

Események naplózásának engedélyezése engedélyezett webhelyek meglátogatásakor:

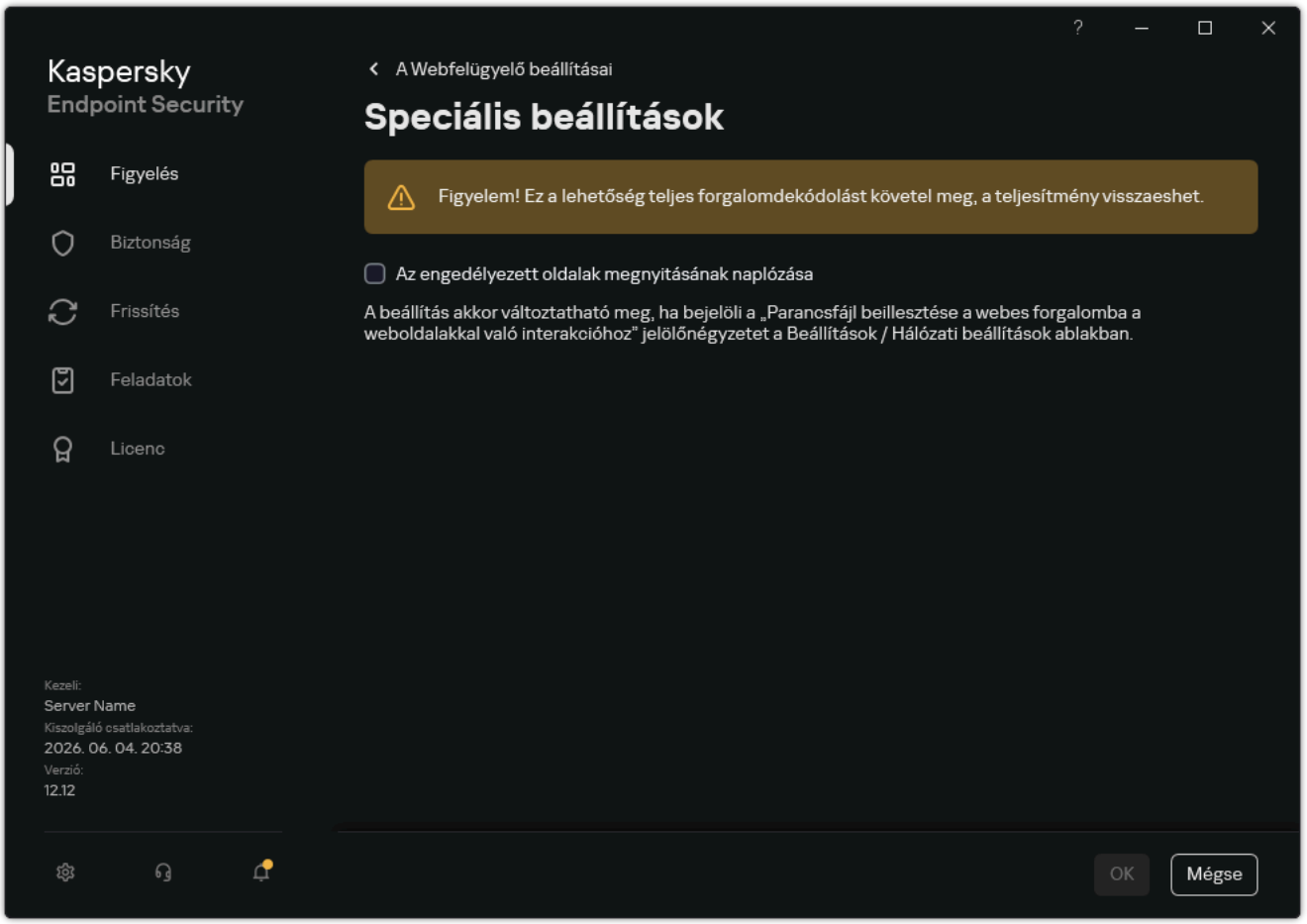
1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. A **További** szakaszban kattintson a **Speciális beállítások** gombra.

4. A megnyíló ablakban válassza **Az engedélyezett oldalak megnyitásának naplózása** jelölőnégyzetet.



A Webfelügyelő speciális beállításai

5. Mentse el a módosításokat.

Ennek eredményeképpen meg fogja tudni tekinteni a böngésző teljes előzményét.

A Webfelügyelő üzenetsablonjainak szerkesztése

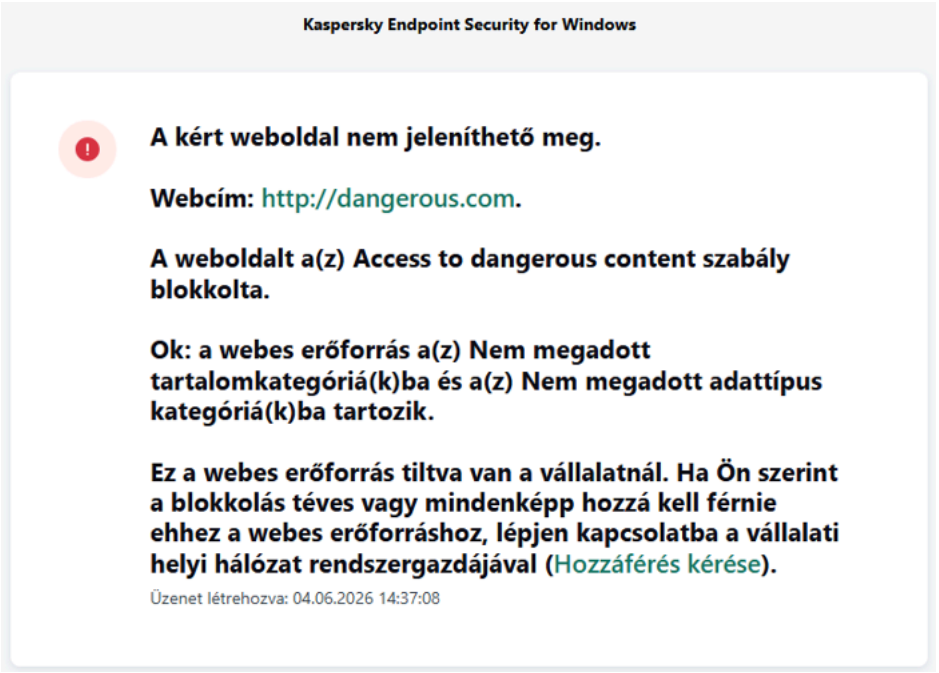
A Webfelügyelő szabályainak tulajdonságaiban megadott művelet típusától függően a Kaspersky Endpoint Security az alábbi típusú üzenetek egyikét jeleníti meg, ha a felhasználó internetes erőforrásokhoz próbál hozzáférni (az alkalmazás felváltja azt üzenetet tartalmazó HTML oldallal a HTTP kiszolgáló válaszát):

- Figyelmeztető üzenet. Ez az üzenet figyelmezteti a felhasználót, hogy a webes erőforrást nem ajánlott felkeresni és / vagy ellentétes a vállalati biztonsági szabályzattal. A Kaspersky Endpoint Security akkor jelenít meg figyelmeztető üzenetet, ha a **Figyelmeztetés** lehetőség van kiválasztva a webes erőforrást leíró szabály beállításaiban.

  Ha a felhasználó úgy véli, hogy a figyelmeztető üzenetet tévedés, akkor a figyelmeztetés szövegében lévő hivatkozásra kattintva üzenetet küldhet a helyi vállalati hálózati rendszergazdának.

- Webes erőforrás blokkolásáról tájékoztató üzenet. A Kaspersky Endpoint Security akkor jelenít meg webes erőforrás blokkolásáról tájékoztató üzenetet (lásd az alábbi ábrát), ha a **Blokkolás** lehetőség van kiválasztva a webes erőforrást leíró szabály beállításaiban.

Ha a felhasználó úgy véli, hogy a webes erőforrás tévedésből van blokkolva, akkor a blokkolásról szóló üzenet szövegében lévő hivatkozásra kattintva üzenetet küldhet a helyi vállalati hálózati rendszergazdának.



Üzenet a webes erőforrás blokkolásról

Külön sablonok állnak rendelkezésre a figyelmeztető üzenethez, a webes erőforrás blokkolásáról tájékoztató üzenethez, illetve ahhoz, amelyet a rendszergazda kap. Az üzenetsablonok kezeléséhez speciális változók állnak rendelkezésre (pl. `%USER_NAME%`). A változók lehetővé teszik egyetlen üzenetsablon használatát a különböző számítógépeken. Üzenet generálásakor a Kaspersky Endpoint Security lekéri a változó értékét az operációs rendszer beállításaiból, és beilleszti azt az adott számítógéphez, felhasználóhoz és eseményhez tartozó üzenetbe.

A Webfelügyelő üzenetsablonjának módosítása az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
4. A megnyíló **Sablonok** részen kattintson az **Üzenetsablon beállításai** gombra.
5. A Webfelügyelő üzenetsablonjainak konfigurálása:

   - **Figyelmeztetés**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely nem kívánatos webes erőforráshoz való hozzáférési próbálkozásra figyelmeztet.
   - **Üzenet a blokkolásról**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely blokkolja a hozzáférést a webes erőforráshoz.
   - **Üzenet a rendszergazdának**. A LAN rendszergazda részére küldendő üzenet sablonját tartalmazza, ha a felhasználó egy blokkolást tévedésnek tekint. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Weboldal hozzáférésének blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

Az alapértelmezett sablonszöveget az **Alapértelmezés szerint** gombra kattintva is visszaállíthatja.

6. Mentse el a módosításokat.

A Webfelügyelői üzenetsablonjának módosítása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **Web Control** elemet.

5. Az **Message templates** részen kattintson az **Message about website blocking** hivatkozásra, és konfigurálja a sablonokat az Webfelügyelő üzeneteihez:

   - **Warning**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely nem kívánatos webes erőforráshoz való hozzáférési próbálkozásra figyelmeztet.

   - **Message about blocking**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely blokkolja a hozzáférést a webes erőforráshoz.

   - **Message to administrator**. A LAN rendszergazda részére küldendő üzenet sablonját tartalmazza, ha a felhasználó egy blokkolást tévedésnek tekint. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Weboldal hozzáférésének blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Add variable** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

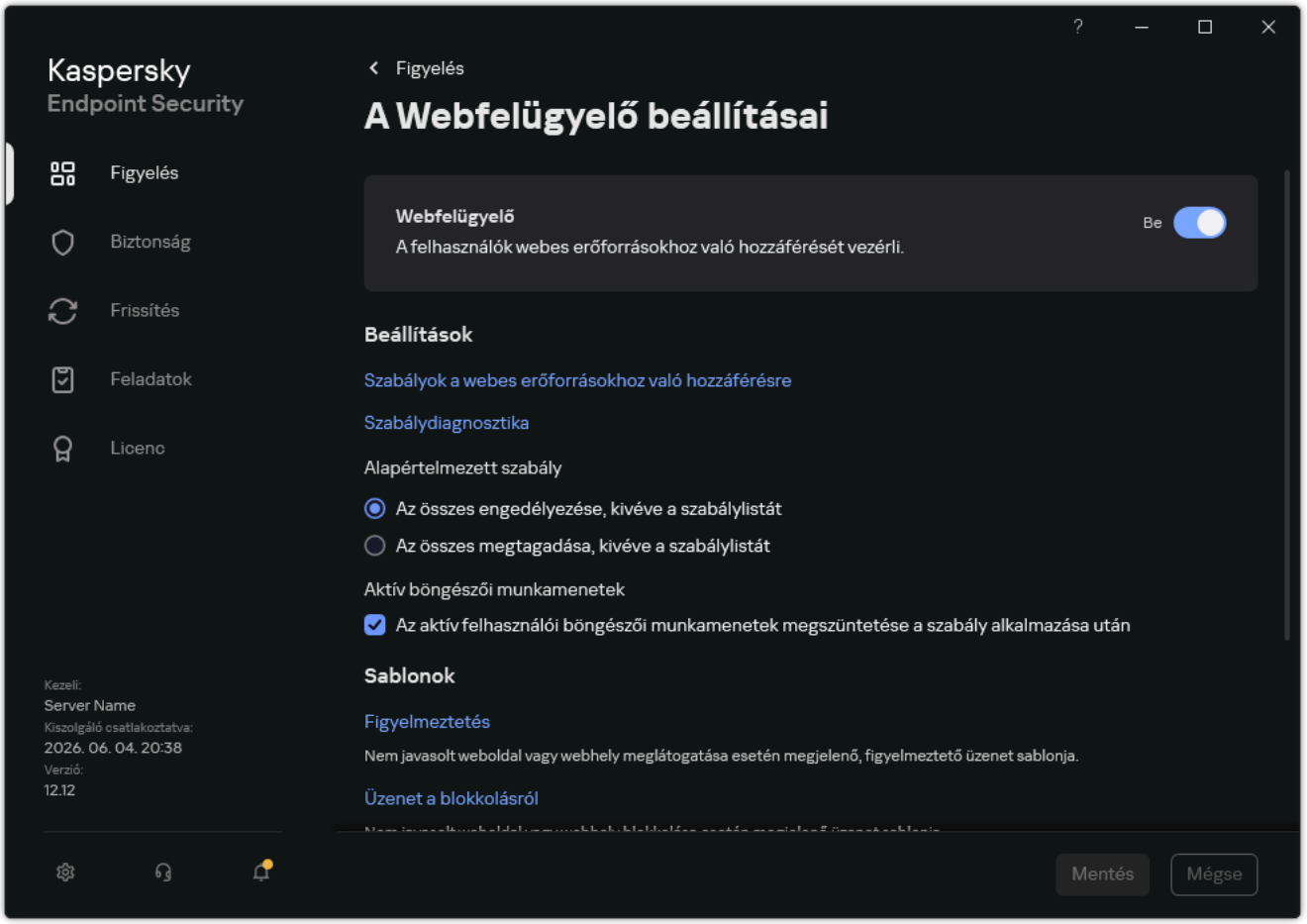
   Az alapértelmezett sablonszöveget a(z) **Reset to default** gombra kattintva is visszaállíthatja.

6. Mentse el a módosításokat.

A Webfelügyelő üzenetsablonjának módosítása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Webfelügyelő** lehetőséget.



Webfelügyelői beállítások

3. A **Sablonok** blokkban konfigurálja a sablonokat az Webfelügyelő üzeneteihez:

   - **Figyelmeztetés**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely nem kívánatos webes erőforráshoz való hozzáférési próbálkozásra figyelmeztet.

   - **Üzenet a blokkolásról**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely blokkolja a hozzáférést a webes erőforráshoz.

   - **Üzenet a rendszergazdának**. A LAN rendszergazda részére küldendő üzenet sablonját tartalmazza, ha a felhasználó egy blokkolást tévedésnek tekint. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Weboldal hozzáférésének blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó hozzáadása** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Az alapértelmezett sablonszöveget a **Visszaállítás** gombra kattintva is visszaállíthatja.

4. Mentse el a módosításokat.

Webes erőforrások címei maszkjainak használata

A *webes erőforrások címmaszkjának* (más néven „címmaszk”) használata akkor jöhet jól, ha a webes erőforrások hozzáférési szabályának létrehozásakor sok hasonló címet kell megadnia. Jól megtervezve egyetlen címmaszk webes erőforrások nagy számú címét válthatja ki.

A címmaszk megtervezésekor tartsa be az alábbi szabályokat:

1. A `*` karakter egy vagy több karaktert tartalmazó bármilyen sorozatot helyettesít.

   Ha például a címmaszkba az `*abc*` szöveget írja be, akkor a hozzáférési szabály minden olyan webes erőforrásra vonatkozik, amelyben megtalálható az `abc` karaktersorozat. Példa: `http://www.example.com/page_0-9abcdef.html`.

2. A `*.` karakterek (más néven *tartománymaszk*) lehetővé teszik a cím összes tartományának kiválasztását. A `*.` tartománymaszk bármilyen tartománynevet, altartománynevet vagy üres sort jelöl.

   Példa: a `*.example.com` maszk a következő címeket jelöli:

   - `http://pictures.example.com`. A `*.` tartománymaszk a következőt jelöli: `pictures.`.
   - `http://user.pictures.example.com`. A `*.` tartománymaszk a következőket jelöli: `pictures.` és `user.`.
   - `http://example.com`. A `*.` tartománymaszk üres sorként értelmezendő.

3. A címmaszk elején álló `www.` karaktersorozatot a rendszer `*.` sorozatként értelmezi.

   Példa: a `www.example.com` címmaszkot a rendszer `*.example.com` címmaszkként kezeli. Ez a maszk a `www2.example.com` és a `www.pictures.example.com` címeket jelöli.

4. Ha egy címmaszk nem `*` karakterrel kezdődik, akkor a címmaszk tartalma megegyezik a `*.` előtaggal ellátott azonos tartalommal.

5. Ha egy címmaszk `/` vagy `*` karaktertől eltérő karakterre végződik, akkor a címmaszk tartalma megegyezik `/*` utótaggal ellátott azonos tartalommal.

   Példa: a `http://www.example.com` címmaszk lefedi az olyan címeket, mint a `http://www.example.com/abc`, ahol az `a`, `b` és `c` bármilyen karakter lehet.

6. Ha egy címmaszk `/` karakterre végződik, akkor a címmaszk tartalma megegyezik a `/*` utótaggal ellátott azonos tartalommal.

7. A címmaszk végén lévő `/*` karaktersorozatot a rendszer `/*` karakterekként vagy üres karakterláncként értelmezi.

8. A webes erőforrások címeinek ellenőrzése címmaszk alapján történik, figyelembe véve a protokollt is (http vagy https):

   - Ha a címmaszkban nem szerepel a hálózati protokoll, akkor bármilyen hálózati protokollt tartalmazó címeket lefedi.

     Példa: az `example.com` címmaszk a `http://example.com` és a `https://example.com` címeket fedi le.

- Ha a címmaszkban szerepel a hálózati protokoll, akkor csak az ilyen hálózati protokollt tartalmazó címeket fedi le.

  Példa: a `http://*.example.com` címmaszk magában foglalja a `http://www.example.com` címet, de a `https://www.example.com` címet nem.

9. A kettős idézőjelben szereplő címmaszkot a rendszer további behelyettesítések nélkül kezeli, kivéve a `*` karaktert, ha az az elején szerepel a címmaszkban. Az 5. és 7. szabály nem vonatkozik a kettős idézőjelbe tett címmaszkokra (lásd a lenti táblázatban a 14–18. példákat).

10. A címmaszkok és webes erőforrások összevetésekor a rendszer nem veszi figyelembe a felhasználónevet és jelszót, a kapcsolódási portot és a kis- vagy nagybetűs írásmódot.

Példák a szabályok használatára a címmaszkok létrehozása során

Szám	Címmaszk	Webes erőforrások ellenőrzendő címe	Lefedi a címet a címmaszk?	Megjegyzés
1	*.pelda.com	http://www.123example.com	Nem	Lásd: 1. szabály.
2	*.pelda.com	http://www.123.example.com	Igen	Lásd: 2. szabály.
3	*pelda.com	http://www.123example.com	Igen	Lásd: 1. szabály.
4	*pelda.com	http://www.123.example.com	Igen	Lásd: 1. szabály.
5	http://www.*.pelda.com	http://www.123example.com	Nem	Lásd: 1. szabály.
6	www.pelda.com	http://www.pelda.com	Igen	Lásd: 3., 2., 1. szabály.
7	www.pelda.com	https://www.pelda.com	Igen	Lásd: 3., 2., 1. szabály.
8	http://www.*.pelda.com	http://123.pelda.com	Igen	Lásd: 3., 4., 1. szabály.
9	www.pelda.com	http://www.example.com/abc	Igen	Lásd: 3., 5., 1. szabály.
10	pelda.com	http://www.pelda.com	Igen	Lásd: 3., 1. szabály.
11	http://pelda.com/	http://pelda.com/abc	Igen	Lásd: 6. szabály.
12	http://pelda.com/*	http://example.com	Igen	Lásd: 7. szabály.
13	http://example.com	https://pelda.com	Nem	Lásd: 8. szabály.
14	"pelda.com"	http://www.pelda.com	Nem	Lásd: 9. szabály.
15	„http://www.pelda.com”	http://www.example.com/abc	Nem	Lásd: 9. szabály.
16	"*.pelda.com"	http://www.pelda.com	Igen	Lásd: 1., 9. szabály.
17	"http://www.pelda.com/*"	http://www.example.com/abc	Igen	Lásd: 1., 9. szabály.
18	"www.pelda.com"	http://www.pelda.com; https://www.pelda.com	Igen	Lásd: 9., 8. szabály.
19	www.pelda.com/abc/123	http://www.example.com/abc	Nem	A címmaszk a webes erőforrás címénél több információt tartalmaz.

Webfelügyelő virtuális gépekhez

A Webfelügyelő a számítógépen és az azon helyileg telepített virtuális gépen is ellenőrzi a forgalmat. Ez anélkül működik, hogy a Kaspersky Endpoint Security alkalmazást telepítenie kellene a helyi virtuális gépre. Ez azt jelenti, hogy ha a felhasználó a *virtuális gépen* lévő böngészőben megpróbál megnyitni egy olyan webhelyet, amelyet a Webfelügyelő egyik szabálya blokkol, akkor a *számítógép* gazdaszámítógépének operációs rendszerére telepített alkalmazás megtagadja a hozzáférést az adott webhelyhez.

A Webfelügyelő eltérő módon működik a különböző virtuális gépeken.

Oracle VM VirtualBox

A Kaspersky Endpoint Security korlátozások nélkül támogatja a webfelügyelői szabályokat az Oracle VM VirtualBox virtuális gépeken. Az alkalmazás irányíthatja a virtuális gép teljes forgalmát. Ha a Webfelügyelő szabályaiban a felhasználó szerinti szűrés be van állítva, az alkalmazás megfelelően működik, mivel a virtuális gépek összes folyamatát a helyi felhasználó indítja el.

VMware Workstation

A Kaspersky Endpoint Security korlátozásokkal támogatja a VMware Workstation virtuális gépeken a webfelügyelői szabályokat. Az alkalmazás nem támogatja a felhasználó szerinti szűrést tartalmazó szabályokat. A virtuális gépi folyamatok a rendszerfelhasználó (SYSTEM) alatt futnak. Ez lehetetlenné teszi annak a felhasználónak az azonosítását, aki megpróbálja megnyitni a webhelyet a virtuális gépen.

Microsoft Hyper-V

A Kaspersky Endpoint Security nem támogatja a webfelügyelői szabályokat a Microsoft Hyper-V virtuális gépeken.

Változók a Web Control üzenetsablonjaiban

A következő változókat használhatja a felhasználói és a rendszergazdai üzenetsablonokban:

- **User** – `%USER_NAME%`.

  Az aktuális felhasználói fiók neve azon a számítógépen, amelyen az üzenet létrejött, `<device name>\<user alias>` formátumban (például `DESKTOP-123\John.Smith`).

- **Web resource address** – `%CANONIC_REQUEST_URL%`.

  A blokkolt webes erőforrás címe.

- **Rule name** – `%RULE%`.

  A webes erőforrást blokkoló szabály neve.

- **Email for sending a message** – `%COMPLAIN_EMAIL%`.

  E-mail-cím a webes erőforrás-blokkolással kapcsolatos visszajelzésekhez. Az e-mail-címre kattintva megnyílik egy ablak, amelyben a felhasználó üzenetet írhat a rendszergazdának.

- **Name of content category** – `%CONTENT_CATEGORY_LIST%`.

  Webhelykategória, amelybe a blokkolt erőforrás tartozik (például *Payment systems*).

- **Name of data type category** – `%TYPE_CATEGORY_LIST%`.

  A blokkolt webes erőforrás adattípus-kategóriája (például *Graphic files*).

- **Link to requested web resource** – `%CONTINUE_PAGE%`.

  A kért weboldalra mutató hivatkozás (például `http://www.example.com/pagename.html`).

- **Link to website** – `%CONTINUE_SITE%`.

  A kért weboldalt tartalmazó webhelyre mutató hivatkozás (például `http://www.example.com/`).

- **Link for access to domains** – `%CONTINUE_DOMAIN%`.

  Hivatkozás, amelyre kattintva a domainnévhez tartozó összes létező weboldalhoz el lehet jutni. Ha például a blokkolt weboldal címe: `http://www.example.com`, a `%CONTINUE_DOMAIN%` változó helyére a `http://*.example.com` hivatkozás kerül. A hivatkozásra kattintva a `http://www.example.com/` alaptartománynév összes webcíméhez hozzáférhet, beleértve az aldomaineket, például `http://start.example.com/*` vagy `http://domain.domain.example.com/*`, ahol a `*` karakter a karakterek bármely sorozatát jelöli (beleértve az üres karakterláncot is).

Eszközfelügyelő

Az Eszközfelügyelő felügyeli az olyan eszközökhöz történő felhasználói elérést, amik csatlakoztatva vannak a számítógéphez (például merevlemezek, kamerák vagy Wi-Fi modulok). Ez lehetővé teszi, hogy megvédje számítógépét a fertőzésektől, ha ilyen eszközök vannak csatlakoztatva, valamint megelőzi az adatvesztést vagy -szivárgást.

Ha az Eszközfelügyelő engedélyezve van, az alkalmazás továbbítja a csatlakoztatott eszközökre vonatkozó információkat a Kaspersky Security Centernek. A csatlakoztatott eszközök listáját a Kaspersky Security Center **Advanced** → **Repositories** → **Hardware** mappájában tekintheti meg.

Eszközhozzáférési szintek

Az Eszközfelügyelő a következő szinteken felügyeli a hozzáférést:

- **Eszköztípus**. Például nyomtatók, cserélhető meghajtók és CD/DVD meghajtók.

  Az eszköz hozzáférésének beállításait az alábbiak szerint lehet megadni:

  - Engedélyezés – .
  - Blokkolás – .
  - Szabályokkal (csak nyomtatók és hordozható eszközök) – .
  - A csatlakozási busztól függ (kivéve Wi-Fi) – .
  - Blokkolás kivételekkel (csak Wi-Fi) – .

- **Csatlakozási busz**. A *csatlakozási busz* egy felület, amivel csatlakoztatni lehet eszközöket a számítógéphez (például USB vagy FireWire). Ha **A csatlakozási busztól függ** mód van kiválasztva az eszköztípusnál, az alkalmazás a csatlakozási felülettől függően engedélyezi vagy letiltja az eszköz elérését (pl. USB).

Az eszköz hozzáférésének beállításait az alábbiak szerint lehet megadni:

- Engedélyezés – ✓.
- Blokkolás – ⊘.

- **Megbízható eszközök**. A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

  Az alábbi adatok alapján hozzáadhat megbízható eszközöket:

  - **Eszközök azonosító alapján**. Minden eszköz egyedi azonosítóval rendelkezik (Hardverazonosítóval, azaz HWID-vel). Megtekintheti az azonosítót az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. Példa az eszközazonosítóra: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Azonosító alapján kényelmesen lehet eszközöket hozzáadni, ha bizonyos meghatározott eszközöket akar hozzáadni.

  - **Eszközök típus alapján**. Minden eszköz rendelkezik egy gyártóazonosítóval (VID) és termékazonosítóval (PID). Megtekintheti az azonosítókat az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. A VID és PID számok megadására szolgáló sablon: `VID_1234&PID_5678`. Modell alapján kényelmesen lehet eszközöket hozzáadni, amennyiben a szervezetében használt bizonyos készülékmodelleket akarja használni. Ilyen módon az adott modell valamennyi példányát hozzáadhatja.

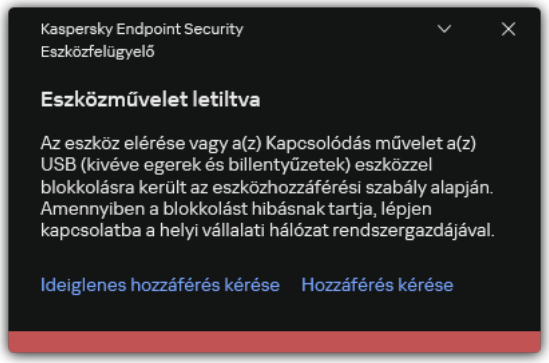
  - **Eszközök azonosítómaszk alapján**. Ha több eszközt használ, amelyek azonosítója megegyezik, akkor maszkok segítségével veheti fel azokat a megbízható listára. A `*` karakter akármilyen karakterláncot helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `WDC_C*`.

  - **Eszközök modellmaszk alapján**. Ha több eszközt használ hasonló VID vagy PID azonosítóval (például ugyanattól a gyártótól származó eszközök), akkor maszkokkal hozzáadhat készülékeket a megbízható listához. A `*` karakter akármilyen karakterláncot helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `VID_05AC&PID_*`.

Az Eszközfelügyelő szabályozza az eszközökhöz történő hozzáférést a *hozzáférési szabályokkal*. Az Eszközfelügyelővel elmentheti a készülék kapcsolódási/lecsatlakozási eseményeit. Az események elmentéséhez meg kell adnia a szabályzatban az események regisztrációját.

Ha a készülék elérése a csatlakozóbusztól függ (a ◔ állapot), akkor a Kaspersky Endpoint Security nem menti el a készülék kapcsolódási/leválasztási eseményeket. Ahhoz, hogy engedélyezze, hogy a Kaspersky Endpoint Security elmentse az eszköz kapcsolódási/leválasztási eseményeket, engedélyezze a megfelelő típusú készülék elérését (a ✓ állapot), vagy adja hozzá a készüléket a megbízható listához.

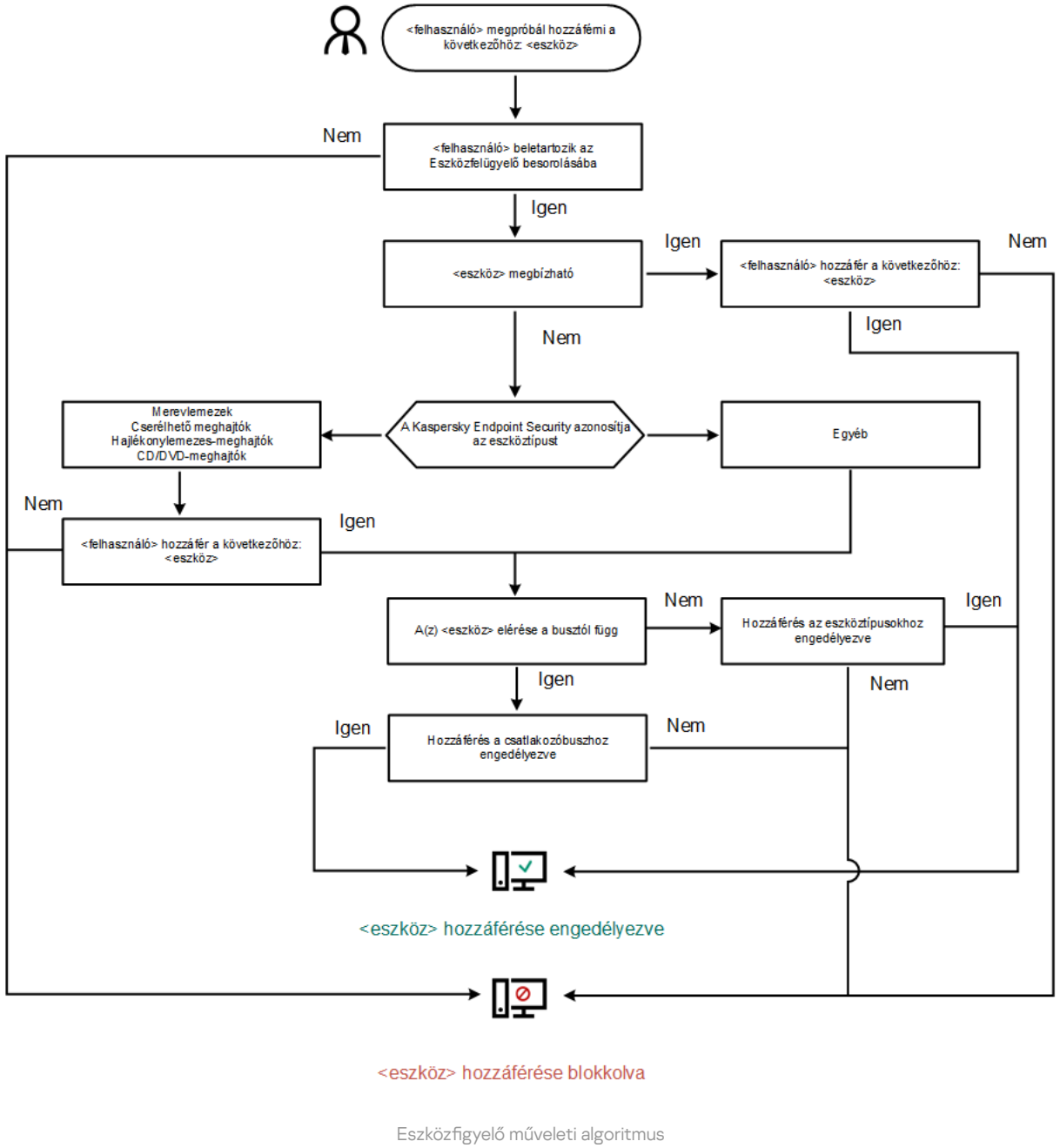
Ha egy olyan eszköz csatlakozik a számítógéphez, ami blokkolva van az Eszközfelügyelő által, akkor a Kaspersky Endpoint Security blokkolja az elérést, és megjelenít egy értesítést (lásd az alábbi ábrát).



Eszközfelügyelő értesítés

Eszközfigyelő műveleti algoritmus

A Kaspersky Endpoint Security döntést hoz az eszközök hozzáférésének engedélyezéséről, miután a felhasználó a számítógéphez csatlakoztatja őket (lásd az alábbi ábrát).



Eszközfigyelő műveleti algoritmus

Ha az eszköz csatlakoztatva van és hozzáférhető, akkor szerkesztheti a hozzáférési és a blokkolási szabályt. Ebben az esetben, ha legközelebb valaki megpróbál hozzáférni az eszközhöz (például ha meg akarja tekinteni a mappalistát, vagy olvasási és írási műveleteket akar elvégezni), akkor a Kaspersky Endpoint Security blokkolja a hozzáférést. A fájlrendszer nélküli eszköz csak a következő csatlakoztatás alkalmával blokkolódik.

Ha telepített Kaspersky Endpoint Security alkalmazással rendelkező számítógép felhasználójának hozzáférést kell kérnie egy olyan eszközhöz, amely a felhasználó szerint tévedésből van blokkolva, küldje el a felhasználónak a hozzáférés-kérési utasításokat.

A hozzáférési szabályokról

Egy *eszközhozzáférési szabály* olyan csoportbeállításokat takar, amelyek meghatározzák, hogyan érhetik el a felhasználók a számítógépre telepített vagy ahhoz csatlakoztatott eszközöket. Ezek a beállítások magukban foglalják a hozzáférést egy adott eszközhöz, a hozzáférés ütemezését, valamint az olvasási vagy írási jogosultságokat. Nem adhat hozzá olyan eszközt, ami kívül esik az Eszközfelügyelő besorolásán. Az ilyen eszközökhöz történő hozzáférés minden felhasználó számára engedélyezve van.

Eszközhozzáférési szabályok

A hozzáférési szabályok csoportbeállításai az eszköz típusától függően eltérőek lehetnek (lásd az alábbi táblázatot).

Hozzáférési szabály beállítások

Eszközök	Hozzáférés-felügyelet	Az eszközökhöz való hozzáférés ütemezése	Felhasználók és/vagy felhasználócsoportok hozzárendelése	Prioritás	Olvasás/írás jogosultság
Merevlemezek	✓	✓	✓	✓	✓
Cserélhető meghajtók (beleértve az USB flash-meghajtókat is)	✓	✓	✓	✓	✓
Hajlékonylemezek	✓	✓	✓	✓	✓
CD/DVD meghajtók	✓	✓	✓	✓	✓
Hordozható eszközök (MTP)	✓	✓	✓	✓	✓
Helyi nyomtatók	✓	–	✓	✓	–
Hálózati nyomtatók	✓	–	✓	✓	–
Modemek	✓	–	–	–	–
Szalagos eszközök	✓	–	–	–	–
Többfunkciós eszközök	✓	–	–	–	–
Intelligens kártyaolvasók	✓	–	–	–	–
Windows CE USB ActiveSync eszközök	✓	–	–	–	–
Külső hálózati csatolók	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Kamerák és szkennerek	✓	–	–	–	–

Hozzáférési szabályok a Wi-Fi hálózatokhoz

Wi-Fi hálózati hozzáférési szabály dönti el, hogy a Wi-Fi hálózatok használata engedélyezett-e (a ✓ állapot) vagy tiltottak-e (a ⊘ állapot). Hozzáadhat egy *megbízható Wi-Fi hálózatot* (a állapot) egy szabályhoz. A megbízható Wi-Fi hálózat használata korlátlanul engedélyezve van. Alapértelmezetten, egy Wi-Fi hálózati hozzáférési szabály bármilyen Wi-Fi hálózat hozzáférését elérhetővé teszi.

Csatlakozási busz hozzáférési szabály.

Ha **A csatlakozási busztól függ** eszköztípus szerint van kiválasztva a hozzáférési szabály értéke, az alkalmazás a csatlakozási felülettől függően engedélyezi vagy letiltja az eszköz elérését. Az Eszközfelügyelő összetevő osztályozásában jelen lévő összes csatlakozási buszhoz alapértelmezés szerint a hozzájuk való hozzáférést engedélyező szabályok jönnek létre.

A csatlakozási busz hozzáférési szabály dönti el, hogy a csatlakoztatott eszközök engedélyezett-e (a ✓ állapot) vagy tiltottak-e (a ⊘ állapot). Az eszköztípus hozzáférési szabályainak prioritása magasabb, mint a csatlakozási busz hozzáférési szabályainak prioritása.

A billentyűzet és az egér nem zárolható az Eszközfelügyelő segítségével. Ha megtiltja az USB csatlakozási buszhoz való hozzáférést, a felhasználó USB-n keresztül csatlakoztatott billentyűzettel és egérrel folytatja a munkát. A BadUSB védelem összetevő megakadályozza azt, hogy a billentyűzetet emuláló fertőzött USB-eszközök a számítógéphez csatlakozzanak.

Az eszközökhöz való hozzáférés kezelése típus szerint

Az Eszközfelügyelő lehetővé teszi az eszközökhöz való hozzáférés típus szerinti kezelését. Az eszköz típusát az operációs rendszer határozza meg, amikor az eszköz csatlakoztatva van. Az eszköztípust az operációs rendszerbe épített Eszközkezelő eszközzel nézheti meg. Az eszközökhöz való hozzáférés kezeléséhez szabályokat kell beállítani. Egy *eszközhozzáférési szabály* olyan csoportbeállításokat takar, amelyek meghatározzák, hogyan érhetik el a felhasználók a számítógépre telepített vagy ahhoz csatlakoztatott eszközöket. Ezek a beállítások magukban foglalják a hozzáférést egy adott eszközhöz, a hozzáférés ütemezését, valamint az olvasási vagy írási jogosultságokat. Nem adhat hozzá olyan eszközt, ami kívül esik az Eszközfelügyelő besorolásán. Az ilyen eszközökhöz történő hozzáférés minden felhasználó számára engedélyezve van.

Alapértelmezés szerint az Eszközfelügyelő minden felhasználó számára engedélyezi az összes eszköz elérését.

Az eszközökhöz való hozzáférést a következők szerint állíthatja be:

- **Engedélyezés**.

  A Kaspersky Endpoint Security minden felhasználó számára teljes hozzáférést biztosít az eszközökhöz.

- **Blokkolás**.

  A Kaspersky Endpoint Security blokkolja az eszközkapcsolatokat. Az alkalmazás csak megbízható eszközök csatlakozását engedélyezi.

- **A csatlakozási busztól függ**.

  A Kaspersky Endpoint Security meghatározza az eszközök csatlakozási felületét, és a buszcsatlakozás állapotának megfelelően korlátozza az eszközökhöz való hozzáférést. Az alkalmazás megbízható eszközök csatlakoztatását is lehetővé teszi.

- **Szabályokkal**.

  Egyes eszköztípusoknál megadhatja az eszközök használatára jogosult egyéni felhasználókat vagy felhasználói csoportokat, beállíthatja az eszközökhöz való hozzáférés ütemezését, valamint konfigurálhatja az írási és olvasási engedélyeket. Az alkalmazás megbízható eszközök csatlakoztatását is lehetővé teszi.

Legyen óvatos a **Merevlemezek** típusú eszközökhöz való hozzáférés konfigurálásakor. Ha blokkolja a rendszerlemezhez való hozzáférést, az alkalmazás összeomlást (kékképernyős összeomlást) okozhat az operációs rendszer indításakor.

Ha egy eszköz nem illeszkedik az Eszközfelügyelő osztályozási rendszerébe, akkor az ilyen eszközhöz való hozzáférés nem korlátozható.

Az eszközök típus szerinti hozzáférésének kezelése a Felügyeleti konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A rendszabály ablakában válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
5. Az **Eszközfelügyelő beállításai** részen válassza ki az **Eszköztípusok** lapot.

   Az **Eszköztípusok** lapon láthatók az Eszközfelügyelő osztályba tartozó összes eszköz hozzáférési szabályai.
6. Hozzáférési szabályok konfigurálása az eszközökhöz:

   a. Válassza ki a hozzáférési módot: **Engedélyezés**, **Blokkolás**, **A csatlakozási busztól függ**, **Szabályokkal**.

   A **Szabályokkal** hozzáférési mód kiválasztásához kattintson duplán a hozzáférési szabály tulajdonságainak megnyitásához.

   b. Ha a **Csatlakozóbusztól függ** hozzáférési módot választja, akkor a **Csatlakozóbuszok** lapon be kell állítania a csatlakozási felületek hozzáférési szabályait.

   c. Tárolóeszközök (például cserélhető adathordozók) esetében beállíthatja az egyes felhasználók hozzáférési engedélyeit. Tárolóeszközök (például cserélhető adathordozók) esetén beállíthatja az egyes felhasználók hozzáférési engedélyeit.

   Lehetősége van felvenni eszközöket a megbízható eszközök listájára. A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

   d. Ha szükséges, konfigurálja a nyomtatási szabályokat.

   e. Ha szükséges, konfigurálja a Bluetooth-eszköz hozzáférési szabályait.

   f. Ha szükséges, konfigurálja a számítógép Wi-Fi csatlakozási szabályait.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az eszközök típus szerinti hozzáférésének kezelése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Device Control** elemet.
5. A **Device access rules** területen válassza a **Devices and Wi-Fi networks** lapot.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.
6. Hozzáférési szabályok konfigurálása az eszközökhöz:

   a. Válassza ki a hozzáférési módot: **Allow**, **Block**, **Depends on bus**, **Custom**.

   Ha a hozzáférési mód nem szerepel a legördülő menüben, nyissa meg a hozzáférési szabály tulajdonságait az eszköz típusára kattintva.

   b. Ha a **Depends on bus** hozzáférési módot választja, akkor a **Connection buses** lapon be kell állítania a csatlakozási felületek hozzáférési szabályait.

   c. Tárolóeszközök (például cserélhető adathordozók) esetében beállíthatja az egyes felhasználók hozzáférési engedélyeit. Tárolóeszközök (például cserélhető adathordozók) esetén beállíthatja az egyes felhasználók hozzáférési engedélyeit.

   Lehetősége van felvenni eszközöket a megbízható eszközök listájára. A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

   d. Ha szükséges, konfigurálja a nyomtatási szabályokat.

   e. Ha szükséges, konfigurálja a Bluetooth-eszköz hozzáférési szabályait.

   f. Ha szükséges, konfigurálja a számítógép Wi-Fi csatlakozási szabályait.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az eszközökhöz való hozzáférés kezelése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** hivatkozásra.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.
4. Hozzáférési szabályok konfigurálása az eszközökhöz:

   a. Válassza ki a hozzáférési módot: **Engedélyezés**, **Blokkolás**, **A csatlakozási busztól függ**, **Szabályokkal**.

   Ha a hozzáférési mód nem szerepel a legördülő menüben, nyissa meg a hozzáférési szabály tulajdonságait az eszköz típusára kattintva.

b. Ha a **Csatlakozóbusztól függ** hozzáférési módot választja, akkor a **Csatlakozóbuszok** lapon be kell állítania a csatlakozási felületek hozzáférési szabályait.

c. Tárolóeszközök (például cserélhető adathordozók) esetében beállíthatja az egyes felhasználók hozzáférési engedélyeit. Tárolóeszközök (például cserélhető adathordozók) esetén beállíthatja az egyes felhasználók hozzáférési engedélyeit.

Lehetősége van felvenni eszközöket a megbízható eszközök listájára. A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

d. Ha szükséges, konfigurálja a nyomtatási szabályokat.

e. Ha szükséges, konfigurálja a Bluetooth-eszköz hozzáférési szabályait.

f. Ha szükséges, konfigurálja a számítógép Wi-Fi csatlakozási szabályait.

5. Mentse el a módosításokat.

Ennek eredményeként, amikor a felhasználó megpróbál hozzáférni egy eszközhöz, az alkalmazás a szabályoknak megfelelően blokkolja a hozzáférést. A Kaspersky Endpoint Security a megfelelő eseményeket is naplózza. Ha szeretne hozzáférést biztosítani az egyes eszközökhöz, hozzáadhatja ezeket az eszközöket a megbízható eszközök listájához.

Az eszközökhöz való hozzáférés kezelése csatlakozási busz szerint

A csatlakozóbuszok hozzáférési szabályainak szerkesztése:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson a **Csatlakozási buszok** gombra.

   A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes csatlakozási busz hozzáférési szabályait jeleníti meg.
4. Válassza ki a szerkeszteni kívánt hozzáférési szabályt.
5. A **Hozzáférés** oszlopban válassza ki, hogy engedélyezi-e vagy sem a csatlakozási buszhoz való hozzáférést: **Engedélyezés** vagy **Blokkolás**.

   Ha megváltoztatja a csatlakozási buszhoz való hozzáférést **Soros port** (COM) vagy **Párhuzamos port** (LPT) értékre, újra kell indítania a számítógépet a hozzáférési szabály aktiválásához.
6. Mentse el a módosításokat.

A felhasználók eszközökhöz való hozzáférési jogainak differenciálása

A felhasználói hozzáférési jogosultságokat eszköztípus szerint vagy megbízható eszközökhöz állíthatja be.

A felhasználói hozzáférési jogok eszköztípus szerinti megkülönböztetése

Az Eszközfelügyelő lehetővé teszi a felhasználók hozzáférési jogainak konfigurálását a *tárolóeszközökön* található adatokhoz. Az ilyen eszközökhöz írási és olvasási engedélyeket konfigurálhat. Az Eszközfelügyelő a következő típusú *tárolóeszközöket* támogatja:

- Merevlemezek.
- Cserélhető meghajtók (beleértve az USB flash-meghajtókat is).
- Hajlékonylemezek.
- CD/DVD meghajtók.
- Hordozható eszközök (MTP). A hordozható eszközök (MTP) közé tartoznak például a mobilkészülékek, a fényképezőgépek, a médialejátszók és így tovább.

Ily módon például a cserélhető adathordozók használatát csak a rendszergazdák csoportjának engedélyezheti. Más eszköztípusok esetén az összes felhasználó számára megtagadhatja vagy engedélyezheti a hozzáférést. Beállíthatja a felhasználók nyomtatóhasználati jogait is.

A tárolóeszközökön lévő adatokhoz való felhasználói hozzáférési jogosultságok konfigurálása a Felügyeleti konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A rendszabály ablakában válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
5. Az **Eszközfelügyelő beállításai** részen válassza ki az **Eszköztípusok** lapot.
   Az **Eszköztípusok** lapon láthatók az Eszközfelügyelő osztályba tartozó összes eszköz hozzáférési szabályai.
6. A tárolóeszköz-hozzáférési szabályok konfigurálásához kattintson duplán a szabályok listájának megnyitásához.
7. Konfigurálja a tárolóeszköz-hozzáférési szabályt:
   a. A **Hozzáférési szabályok** részen kattintson a **Hozzáadás** gombra.
      Ekkor megnyitja az új tárolóeszköz-hozzáférési szabály hozzáadására szolgáló ablakot.

b. A **Szabályprioritás** mezőben állítsa be a *szabályírási* prioritást. A szabály a következő attribútumokat tartalmazza: felhasználói fiók, ütemezés, engedélyek (olvasás/írás) és prioritás.

A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

c. A **Felhasználókra és csoportokra vonatkozó szabály** részen válassza ki a felhasználókat vagy a felhasználói csoportokat. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

d. Kattintson az **OK** gombra.

8. **A kiválasztott hozzáférési szabály ütemezései** részen konfigurálja a tárolóeszköz-hozzáférési ütemezést a felhasználók számára.

   Például engedélyezheti a felhasználók számára, hogy tárolóeszközöket csak munkaidőben használjanak.

9. Konfigurálhatja a felhasználók hozzáférési jogosultságait a tárolóeszközökhöz a fájlkezelőben (**olvasás** / **írás**).

10. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A tárolóeszközökön lévő adatokhoz való felhasználói hozzáférési jogosultságok konfigurálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **Device Control** elemet.

5. A(z) **Device access rules** blokkban a hozzáférési szabályok táblázatában nyissa meg a tárolóeszközök hozzáférési szabályainak tulajdonságait.

6. A **Device access rules** területen válassza az **Custom** opciót.

7. Konfigurálja a tárolóeszköz-hozzáférési szabályt:

   a. A **Users and their rights** részen kattintson a **Add** gombra.

   Ekkor megnyitja az új tárolóeszköz-hozzáférési szabály hozzáadására szolgáló ablakot.

   b. A(z) **Priority** mezőben állítsa be a *szabályírási* prioritást. A szabály a következő attribútumokat tartalmazza: felhasználói fiók, ütemezés, engedélyek (olvasás/írás) és prioritás.

A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

c. A(z) **User or group** területen válassza ki a felhasználókat vagy felhasználócsoportokat. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

d. A(z) **Access schedule** területen konfigurálja az eszközhozzáférési ütemezést a felhasználók számára.

Például engedélyezheti a felhasználók számára, hogy tárolóeszközöket csak munkaidőben használjanak.

e. A felhasználók tárolóeszközökhöz való hozzáférési jogosultságait a a fájlkezelőben (**Read** / **Write**) konfigurálhatja.

f. Kattintson az **Save** gombra.

8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A tárolóeszközökön lévő adatokhoz való felhasználói hozzáférési jogosultságok konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** hivatkozásra.

A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.

4. A tárolóeszköz-hozzáférési szabályok konfigurálásához kattintson az egér jobb gombjával a szabályok listájának megnyitásához.

5. Konfigurálja a tárolóeszköz-hozzáférési szabályt:

a. A **Felhasználói jogok** részen kattintson a **Hozzáadás** gombra.

Ekkor megnyitja az új tárolóeszköz-hozzáférési szabály hozzáadására szolgáló ablakot.

b. A **Prioritás** mezőben állítsa be a *szabályírási* prioritást. A szabály a következő attribútumokat tartalmazza: felhasználói fiók, ütemezés, engedélyek (olvasás/írás) és prioritás.

A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

c. A **Felhasználók** részen válassza ki a felhasználókat vagy felhasználócsoportokat. Kiválaszthatja a felhasználókat az Active Directory-ból, vagy manuálisan beírhat egy helyi felhasználónevet. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

d. Kattintson az **OK** gombra.

6. **Az eszközökhöz való hozzáférés ütemezése** részen konfigurálja a tárolóeszközök hozzáférési ütemezését a felhasználók számára.

   Például engedélyezheti a felhasználók számára, hogy tárolóeszközöket csak munkaidőben használjanak.

7. Konfigurálhatja a felhasználók hozzáférési jogosultságait a tárolóeszközökhöz a fájlkezelőben (**olvasás** / **írás**).

8. Mentse el a módosításokat.

A felhasználók megbízható eszközökhöz való hozzáférési jogainak differenciálása

A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva. A megbízható eszközökkel való munkavégzéshez lehetősége van hozzáférést biztosítani egy adott felhasználónak, a felhasználók adott csoportjának vagy a szervezet minden felhasználójának. A felhasználói hozzáférési jogokat a megbízható eszköz tulajdonságaiban állíthatja be.

A mobileszközökhöz való hozzáférés kezelése

A Kaspersky Endpoint Security lehetővé teszi az adatokhoz való hozzáférés szabályozását Android és iOS rendszerű mobileszközökön. A mobileszközök a hordozható eszközök (MTP) kategóriájába tartoznak. Ezért a mobileszközök adathozzáférésének konfigurálásához a hordozható eszközök (MTP) hozzáférési beállításait kell szerkesztenie.

Ha egy mobilkészülék csatlakoztatva van a számítógéphez, akkor az operációs rendszer határozza meg a készülék típusát. Ha az Android Debug Bridge (ADB), iTunes vagy egy ezekhez hasonló alkalmazás van telepítve a számítógépen, az operációs rendszer ADB vagy iTunes eszközként fogja azonosítani a mobilkészülékeket. Az operációs rendszer minden más esetben fájlátvitelhez tartozó hordozható eszközként (MTP), képátvitelhez tartozó PTP-eszközként (kamera) vagy egyéb eszköztípusként azonosítja a mobilkészüléket. Az eszköztípus a mobileszköz típusától és a kiválasztott USB-csatlakozási módtól függ. A Kaspersky Endpoint Security segítségével egyéni hozzáférési engedélyeket konfigurálhat a mobileszközökön lévő adatokhoz az ADB alkalmazásokban, az iTunes-ban vagy a fájlkezelőben. Minden más esetben az Eszközfelügyelő lehetővé teszi a mobileszközökhöz való hozzáférést a hordozható eszközök (MTP) hozzáférési szabályai szerint.

Mobileszközökhöz való hozzáférés

A mobileszközök a hordozható eszközök (MTP) kategóriájába tartoznak, ezért a beállítások ugyanazok. A mobileszközökhöz való hozzáféréshez a következő módok közül választhat:

- **Engedélyezés**. A Kaspersky Endpoint Security teljes hozzáférést biztosít a mobileszközökhöz. Fájlokat nyithat meg, hozhat létre, módosíthat, másolhat vagy törölhet a mobileszközökön a fájlkezelő vagy az ADB és az iTunes alkalmazások segítségével. Az akkumulátort úgy is feltöltheti, hogy a mobileszközt a számítógép USB-portjához csatlakoztatja.

- **Blokkolás**. A Kaspersky Endpoint Security korlátozza a mobileszközök hozzáférését a fájlkezelőben, valamint az ADB és az iTunes alkalmazásokban. Az alkalmazás csak megbízható mobileszközökhöz való hozzáférést tesz lehetővé. Az akkumulátort úgy is feltöltheti, hogy a mobileszközt a számítógép USB-portjához csatlakoztatja.

- **A csatlakozási busztól függ**. A Kaspersky Endpoint Security lehetővé teszi a mobileszközökhöz való csatlakozást az USB-kapcsolat állapotának megfelelően (**Engedélyezés** vagy **Blokkolás**).

- **Szabályok szerint**. A Kaspersky Endpoint Security a szabályoknak megfelelően korlátozza a mobileszközökhöz való hozzáférést. A szabályokban konfigurálhatja a hozzáférési jogokat (olvasás/írás), kiválaszthatja a felhasználókat vagy a felhasználók egy csoportját, akik hozzáférhetnek a mobileszközökhöz, és hozzáférés-ütemezést konfigurálhat a mobileszközökhöz. A mobileszközökön lévő adatokhoz való hozzáférést az ADB és az iTunes alkalmazásokon keresztül is korlátozhatja.

Mobileszköz-hozzáférési szabályok konfigurálása

A hordozható eszközök (MTP), az ADB-eszközök és az iTunes-eszközök hozzáférési szabályai eltérő módon vannak konfigurálva. A hordozható eszközök (MTP) és az ADB-eszközök esetében szabályokat állíthat be egyes felhasználók vagy felhasználói csoportok számára, és ütemezést hozhat létre arra vonatkozóan, hogy a szabályok mikor alkalmazandók. Az iTunes-eszközök esetében ez nem lehetséges. Az adatokhoz való hozzáférést csak az iTunes alkalmazáson keresztül engedélyezheti vagy tilthatja meg minden felhasználó számára.

Mobileszköz-hozzáférési szabályok konfigurálása az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

4. Az **Eszközfelügyelő beállításai** részen válassza ki az **Eszköztípusok** lapot.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.

5. A **Hordozható eszközök (MTP)** eszköztípus helyi menüjében konfigurálja a mobileszköz-hozzáférés módját: **Engedélyezés**, **Blokkolás** vagy **A csatlakozási busztól függ**.

6. A mobileszköz-hozzáférési szabályok konfigurálásához kattintson duplán a szabályok listájának megnyitásához.

7. Konfigurálja a mobileszköz-hozzáférési szabályt:

   a. A **Hozzáférési szabályok** részen kattintson a **Hozzáadás** gombra.

      Ekkor megnyitja az új mobileszköz-hozzáférési szabály hozzáadására szolgáló ablakot.

   b. A **Prioritás** mezőben állítsa be a szabály írási prioritását. A szabály a következő attribútumokat tartalmazza: felhasználói fiók, ütemezés, engedélyek (olvasás/írás/ADB hozzáférés) és prioritás.

      A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

      Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

      A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

   c. A **Felhasználókra és csoportokra vonatkozó szabály** részen válassza ki a felhasználókat vagy a felhasználói csoportokat. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   d. Kattintson az **OK** gombra.

8. **A kiválasztott hozzáférési szabály ütemezései** részen konfigurálja a mobileszköz-hozzáférési ütemezést a felhasználók számára.

   Külön hozzáférési ütemezés konfigurálása az ADB-eszközökhöz nem lehetséges. Beállíthat egy közös hozzáférési ütemezést az ADB-eszközökhöz és a hordozható eszközökhöz (MTP).

9. Konfigurálhatja a felhasználók hozzáférési jogosultságait a mobileszközökhöz a fájlkezelőben (**olvasás** / **írás**).

10. Konfigurálhatja a mobileszközön lévő adatokhoz való hozzáférést az ADB alkalmazáson keresztül a **Hozzáférés ADB-n keresztül** jelölőnégyzet segítségével.

    Ha a jelölőnégyzet nincs bejelölve, akkor a mobileszköz csatlakoztatásakor az ADB alkalmazás nem tudja észlelni az eszközt.

11. A **Hozzáférés iTunes-on keresztül** részen konfigurálhatja a mobileszközön lévő adatokhoz való hozzáférést az iTunes alkalmazáson keresztül.

    A Kaspersky Endpoint Security minden felhasználóra alkalmazza a mobileszközök iTunes alkalmazáson keresztüli eléréséhez szükséges beállításokat. Külön hozzáférési ütemezés konfigurálása az iTunes-eszközökhöz nem lehetséges.

12. Mentse el a módosításokat.

A mobileszköz-hozzáférési szabályok konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Device Control** elemet.
5. A **Device access rules** részen kattintson a **Devices and Wi-Fi networks** hivatkozásra.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.
6. Válassza ki a **Portable devices (MTP)** eszköztípust.

   Ez megnyitja a hordozható eszközök (MTP) hozzáférési jogait.
7. Konfigurálja a mobileszköz-hozzáférési módot: **Allow**, **Block**, **Depends on bus** vagy **Custom**.
8. A **Access via iTunes for all users ENABLED** kapcsolóval konfigurálhatja a mobileszközön lévő adatokhoz való hozzáférést az iTunes alkalmazáson keresztül.

   A Kaspersky Endpoint Security minden felhasználóra alkalmazza a mobileszközök iTunes alkalmazáson keresztüli eléréséhez szükséges beállításokat. Külön hozzáférési ütemezés konfigurálása az iTunes-eszközökhöz nem lehetséges.
9. Ha az **Custom** módot választja, hozzáférési szabályokat kell hozzáadnia az eszközökhöz. Ehhez a **Users and their rights** területen kattintson a **Add** gombra, és konfigurálja a mobileszköz-hozzáférési szabályt:

   a. A **Priority** mezőben állítsa be a szabályírási prioritást. A szabály a következő attribútumokat tartalmazza: felhasználói fiók, ütemezés, engedélyek (olvasás/írás/ADB hozzáférés) és prioritás.

   A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

   Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

   A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

   b. A **User or group** területen válassza ki a felhasználókat vagy felhasználói csoportokat a mobileszközökhöz való hozzáféréshez. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

c. A **Access schedule** területen konfigurálhatja az eszközhozzáférési ütemezést a felhasználók számára.

> Külön hozzáférési ütemezés konfigurálása az ADB-eszközökhöz nem lehetséges. Beállíthat egy közös hozzáférési ütemezést az ADB-eszközökhöz és a hordozható eszközökhöz (MTP).

d. A felhasználók mobileszközökhöz való hozzáférési jogosultságait a fájlkezelőben konfigurálhatja (**Read** / **Write**).

e. A mobileszközön lévő adatokhoz való hozzáférést az ADB alkalmazáson keresztül konfigurálhatja a **Access via ADB** jelölőnégyzet segítségével.

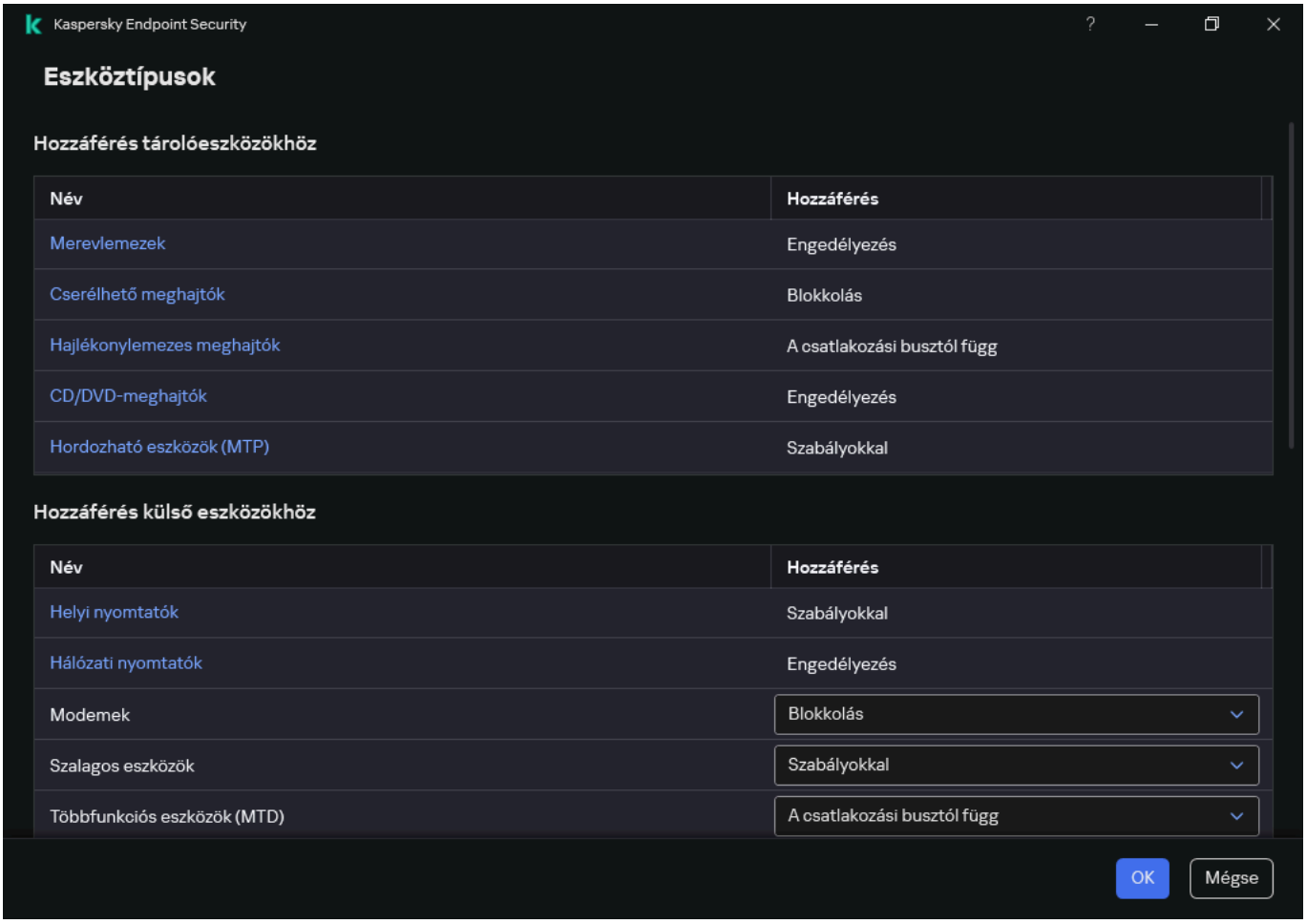
Ha a jelölőnégyzet nincs bejelölve, akkor a mobileszköz csatlakoztatásakor az ADB alkalmazás nem tudja észlelni az eszközt.

10. Mentse el a módosításokat.

Mobileszköz-hozzáférési szabályok konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** gombra.

A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes eszköz hozzáférési szabályait megjeleníti.



Eszköztípusok az Eszközfelügyelő összetevőben

4. A **Hozzáférés tárolóeszközökhöz** részen kattintson a **Hordozható eszközök (MTP)** hivatkozásra.

   Ezzel megnyílik egy ablak, amely tartalmazza a hordozható eszközök (MTP) hozzáférési szabályait.

5. A **Hozzáférés** részen állítsa be a mobileszközök hozzáférési módját: **Engedélyezés**, **Blokkolás**, **A csatlakozási busztól függ** vagy **Szabályokkal**.

6. Ha kiválasztja a **Szabályokkal** módot, hozzáférési szabályokat kell hozzáadnia az eszközökhöz:

   a. A **Felhasználói jogok** részen kattintson a **Hozzáadás** gombra.

      Ekkor megnyitja az új mobileszköz-hozzáférési szabály hozzáadására szolgáló ablakot.

   b. A **Prioritás** mezőben állítsa be a szabály írási prioritását. A szabály a következő attribútumokat tartalmazza: felhasználói fiók, ütemezés, engedélyek (olvasás/írás/ADB hozzáférés) és prioritás.

      A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

      Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

      A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

   c. Az **Állapot** részen kapcsolja be a mobileszköz-hozzáférési szabályt.

   d. A **Hozzáférési szabályok** részen konfigurálja a mobileszköz-hozzáférési engedélyeket a felhasználók számára.

      - Konfigurálhatja a felhasználók hozzáférési jogosultságait a mobileszközökhöz a fájlkezelőben (**olvasás** / **írás**).

      - Konfigurálhatja a mobileszközön lévő adatokhoz való hozzáférést az ADB alkalmazáson keresztül a **Hozzáférés ADB-n keresztül** jelölőnégyzet segítségével.

        Ha a jelölőnégyzet nincs bejelölve, akkor a mobileszköz csatlakoztatásakor az ADB alkalmazás nem tudja észlelni az eszközt.

   e. A **Felhasználók** részen válassza ki a felhasználókat vagy felhasználói csoportokat a mobileszközökhöz való hozzáféréshez. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   f. **Az eszközökhöz való hozzáférés ütemezése** részen konfigurálja az eszközök hozzáférési ütemezését a felhasználók számára.

      Külön hozzáférési ütemezés konfigurálása az ADB-eszközökhöz nem lehetséges. Beállíthat egy közös hozzáférési ütemezést az ADB-eszközökhöz és a hordozható eszközökhöz (MTP).

g. A **Hozzáférés iTunes-on keresztül** részen konfigurálhatja a mobileszközön lévő adatokhoz való hozzáférést az iTunes alkalmazáson keresztül.

A Kaspersky Endpoint Security minden felhasználóra alkalmazza a mobileszközök iTunes alkalmazáson keresztüli eléréséhez szükséges beállításokat. Külön hozzáférési ütemezés konfigurálása az iTunes-eszközökhöz nem lehetséges.

7. Mentse el a módosításokat.

Ennek eredményeként a felhasználók mobileszközökhöz való hozzáférését a szabályoknak megfelelően korlátozzuk. Ha az ADB és az iTunes alkalmazásokban megtiltotta a mobileszközökhöz való hozzáférést, akkor a mobileszközök csatlakoztatásakor az ADB és az iTunes alkalmazások nem képesek észlelni az adott mobileszközt.

Megbízható mobileszközök

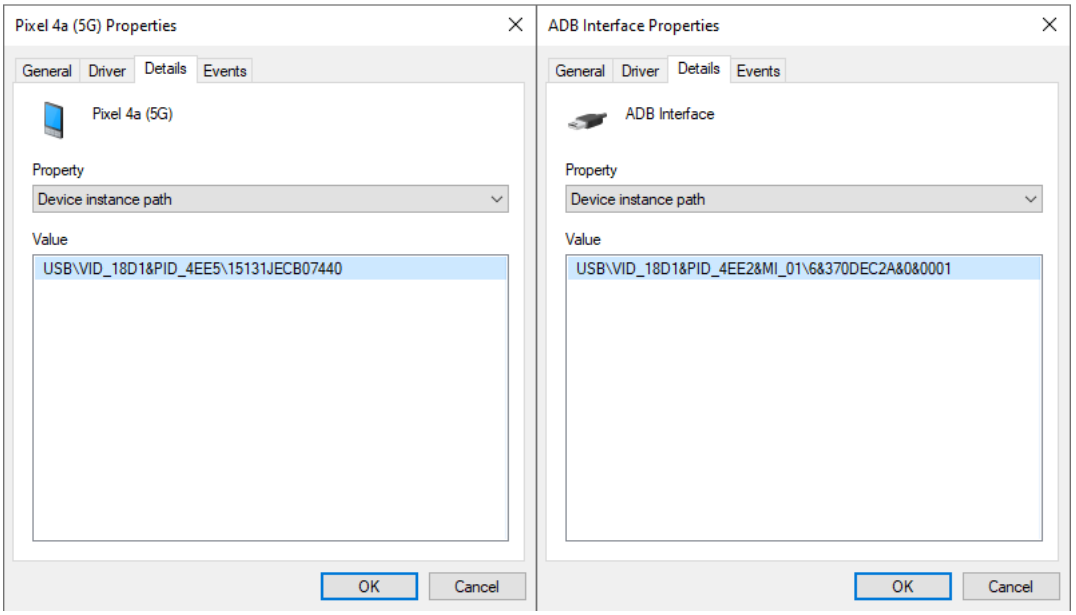
A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

A megbízható mobileszköz hozzáadására szolgáló eljárás pontosan ugyanaz, mint a többi megbízható eszköz esetében. Mobileszközöket azonosító vagy eszközmodell alapján adhat hozzá.

Megbízható mobileszköz azonosító alapján történő hozzáadásához egyedi azonosítóra (Hardware ID – HWID) lesz szüksége. Az azonosítót az eszköz tulajdonságainál találja az operációs rendszerben (lásd az alábbi ábrát). Az Eszközkezelő eszköz biztosítja ezt. A hordozható eszközök (MTP), az ADB-eszközök és az iTunes-eszközök azonosítói még ugyanazon mobileszközön is különböznek. Egy hordozható eszköz (MTP) azonosítója így nézhet ki: `15131JECB07440`. Az ADB-eszköz azonosítója így nézhet ki: `6&370DEC2A&0&0001`. Azonosító alapján kényelmesen lehet eszközöket hozzáadni, ha bizonyos meghatározott eszközöket akar hozzáadni. Használhat maszkokat is.

Ha az ADB vagy iTunes alkalmazásokat azután telepítette, hogy az eszközt a számítógéphez csatlakoztatta, akkor az eszköz egyedi azonosítóját lehet, hogy alaphelyzetbe állította a rendszer. Ez azt jelenti, hogy a Kaspersky Endpoint Security új eszközként fogja felismerni az eszközt. Ha az eszköz megbízható, adja hozzá a újból a megbízható listához.

Megbízható mobileszköz eszközmodell szerinti hozzáadásához szükség lesz annak Vendor ID (VID) és Product ID (PID) azonosítójára. Az azonosítókat az eszköz tulajdonságainál találja az operációs rendszerben (lásd az alábbi ábrát). A VID és PID számok megadására szolgáló sablon: `VID_18D1&PID_4EE5`. Modell alapján kényelmesen lehet eszközöket hozzáadni, amennyiben a szervezetében használt bizonyos készülékmodelleket akarja használni. Ilyen módon az adott modell valamennyi példányát hozzáadhatja.



Eszközazonosító az Eszközkezelőben

Bluetooth-eszközökhöz való hozzáférés kezelése

A Kaspersky Endpoint Security lehetővé teszi a Bluetooth-eszközökhöz való hozzáférés kezelését. A Bluetooth-eszközök közé tartoznak a vezeték nélküli billentyűzetek, egerek, fejhallgatók, nyomtatók stb. A Bluetooth-t kommunikációra is használhatja, pl. egy mobileszközzel.

Bluetooth-eszközök csatlakoztatásakor vagy leválasztásakor az alkalmazás több eseményt is létrehozhat az eszközzel kapcsolatban. Ennek az az oka, hogy az operációs rendszer egy Bluetooth-eszközt több különböző típusú eszközként érzékelhet. A Kaspersky Endpoint Security külön eszközként kezeli a Bluetooth-adaptert is, amelyen keresztül az eszköz csatlakozik. Ezért az alkalmazás minden észlelt eszközhöz létrehoz egy eseményt.

A Bluetooth-eszközökhöz való hozzáféréshez a következő módok közül választhat:

- **Engedélyezés és nem naplózás** . A Kaspersky Endpoint Security lehetővé teszi bármely Bluetooth-eszköz csatlakoztatását, és nem menti el a kapcsolattal kapcsolatos információkat az eseménynaplóban. Csatlakoztathat Bluetooth alapú bemeneti eszközöket (billentyűzetek, egerek stb.), adatokat küldhet Bluetooth-on keresztül, kezelhet más Bluetooth-eszközöket (headset, fejhallgató stb.).

- **Engedélyezés** . A Kaspersky Endpoint Security lehetővé teszi bármely Bluetooth-eszköz csatlakoztatását. Csatlakoztathat Bluetooth alapú bemeneti eszközöket (billentyűzetek, egerek stb.), adatokat küldhet Bluetooth-on keresztül, kezelhet más Bluetooth-eszközöket (headset, fejhallgató stb.).

- **Blokkolás** . A Kaspersky Endpoint Security korlátozza a hozzáférést a Bluetooth-eszközökhöz. Engedélyezheti, hogy csak Bluetooth-alapú bemeneti eszközöket lehessen csatlakoztatni (Human Interface Devices osztály). Ilyen eszközök a billentyűzetek, az egerek, a joystickek stb.

Nem lehet listát készíteni a megbízható Bluetooth-eszközökről. Ha korlátozott hozzáférése van a Bluetooth-eszközökhöz, akkor csak Bluetooth bemeneti eszközöket csatlakoztathat.

Bluetooth-eszközhozzáférési szabályok konfigurálása az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
5. Az **Eszközfelügyelő beállításai** részen válassza ki az **Eszköztípusok** lapot.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.
6. A **Bluetooth** eszköztípus helyi menüjében konfigurálja a Bluetooth-eszköz hozzáférési módját: **Engedélyezés** , **Blokkolás** , **Engedélyezés és naplózás mellőzése** .
7. Ha a **Blokkolás** módot választja, csak Bluetooth bemeneti eszközök (billentyűzetek, egerek stb.) csatlakoztatását engedélyezheti. Ehhez a **Kizárások** részen jelölje be a **Beviteli eszközök (egerek és billentyűzetek)** jelölőnégyzetet.
8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Bluetooth-eszközhozzáférési szabályok konfigurálása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Device Control** elemet.

5. A **Device access rules** részen kattintson a **Devices and Wi-Fi networks** hivatkozásra.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.

6. Válassza ki a **Bluetooth devices** eszköztípust.

   Ez megnyitja a Bluetooth-eszköz hozzáférési beállításait.

7. A Bluetooth-eszköz hozzáférési módjának konfigurálása: **Allow**, **Block**, **Allow and do not log**.

8. Ha az **Block** módot választja, csak Bluetooth bemeneti eszközök (billentyűzetek, egerek stb.) csatlakoztatását engedélyezheti. Ehhez a **Exclusions** területen jelölje be a **Input devices (mice and keyboards)** négyzetet.

9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

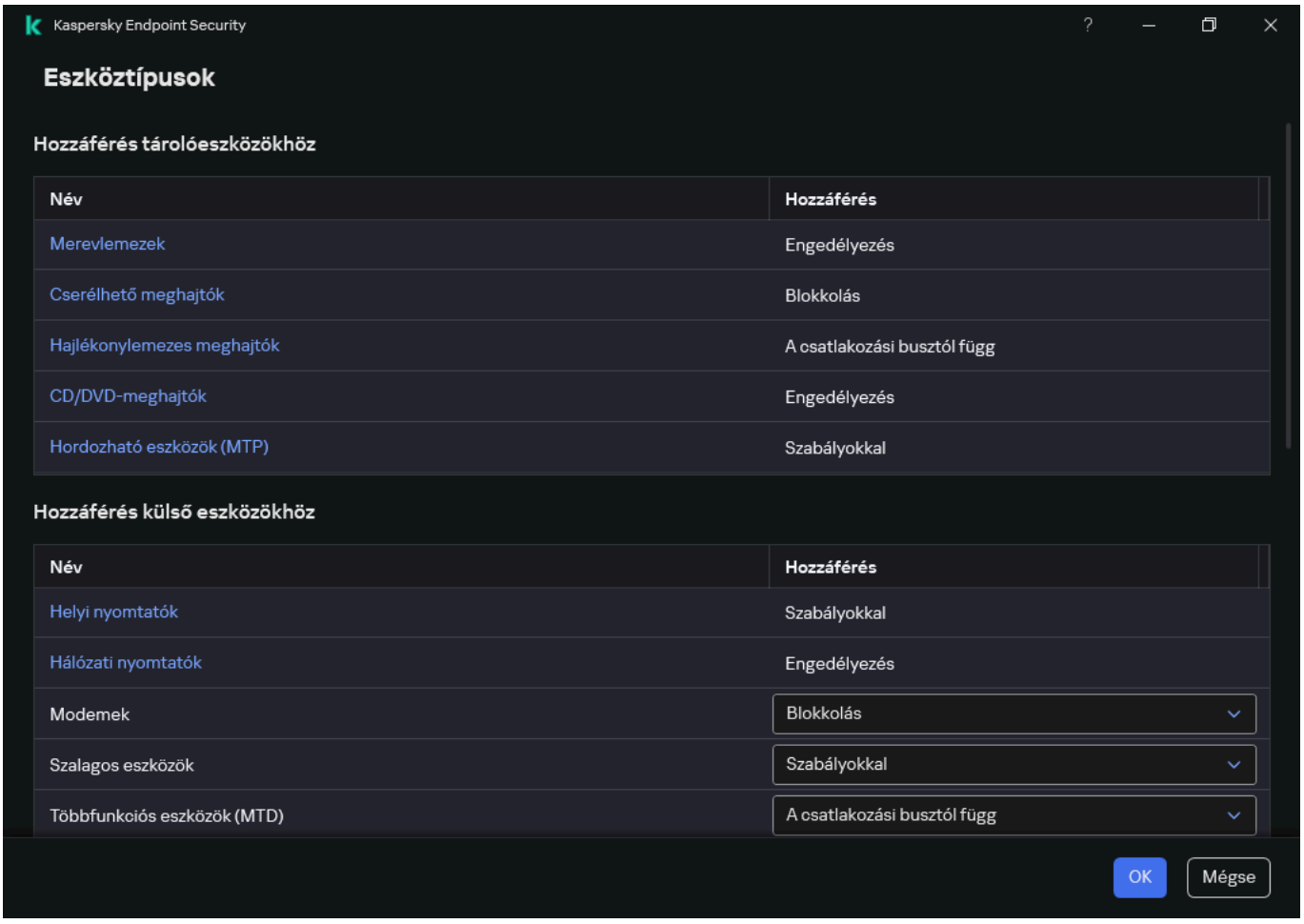
Bluetooth-eszközhozzáférési szabályok konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.

3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** gombra.

   A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes eszköz hozzáférési szabályait megjeleníti.



Eszköztípusok az Eszközfelügyelő összetevőben

4. A **Hozzáférés külső eszközökhöz** részen kattintson a **Bluetooth** hivatkozásra.

   Ez megnyitja a Bluetooth-eszköz hozzáférési beállításait.

5. A **Hozzáférés** részen konfigurálja a Bluetooth-eszköz hozzáférési módját: **Engedélyezés**, **Blokkolás**, **Engedélyezés és naplózás mellőzése**.

6. Ha a **Blokkolás** módot választja, csak Bluetooth bemeneti eszközök (billentyűzetek, egerek stb.) csatlakoztatását engedélyezheti. Ehhez a **Kizárások** részen jelölje be a **Beviteli eszközök (egerek és billentyűzetek)** jelölőnégyzetet.

7. Mentse el a módosításokat.

Nyomtatás szabályozása

A nyomtatásvezérlés nem támogatott az ARM alapú számítógépeken.

A Nyomtatás szabályozása segítségével konfigurálhatja a felhasználói hozzáférést a helyi és hálózati nyomtatókhoz.

Helyi nyomtató szabályozása

A Kaspersky Endpoint Security két szinten teszi lehetővé a helyi nyomtatókhoz való hozzáférés konfigurálását: *kapcsolódás* és *nyomtatás*.

A Kaspersky Endpoint Security a helyi nyomtatókapcsolatot a következő buszokon felügyeli: USB, soros port (COM), párhuzamos port (LPT).

A Kaspersky Endpoint Security csak a busz szintjén szabályozza a helyi nyomtatók COM- és LPT-portokhoz való csatlakozását. Ezért a COM- és LPT-portokon keresztüli nyomtatókapcsolatok megakadályozása érdekében ki kell választania A kapcsolati busztól függ hozzáférési módot a helyi nyomtatókhoz és le kell tiltania a COM- és LPT-buszokhoz való csatlakozást.

Az USB-hez csatlakoztatott nyomtatók esetében az alkalmazás két szinten gyakorolja a vezérlést: eszköztípus (helyi nyomtatók) és csatlakozási busz (USB).

A helyi nyomtatók USB-n keresztüli elérési módjai közül választhat:

- **Engedélyezés** ✓. A Kaspersky Endpoint Security minden felhasználó számára teljes hozzáférést biztosít a helyi nyomtatókhoz. A felhasználók az operációs rendszer által biztosított eszközökkel nyomtatókat csatlakoztathatnak és dokumentumokat nyomtathatnak.

- **Blokkolás** ⊘. A Kaspersky Endpoint Security blokkolja a helyi nyomtatók csatlakozását. Az alkalmazás csak megbízható nyomtatókhoz való csatlakozást tesz lehetővé.

- **A csatlakozási busztól függ**. A Kaspersky Endpoint Security lehetővé teszi a helyi nyomtatókhoz való csatlakozást az USB-busz kapcsolati állapotának megfelelően (**Engedélyezés** vagy **Blokkolás**).

- **Szabályok szerint**. A nyomtatás szabályozásához hozzá kell adnia a *nyomtatási szabályokat*. A szabályokban kiválaszthat olyan felhasználókat vagy felhasználói csoportokat, amelyek számára engedélyezni vagy blokkolni szeretné a dokumentumok helyi nyomtatókon történő nyomtatását.

Hálózati nyomtató szabályozása

A Kaspersky Endpoint Security lehetővé teszi a hálózati nyomtatókon való nyomtatás hozzáférésének konfigurálását. A hálózati nyomtatók elérési módjai közül választhat:

- **Engedélyezés és nem naplózás**. A Kaspersky Endpoint Security nem szabályozza a hálózati nyomtatókon történő nyomtatást. Az alkalmazás minden felhasználó számára hozzáférést biztosít a nyomtatáshoz, és nem menti a nyomtatással kapcsolatos információkat az eseménynaplóba.

- **Engedélyezés**. A Kaspersky Endpoint Security minden felhasználó számára hozzáférést biztosít a hálózati nyomtatókon történő nyomtatáshoz.

- **Blokkolás**. A Kaspersky Endpoint Security minden felhasználó számára korlátozza a hálózati nyomtatókhoz való hozzáférést. Az alkalmazás csak megbízható nyomtatókhoz való hozzáférést tesz lehetővé.

- **Szabályok szerint**. A Kaspersky Endpoint Security a nyomtatási szabályoknak megfelelően biztosít hozzáférést a nyomtatáshoz. A szabályokban kiválaszthat olyan felhasználókat vagy felhasználói csoportokat, amelyek számára engedélyezheti vagy blokkolhatja a dokumentumok nyomtatását a hálózati nyomtatón.

Nyomtatási szabályok hozzáadása a nyomtatókhoz

Nyomtatási szabályok hozzáadása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

4. Az **Eszközfelügyelő beállításai** részen válassza ki az **Eszköztípusok** lapot.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.

5. A **Helyi nyomtatók** és a **Hálózati nyomtatók** eszköztípusok helyi menüjében konfigurálja a megfelelő nyomtatók hozzáférési módját: **Engedélyezés**, **Blokkolás**, **Engedélyezés és nem naplózás** (csak hálózati nyomtatóknál) vagy **A csatlakozási busztól függ** (csak helyi nyomtatóknál).

6. A nyomtatási szabályok helyi és hálózati nyomtatókon történő konfigurálásához kattintson duplán a szabálylistákra a megnyitáshoz.

7. Válassza ki a **Szabályokkal** elemet a nyomtató hozzáférési módjaként.

8. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, amelyekre alkalmazni szeretné a nyomtatási szabályt.

   a. Kattintson **Hozzáadás** gombra.

      Ekkor megnyílik az új nyomtatási szabály hozzáadására szolgáló ablak.

   b. Rendeljen prioritást a szabálybejegyzéshez. A szabálybejegyzés a következő attribútumokat tartalmazza: felhasználói fiók, művelet (engedélyezés/blokkolás) és prioritás.

      A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

      Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

      A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

   c. A **Művelet** részen konfigurálja a felhasználó hozzáférését a nyomtatón történő nyomtatáshoz.

   d. A **Felhasználók és csoportok** részre kattintva válassza ki a felhasználókat vagy felhasználói csoportokat a nyomtatáshoz való hozzáféréshez. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   e. Kattintson az **OK** gombra.

9. Mentse el a módosításokat.

Nyomtatási szabályok hozzáadása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **Device Control** elemet.

5. A **Device access rules** részen kattintson a **Devices and Wi-Fi networks** hivatkozásra.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.

6. Válassza a **Local printers** vagy a **Network printers** eszköztípust.

   Ezzel megnyitja a nyomtató hozzáférési szabályait.

7. **Allow**, **Block**, **Allow and do not log** (), **Depends on bus** (csak helyi nyomtatókhoz) vagy **Custom**.

8. Ha az **Custom** módot választja, nyomtatási szabályokat kell hozzáadnia a helyi vagy hálózati nyomtatókhoz. Ehhez kattintson a **Add** gombra a nyomtatási szabályok táblájában.

   Ezzel megnyitja az új nyomtatási szabály beállításait.

9. Rendeljen prioritást a szabálybejegyzéshez. A szabálybejegyzés a következő attribútumokat tartalmazza: felhasználói fiók, művelet (engedélyezés/blokkolás) és prioritás.

   A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

   Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

   A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

10. Az **Action** részen konfigurálja a felhasználó hozzáférését a nyomtatón történő nyomtatáshoz.

11. Az **User or group** részen válassza ki a felhasználókat vagy felhasználói csoportokat a nyomtatáshoz való hozzáféréshez. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

12. Mentse el a módosításokat.

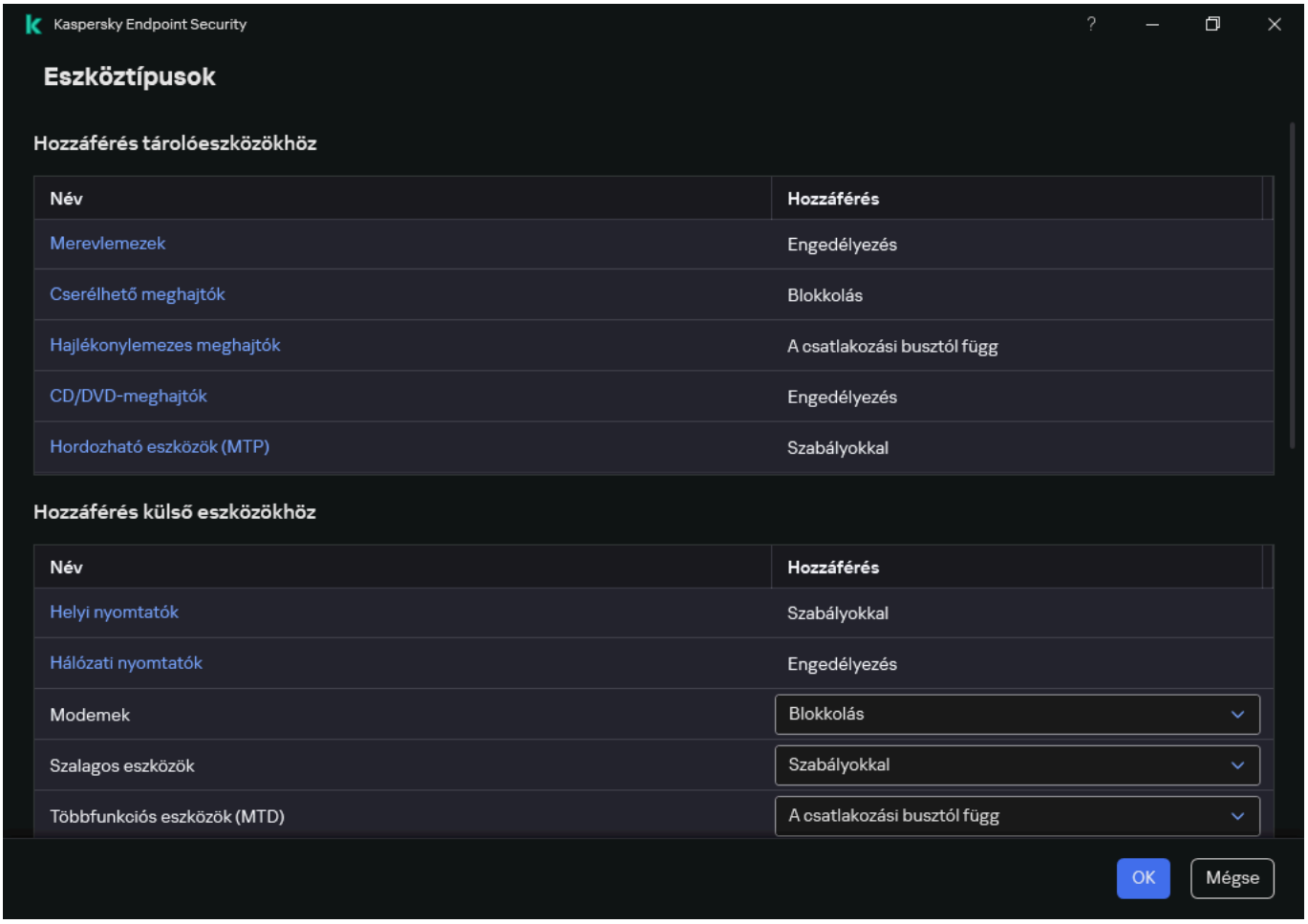
Nyomtatási szabályok hozzáadása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** gombra.

A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes eszköz hozzáférési szabályait megjeleníti.



Eszköztípusok az Eszközfelügyelő összetevőben

4. A **Hozzáférés külső eszközökhöz** részen kattintson a **Helyi nyomtatók** vagy **Hálózati nyomtatók** elemre.

   Ezzel megnyitja a nyomtató hozzáférési szabályait tartalmazó ablakot.

5. A **Hozzáférés a helyi nyomtatókhoz** vagy a **Hozzáférés a hálózati nyomtatókhoz** részen konfigurálja a nyomtatók hozzáférési módját: **Engedélyezés**, **Blokkolás**, **Engedélyezés és nem naplózás** (csak hálózati nyomtatóknál) vagy **A csatlakozási busztól függ** (csak helyi nyomtatóknál) vagy **Szabályokkal**.

6. Ha kiválasztja a **Szabályokkal** módot, nyomtatási szabályokat kell hozzáadnia a nyomtatókhoz. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, amelyekre alkalmazni szeretné a nyomtatási szabályt.

   a. Kattintson **Hozzáadás** gombra.

      Ekkor megnyílik az új nyomtatási szabály hozzáadására szolgáló ablak.

   b. Rendeljen prioritást a szabálybejegyzéshez. A szabálybejegyzés a következő attribútumokat tartalmazza: felhasználói fiók, engedélyek (engedélyezés/blokkolás) és prioritás.

      A szabálynak meghatározott prioritása van. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. A Kaspersky Endpoint Security lehetővé teszi, hogy 0 és 10 000 közötti prioritást adjon meg. Minél magasabb az érték, annál magasabb a prioritás. Más szóval, a 0 értékű bejegyzésnek van a legalacsonyabb prioritása.

      Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 1-s prioritást a rendszergazdák csoporthoz, és rendeljen 0-es prioritást a Mindenki csoporthoz.

A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Más szóval, ha egy felhasználó több csoporthoz lett hozzáadva, és az összes szabály prioritása megegyezik, a Kaspersky Endpoint Security bármely meglévő blokkolási szabály alapján szabályozza az eszközhozzáférést.

c. A **Művelet** részen konfigurálja a felhasználói engedélyeket a nyomtatáshoz való hozzáféréshez.

d. A **Felhasználók és csoportok** részen válassza ki a felhasználókat vagy felhasználói csoportokat a nyomtatáshoz való hozzáféréshez. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

7. Mentse el a módosításokat.

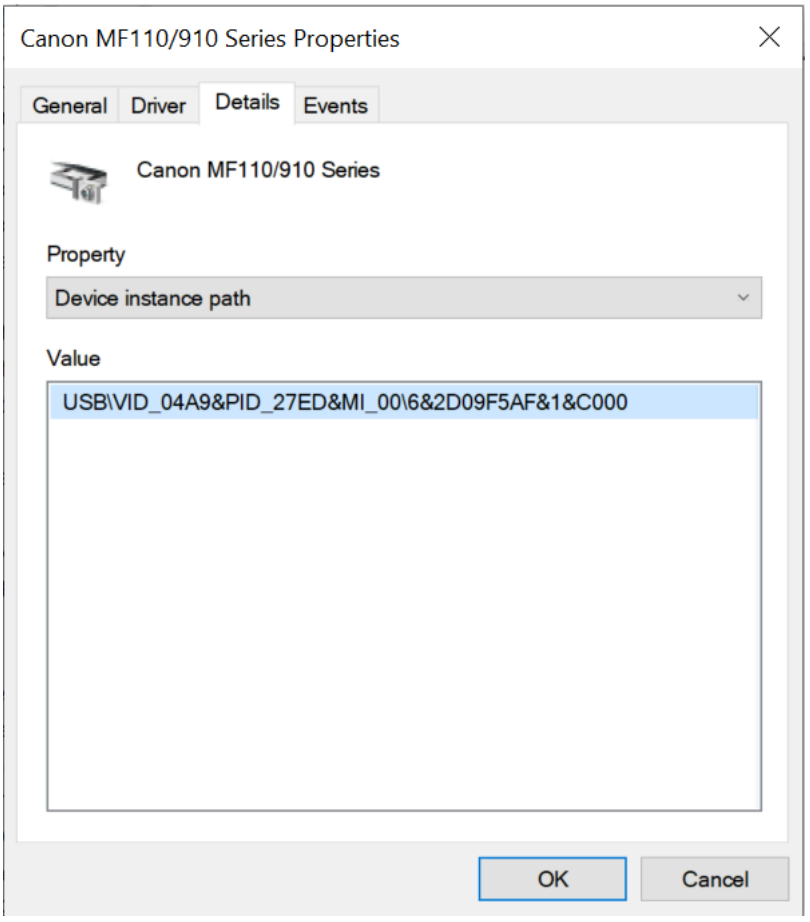
Megbízható nyomtatók

A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

A megbízható nyomtatók hozzáadására szolgáló eljárás pontosan ugyanaz, mint a többi megbízható eszköz esetében. Helyi nyomtatókat azonosító vagy eszközmodell alapján adhat hozzá. Hálózati nyomtatókat csak eszközazonosító alapján adhat hozzá.

Megbízható helyi nyomtató azonosító alapján történő hozzáadásához egyedi azonosítóra (Hardware ID – HWID) lesz szüksége. Az azonosítót az eszköz tulajdonságainál találja az operációs rendszerben (lásd az alábbi ábrát). Az Device Manager eszköz biztosítja ezt. A helyi nyomtató azonosítója így nézhet ki: `6&2D09F5AF&1&C000`. Azonosító alapján kényelmesen lehet eszközöket hozzáadni, ha bizonyos meghatározott eszközöket akar hozzáadni. Használhat maszkokat is.

Megbízható helyi nyomtató eszközmodell szerinti hozzáadásához szükség lesz annak Vendor ID (VID) és Product ID (PID) azonosítójára. Az azonosítókat az eszköz tulajdonságainál találja az operációs rendszerben (lásd az alábbi ábrát). A VID és PID számok megadására szolgáló sablon: `VID_04A9&PID_27FD`. Modell alapján kényelmesen lehet eszközöket hozzáadni, amennyiben a szervezetében használt bizonyos készülékmodelleket akarja használni. Ilyen módon az adott modell valamennyi példányát hozzáadhatja.



Eszközazonosító az Eszközkezelőben

Megbízható hálózati nyomtató hozzáadásához szüksége lesz annak eszközazonosítójára. Hálózati nyomtatók esetén az eszközazonosító lehet a nyomtató hálózati neve (a megosztott nyomtató neve), a nyomtató IP-címe vagy a nyomtató URL-címe.

Wi-Fi kapcsolatok szabályozása

Az Eszközfelügyelő lehetővé teszi a számítógép (laptop) Wi-Fi kapcsolatának kezelését. Előfordulhat, hogy a nyilvános Wi-Fi hálózatok nem biztonságosak, és az ilyen hálózatok használata adatvesztéshez vezethet. Az Eszközfelügyelő lehetővé teszi, hogy megakadályozza, hogy egy felhasználó csatlakozzon a Wi-Fi-hálózathoz, vagy csak megbízható hálózatokhoz csatlakozzon. Például csak a kellően biztonságos céges Wi-Fi hálózathoz engedélyezheti a csatlakozást. Az Eszközfelügyelő a megbízható listán megadottak kivételével az összes Wi-Fi-hálózathoz való hozzáférést blokkolja.

A Windows 11 rendszert futtató számítógépeken engedélyeznie kell a Helymeghatározási szolgáltatásokat a Wi-Fi-kapcsolatok felügyeletéhez. Ehhez engedélyeznie kell a **Helymeghatározási szolgáltatások** kapcsolót az operációs rendszer beállításaiban (**Beállítások → Adatvédelem és biztonság → Helymeghatározás**). Ha a Helymeghatározási szolgáltatások le vannak tiltva, a Kaspersky Endpoint Security nem ellenőrzi a Wi-Fi hálózatokhoz való kapcsolódásokat.

A háttérvizsgálat engedélyezése az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
4. Az **Eszközfelügyelő beállításai** részen válassza ki az **Eszköztípusok** lapot.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.
5. A **Wi-Fi** eszköztípus helyi menüjében válassza ki a Wi-Fi-hez való csatlakozáskor végrehajtott eszközfelügyelői műveletet: **Engedélyezés** (), **Blokkolás** () vagy **Blokkolás kivételekkel** ().
6. Ha kiválasztotta a **Blokkolás kivételekkel** lehetőséget, hozzon létre egy listát a megbízható Wi-Fi hálózatokkal:

   a. Kattintson duplán a megbízható Wi-Fi hálózatok listájának megnyitásához.

   b. A **Megbízható Wi-Fi-hálózatok** részen kattintson a **Hozzáadás** gombra.

   c. Ezzel megnyílik egy ablak, ahol konfigurálhatja a megbízható Wi-Fi hálózatot (lásd az alábbi ábrát):

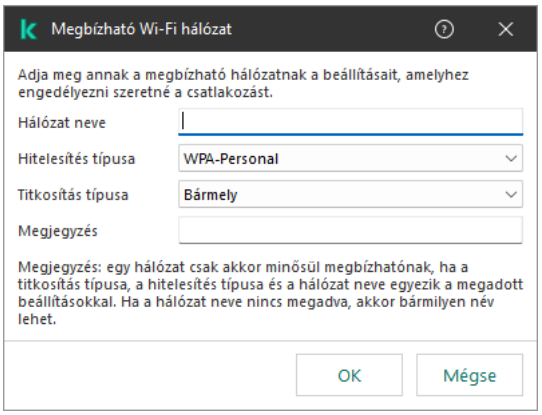
   - **Hálózat neve**. A Wi-Fi hálózat neve vagy SSID-je (Service Set Identifier).
   - **Hitelesítés típusa**. A Wi-Fi hálózathoz való csatlakozáskor használt hitelesítési típus.

     A Kaspersky Endpoint Security for Windows 12.0-s verziójától kezdve a WPA3 protokoll támogatása hozzáadásra került az alkalmazáshoz. Ha a Kaspersky Endpoint Security 12.2 verziójú házirendjét alkalmazza egy számítógépen, a Kaspersky Endpoint Security 11.11.0 és korábbi verziójú számítógépeken a WPA2 protokoll van kiválasztva; a 12.0-12.1 verziók esetében a WPA2 / WPA3; a 12.2 és újabb verziók esetében a WPA3.
   - **Titkosítás típusa**. A Wi-Fi forgalom védelmére használt titkosítási típus.
   - **Megjegyzés**. További információ a hozzáadott Wi-Fi hálózatról.

   A megbízható Wi-Fi hálózat beállításait az útválasztó beállításainál tekintheti meg.

   A Wi-Fi-hálózatok akkor minősülnek megbízhatónak, ha beállításaik a szabályban megadott összes szabállyal egyeznek.

7. Mentse el a módosításokat.



Megbízható Wi-Fi hálózati beállítások

A Wi-Fi-kapcsolatok korlátozása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Device Control** elemet.
5. A **Device access rules** területen válassza a **Devices and Wi-Fi networks** lapot.

   A táblázat az Eszközfelügyelő összetevő besorolásában szereplő összes eszköz hozzáférési szabályait tartalmazza.
6. A **Wi-Fi networks** részen kattintson a **Wi-Fi** hivatkozásra.
7. A megnyíló ablakban válassza ki a wifihálózathoz való csatlakozáskor végrehajtott eszközfelügyeleti műveletet: **Allow**, **Block** vagy **Block with exclusions**.
8. Ha kiválasztotta a **Block with exclusions** lehetőséget, hozzon létre egy listát a megbízható Wi-Fi hálózatokkal:

   a. Kattintson duplán a megbízható Wi-Fi hálózatok listájának megnyitásához.

   b. A **Trusted Wi-Fi networks** részen kattintson a **Add** gombra.

   c. Ezzel megnyílik egy ablak, ahol konfigurálhatja a megbízható Wi-Fi hálózatot (lásd az alábbi ábrát):

   - **Name**. A Wi-Fi hálózat neve vagy SSID-je (Service Set Identifier).
   - **Authentication type**. A Wi-Fi hálózathoz való csatlakozáskor használt hitelesítési típus.

     A Kaspersky Endpoint Security for Windows 12.0-s verziójától kezdve a WPA3 protokoll támogatása hozzáadásra került az alkalmazáshoz. Ha a Kaspersky Endpoint Security 12.2 verziójú házirendjét alkalmazza egy számítógépen, a Kaspersky Endpoint Security 11.11.0 és korábbi verziójú számítógépeken a WPA2 protokoll van kiválasztva; a 12.0-12.1 verziók esetében a WPA2 / WPA3; a 12.2 és újabb verziók esetében a WPA3.

- **Encryption type**. A Wi-Fi forgalom védelmére használt titkosítási típus.
- **Comment**. További információ a hozzáadott Wi-Fi hálózatról.

A megbízható Wi-Fi hálózat beállításait az útválasztó beállításainál tekintheti meg.

> A Wi-Fi-hálózatok akkor minősülnek megbízhatónak, ha beállításaik a szabályban megadott összes szabállyal egyeznek.

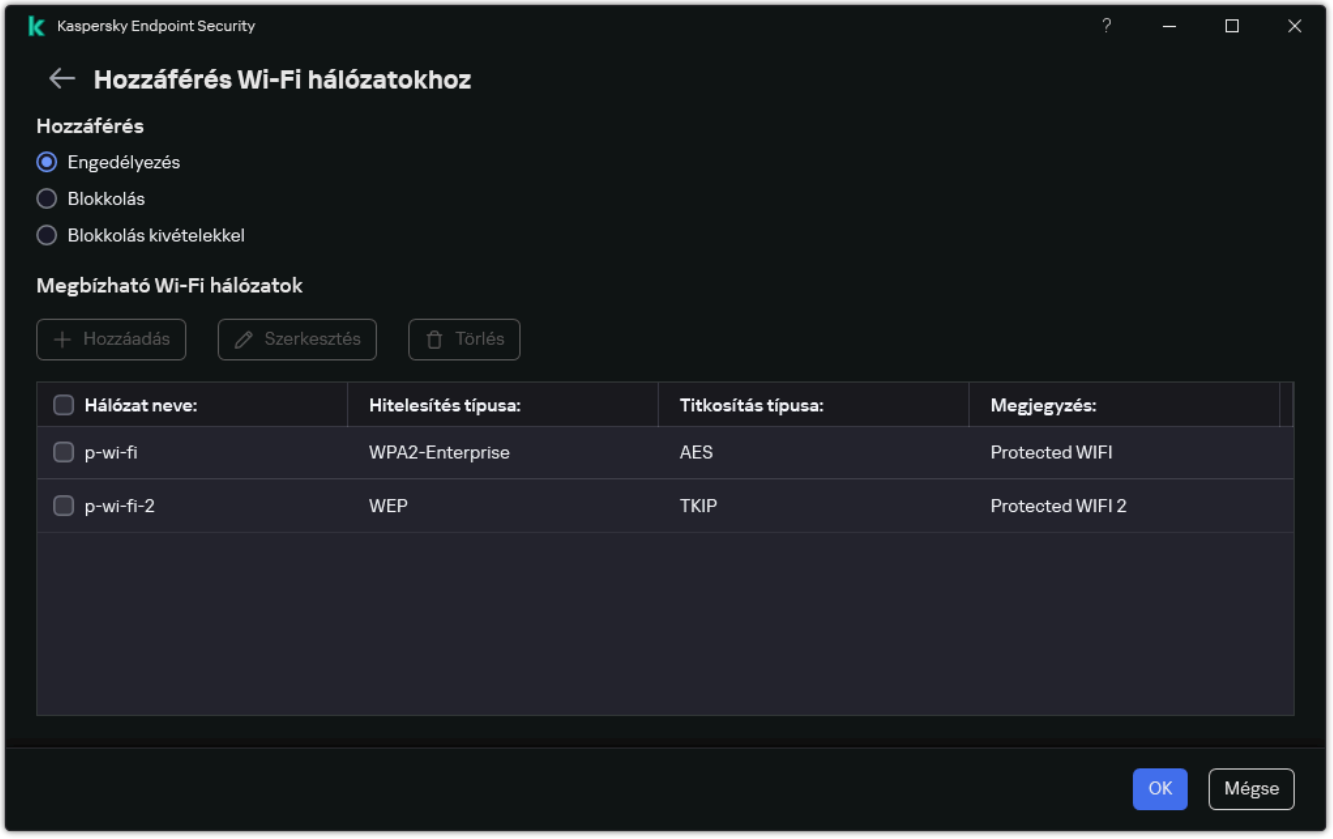
9. Mentse el a módosításokat.

A Wi-Fi kapcsolatok korlátozása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** gombra.

   A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes eszköz hozzáférési szabályait megjeleníti.
4. A **Hozzáférés Wi-Fi hálózatokhoz** blokkban kattintson a **Wi-Fi** hivatkozásra.

   A megnyitott ablakban a Wi-Fi hálózati hozzáférési szabályok láthatók.



Wi-Fi hozzáférési beállítások

5. A **Hozzáférés** részen válassza ki a Wi-Fi-hez való csatlakozáskor végrehajtott eszközfelügyelői műveletet: **Engedélyezés**, **Blokkolás** vagy **Blokkolás kivételekkel**.

6. Ha kiválasztotta a **Blokkolás kivételekkel** lehetőséget, hozzon létre egy listát a megbízható Wi-Fi hálózatokkal:

   a. A **Megbízható Wi-Fi-hálózatok** részen kattintson a **Hozzáadás** gombra.

   b. Ezzel megnyílik egy ablak, ahol konfigurálhatja a megbízható Wi-Fi hálózatot (lásd az alábbi ábrát):

   - **Hálózat neve**. A Wi-Fi hálózat neve vagy SSID-je (Service Set Identifier).
   - **Hitelesítés típusa**. A Wi-Fi hálózathoz való csatlakozáskor használt hitelesítési típus.

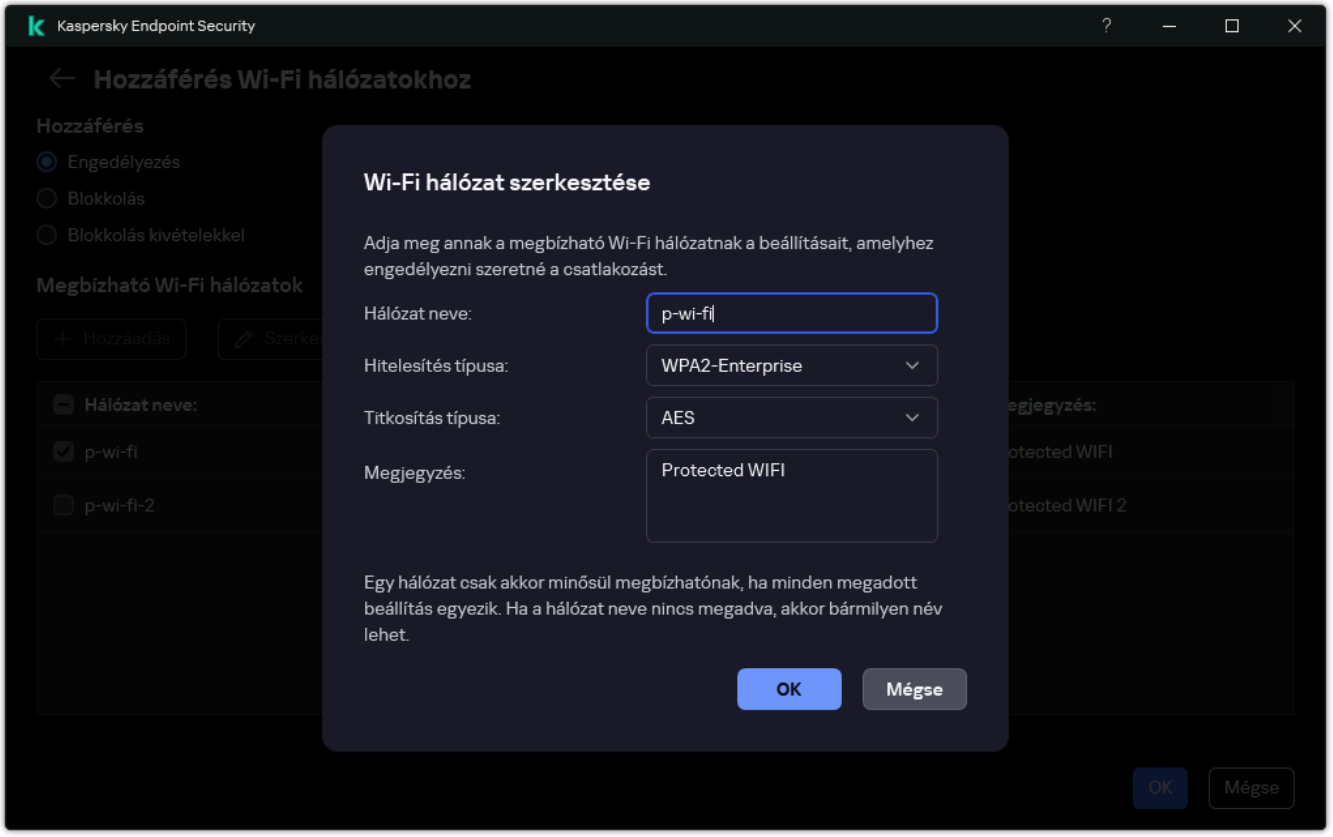
     A Kaspersky Endpoint Security for Windows 12.0-s verziójától kezdve a WPA3 protokoll támogatása hozzáadásra került az alkalmazáshoz. Ha a Kaspersky Endpoint Security 12.2 verziójú házirendjét alkalmazza egy számítógépen, a Kaspersky Endpoint Security 11.11.0 és korábbi verziójú számítógépeken a WPA2 protokoll van kiválasztva; a 12.0-12.1 verziók esetében a WPA2 / WPA3; a 12.2 és újabb verziók esetében a WPA3.

   - **Titkosítás típusa**. A Wi-Fi forgalom védelmére használt titkosítási típus.
   - **Megjegyzés**. További információ a hozzáadott Wi-Fi hálózatról.

   A megbízható Wi-Fi hálózat beállításait az útválasztó beállításainál tekintheti meg.

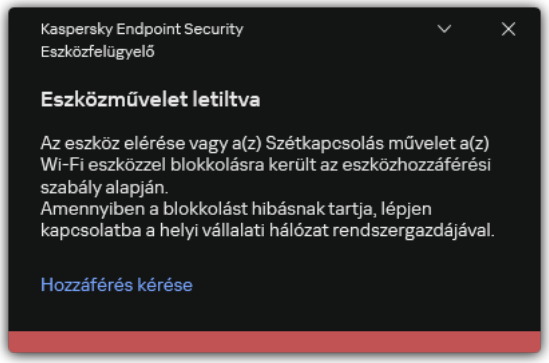
   A Wi-Fi-hálózatok akkor minősülnek megbízhatónak, ha beállításaik a szabályban megadott összes szabállyal egyeznek.

7. Mentse el a módosításokat.



Megbízható Wi-Fi hálózati beállítások

Ennek eredményeként, ha a felhasználó olyan Wi-Fi hálózathoz próbál csatlakozni, amely nem szerepel a megbízhatóként azonosított hálózatok listáján, az alkalmazás blokkolja a kapcsolatot, és értesítést jelenít meg (lásd az alábbi ábrát).



Eszközfelügyelő értesítés

Cserélhető meghajtók használatának figyelése

A cserélhető meghajtók használatának figyelése magában foglalja:

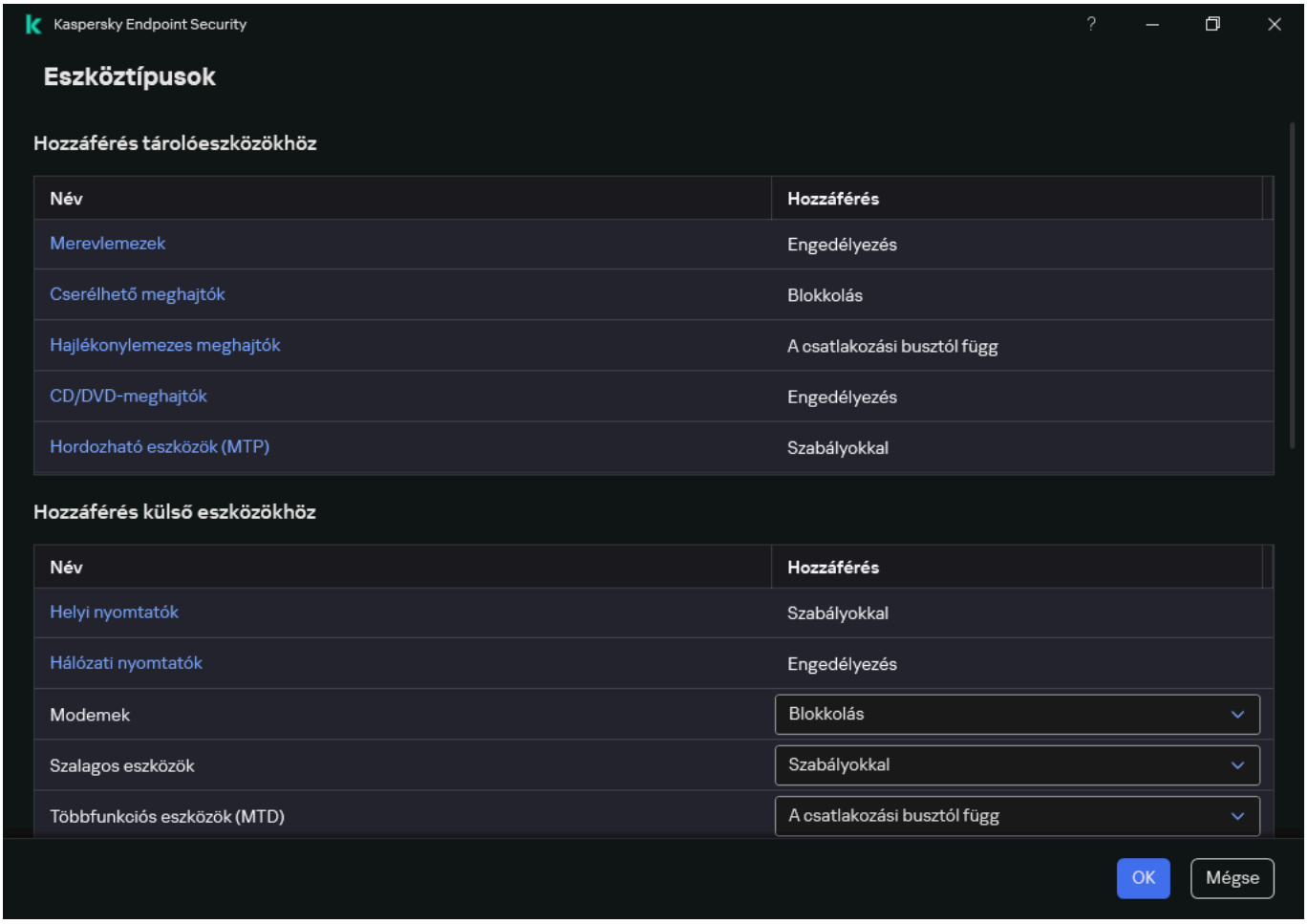
- A cserélhető meghajtók fájljainak figyelése.
- A megbízható cserélhető meghajtók csatlakoztatásának és leválasztásának figyelése.

  A Kaspersky Endpoint Security lehetővé teszi az összes megbízható eszköz – és nem csak a cserélhető meghajtók – csatlakoztatásának és leválasztásának felügyeletét. Bekapcsolhatja az eseménynaplózást az Eszközfelügyelő összetevő értesítési beállításaiban. Az események *Információs üzenet* súlyossági szinttel rendelkeznek.

A cserélhető meghajtók használata figyelésének engedélyezése:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson a **Készülékek és Wi-Fi hálózatok** gombra.

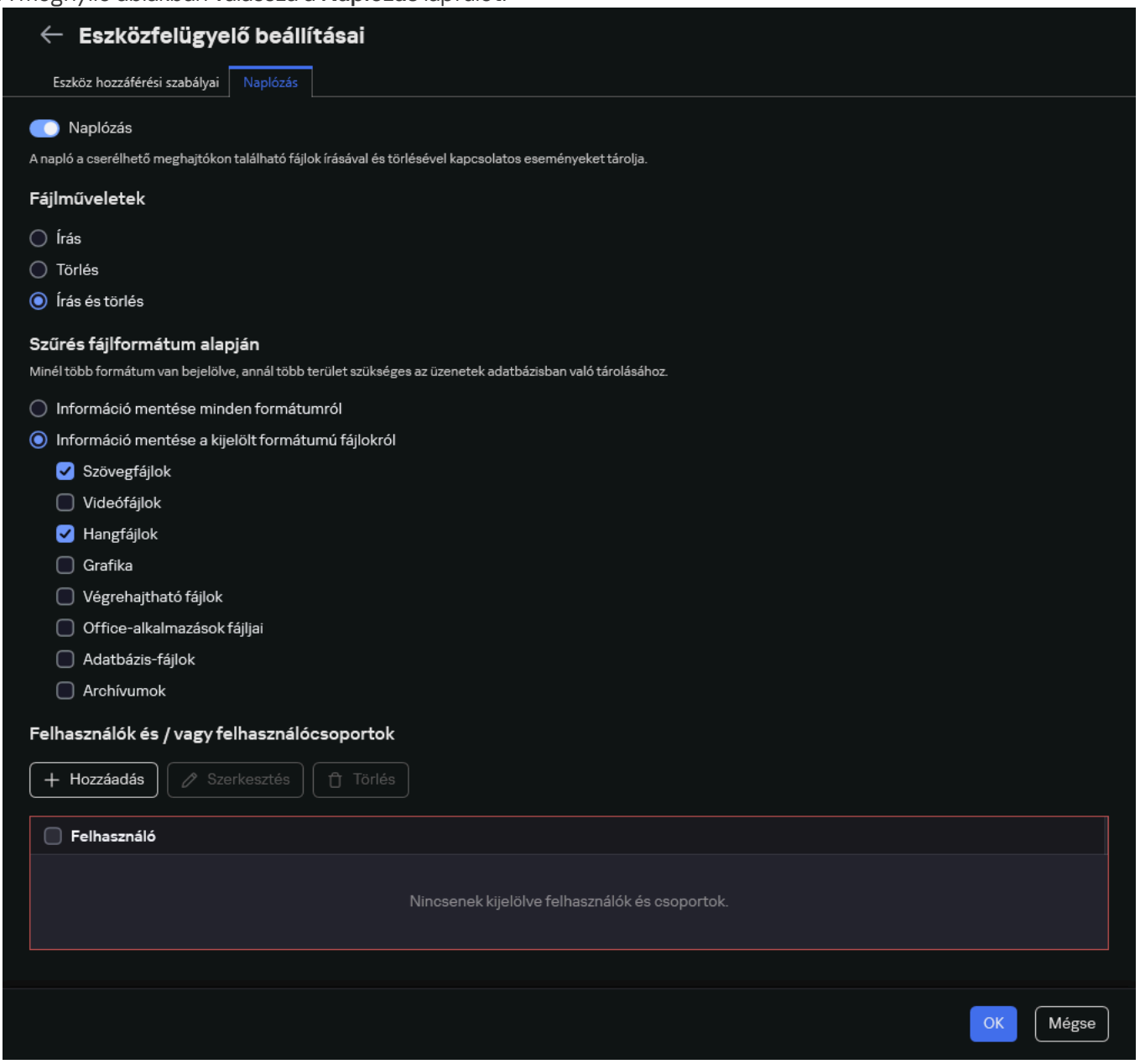
A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes eszköz hozzáférési szabályait megjeleníti.



Eszköztípusok az Eszközfelügyelő összetevőben

4. A **Hozzáférés tárolóeszközökhöz** részen válassza a **Cserélhető meghajtók** lehetőséget.

5. A megnyíló ablakban válassza a **Naplózás** lapfület.



A cserélhető meghajtó használatának figyelési beállításai

6. Kapcsolja be a **Naplózás** kapcsolót.

7. A **Fájlműveletek** blokkban válassza ki a megfigyelni kívánt műveletet: **Írás**, **Törlés**.

8. A **Szűrés fájlformátum alapján** blokkban válassza ki a fájlformátumokat, amelyek társított műveleteit naplóznia kell az Eszközfelügyelőnek.

9. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, akiknél a cserélhető meghajtók használatát figyelni szeretné.

10. Mentse el a módosításokat.

Ennek eredményeként, ha a felhasználók cserélhető meghajtókon lévő fájlokba írnak vagy onnan fájlokat törölnek, a Kaspersky Endpoint Security az e műveletekre vonatkozó információkat menti az eseménynaplóba, és az eseményeket elküldi a Kaspersky Security Centerbe. A cserélhető meghajtókon lévő fájlokhoz kapcsolódó eseményeket a Kaspersky Security Center Adminisztrációs Konzolon az **Administration Server** csomópont munkaterületén, az **Events** lapon tekintheti meg. Ahhoz, hogy az események a helyi Kaspersky Endpoint Security-eseménynaplóban megjelenjenek, be kell jelölni a **Fájlművelet elvégezve** jelölőnégyzetet az Eszközfelügyelő összetevő értesítési beállításaiban.

A gyorsítótárazás időtartamának módosítása

Az Eszközfelügyelő összetevő regisztrálja a felügyelt eszközökkel kapcsolatos eseményeket, például egy eszköz csatlakoztatását és leválasztását, fájlolvasást eszközről, fájlírást eszközre és más eseményeket. Az Eszközfelügyelő ekkor a Kaspersky Endpoint Security beállításainak megfelelően engedélyezi vagy blokkolja a műveletet.

Az Eszközfelügyelő meghatározott ideig, az úgynevezett *gyorsítótárazás időtartamáig*, információkat tárol az eseményekről. Ha az eseményre vonatkozó információk gyorsítótárazva vannak és ez az esemény megismétlődik, akkor nem kell erről értesíteni a Kaspersky Endpoint Security-t, és nem kell új kérést megjeleníteni a megfelelő művelethez való hozzáférés megadásához, például az eszköz csatlakoztatásához. Ez megkönnyíti az eszközzel való munkát.

Egy esemény duplikált eseménynek minősül, ha a következő eseménybeállítások mindegyike megegyezik a gyorsítótárban található bejegyzéssel:

- eszközazonosító;
- a hozzáférést megkísérlő felhasználói fiók SID-je;
- eszközkategória;
- az eszközzel végrehajtott művelet;
- Alkalmazási engedély erre a műveletre: engedélyezett vagy elutasított
- a művelethez használt folyamat elérési útja;
- az elérni kívánt fájl.

A gyorsítótárazási időtartam megváltoztatása előtt tiltsa le a Kaspersky Endpoint Security Önvédelmet. A gyorsítótárazási időtartam megváltoztatása után engedélyezze az Önvédelmet.

A gyorsítótárazási időtartam megváltoztatásához:

1. Nyissa meg a rendszerleíróadatbázis-szerkesztőt a számítógépen.
2. A rendszerleíróadatbázis-szerkesztőben lépjen a következő szakaszra:
   - 64 bites operációs rendszereknél:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - 32 bites operációs rendszereknél:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. Nyissa meg szerkesztésre a `DeviceControlEventsCachePeriod` beállítást.
4. Adja meg, hány percig kell az Eszközfelügyelőnek elmentenie az információkat egy eseményről, mielőtt ezek az információk törlődnek.

Megbízható eszközökkel végzett műveletek

A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

A megbízható eszközökkel való munkavégzéshez lehetősége van hozzáférést biztosítani egy adott felhasználónak, a felhasználók adott csoportjának vagy a szervezet minden felhasználójának.

Ha például a szervezet nem engedélyezi cserélhető meghajtó használatát, de a rendszergazdák használnak ilyet a munkájuk során, lehetősége van engedélyezni a cserélhető meghajtók használatát csak a rendszergazdák csoportja számára. Ehhez vegye fel a cserélhető meghajtókat a megbízható eszközök listájára, és konfigurálja a felhasználói hozzáférési jogosultságokat.

Nem ajánlott 5000-nél több megbízható eszközt hozzáadni, mivel ez a rendszer instabilitását okozhatja.

A Kaspersky Endpoint Security a következő módokat kínálja ahhoz, hogy eszközt vegyen fel a megbízható eszközök listájára:

- Ha a Kaspersky Security Center nincs telepítve a szervezetében, csatlakoztathatja az eszközt a számítógéphez, majd felveheti a megbízható eszközök listájára az alkalmazás beállításaiban. Ha a szervezet minden számítógépéhez el kívánja juttatni a megbízható eszközök listáját, engedélyezheti rendszabályban a megbízható eszközök listáinak egyesítését, illetve használhatja az exportálási/importálási eljárást.

- Ha a Kaspersky Security Center telepítve van a szervezetében, lehetősége van távolról észlelni minden csatlakoztatott eszközt, és létrehozni a megbízható eszközök listáját a rendszabályban. A megbízható eszközök listája minden olyan számítógépen rendelkezésre fog állni, amelyen be van vezetve a rendszabály.

A Kaspersky Endpoint Security lehetővé teszi a megbízható eszközök használatának ellenőrzését (kapcsolódás és leválasztás). Bekapcsolhatja az eseménynaplózást az Eszközfelügyelő összetevő értesítési beállításaiban. Az események *Informational messages* súlyossági szinttel rendelkeznek.

Eszköz felvétele a megbízható listára az alkalmazás kezelőfelületén

Alapértelmezés szerint eszköz megbízható eszközök listájára történő felvételekor minden felhasználó (a Mindenki felhasználói csoport) hozzáférést kap hozzá.

Eszköz felvétele a megbízható listára az alkalmazás kezelőfelületén:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

3. A **Hozzáférési beállítások** részen kattintson a **Megbízható eszközök** gombra.

   Erre megnyílik a megbízható eszközök listája.

4. Kattintson **Kijelölés** gombra.

   Erre megnyílik a csatlakoztatott eszközök listája. Az eszközök listája a **Csatlakoztatott eszközök megjelenítése** legördülő listán kiválasztott értéktől függ.

5. Az eszközök listájában jelölje ki azt az eszközt, amelyet hozzá szeretne adni a megbízhatók listájához.

   A Kaspersky Endpoint Security nem támogatja a **floppylemez** típusú eszközök hozzáadását a megbízható listához.

6. A **Megjegyzés** mezőben a megbízható eszközre vonatkozó minden lényeges információt megadhat.

7. Válassza ki azokat a felhasználókat vagy felhasználói csoportokat, amelyeknek engedélyezni szeretné a hozzáférést a megbízható eszközökhöz.

   A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

8. Mentse el a módosításokat.

Eszköz felvétele a megbízható listára a Kaspersky Security Centerben.

A Kaspersky Security Center akkor kap információt az eszközökről, ha a Kaspersky Endpoint Security telepítve van, és aktiválva van az Eszközfelügyelő. Nem lehet felvenni eszközt a megbízható eszközök listájára, hacsak nem áll rendelkezésre rá vonatkozó adat a Kaspersky Security Centerben.

Eszközt a következő adatok alapján lehet felvenni a megbízható eszközök listájára:

- **Eszközök azonosító alapján**. Minden eszköz egyedi azonosítóval rendelkezik (Hardverazonosítóval, azaz HWID-vel). Megtekintheti az azonosítót az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. Példa az eszközazonosítóra: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Azonosító alapján kényelmesen lehet eszközöket hozzáadni, ha bizonyos meghatározott eszközöket akar hozzáadni.

- **Eszközök típus alapján**. Minden eszköz rendelkezik egy gyártóazonosítóval (VID) és termékazonosítóval (PID). Megtekintheti az azonosítókat az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. A VID és PID számok megadására szolgáló sablon: `VID_1234&PID_5678`. Modell alapján kényelmesen lehet eszközöket hozzáadni, amennyiben a szervezetében használt bizonyos készülékmodelleket akarja használni. Ilyen módon az adott modell valamennyi példányát hozzáadhatja.

- **Eszközök azonosítómaszk alapján**. Ha több eszközt használ, amelyek azonosítója megegyezik, akkor maszkok segítségével veheti fel azokat a megbízható listára. A `*` karakter akármilyen karakterláncot helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `WDC_C*`.

- **Eszközök modellmaszk alapján**. Ha több eszközt használ hasonló VID vagy PID azonosítóval (például ugyanattól a gyártótól származó eszközök), akkor maszkokkal hozzáadhat készülékeket a megbízható listához. A `*` karakter akármilyen karakterláncot helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `VID_05AC&PID_*`.

A megbízható eszközök listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Eszköz hozzáadása a megbízható eszközök listájához:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
4. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.
5. Válassza az **Értékek egyesítése öröklésкor** jelölőnégyzetet, ha egy összesített listát szeretne létrehozni a vállalat összes számítógépén lévő megbízható eszközökről.

   A szülő és gyermek rendszabályokban lévő megbízható eszközök listája egyesítve lesz. A lista egyesítve lesz, ha öröklésкor az értékek egyesítése öröklésкor engedélyezve van. A szülő rendszabályban lévő megbízható eszközök a gyermek rendszabályokban csak olvasható nézetben jelennek meg. A szülő rendszabályban lévő megbízható eszközöket nem tudja módosítani vagy törölni.
6. Kattintson a **Hozzáadás** gombra, és válasszon módszert az eszköz megbízható listára történő felvételéhez.

7. Az eszközök szűréséhez válasszon egy eszköztípust az **Eszköztípus** legördülő listában (például: **Cserélhető meghajtók**).

   A Kaspersky Endpoint Security nem támogatja a **floppylemez** típusú eszközök hozzáadását a megbízható listához.

8. A **Név/modell** mezőben adja meg az eszközazonosítót, a modellt (VID és a PID-azonosító) vagy a maszkot a választott hozzáadási metódusnak megfelelően.

   A eszközök modellmaszk (VID és PID) alapján történő hozzáadása a következő módon működik: ha olyan modellmaszkot ad meg, ami nem egyezik egy modellel sem, a Kaspersky Endpoint Security ellenőrizni fogja, hogy az eszközazonosító (HWID) megegyezik-e a maszkkal. A Kaspersky Endpoint Security az eszközazonosító csak azon részét ellenőrzi, amely meghatározza a gyártót és a készülék típusát (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Ha a modellmaszk megegyezik az eszközazonosító ezen részével, akkor a maszkkal megegyező készülékek hozzá lesznek adva a számítógépen a megbízható eszközök listájához. Ugyanakkor a Kaspersky Security Center eszközlistája üres marad, ha a **Refresh** gombra kattint. Ahhoz, hogy helyesen jelenítse meg az eszközök listáját, hozzáadhat eszközöket azonosítómaszk alapján.

9. Az eszközök szűréséhez a **Számítógép** mezőben adja meg annak a számítógépnek a nevét – vagy egy maszkot annak a számítógépnek a nevéhez –, amelyhez az eszköz csatlakoztatva van.

   A `*` karakter akármilyen karakterláncot helyettesíthet. A `?` karakter bármilyen karaktert helyettesíthet.

10. Kattintson az **Refresh** gombra.

    A táblázatban szerepel a megadott szűrési feltételeknek megfelelő eszközök listája.

11. A nevük melletti jelölőnégyzettel válassza ki a megbízható eszközök listájára felvenni kívánt eszközöket.

12. A **Megjegyzés** mezőben írja le, hogy mi indokolja az eszközök felvételét a megbízható eszközök listájára.

13. Kattintson a **Select** gombra, amely az **Engedélyezve a következő felhasználók és/vagy csoportok számára** mezőtől jobbra található.

14. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

    Alapértelmezés szerint a megbízható eszközök a „Mindenki” csoport számára érhetők el.

15. Mentse el a módosításokat.

    Eszköz csatlakoztatásakor a Kaspersky Endpoint Security összeveti az eszközt a megbízható eszközök listájával, bejelentkezett felhasználó esetén. Ha az eszköz megbízható, a Kaspersky Endpoint Security akkor is minden jogosultsággal együtt lehetővé teszi a hozzáférést az eszközhöz, ha az adott eszköztípus vagy csatlakozási busz elérése tiltott. Ha az eszköz nem megbízható és a hozzáférés nem engedélyezett, Önnek lehetősége kérelmezni a hozzáférést a zárolt eszközhöz.

Megbízható eszközök listájának exportálása és importálása

Ha a szervezet minden számítógépéhez el kívánja juttatni a megbízható eszközök listáját, használhatja az exportálási/importálási eljárást.

Ha például a megbízható cserélhető meghajtók listáját szeretné szétküldeni, a következőket kell tennie:

1. Egymás után csatlakoztassa a cserélhető meghajtókat a számítógépéhez.
2. A Kaspersky Endpoint Security beállításai között vegye fel a cserélhető meghajtókat a megbízható eszközök listájára. Ha szükséges, konfigurálja a felhasználói hozzáférési jogosultságokat. Lehetősége van például csak a rendszergazdák számára engedélyezni a cserélhető meghajtók tartalmának elérését.
3. Exportálja a Kaspersky Endpoint Security beállításaiban szereplő, megbízható eszközök listáját (részletek az alábbi útmutatóban).
4. Küldje el a megbízható eszközök listáját tartalmazó fájlt a szervezet többi számítógépének. Például helyezze a fájlt egy megosztott mappába.
5. Importálja a Kaspersky Endpoint Security beállításaiban szereplő, megbízható eszközök listáját a szervezet többi számítógépén (részletek az alábbi útmutatóban).

Megbízható eszközök listájának importálása vagy exportálása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet → Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson a **Megbízható eszközök** gombra.

   Erre megnyílik a megbízható eszközök listája.
4. Megbízható eszközök listájának exportálása:
   a. Jelölje ki az exportálni kívánt megbízható eszközöket.
   b. Kattintson az **Export** gombra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a megbízható eszközök listáját, és válassza a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.

      A Kaspersky Endpoint Security a megbízható eszközök teljes listáját exportálja az XML-fájlba.
5. Megbízható eszközök listájának importálása:
   a. Az **Importálás** legördülő listában válassza ki a vonatkozó műveletet: **Importálás és hozzáadás a meglévőkhöz** vagy **Importálás és a meglévők cseréje**.
   b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a megbízható eszközök listáját.
   c. Nyissa meg a fájlt.
6. Mentse el a módosításokat.

Eszköz csatlakoztatásakor a Kaspersky Endpoint Security összeveti az eszközt a megbízható eszközök listájával, bejelentkezett felhasználó esetén. Ha az eszköz megbízható, a Kaspersky Endpoint Security akkor is minden jogosultsággal együtt lehetővé teszi a hozzáférést az eszközhöz, ha az adott eszköztípus vagy csatlakozási busz elérése tiltott.

Blokkolt eszközhöz való hozzáférés megszerzése

Ha beállítja az Eszközfelügyelőt, akkor véletlenül blokkolhatja egy olyan eszköz elérését, ami a munkához szükséges.

Ha a Kaspersky Security Center nem működik a rendszerében, megadhatja az eszköz elérését a Kaspersky Endpoint Security beállításaiban. Például hozzáadhat egy eszközt a megbízható listához, vagy átmenetileg kikapcsolhatja az Eszközfelügyelőt.

Ha a Kaspersky Security Center működik a rendszerében, és a rendszabály alkalmazva van a számítógépeknél, akkor hozzáférést adhat az eszközhöz az Adminisztrációs Konzolban.

Online mode a hozzáférés megadásához

Csak akkor adhat online módban való hozzáférést a blokkolt eszközökhöz, ha a Kaspersky Security Center működik a rendszerben, és a rendszabály alkalmazva van a számítógépen. A számítógépnek képesnek kell lennie kapcsolatot létrehozni az Adminisztrációs kiszolgálóval.

Ha online módban ad hozzáférést, az a következő lépésekből áll:

1. A felhasználó üzenetet küld a rendszergazdának, ami egy hozzáférési kérelmet tartalmaz.
2. A rendszergazda üzenetet kap a kéréssel a Kaspersky Security Center konzolon.

   A Kaspersky Security Center konzol előre beállított eseményválasztással rendelkezik *User requests* a felhasználóktól érkező üzenetek egyszerű nyomon követéséhez.
3. A rendszergazda hozzáadja az eszközt a megbízható listához.

   Hozzáadhat egy megbízható eszközt egy egyéni számítógépnek az adminisztrációs csoport rendszabályában vagy a helyi alkalmazásbeállításokban.
4. A rendszergazda frissíti a Kaspersky Endpoint Security beállításait a felhasználói számítógépen.



Vázlat az eszközök hozzáférésének megadásához online módban

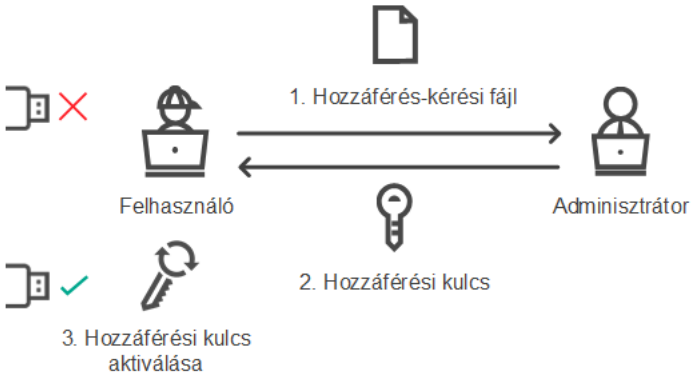
Offline mode a hozzáférés megadásához

Csak akkor adhat offline módban való hozzáférést a blokkolt eszközökhöz, ha a Kaspersky Security Center működik a rendszerben, és a rendszabály alkalmazva van a számítógépen. A rendszabálybeállításokban az **Device control** részben az **Ideiglenes hozzáférési kérelem engedélyezése** jelölőnégyzetet be kell jelölni.

Ha átmeneti hozzáférést akar adni egy blokkolt eszköznek, de nem tudja hozzáadni az eszközt a megbízható listához, akkor offline módban is hozzáférést adhat az eszközhöz. Így még akkor is hozzáférést adhat egy blokkolt eszközhöz, ha a számítógépen nincs hálózati hozzáférés, vagy akkor, ha a számítógép nincs a vállalati hálózaton belül.

Ha offline módban ad hozzáférést, az a következő lépésekből áll:

1. A felhasználó létrehoz egy hozzáférés-kérési fájlt, és elküldi a rendszergazdának.
2. A rendszergazda hozzáad egy hozzáférési kulcsot a hozzáférés-kérési fájlból, majd elküldi a felhasználónak.
3. A felhasználó aktiválja a hozzáférési kulcsot.



Vázlat az eszközök hozzáférésének megadásához offline módban

Online mode a hozzáférés megadásához

Csak akkor adhat online módban való hozzáférést a blokkolt eszközökhöz, ha a Kaspersky Security Center működik a rendszerben, és a rendszabály alkalmazva van a számítógépen. A számítógépnek képesnek kell lennie kapcsolatot létrehozni az Adminisztrációs kiszolgálóval.

A blokkolt eszközök elérésére irányuló felhasználói kérelmek a következőek:

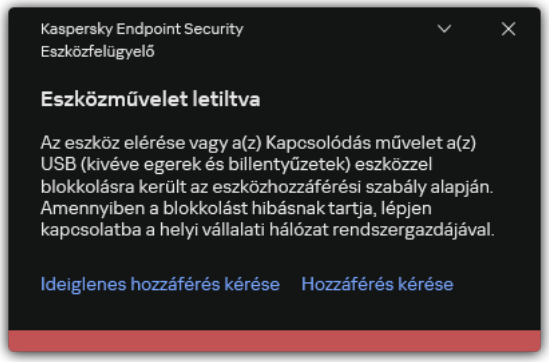
1. Csatlakoztassa az eszközt a számítógéphez.

   A Kaspersky Endpoint Security megjelenít egy értesítést, miszerint az eszköz elérést blokkolva van (lásd az alábbi ábrát).

2. Kattintson a **Hozzáférési kérése** hivatkozásra.

   Ekkor megnyílik egy ablak a rendszergazdának szóló üzenettel. Ez az üzenet információt tartalmaz a blokkolt eszközről.

3. Kattintson a **Küldés** gombra.



Eszközfelügyelő értesítés

Ezután a Kaspersky Security Center konzolon a rendszergazda megkapja az *Eszközhozzáférés blokkolására vonatkozó üzenet az adminisztrátornak* eseményt. Az esemény tartalmazza a felhasználónevet, a számítógép nevét, annak az eszköznek a részleteit, amelyhez a felhasználó hozzáférni próbál, valamint egyéb információkat. Beállíthatja, hogy a rendszergazda hogyan kapjon értesítést az ilyen eseményekről, és például választhatja az e-mail-értesítést. A Kaspersky Security Center konzol előre beállított eseményválasztással rendelkezik *User requests* a felhasználóktól érkező üzenetek egyszerű nyomon követéséhez.

A hozzáférés engedélyezéséhez hozzá kell adnia az eszközt a megbízható eszközök listájához. Miután frissíti a Kaspersky Endpoint Security beállításait a számítógépen, a felhasználó hozzáférést kap az eszközhöz.

Offline mode a hozzáférés megadásához

Csak akkor adhat offline módban való hozzáférést a blokkolt eszközökhöz, ha a Kaspersky Security Center működik a rendszerben, és a rendszabály alkalmazva van a számítógépen. A rendszabálybeállításokban az **Device control** részben az **Ideiglenes hozzáférési kérelem engedélyezése** jelölőnégyzetet be kell jelölni.

A blokkolt eszközök elérésére irányuló felhasználói kérelmek a következőek:

1. Csatlakoztassa az eszközt a számítógéphez.

   A Kaspersky Endpoint Security megjelenít egy értesítést, miszerint az eszköz elérést blokkolva van (lásd az alábbi ábrát).

2. Kattintson az **Ideiglenes hozzáférés kérése** hivatkozásra.

   Ez megnyitja a csatlakoztatott eszközök listáját tartalmazó ablakot.

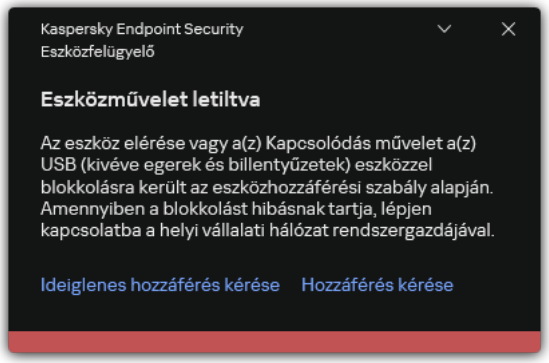
3. Válassza ki a csatlakoztatott eszközök listáján azt az eszközt, amelyhez hozzáférést szeretne kapni.

4. Kattintson a **Hozzáférés-kérési fájl előállítása** elemre.

5. Adja meg a **Hozzáférés időtartama** mezőben azt az időszakot, ameddig hozzáférést szeretne az eszközhöz.

6. Fájl mentése a számítógépes memóriába.

Ennek eredményeképpen a *.akey kiterjesztésű hozzáférés-kérési fájl letöltődik a számítógépes memóriába. Használja az elérhető módszereket, hogy eszköz hozzáférés-kérési fájlt küldjön a vállalat LAN-rendszergazdájának.



Eszközfelügyelő értesítés

Hogyan hozhat létre a rendszergazda hozzáférési kulcsot a blokkolt eszközhöz az adminisztrációs konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógép tartozik.

3. Válassza ki a munkaterületen a **Devices** lapot.

4. Válassza ki az ügyfélszámítógépek listáján azt a számítógépet, amelynek a felhasználója részére ideiglenes hozzáférést szeretne adni egy blokkolt eszközhöz.

5. A számítógép helyi menüjében válassza ki a **Hozzáférés engedélyezése offline módban** elemet.

6. Ezzel megnyílik egy ablak, amelyben kiválaszthatja az **Eszközfelügyelő** lapot.

7. Kattintson a **Tallózás** gombra, és töltse le a felhasználótól kapott hozzáférés-kérési fájlt.

   Látni fog információkat a blokkolt eszközről, amihez a felhasználó hozzáférést kért.

8. Ha szükséges, módosítsa a **Hozzáférés időtartama** beállítás értékét.

   Alapértelmezetten a **Hozzáférés időtartama** beállítás azt az értéket veszi figyelembe, amit a felhasználó a hozzáférés-kérési fájl létrehozásakor adott meg.

9. Adja meg az **Aktiválta** beállítás értékét.

   Ez a beállítás szabja meg, hogy a felhasználó a kapott hozzáférési kulcs segítségével mennyi ideig aktiválhatja a blokkolt eszközhöz való hozzáférést.

10. Hozzáférési kulcsfájl mentése a számítógépes memóriába.

Hogyan hozhat létre a rendszergazda hozzáférési kulcsot a blokkolt eszközhöz a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki az ügyfélszámítógépek listáján azt a számítógépet, amelynek a felhasználója részére ideiglenes hozzáférést szeretne adni egy blokkolt eszközhöz.
3. Kattintson a három pont gombra (...) a számítógépek listája felett, majd kattintson a **Grant access to the device in offline mode** gombra.
4. A megnyíló ablakban válassza a **Device Control** szakaszt.
5. Kattintson a **Browse** gombra, és töltse le a felhasználótól kapott hozzáférés-kérési fájlt.

   Látni fog információkat a blokkolt eszközről, amihez a felhasználó hozzáférést kért.
6. Ha szükséges, módosítsa a **Access duration (hours)** beállítás értékét.

   Alapértelmezetten a **Access duration (hours)** beállítás azt az értéket veszi figyelembe, amit a felhasználó a hozzáférés-kérési fájl létrehozásakor adott meg.
7. Adja meg azt az időtartamot, amely alatt a hozzáférési kulcs aktiválható a készüléken.

   Ez a beállítás szabja meg, hogy a felhasználó a kapott hozzáférési kulcs segítségével mennyi ideig aktiválhatja a blokkolt eszközhöz való hozzáférést.
8. Hozzáférési kulcsfájl mentése a számítógépes memóriába.

Ennek eredményeképpen a blokkolt eszköz hozzáférési kulcsa letöltődik a számítógépes memóriába. A hozzáférési kulcs a *.acode kiterjesztéssel rendelkezik. Használja az elérhető módszereket, hogy elküldje a blokkolt eszköz hozzáférési kulcsát a felhasználónak.

A felhasználó a következő módon aktiválja a hozzáférési kulcsot:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési kérés** blokkban kattintson a **Hozzáférés kérése az eszközhöz** gombra.
4. A megnyíló ablakban kattintson a **Hozzáférési kulcs aktiválása** gombra.
5. A megnyíló ablakban válassza ki azt a fájlt, amely rendelkezik a vállalati LAN-rendszergazdától kapott eszköz hozzáférési kulcsával.

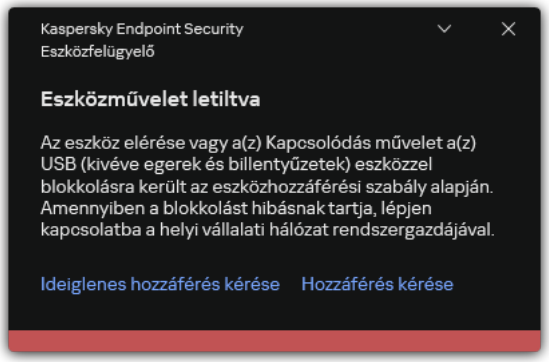
   Ez megnyitja a hozzáférés információit tartalmazó ablakot.
6. Kattintson az **OK** gombra.

Ennek eredményeképpen a felhasználó a rendszergazda által megadott időtartamig hozzáférést kap az eszközhöz. A felhasználó teljes körű jogokat kap az eszközhöz való hozzáféréshez (olvasás és írás). Ha a kulcs lejár, akkor az eszközhöz való hozzáférés blokkolva lesz. Ha a felhasználó örök hozzáférést kér az eszközhöz, akkor adja hozzá az eszközt a megbízható listához.

Az Eszközfelügyelő üzenetsablonjainak szerkesztése

Ha a felhasználó megpróbál egy blokkolt eszközhöz hozzáférni, a Kaspersky Endpoint Security üzenetet jelenít meg arról, hogy az eszközhöz való hozzáférés blokkolva van, illetve az eszköz tartalmával végzett művelet tilos. A Kaspersky szakértői egy üzenetsablont biztosítanak a felhasználónak, amely ismerteti az eszközhöz való hozzáférés letiltásának okait (lásd az alábbi ábrát).

Az üzenetsablonok kezeléséhez speciális változók állnak rendelkezésre (pl. `%USER_NAME%`). A változók lehetővé teszik egyetlen üzenetsablon használatát a különböző számítógépeken. Üzenet generálásakor a Kaspersky Endpoint Security lekéri a változó értékét az operációs rendszer beállításaiból, és beilleszti azt az adott számítógéphez, felhasználóhoz és eseményhez tartozó üzenetbe.



Eszközfelügyelő értesítés

Ha a felhasználó úgy véli, hogy az eszközhöz való hozzáférés blokkolása, illetve az eszköz tartalmával végzett művelet tiltása tévedés, akkor üzenetet küldhet a helyi vállalati hálózatok rendszergazdájának, ha a blokkolt műveletről megjelenített üzenetben lévő hivatkozásra kattint. Ehhez a felhasználónak a **Hozzáférés kérése** vagy az **Ideiglenes hozzáférés kérése** gombra kell kattintania, és üzenetet kell küldenie a rendszergazdának, amelyben leírja a helyzetet. Készíthet egy sablont is a rendszergazdának küldött üzenetről, és hozzáadhat olyan adatokat, amelyek alapján dönthet az eszközhöz való hozzáférés engedélyezéséről vagy letiltásáról. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Eszközhozzáférés blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

Az Eszközfelügyelő üzenetsablonjainak módosítása az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
4. A megnyíló **Sablonok** részen kattintson az **Üzenetsablon beállításai** gombra.

5. Ekkor megnyílik egy ablak, amelyben konfigurálhatja az Alkalmazásfelügyelő sablonjait:

   - **Üzenet a blokkolásról**. Annak az üzenetnek a sablonja, ami akkor jelenik meg, amikor a felhasználó megpróbál hozzáférni egy blokkolt készülékhez. Ez az üzenet akkor is megjelenik, amikor a felhasználó megpróbál végrehajtani egy olyan műveletet a készülék tartalmán, ami blokkolva van számára.

   - **Üzenet a rendszergazdának**. Annak az üzenetnek a sablonja, amelyet a LAN-rendszergazda kap, ha a felhasználó úgy véli, hogy az eszközhöz való hozzáférés blokkolása, illetve az eszköz tartalmával végzett művelet tiltása tévedés.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Visszaállíthatja az alapértelmezett sablonszöveget is.

6. Mentse el a módosításokat.

Az Eszközfelügyelő üzenetsablonjainak módosítása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **Device Control** elemet.

5. A(z) **Message templates** területen konfigurálja a sablonokat az Alkalmazásfelügyelő üzeneteihez:

   - **Message to user**. Annak az üzenetnek a sablonja, ami akkor jelenik meg, amikor a felhasználó megpróbál hozzáférni egy blokkolt készülékhez. Ez az üzenet akkor is megjelenik, amikor a felhasználó megpróbál végrehajtani egy olyan műveletet a készülék tartalmán, ami blokkolva van számára.

   - **Message to administrator**. Annak az üzenetnek a sablonja, amelyet a LAN-rendszergazda kap, ha a felhasználó úgy véli, hogy az eszközhöz való hozzáférés blokkolása, illetve az eszköz tartalmával végzett művelet tiltása tévedés.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Add variable** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Visszaállíthatja az alapértelmezett sablonszöveget is.

6. Mentse el a módosításokat.

Az Eszközfelügyelő üzenetsablonjainak módosítása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.

3. Az **Üzenetsablonok** részen konfigurálja a sablonokat az Alkalmazásfelügyelő üzeneteihez:

   - **Üzenet a blokkolásról**. Annak az üzenetnek a sablonja, ami akkor jelenik meg, amikor a felhasználó megpróbál hozzáférni egy blokkolt készülékhez. Ez az üzenet akkor is megjelenik, amikor a felhasználó megpróbál végrehajtani egy olyan műveletet a készülék tartalmán, ami blokkolva van számára.

   - **Üzenet a rendszergazdának**. Annak az üzenetnek a sablonja, amelyet a LAN-rendszergazda kap, ha a felhasználó úgy véli, hogy az eszközhöz való hozzáférés blokkolása, illetve az eszköz tartalmával végzett művelet tiltása tévedés.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó hozzáadása** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Visszaállíthatja az alapértelmezett sablonszöveget is.

4. Mentse el a módosításokat.

Anti-Bridging

Az Anti-Bridging gátolja a hálózati hidak létrehozását azzal, hogy megelőzi, hogy a számítógépen egyszerre több hálózati kapcsolat legyen létrehozva. Ezzel megvédheti a vállalati hálózatát a védtelen, engedély nélküli hálózatokon keresztül érkező támadásoktól.

Az Anti-Bridging a hálózati kapcsolatok létrehozását szabályozza *csatlakozási szabályok* alkalmazásával.

A csatlakozási szabályok a következő előre megadott eszköztípusok számára lettek létrehozva:

- Hálózati adapterek;
- Wi-Fi adapterek;
- Modemek.

A csatlakozási szabály bekapcsolása esetén a Kaspersky Endpoint Security:

- Blokkolja az aktív kapcsolatot új kapcsolat létrehozásakor, ha a szabályban megadott eszköztípus van használatban mindkét kapcsolatnál;
- Blokkolja az alacsonyabb prioritású szabályokat használó eszköztípusok által létrehozott kapcsolatokat.

Anti-Bridging engedélyezése

Az Anti-Bridging alapértelmezetten ki van kapcsolva.

Az Anti-Bridging engedélyezése:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
3. A **Hozzáférési beállítások** részen kattintson az **Anti-Bridging** gombra.

4. Az **Anti-Bridging engedélyezése** kapcsolóval engedélyezze vagy tiltsa le a funkciót.

5. Mentse el a módosításokat.

Az Anti-Bridging bekapcsolása után a Kaspersky Endpoint Security a csatlakozási szabályok alapján blokkolja a létesített kapcsolatokat.

A csatlakozószabály állapotának módosítása

A csatlakozási szabály állapotának módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

3. A **Hozzáférési beállítások** részen kattintson az **Anti-Bridging** gombra.

4. Az **Eszközök szabályai** blokkban válassza ki azt a szabályt, amelynek módosítani szeretné az állapotát.

5. A **Szabályozás** oszlopban lévő kapcsolókkal engedélyezze vagy tiltsa le a szabályt.

6. Mentse el a módosításokat.

A csatlakozószabály prioritásának módosítása

A csatlakozási szabály prioritásának módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

3. A **Hozzáférési beállítások** részen kattintson az **Anti-Bridging** gombra.

4. Az **Eszközök szabályai** blokkban válassza ki azt a szabályt, amelynek módosítani szeretné a prioritását.

5. Állítsa be a **Fel** / **Le** gombokkal a kapcsolati szabály prioritását.

   Minél magasabban van a szabály a szabálylistában, annál magasabb a prioritása. Anti-Bridging minden csatlakozást letilt, kivéve azt az eszköz által létrehozott kapcsolatot, mely a legmagasabb prioritással rendelkező szabályt használja.

6. Mentse el a módosításokat.

Adaptív Anomáliafelügyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

Az Adaptív Anomáliafelügyelő összetevő megfigyeli és letiltja azokat a tevékenységeket, amelyek nem megszokottak a cég hálózatán található számítógépeken. Az Adaptív Anomáliafelügyelő egy szabálycsoport alapján követi nyomon a nem jellemző viselkedést (például a *Start of Microsoft PowerShell from office application* szabályt). A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján. Konfigurálhatja, hogy az Adaptív Anomáliafelügyelő miként kezelje az egyes szabályokat és engedélyezheti olyan PowerShell szkriptek végrehajtását, amelyek bizonyos feladatokat automatizálnak. A Kaspersky Endpoint Security az alkalmazás adatbázisával együtt frissíti a szabálycsoportokat. A szabálycsoportok frissítését manuálisan kell megerősíteni.

Az Adaptív Anomáliafelügyelő beállításai

Az Adaptív Anomáliafelügyelő beállítása a következő lépésekből áll:

1. Az Adaptív Anomáliafelügyelő betanítása.

   Miután engedélyezte az Adaptív Anomáliafelügyelőt, a szabályok *tanuló módban* vannak. A tanulás során az Adaptív Anomáliafelügyelő nyomon követi a szabályok végrehajtását kiváltó tevékenységeket és eseményriasztásokat küld a Kaspersky Security Center részére. Minden szabálynak megvan a saját tanulási ideje. A tanulási mód időtartamát a Kaspersky szakemberei határozták meg. Normális esetben a tanulási mód két hétig aktív.

   Ha egy szabály betartását a tanulási időszak során egyszer se váltották ki, akkor az Adaptív Anomáliafelügyelő az adott szabályhoz kapcsolódó tevékenységeket gyanúsnak fogja minősíteni. A Kaspersky Endpoint Security le fog tiltani az adott szabályhoz kapcsolódó minden tevékenységet.

   Ha egy szabály végrehajtását kiváltották a tanulási időszakban, akkor a Kaspersky Endpoint Security naplóbejegyzést készít az eseményekről a szabálykiváltó jelentésben és a **Rule triggers in Smart Training state** gyűjteményben.

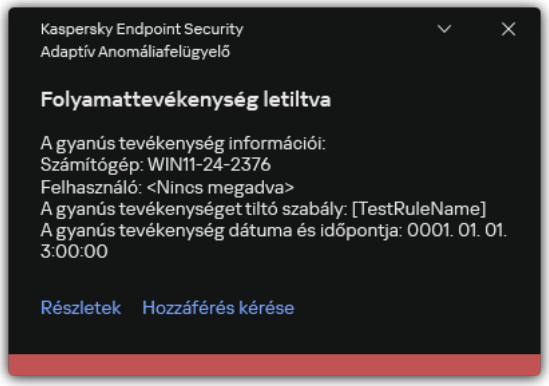
2. A szabálykiváltó jelentés értelmezése.

   A szabálykiváltó jelentést vagy a **Rule triggers in Smart Training state** gyűjteményt a rendszergazdának kell értelmezni. A rendszergazda ezt követően kiválaszthatja az Adaptív Anomáliafelügyelő viselkedését az adott helyzetben, hogy blokkolja vagy engedélyezi a szabály betartását. A rendszergazda emellett folyamatosan nyomon követheti az adott szabály működését és kibővítheti a tanulási mód időtartamát. Ha a rendszergazda nem tesz semmit, az alkalmazás továbbra is tanulási módban fog működni. Az útmutató mód feltételek újraindultak.

Az Adaptív Anomáliafelügyelő konfigurálása valós időben a következő csatornákon történik:

- Az Adaptív Anomáliafelügyelő automatikusan letiltja vagy engedélyezi a szabályokhoz társított tevékenységeket, amelyek nem lettek kiváltva tanulási módban.
- A Kaspersky Endpoint Security új szabályokat ad hozzá és eltávolítja az elavultakat.
- A rendszergazda azt követően konfigurálja az Adaptív Anomáliafelügyelő működését, hogy áttekintette a szabálykiváltó jelentést és a **Rule triggers in Smart Training state** gyűjtemény tartalmát. Javasoljuk, hogy ellenőrizze a szabályokat kiváltó jelentést és a **Rule triggers in Smart Training state** tárhely tartalmát.

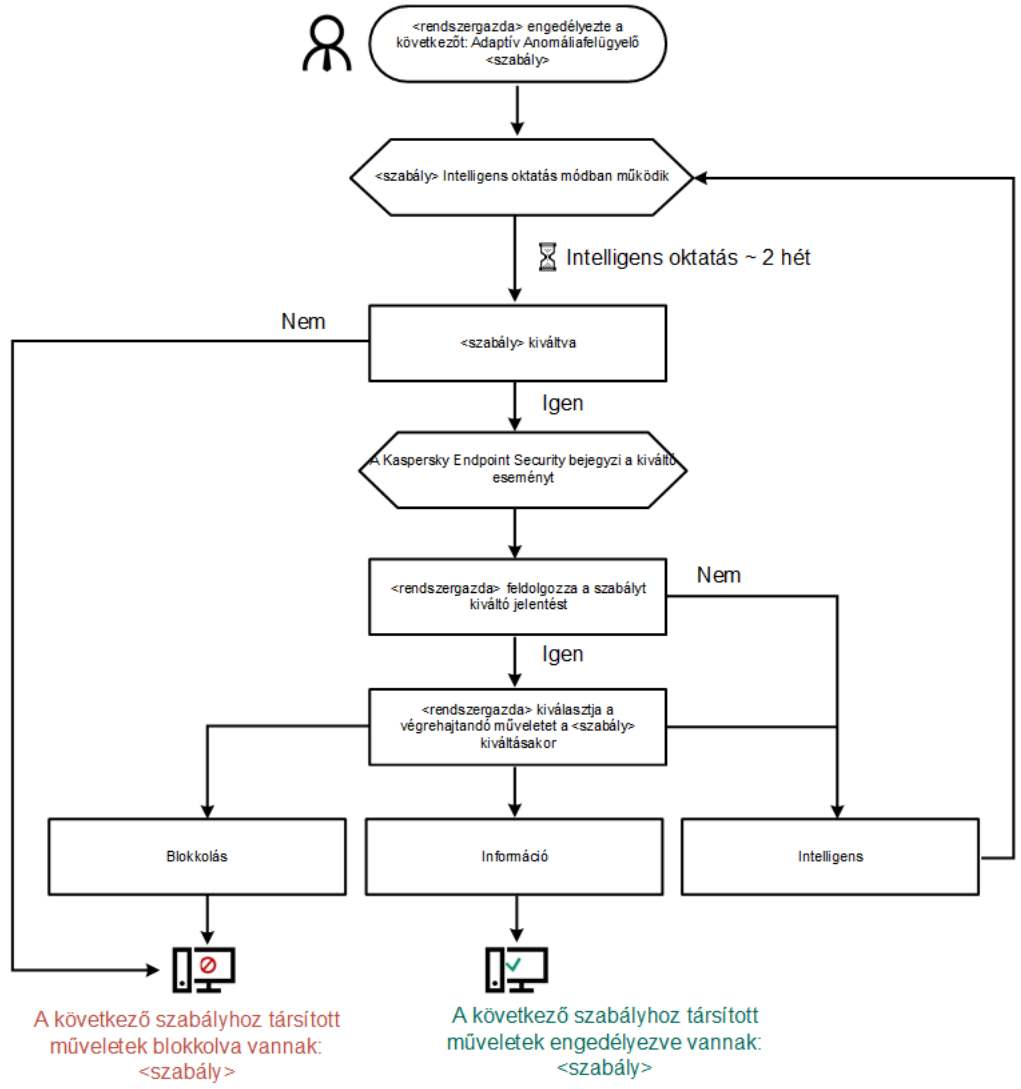
Amikor egy rosszindulatú alkalmazás megpróbál műveletet végrehajtani, a Kaspersky Endpoint Security letiltja a műveletet és értesítést jelenít meg (lásd az alábbi ábrát).



Adaptív Anomáliafelügyeleti értesítés

Adaptive Anomaly Control operating algorithm

A Kaspersky Endpoint Security a következő algoritmus alapján dönti el, hogy engedélyezze vagy letiltsa az adott szabályhoz társított műveletet (lásd az alábbi ábrán).



Adaptive Anomaly Control operating algorithm

Az Adaptív Anomáliafelügyelő betanítása

Az Adaptív Anomáliafelügyelő szabálykészletet (viselkedési mintákat) tartalmaz. Miután engedélyezte az Adaptív Anomáliafelügyelőt, a szabályok *tanuló módban* vannak. A tanulás során az Adaptív Anomáliafelügyelő nyomon követi a szabályok végrehajtását kiváltó tevékenységeket és eseményriasztásokat küld a Kaspersky Security Center részére. Az Adaptív Anomáliafelügyelő nem blokkolja az alkalmazások tevékenységét a számítógépen, csak értesíti a rendszergazdát. Az Adaptív Anomáliafelügyeleti szabály aktiválásakor végrehajtandó műveletet manuálisan is kiválaszthatja.

Az Adaptív Anomáliafelügyeleti szabályok listájának megtekintése a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Policies** lehetőséget.

3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

4. A házirend ablakban válassza ki az **Security Controls** → **Adaptive Anomaly Control** lehetőséget.

5. Jelölje be az **Adaptív Anomáliafelügyelő** jelölőnégyzetet.

6. Az **Adaptív Anomáliafelügyeleti szabály beállításainál** nézze meg a szabályok listáját.

   Alapértelmezés szerint minden szabály működik az **Intelligens** módban.

7. Ha szükséges, erősítse meg az Adaptív Anomáliafelügyeleti szabály frissítését.

8. Ha szükséges, válasszon egy műveletet az Adaptív Anomáliafelügyeleti szabály aktiválásakor:

   - **Blokkolás**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security blokkolja a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

   - **Tájékoztatás**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security engedélyezi a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

9. Ha szükséges, tiltsa le a használni nem kívánt szabályokat.

10. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az Adaptív Anomáliafelügyeleti szabályok megtekintése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **Adaptive Anomaly Control** elemet.

5. Kapcsolja be az **Adaptive Anomaly Control ENABLED** kapcsolót.

6. A **Rules** részen nézze meg a szabálylistát.

   Alapértelmezés szerint minden szabály működik az **Smart** módban.

7. Ha szükséges, erősítse meg az Adaptív Anomáliafelügyeleti szabály frissítését.

8. Ha szükséges, válasszon egy műveletet az Adaptív Anomáliafelügyeleti szabály aktiválásakor:

   - **Block**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security blokkolja a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

   - **Inform**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security engedélyezi a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

9. Ha szükséges, tiltsa le a használni nem kívánt szabályokat.

10. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az Adaptív Anomáliafelügyeleti szabályok listájának megtekintése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazáskonfigurációs ablakban válassza ki a **Security Controls** → **Adaptive Anomaly Control** lehetőséget.

3. Kapcsolja be az **Adaptív Anomáliafelügyelő** kapcsolót.

4. A **Szabályok** részen kattintson a **Szabályok szerkesztése** hivatkozásra.

   Az Adaptív Anomáliafelügyeleti szabálylista nyílik meg. Alapértelmezés szerint minden szabály működik az **Intelligens** módban.

5. Ha szükséges, erősítse meg az Adaptív Anomáliafelügyeleti szabály frissítését.

6. Ha szükséges, válasszon egy műveletet az Adaptív Anomáliafelügyeleti szabály aktiválásakor:

   - **Blokkolás**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security blokkolja a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

   - **Tájékoztatás**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security engedélyezi a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

7. Ha szükséges, tiltsa le a használni nem kívánt szabályokat.

8. Mentse el a módosításokat.

Minden szabálynak megvan a saját tanulási ideje. A tanulási mód időtartamát a Kaspersky szakemberei határozták meg. Normális esetben a tanulási mód két hétig aktív.

Ha a tanítás során egy szabály soha nem vált ki riasztást, az Adaptív Anomáliafelügyelő ezt a viselkedést atipikusnak tekinti, és a szabály állapotát **Intelligens blokkolásra** változtatja. Ezt követően az alkalmazás minden olyan tevékenységet blokkol, amely megfelel a szabálynak.

Ha egy szabály a tanítás során aktiválódik, akkor manuálisan kell konfigurálnia azt a műveletet, amelyet az alkalmazás az e szabálynak megfelelő észlelt tevékenységre alkalmaz. Ha nem választja ki a szabály aktiválásakor végrehajtandó műveletet, az Adaptív Anomáliafelügyelő továbbra is tanítási módban működik.

Adaptív Anomáliafelügyeleti szabály engedélyezése és letiltása

Egy Adaptív Anomáliafelügyeleti szabály engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáliafelügyelő** lehetőséget.

3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.

   Az Adaptív Anomáliafelügyeleti szabálylista nyílik meg.

4. A táblázatban válassza ki a szabálykészletet (például *Activity of office applications*), és bontsa ki a készletet.

5. Válasszon ki egy szabályt (például *Start of Microsoft PowerShell from office application*).

6. Az **Állapot** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le az Adaptív Anomáliafelügyelő szabályát.

7. Mentse el a módosításokat.

Az Adaptív Anomáliafelügyeleti szabály kiváltásakor végrehajtott művelet módosítása

Az Adaptív Anomáliafelügyeleti szabály kiváltásakor végrehajtott művelet szerkesztése:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Adaptív Anomáliafelügyelő** lehetőséget.

3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.

   Az Adaptív Anomáliafelügyeleti szabálylista nyílik meg.

4. Jelöljön ki egy szabályt a táblázatban.

5. Kattintson a **Szerkesztés** gombra.

   Az Adaptív Anomáliafelügyeleti szabály tulajdonságainak ablaka nyílik meg.

6. A **Művelet** blokkban válassza ki a következő opciók egyikét:

   - **Intelligens**. Ha ez a lehetőség ki van jelölve, akkor egy Adaptív Anomáliafelügyeleti szabály Intelligens tanulás állapotban működik a Kaspersky szakemberei által megadott ideig. Ebben a módban egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security engedélyezi a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a Kaspersky Security Center felügyeleti kiszolgáló **Rule triggers in Smart Training state** tárolójában. Ha véget ér az Intelligens tanulás állapothoz beállított időtartam, a Kaspersky Endpoint Security blokkolja az Adaptív Anomáliafelügyeleti szabályok tevékenységeit, és naplóz egy bejegyzést a tevékenységről.

   - **Blokkolás**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security blokkolja a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

   - **Tájékoztatás**. Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáliafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security engedélyezi a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.

7. Mentse el a módosításokat.

Kizárás létrehozása Adaptív Anomáliafelügyeleti szabályhoz

1000 kizárásnál többet nem hozhat létre az Adaptív Anomáliafelügyeleti szabályokból. Nem javasolt 200 kizárásnál többet létrehozni. A használt kizárások számának csökkentéséhez javasolt maszkokat használni a kizárások beállításaiban.

Az Adaptív Anomáliafelügyeleti szabályának egy kizárása tartalmazza a forrás- és célobjektumok leírását. A *forrásobjektum* egy objektum, ami végrehajtja a tevékenységeket. A *célobjektum* egy objektum, amin a tevékenységet végre vannak hajtva. Például megnyitott egy `file.xlsx` nevű fájlt. Ennek eredményeképpen a DLL kiterjesztésű könyvtárfájl betöltődik a számítógépes memóriába. A könyvtárat a böngésző használja (a `browser.exe` nevű végrehajtható fájl). Ebben a példában a `file.xlsx` a forrásobjektum, az Excel a forrásfolyamat, a `browser.exe` a célfájl, a Böngésző pedig a célobjektum.

Kizárás létrehozása Adaptív Anomáliafelügyeleti szabályhoz:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáliafelügyelő** lehetőséget.
3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.

   Az Adaptív Anomáliafelügyeleti szabálylista nyílik meg.
4. Jelöljön ki egy szabályt a táblázatban.
5. Kattintson a **Szerkesztés** gombra.

   Az Adaptív Anomáliafelügyeleti szabály tulajdonságainak ablaka nyílik meg.
6. A **Kizárások** blokkban kattintson a **Hozzáadás** gombra.

   Megnyílik a kizárások tulajdonságai ablak.
7. Válassza ki azt a felhasználót, akihez kizárást szeretne konfigurálni.

   A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   Az Adaptív Anomáliafelügyelő a felhasználói csoportok esetében nem támogatja a kizárást. Felhasználói csoport kiválasztása esetén a Kaspersky Endpoint Security nem alkalmazza a kizárást.
8. A **Leírás** mezőben adja meg a kizárás leírását.
9. Adja meg az objektum által elindított forrásobjektum vagy forrásfolyamat beállításait:

   - **Forrásfolyamat**. A fájl vagy a fájlt tartalmazó mappa elérési útja vagy annak maszkja (például: `C:\Dir\File.exe` vagy `Dir\*.exe`).
   - **Forrásfolyamat kivonata**. a fájl SHA256 kivonata.

- **Forrásobjektum**. A fájl vagy a fájlt tartalmazó mappa elérési útja vagy annak maszkja (például: `C:\Dir\File.exe` vagy `Dir\*.exe`). Például a `document.docm` fájlelérési útvonal, amely parancsfájl vagy makró használatával indítja el a célfolyamatokat.

  Megadhat egyéb objektumokat a kizáráshoz, például webcímeket, makrókat, parancsokat a parancssorban, beállításjegyzék útvonalakat és egyebeket. Adja meg az objektumot a következő sablon alapján: `object://<object>` ahol az `<object>` az objektum nevét jelenti, például: `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Maszkokat is használhat, például: `object://*C:\Windows\temp\*`.

- **Forrásobjektum kivonata**. a fájl SHA256 kivonata.

Az Adaptív Anomáliafelügyeleti szabály nincs alkalmazva az objektum által végrehajtott tevékenységeken, valamint az objektum által elindított folyamatokon.

10. Adja meg az objektum által elindított célobjektum vagy célfolyamatok beállításait.

    - **Célfolyamat** A fájl vagy a fájlt tartalmazó mappa elérési útja vagy annak maszkja (például: `C:\Dir\File.exe` vagy `Dir\*.exe`).

    - **Célfolyamat kivonata**. a fájl SHA256 kivonata.

    - **Célobjektum**. A célfolyamatokat indító parancs. Adja meg a parancsot a következő sablon használatával: `object://<command>`, például `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Maszkokat is használhat, például: `object://*C:\Windows\temp\*`.

    - **Célobjektum kivonata**. a fájl SHA256 kivonata.

    Az Adaptív Anomáliafelügyeleti szabály nincs alkalmazva az objektum által végbevitt tevékenységeken vagy az objektum által indított folyamatokon.

11. Mentse el a módosításokat.

Kizárások exportálása és importálása az Adaptív Anomáliafelügyeleti szabályokhoz

A kijelölt szabályok kizárási listájának exportálása vagy importálása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Adaptív Anomáliafelügyelő** lehetőséget.

3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.

   Az Adaptív Anomáliafelügyeleti szabálylista nyílik meg.

4. A szabályok listájának exportálása:

   a. Válassza ki azokat a szabályokat, amelynek exportálni szeretné a kivételeit.

   b. Kattintson az **Export** gombra.

c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.

d. Erősítse meg, hogy csak a kijelölt kizárásokat, vagy a kizárások teljes listáját szeretné exportálni.

e. Mentse a fájlt.

5. A kizárások listájának importálása:

a. Kattintson az **Import** gombra.

b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kizárások listáját.

c. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

6. Mentse el a módosításokat.

Az Adaptív Anomáliafelügyeleti szabályok frissítéseinek alkalmazása

Új Adaptív Anomáliafelügyeleti szabályok adhatók hozzá a szabályok táblázatához, és a meglévő Adaptív Anomáliafelügyeleti szabályok törölhetők a szabályok táblázatából a víruskereső-adatbázisok frissítésekor. A Kaspersky Endpoint Security megkülönbözteti a táblázatból törölni, vagy ahhoz hozzáadni kívánt Adaptív Anomáliafelügyeleti szabályokat, ha egy frissítés nem lett alkalmazva ezekre a szabályokra.

Amíg a frissítés alkalmazva van, a Kaspersky Endpoint Security a szabályok táblázatában megjeleníti frissítés által törlendő Adaptív Anomáliafelügyeleti szabályokat, és a *Letiltott* állapotot rendeli hozzájuk. E szabályok beállításainak módosítása nem lehetséges.

Az Adaptív Anomáliafelügyeleti szabályok frissítéseinek alkalmazása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Adaptív Anomáliafelügyelő** lehetőséget.

3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.

Az Adaptív Anomáliafelügyeleti szabálylista nyílik meg.

4. Az ablakban kattintson a **Frissítések elfogadása** gombra.

A **Frissítések elfogadása** gomb elérhető, ha van elérhető frissítés az Adaptív Anomáliafelügyeleti szabályokhoz.

5. Mentse el a módosításokat.

Adaptív Anomáliafelügyelő üzenetsablonok szerkesztése

Ha egy felhasználó megpróbál végrehajtani egy tevékenységet, amit blokkolnak az Adaptív Anomáliafelügyeleti szabályok, akkor a Kaspersky Endpoint Security megjelenít egy üzenetet arról, hogy potenciálisan rosszindulatú tevékenységek voltak blokkolva. Ha a felhasználó úgy véli, hogy a tevékenység tévedésből van blokkolva, akkor az üzenet szövegében lévő hivatkozás segítségével üzenetet küldhet a helyi vállalati hálózati rendszergazdának.

Speciális sablonok állnak rendelkezésre az adminisztrátornak küldött üzenetekhez, amelyek potenciálisan káros tevékenységek blokkolásáról szólnak. Az üzenetsablonok kezeléséhez speciális változók állnak rendelkezésre (pl. `%USER_NAME%`). A változók lehetővé teszik egyetlen üzenetsablon használatát a különböző számítógépeken. Üzenet generálásakor a Kaspersky Endpoint Security lekéri a változó értékét az operációs rendszer beállításaiból, és beilleszti azt az adott számítógéphez, felhasználóhoz és eseményhez tartozó üzenetbe.

Üzenetsablonok szerkesztése:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Adaptív Anomáliafelügyelő** lehetőséget.
3. A **Sablonok** blokkban konfigurálja a sablonokat az Adaptív Anomáliafelügyelő üzeneteihez:
   - **Üzenet a blokkolásról**. Üzenetsablon, ami akkor jelenik meg a felhasználónak, amikor aktiválódik az Adaptív Anomáliafelügyelő egy olyan szabálya, amely blokkolja a gyanús tevékenységet.
   - **Üzenet a rendszergazdának**. Üzenetsablon a felhasználó számára, ami t a felhasználó a helyi hálózat rendszergazdája részére tud küldeni abban az esetben, ha a művelet letiltása szerinte téves döntés volt. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Alkalmazástevékenység blokkolásáról szóló üzenet a rendszergazdának**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó hozzáadása** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Az alapértelmezett sablonszöveget a **Visszaállítás** gombra kattintva is visszaállíthatja.
4. Mentse el a módosításokat.

Az Adaptív Anomáliafelügyelő műveleteinek figyelése

Az Adaptív Anomáliafelügyelő számos felügyeleti eszközt tartalmaz. Az Adaptív Anomáliafelügyelő felügyeletének fő célja az összetevő konfigurálása a betanítás során.

Az Adaptív Anomáliafelügyelő jelentései

Az Adaptív Anomáliafelügyelő a következő jelentéseket használja:

- **Jelentés az Adaptív Anomáliafelügyeleti szabályok állapotáról**. A jelentés információkat tartalmaz az Adaptív Anomáliafelügyeleti szabályok állapotáról (*Off*, *Smart Training*, *Smart Block*, *Notify*, *Block*). Ez a jelentés lehetővé teszi az Adaptív Anomáliafelügyelő betanítási szintjének elemzését és az *Smart Training* módból normál üzemmódba váltott szabályok (például *Smart Block*) számának értékelését.

- **Jelentés az Adaptív Anomáliafelügyelő aktívan alkalmazott szabályairól**. A jelentés információkat tartalmaz a szabályindítókról. A jelentés a szabály kiváltó módját is megmutatja: *Block* (including *Smart Block*) vagy *Notify*. Ez a jelentés lehetővé teszi az Adaptív Anomáliafelügyelő tevékenységének értékelését a felhasználói számítógépeken.

Az Adaptív Anomáliafelügyelő jelentéseinek megtekintése a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Adaptív Anomáliafelügyelő** lehetőséget.
4. Végezze el az alábbiak egyikét:
   - Ha meg szeretné tekinteni az adaptív anomáliafelügyeleti szabályok állapotáról szóló jelentést, kattintson a **Jelentés az Adaptív Anomáliafelügyeleti szabályok állapotáról** hivatkozásra.
   - Ha meg szeretné tekinteni az adaptív anomáliafelügyelő aktívan alkalmazott szabályairól szóló jelentést, kattintson a **Jelentés az Adaptív Anomáliafelügyelő aktívan alkalmazott szabályairól** hivatkozásra.
5. Megkezdődik a jelentés előállítási folyamata.

   A jelentés egy új ablakban jelenik meg.

Az Adaptív Anomáliafelügyelő jelentéseinek megtekintése a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls → Adaptive Anomaly Control** elemet.
5. A **Rules** részen hajtsa végre a következő műveletek valamelyikét:
   - Ha meg szeretné tekinteni a jelentést az Adaptív Anomáliafelügyelői szabályok állapotáról, válassza a **View report → Rules state** lehetőséget.
   - Ha meg szeretné tekinteni a kiváltott Adaptív Anomáliafelügyelői szabályokról szóló jelentést, kattintson a **View report → Detections** lehetőségre.
6. Megkezdődik a jelentés előállítási folyamata.

A jelentés egy új ablakban jelenik meg.

A Kaspersky Security Center konzolban a jelentések létrehozásához engedélyeznie kell az adatok átvitelét az adminisztrációs kiszolgálóra. Az adatátvitel alapértelmezés szerint engedélyezve van.

Adatátvitel engedélyezése az Adaptív Anomáliafelügyelő számára az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirendek ablakában válassza az **Általános beállítások → Jelentések és tároló** lehetőséget.
4. Az **Adatátvitel az adminisztrációs kiszolgálóra** részen kattintson a **Beállítások** gombra.
5. Jelölje be a következő jelölőnégyzeteket:
   - **Jelentés az Adaptív Anomáliafelügyeleti szabályok állapotáról**.
   - **Jelentés az Adaptív Anomáliafelügyelő aktívan alkalmazott szabályairól**.
6. Mentse el a módosításokat.

Adatátvitel engedélyezése az Adaptív Anomáliafelügyelő számára a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings → KSC Integration** elemet.
5. A **Data transfer to Administration Server** részen jelölje be a következő jelölőnégyzeteket:
   - **Report on Adaptive Anomaly Control rules state**.
   - **Report on triggered Adaptive Anomaly Control rules**.
6. Mentse el a módosításokat.

Rule triggers in Smart Training state tár

Tanítási módban az Adaptív Anomáliafelügyelő az aktivált szabályokról szóló információkat egy külön tárolóba – **Rule triggers in Smart Training state** – küldi. Az aktivált szabályokkal kapcsolatos információk a tárolóban eseménylistaként jelennek meg. Az Adaptív Anomáliafelügyelő finomhangolásához megerősítheti a számítógépen észlelt atipikus viselkedést, vagy hozzáadhat egy kivételt a szabályhoz.

Adaptív Anomáliafelügyelő eseményei

Az Adaptív Anomáliafelügyelő naplózza a szabályok kiváltó eseményeit a *Block* (beleértve *Smart Block*) és az *Notify* módban. E célból az alábbi események állnak rendelkezésre:

Process action blocked

Process action skipped

Az események információkat tartalmaznak a gyanús tevékenységről, beleértve a fájlok ellenőrzőösszegeit, az érintett felhasználókat, a szabály kiváltásának idejét és a számítógép nevét. Az esemény elemzése után azonnal hozzáadhat kizárásokat a szabályhoz, ha a tevékenységet jogosnak találja.

Alkalmazásfelügyelő

Az Alkalmazásfelügyelő kezeli az alkalmazások indítását a felhasználók számítógépén. Ez lehetővé teszi a vállalati biztonsági házirend bevezetését az alkalmazások használatára vonatkozóan. Az Alkalmazásfelügyelő emellett csökkenti a számítógép megfertőződésének kockázatát is azzal, hogy korlátozza a hozzáférést az alkalmazásokhoz.

Az Alkalmazásfelügyelő konfigurálásának lépései a következők:

1. Alkalmazáskategóriák létrehozása.

   A rendszergazda létrehoz kategóriákat az általa kezelni kívánt alkalmazásokhoz. Az alkalmazáskategóriák a vállalati hálózat minden számítógépére vonatkoznak, függetlenül a rendszergazdai csoportoktól. Kategória létrehozásához a következő feltételeket használhatja: KL-kategória (például *Böngészők* vagy más kategória), fájlkivonat, az alkalmazás gyártója és egyéb feltételek.

2. Alkalmazásfelügyeleti szabályok létrehozása.

   A rendszergazda alkalmazásfelügyeleti szabályokat hoz létre a rendszergazdai csoport házirendjében. A szabályban alkalmazáskategóriák szerepelnek, és ezen kategóriák alkalmazásainak rendszerindításkori állapota lehet „letiltva” vagy „engedélyezett”. Az adminisztrátor sok szabályt hozhat létre. Egy alkalmazás több szabály feltételeinek is megfelelhet. A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. A Kaspersky Endpoint Security minden indításkor ellenőrzi, hogy az alkalmazás megfelel-e a szabálynak. A Kaspersky Endpoint Security egymás után elvégzi az alkalmazás összes Alkalmazásfelügyeleti szabályának megfelelőségét.

3. Az Alkalmazásfelügyelő módjának kiválasztása.

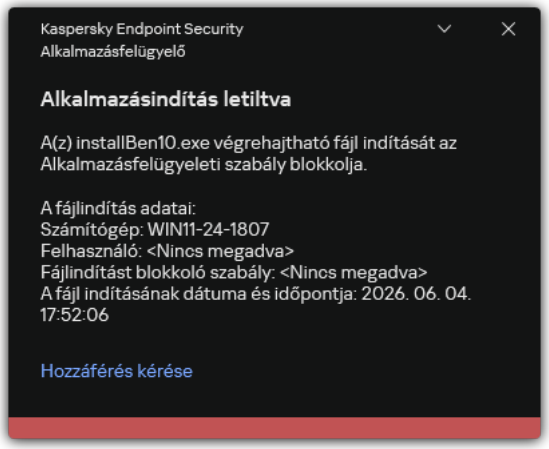
   A rendszergazda kiválasztja azt a módot, amelyet a szabályok egyikében sem szereplő alkalmazásokkal folytatott munka során használni kíván (alkalmazás tiltólista és engedélyezési lista).

Ha egy felhasználó megkísérli egy tiltott alkalmazás elindítását, a Kaspersky Endpoint Security blokkolja az alkalmazás elindítását, és értesítést jelenít meg (részletek az alábbi ábrán).

Elérhető a *tesztelési mód*, amellyel ellenőrizheti az Alkalmazásfelügyelő beállításait. Ebben a módban a Kaspersky Endpoint Security a következőt teszi:

- lehetővé teszi az alkalmazások betöltését rendszerindításkor, köztük a letiltottakét is;
- értesítést jelenít a tiltott alkalmazások elindításáról, és a felhasználó számítógépére vonatkozó információt rögzít a jelentésben;

- adatokat küld a tiltott alkalmazások indításáról a Kaspersky Security Center számára.



Az Alkalmazásfelügyelő értesítései

Az Alkalmazásfelügyelő üzemmódjai

Az Alkalmazásfelügyelő összetevő két módban működhet:

- **Tiltólista**. Ebben a módban az Alkalmazásfelügyelő a felhasználók számára engedélyezi minden alkalmazás elindítását, kivéve az Alkalmazásfelügyelő blokkolási szabályai által letiltottakat.

  Alapértelmezés szerint ez a mód van engedélyezve az Alkalmazásfelügyelőben.

- **Engedélyezési lista**. Ebben a módban az Alkalmazásfelügyelő a felhasználók számára blokkolja az összes olyan alkalmazás elindítását, amely engedélyezett, és nincs letiltva az Alkalmazásfelügyeleti szabályaiban.

  Ha az Alkalmazásfelügyelő engedélyezési szabályai teljes mértékben meg vannak adva, az összetevő minden, a helyi hálózati rendszergazda által nem ellenőrzött új alkalmazás indítását blokkolja, miközben engedélyezi az operációs rendszer és a felhasználók számára munkájukhoz szükséges megbízható alkalmazások működését.

  Elolvashatja az Alkalmazásfelügyelői szabályok engedélyezési lista módban történő konfigurálására vonatkozó ajánlásokat.

Az Alkalmazásfelügyelő e módokban való működése egyaránt beállítható a Kaspersky Endpoint Security helyi felületén, illetve a Kaspersky Security Center segítségével.

A Kaspersky Security Center azonban olyan eszközöket is kínál, amelyek a Kaspersky Endpoint Security helyi felületén nem találhatók meg, köztük az alábbi feladatokhoz szükséges eszközöket:

- Alkalmazáskategóriák létrehozása.

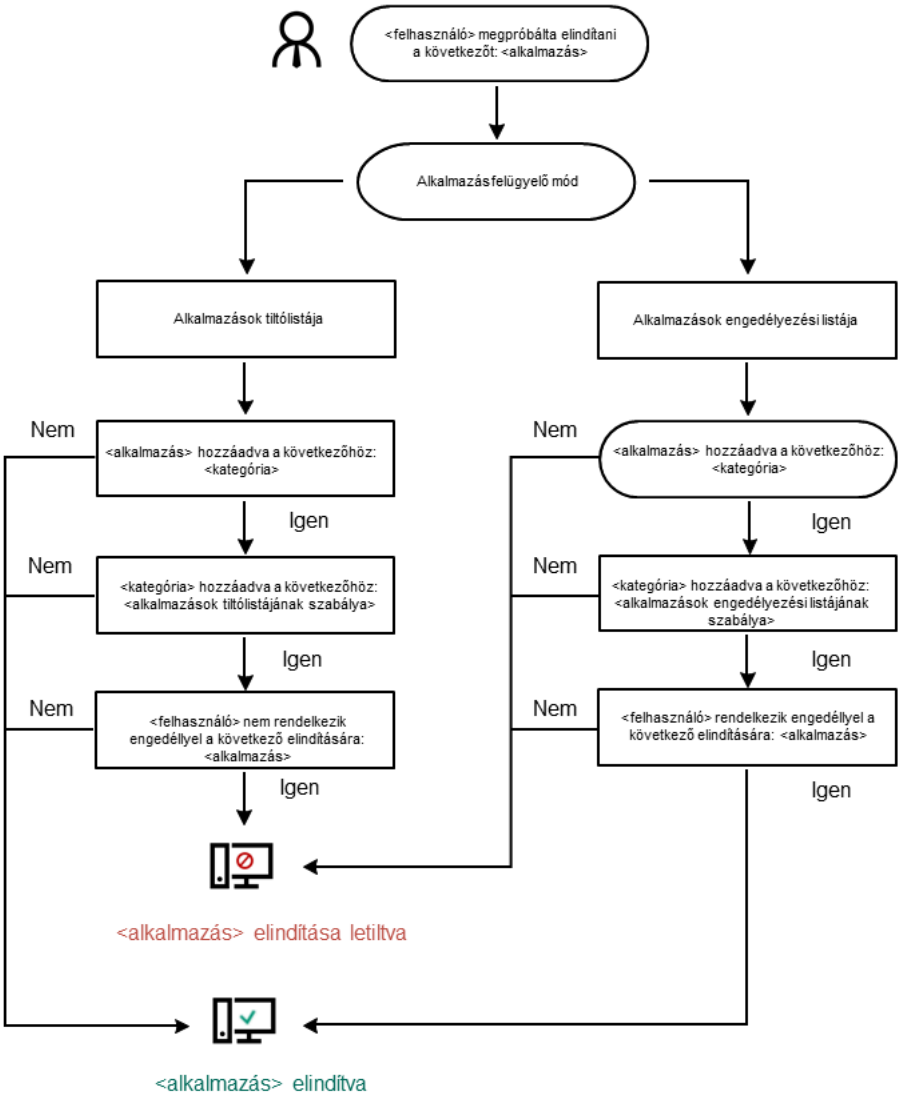
  A Kaspersky Security Center Adminisztrációs Konzolban előállított Alkalmazásfelügyeleti szabályok egyedi alkalmazáskategóriákon alapulnak, nem pedig szerepeltetési és kizárási feltételeken, mint a Kaspersky Endpoint Security helyi felülete esetén.

- A vállalati LAN számítógépeken telepített alkalmazásokra vonatkozó információk fogadása.

Ezért javasoljuk az Alkalmazásfelügyelő összetevő működésének beállítását a Kaspersky Security Center segítségével.

Alkalmazásfelügyelő műveleti algoritmusa

A Kaspersky Endpoint Security algoritmust használva hoz döntést egy adott alkalmazás elindításáról (részletek a lentebbi ábrán).



Alkalmazásfelügyelő műveleti algoritmusa

Az Alkalmazásfelügyelő funkciónak korlátozásai

Az Alkalmazásfelügyelő összetevő működése az alábbi esetekben korlátozott:

- Az alkalmazás verziófrissítésekor az Alkalmazásfelügyelő összetevő beállításainak importálása nem támogatott.
- Ha nincs kapcsolat a KSN kiszolgálókkal, a Kaspersky Endpoint Security az alkalmazások és moduljaik reputációjára vonatkozó információkat csak a helyi adatbázisokból szerzi be.

  Azon alkalmazások listája, amelyeket a Kaspersky Endpoint Security KL kategóriának jelöl **Other Software\Applications, trusted according to reputation in KSN** eltérhet attól függően, hogy elérhető-e a kapcsolat a KSN-kiszolgálókkal.

- A Kaspersky Security Center adatbázisában 150 000 feldolgozott fájlra vonatkozó adat tárolható. E bejegyzésszám elértével az új fájlok feldolgozására nem kerül sor. A leltározási műveletek folytatásához törölnie kell a korábban a Kaspersky Security Center adatbázisban leltárba vett fájlokat azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van.
- Az összetevő csak akkor felügyeli a szkriptek indítását, ha a szkript a parancssoron keresztül kerül az értelmezőhöz.

  Ha az értelmező indítását az Alkalmazásfelügyeleti szabályok lehetővé teszik, az összetevő nem blokkolja az adott értelmezőből indított szkripteket.

  Ha az értelmező parancssorban legalább egy szkript nem indítható el az Alkalmazásfelügyeleti szabályokkal, akkor az összetevő blokkol minden szkriptet az értelmező parancssorban.

- Az összetevő nem felügyeli a Kaspersky Endpoint Security által nem támogatott értelmezőkből történő szkriptindítást.

  A Kaspersky Endpoint Security az alábbi értelmezőket támogatja:

  - Java
  - PowerShell

  Az alábbi értelmezőtípusok támogatottak:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe
  - %SystemRoot%\system32\wscript.exe

- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

A felhasználói számítógépeken telepített alkalmazásokra vonatkozó információk fogadása

Optimális Alkalmazásfelügyeleti szabályok létrehozása érdekében javasoljuk, hogy először mérje fel a vállalati hálózaton lévő számítógépeken használt alkalmazásokat. Ehhez az alábbi adatokat szerezheti be:

- A vállalati helyi hálózaton használt alkalmazások forgalmazói, verziói és nyelvi változatai.
- Az alkalmazásfrissítések gyakorisága.
- A vállalatnál bevezetett alkalmazáshasználati rendszabályok (melyek lehetnek biztonsági és adminisztratív rendszabályok).
- Az alkalmazások terjesztőcsomagjainak tárolási helye.

Alkalmazás információinak megtekintése

A telepített alkalmazásokra vonatkozó információkat a Kaspersky Security Center Network Agent biztosítja. A telepített alkalmazásokra vonatkozó információk elérhetők a Kaspersky Security Center konzolban a **Applications registry** mappában. A Hálózati ügynök a Kaspersky Security Centerrel történő minden egyes szinkronizáláskor frissíti az információkat. A Hálózati ügynök által küldött információkkal kapcsolatos részletekért olvassa el a Kaspersky Security Center súgóját.

Az alkalmazástulajdonságok ablak megnyitásához az Applications registry mappában:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Application management** → **Applications registry** lehetőséget.
3. Válasszon ki egy alkalmazást.
4. Az alkalmazás helyi menüjében válassza ki a **Properties** elemet.

Információk megtekintése a futtatható fájlokról

Csökkentheti az adatbázis terhelését, amikor futtatható fájlokkal kapcsolatos információkat kérdez le. Ehhez javasoljuk a *Leltár* feladat futtatását több referenciaszámítógépen, amelyeken a szabványos szoftverek telepítve vannak.

A futtatható fájlok listáját a Kaspersky Endpoint Security *Leltár* feladatának segítségével kérheti le. A futtatható fájlok listáját a Kaspersky Security Center konzolon tekintheti meg a **Executable files** mappában.

Mielőtt futtatná a *Leltár* feladatot, győződjön meg arról, hogy az adatbázis megfelel a Kaspersky Security Center ajánlásainak. Az adatbázis-korlátozásokkal kapcsolatos részletekért olvassa el a Kaspersky Security Center Súgót.

A Leltár feladat futtatása a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.
2. Kattintson az **New task** gombra.

   Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Leltár** elemet.

2. lépés: Leltár hatóköre

Hozzon létre egy listát azokról a mappákról, amelyekben azt szeretné, hogy a Kaspersky Endpoint Security futtatható fájlokat keressen. Konfigurálja a leltár beállításait (lásd az alábbi táblázatot).

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válasszon fiókot a *Leltár* feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot. Ha a leltár hatókörébe hálózati meghajtók vagy egyéb, korlátozott hozzáférésű objektumok tartoznak, válasszon elegendő hozzáférési joggal rendelkező felhasználói fiókot.

5. lépés Feladatindítási ütemezés konfigurálása

Konfigurálja a feladat ütemezését, például manuálisan.

6. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *Alapszintű leltár*.

7. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Ennek eredményeként a konfigurált ütemezésnek megfelelően a végrehajtható fájlok keresése a felhasználók számítógépein történik.

Leltár feladat futtatása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Inventory** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például *Alapszintű leltár*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. A feladat konfigurálásához lépjen a feladat tulajdonságaihoz (lásd az alábbi táblázatot).

8. Válassza ki a feladat melletti jelölőnégyzetet.

9. Kattintson az **Start** gombra.

   Megfigyelheti a feladat állapotát, valamint az eszközök számát, ahol a feladat sikeresen vagy hibásan lett végrehajtva. Ennek eredményeként a futtatható fájlok a megadott ütemezés szerint kerülnek átvizsgálásra a felhasználói számítógépeken.

Leltárbeállítások

Paraméter	Leírás
Inventory scopes	A leltár hatókörét alkotó objektumok listája.
DLL modules inventory	A Kaspersky Endpoint Security megkeresi a DLL modulokat a leltár hatókörében, és elküldi az információkat a Kaspersky Security Centernek. A DLL modulleltár engedélyezése jelentősen megnöveli a Leltár feladat elvégzéséhez szükséges időt és az adatbázis méretét.
Script files inventory	A Kaspersky Endpoint Security megkeresi a szkripteket a leltár hatókörében, és elküldi az információkat a Kaspersky Security Centernek. A szkriptfájlok leltárjának engedélyezése jelentősen megnöveli a Leltár feladat elvégzéséhez szükséges időt és az adatbázis méretét.
Run only when the computer is idle	A feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították. Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.
Scan only new and modified files	Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.
Skip file that is scanned for longer than (sec) N mp	A feladat végrehajtási idejének korlátozása. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejezettként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.

Paraméter	Leírás
Scan archives	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.
Scan distribution packages	Harmadik féltől származó alkalmazások terjesztőcsomagjainak vizsgálata.
Do not unpack large compound files	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás minden összetett fájlt megvizsgál. Az alkalmazás megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.

A végrehajtható fájlok tulajdonságok ablakának megnyitásához az Executable files mappában:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Application management** → **Executable files** lehetőséget.
3. Válasszon ki egy végrehajtható fájlt.
4. A végrehajtható fájl helyi menüjében válassza ki a **Properties** elemet.

Az alkalmazással és végrehajtható fájljaival kapcsolatos általános információk és számítógépek listájának megtekintéséhez, amelyeken az alkalmazás telepítve van, nyissa meg az **Applications registry** mappában vagy az **Executable files** mappában kiválasztott alkalmazás tulajdonságainak ablakát.

A telepített alkalmazásokra és futtatható fájlokra vonatkozó információk frissítése

A Kaspersky Endpoint Security 12.3 for Windows verziótól kezdve az Alkalmazásfelügyelő összetevő végrehajtható fájlok adatbázisával való működése optimalizálva van. A Kaspersky Endpoint Security 12.3 for Windows automatikusan frissíti az adatbázist, miután a fájlt törölték a számítógépről. Ez lehetővé teszi az adatbázis naprakészen tartását és a Kaspersky Security Center erőforrásainak kímélését.

A telepített alkalmazások adatbázisának naprakészen tartásához engedélyezni kell az alkalmazásinformációk küldését az adminisztrációs kiszolgálóra (alapértelmezés szerint engedélyezve van).

Az alkalmazásadatok küldésének engedélyezése az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirendek ablakában válassza az **Általános beállítások** → **Jelentések és tároló** lehetőséget.
4. Az **Adatátvitel az adminisztrációs kiszolgálóra** részen kattintson a **Beállítások** gombra.
5. Jelölje be **Indított alkalmazások** jelölőnégyzetet.
6. Mentse el a módosításokat.

Az alkalmazásra vonatkozó információk eltávolítása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **KSC Integration** elemet.
5. A **Data transfer to Administration Server** részen kattintson a **Advanced settings** gombra.
6. A megnyíló ablakban jelölje be a **About started applications** négyzetet.
7. Mentse el a módosításokat.

A Blokkolt alkalmazások mód engedélyezése

A *Blokkolt alkalmazások* módban az Alkalmazásfelügyelő a felhasználók számára engedélyezi minden alkalmazás elindítását, kivéve az Alkalmazásfelügyelő blokkolási szabályai által letiltottakat. Vagyis, ha nincs tiltó szabály, az Alkalmazásfelügyelő engedélyezi az alkalmazás indítását. Alapértelmezés szerint ez a mód van engedélyezve az Alkalmazásfelügyelőben.

A *Blokkolt alkalmazások* mód engedélyezése előtt ajánlott tesztelni az Alkalmazásfelügyeleti szabályokat. Ehhez engedélyezheti a teszt üzemmódot.

A Blokkolt alkalmazások mód engedélyezése az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
5. Jelölje be az **Alkalmazásfelügyelő** jelölőnégyzetet.
6. **Az Alkalmazásfelügyelő beállításai** részen a **Szabályozási mód** legördülő listából válassza ki **Tiltólista** elemet.
7. A **Művelet** legördülő listából válassza ki az Alkalmazásfelügyelő műveletét:
   - **Tesztszabályok**. Az Alkalmazásfelügyelő nem blokkolja azokat az alkalmazásokat, amelyek futását a szabályok tiltják, de eseményeket generál azokról az alkalmazásokról, amelyek futását egyébként blokkolná.
   - **Szabályok alkalmazása**. Az Alkalmazásfelügyelő blokkolja a tiltott alkalmazásokat, és létrehoz egy megfelelő eseményt.

8. Válassza ki az Alkalmazásfelügyeleti szabályok állapotát:

   - **Be**. Ez az állapot azt jelenti, hogy a szabály akkor van használatban, ha az Alkalmazásfelügyelő összetevő fut.
   - **Ki**. Ez az állapot azt jelenti, hogy a szabály akkor van mellőzve, ha az Alkalmazásfelügyelő összetevő fut.
   - **Teszt** Ez az állapot azt jelenti, hogy a Kaspersky Endpoint Security mindig engedélyezi az olyan alkalmazások elindítását, melyekre vonatkozik a szabály, de az indítások információit jelentésben rögzíti.

   Ha szükséges, adjon hozzá új Alkalmazásfelügyeleti szabályokat.

9. Konfigurálja az Alkalmazásfelügyelő speciális beállításait:

   - **A DLL-modulok betöltésének figyelése (jelentősen megnöveli a rendszer terhelését)**. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security szabályozza a DLL modulok betöltését, ha a felhasználó alkalmazásokat próbál elindítani. A DLL modullal és az azt betöltő alkalmazással kapcsolatos információk bekerülnek a jelentésbe.

     Amikor engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, győződjön meg arról, hogy az Alkalmazásfelügyelő beállításaiban engedélyezve van a következő szabályok egyike: **Golden Image** szabály, illetve egy másik szabály, amely tartalmazza a **Golden Image\Trusted Certificates** KL-kategóriát, és gondoskodik a megbízható DLL-modulok és illesztőprogramok betöltéséről a Kaspersky Endpoint Security indítása előtt. Ha úgy engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, hogy a **Golden Image** szabály ki van kapcsolva, az instabilitást okozhat az operációs rendszerben.

     A Kaspersky Endpoint Security kizárólag a jelölőnégyzet bejelölését követően betöltött DLL modulokat és illesztőprogramokat figyeli. A jelölőnégyzet bejelölése után ajánlott a számítógép újraindítása annak érdekében, hogy az alkalmazás minden DLL-modult és illesztőprogramot figyeljen, beleértve a Kaspersky Endpoint Security indítása előtt betöltött modulokat is.

   - **Szigorú digitális aláírás-ellenőrzés használata**. Kiválaszthat egy tanúsítványt egy alkalmazásfelügyeleti szabály kiváltó feltételeként. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security csak a megbízható rendszertanúsítvány-tárhelytől származó tanúsítványokkal aláírt alkalmazásokra alkalmaz szabályokat. Az ilyen tanúsítvánnyal aláírt alkalmazásokat a védelmi összetevők is megbízhatónak tekintik, például a *Kártevő vizsgálata* feladat. Ha azonban egy másik tárolóból származó tanúsítványt ad meg egy alkalmazásfelügyeleti szabályban, a Kaspersky Endpoint Security nem alkalmaz ilyen szabályt.

     Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security szabályokat alkalmaz a Windows Trusted Root Certificate Store származó tanúsítvánnyal aláírt alkalmazásokra. Az ilyen alkalmazások nem részei a megbízható zónának. A védelmi összetevők figyelik az ilyen alkalmazások tevékenységét.

   - **Üzenet a blokkolásról**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.
   - **Üzenet a rendszergazdának**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer.

10. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Blokkolt alkalmazások mód engedélyezése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **App Control** elemet.
5. Kapcsolja be az **Application Control ENABLED** kapcsolót.
6. A **Operating mode** területen válassza az **Block all except the rules list** opciót.
7. A **Action** területen válassza ki a megfelelő műveletet az Alkalmazásfelügyelőhöz:
   - **Inform**. Az Alkalmazásfelügyelő nem blokkolja azokat az alkalmazásokat, amelyek futását a szabályok tiltják, de eseményeket generál azokról az alkalmazásokról, amelyek futását egyébként blokkolná.
   - **Apply rules**. Az Alkalmazásfelügyelő blokkolja a tiltott alkalmazásokat, és létrehoz egy megfelelő eseményt.
8. Válassza ki az Alkalmazásfelügyeleti szabályok állapotát:
   - **Enabled**. Ez az állapot azt jelenti, hogy a szabály akkor van használatban, ha az Alkalmazásfelügyelő összetevő fut.
   - **Disabled**. Ez az állapot azt jelenti, hogy a szabály akkor van mellőzve, ha az Alkalmazásfelügyelő összetevő fut.
   - **Test mode**. Ez az állapot azt jelenti, hogy a Kaspersky Endpoint Security mindig engedélyezi az olyan alkalmazások elindítását, melyekre vonatkozik a szabály, de az indítások információit jelentésben rögzíti.

   Ha szükséges, adjon hozzá új Alkalmazásfelügyeleti szabályokat.
9. Konfigurálja az Alkalmazásfelügyelő speciális beállításait:
   - **Monitor loading of DLL modules**. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security szabályozza a DLL modulok betöltését, ha a felhasználó alkalmazásokat próbál elindítani. A DLL modullal és az azt betöltő alkalmazással kapcsolatos információk bekerülnek a jelentésbe.

     Amikor engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, győződjön meg arról, hogy az Alkalmazásfelügyelő beállításaiban engedélyezve van a következő szabályok egyike: **Golden Image** szabály, illetve egy másik szabály, amely tartalmazza a **Golden Image\Trusted Certificates** KL-kategóriát, és gondoskodik a megbízható DLL-modulok és illesztőprogramok betöltéséről a Kaspersky Endpoint Security indítása előtt. Ha úgy engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, hogy a **Golden Image** szabály ki van kapcsolva, az instabilitást okozhat az operációs rendszerben.

     A Kaspersky Endpoint Security kizárólag a jelölőnégyzet bejelölését követően betöltött DLL modulokat és illesztőprogramokat figyeli. A jelölőnégyzet bejelölése után ajánlott a számítógép újraindítása annak érdekében, hogy az alkalmazás minden DLL-modult és illesztőprogramot figyeljen, beleértve a Kaspersky Endpoint Security indítása előtt betöltött modulokat is.

- **Use strict digital signature verification**. Kiválaszthat egy tanúsítványt egy alkalmazásfelügyeleti szabály kiváltó feltételeként. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security csak a megbízható rendszertanúsítvány-tárhelytől származó tanúsítványokkal aláírt alkalmazásokra alkalmaz szabályokat. Az ilyen tanúsítvánnyal aláírt alkalmazásokat a védelmi összetevők is megbízhatónak tekintik, például a *Kártevő vizsgálata* feladat. Ha azonban egy másik tárolóból származó tanúsítványt ad meg egy alkalmazásfelügyeleti szabályban, a Kaspersky Endpoint Security nem alkalmaz ilyen szabályt.

  Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security szabályokat alkalmaz a Windows Trusted Root Certificate Store származó tanúsítvánnyal aláírt alkalmazásokra. Az ilyen alkalmazások nem részei a megbízható zónának. A védelmi összetevők figyelik az ilyen alkalmazások tevékenységét.

- **Message to user**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.

- **Message to administrator**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer.

10. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Blokkolt alkalmazások mód engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.

3. Kapcsolja be az **Alkalmazásfelügyelő** kapcsolót.

4. Az **Alkalmazásindítás vezérlésének módja** részen válassza a **Tiltólista elemet. A szabálylistán szereplők kivételével minden alkalmazás engedélyezett**.

5. A **Művelet szabályok által blokkolt alkalmazások indításakor** részen válassza ki az Alkalmazásfelügyelő műveletét:

   - **Információ (teszt üzemmód) és események naplózása jelentésben**. Az Alkalmazásfelügyelő nem blokkolja azokat az alkalmazásokat, amelyek futását a szabályok tiltják, de eseményeket generál azokról az alkalmazásokról, amelyek futását egyébként blokkolná.

   - **Blokkolás**. Az Alkalmazásfelügyelő blokkolja a tiltott alkalmazásokat, és létrehoz egy megfelelő eseményt.

6. Válassza ki az Alkalmazásfelügyeleti szabályok állapotát:

   - **Engedélyezve**. Ez az állapot azt jelenti, hogy a szabály akkor van használatban, ha az Alkalmazásfelügyelő összetevő fut.

   - **Letiltva**. Ez az állapot azt jelenti, hogy a szabály akkor van mellőzve, ha az Alkalmazásfelügyelő összetevő fut.

   - **Teszt üzemmód**. Ez az állapot azt jelenti, hogy a Kaspersky Endpoint Security mindig engedélyezi az olyan alkalmazások elindítását, melyekre vonatkozik a szabály, de az indítások információit jelentésben rögzíti.

   Ha szükséges, adjon hozzá új Alkalmazásfelügyeleti szabályokat.

7. Konfigurálja az Alkalmazásfelügyelő speciális beállításait:

   - **A DLL-modulok betöltésének figyelése**. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security szabályozza a DLL modulok betöltését, ha a felhasználó alkalmazásokat próbál elindítani. A DLL modullal és az azt betöltő alkalmazással kapcsolatos információk bekerülnek a jelentésbe.

Amikor engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, győződjön meg arról, hogy az Alkalmazásfelügyelő beállításaiban engedélyezve van a következő szabályok egyike: **Golden Image** szabály, illetve egy másik szabály, amely tartalmazza a **Golden Image\Trusted Certificates** KL-kategóriát, és gondoskodik a megbízható DLL-modulok és illesztőprogramok betöltéséről a Kaspersky Endpoint Security indítása előtt. Ha úgy engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, hogy a **Golden Image** szabály ki van kapcsolva, az instabilitást okozhat az operációs rendszerben.

A Kaspersky Endpoint Security kizárólag a jelölőnégyzet bejelölését követően betöltött DLL modulokat és illesztőprogramokat figyeli. A jelölőnégyzet bejelölése után ajánlott a számítógép újraindítása annak érdekében, hogy az alkalmazás minden DLL-modult és illesztőprogramot figyeljen, beleértve a Kaspersky Endpoint Security indítása előtt betöltött modulokat is.

- **Szigorú digitális aláírás-ellenőrzés használata**. Kiválaszthat egy tanúsítványt egy alkalmazásfelügyeleti szabály kiváltó feltételeként. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security csak a megbízható rendszertanúsítvány-tárhelytől származó tanúsítványokkal aláírt alkalmazásokra alkalmaz szabályokat. Az ilyen tanúsítvánnyal aláírt alkalmazásokat a védelmi összetevők is megbízhatónak tekintik, például a *Kártevő vizsgálata* feladat. Ha azonban egy másik tárolóból származó tanúsítványt ad meg egy alkalmazásfelügyeleti szabályban, a Kaspersky Endpoint Security nem alkalmaz ilyen szabályt.

  Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security szabályokat alkalmaz a Windows Trusted Root Certificate Store származó tanúsítvánnyal aláírt alkalmazásokra. Az ilyen alkalmazások nem részei a megbízható zónának. A védelmi összetevők figyelik az ilyen alkalmazások tevékenységét.

- **Alkalmazásblokkolással kapcsolatos üzenetsablonok**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.

- **Alkalmazás indításának blokkolása esetén megjelenő üzenetsablon**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer.

8. Mentse el a módosításokat.

Ennek eredményeként az Alkalmazásfelügyelő blokkolja a blokkolt alkalmazásokat. A Kaspersky Endpoint Security is generál *Alkalmazásindítás letiltva* eseményeket. Ezeket az eseményeket felhasználhatja a *Report on prohibited applications* jelentés generálásához a Kaspersky Security Center konzolon. A jelentés összefoglalójában megtekintheti azon alkalmazások és számítógépek listáját, amelyeknél az Alkalmazásfelügyeleti szabály aktiválódott.

Alapszámítógépen alapuló Alkalmazásfelügyelő

Alapszámítógépet használhat egy olyan lemezkép létrehozásához, amely tartalmazza az Ön számára szükséges alkalmazásokat. A lemezkép segítségével ezután telepítheti az operációs rendszert és az alkalmazásokat más számítógépekre. A lemezképet nem mindig lehet naprakészen tartani. Az Alkalmazásfelügyelő lehetővé teszi az engedélyezett alkalmazások listájának karbantartását egy alapszámítógép alapján. Az Alkalmazásfelügyelő automatikusan meghatározza, hogy mely alkalmazások vannak telepítve az alapszámítógépre, és frissíti a kategóriát. Ily módon a számítógépek naprakész listát kapnak az engedélyezett alkalmazásokról.

Az Alkalmazásfelügyelő alapszámítógép alapján történő konfigurálása a következő lépésekből áll:

1. Automatikusan frissülő kategória létrehozása. Az új kategória létrehozásakor válassza ki a **Category that includes executable files from a specific folder** kategóriát, és válassza ki az alapszámítógépet.

Automatikusan frissülő kategória létrehozása az adminisztrációs konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Application management** → **Application categories** lehetőséget.
3. Kattintson a munkaterületen az **New category** gombra.

   Ezzel elindítja az alkalmazáskategóriaát létrehozó varázslót.
4. Kövesse az alkalmazáskategória-létrehozási varázsló utasításait.

1. lépés A kategória típusának kiválasztása

Válassza ki **Category that includes executable files from selected devices** kategóriatípusként.

2. lépés Felhasználói kategórianév megadása

Ennél a lépésnél adja meg az alkalmazáskategória nevét.

3. lépés Beállítások

> Ez a lépés akkor érhető el, ha a **Category that includes executable files from selected devices** kategóriatípust választotta ki.

Ennél a lépésnél kattintson a **Add** gombra és adja meg a számítógépeket, melyeknek végrehajtható fájljait a Kaspersky Security Center hozzáadja az alkalmazáskategóriához. Az adott számítógépeknek a **Executable files** mappában található végrehajtható fájljait a Kaspersky Security Center hozzáadja az alkalmazáskategóriához.

Ennél a lépésnél beállíthatja a következő beállításokat is:

- Algoritmus a hash-függvény kiszámításához. Az algoritmus kiválasztásához be kell jelölnie legalább az egyik jelölőnégyzetet:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- A **Synchronize data with Administration Server repository** jelölőnégyzet. Jelölje be ezt a jelölőnégyzetet, ha azt akarja, hogy a Kaspersky Security Center időnként törölje az alkalmazáskategóriát, és hozzáadja ehhez az adott számítógépek végrehajtható fájljait, melyek a **Executable files** mappában találhatóak.

  Ha az **Synchronize data with Administration Server repository** jelölőnégyzet ki van törölve, a Kaspersky Security Center nem hajt végre módosításokat egy alkalmazáskategórián a létrehozása után.

4. lépés Szűrő

Ebben a lépésben állítson be egy szűrőt a fájlokhoz.

Megadhatja az alkalmazáskategória létrehozásához használni kívánt fájltípust.

- **All files**. A kategória minden fájlt meg fog találni. Alapértelmezésben ez a lehetőség van kiválasztva.
- **Only files outside the application categories**. A kategória csak az alkalmazáskategóriákon kívüli fájlokat fogja megtalálni.

Megadhatja a kiválasztott számítógépek azon mappáit, amelyek az alkalmazáskategória létrehozásához használni kívánt fájlokat tartalmazzák.

- **All folders**. A kategória minden mappát meg fog találni. Alapértelmezésben ez a lehetőség van kiválasztva.
- **Specified folder**. A kategória csak a megadott mappát fogja megtalálni. Ha ezt a lehetőséget választja, meg kell adnia a mappa elérési útját.

5. lépés Egyéni kategória létrehozása

Lépjen ki a varázslóból.

Kategória létrehozása automatikusan hozzáadott tartalommal a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza az **Operations → Third-party applications → Application categories** lehetőséget.

   Ezzel megnyitja az alkalmazáskategóriák listáját.

2. Kattintson az **Add** gombra.

   Ezzel elindítja az alkalmazáskategóriaát létrehozó varázslót.

3. Konfigurálja az alkalmazáskategória általános beállításait:

   - Kategória neve.
   - Kategória létrehozási módszere. Válassza ki **Category that includes executable files from selected devices** kategóriatípusként.

   Lépjen a következő lépésre.

4. Konfigurálja az alkalmazáskategória speciális beállításait:

   - Adja meg azokat a számítógépeket, amelyekről a Kaspersky Security Center hozzáadja a futtatható fájlokat az alkalmazáskategóriához. Az adott számítógépeknek a **Executable files** mappában található végrehajtható fájljait a Kaspersky Security Center hozzáadja az alkalmazáskategóriához.
   - Válasszon algoritmust a kivonat kiszámításához.

- Konfigurálja az adatok és az Administration Server tároló közötti szinkronizálás időközét.
- Állítson be egy szűrőt a fájlokhoz.

5. Lépjen ki a varázslóból.

Automatikusan frissülő kategória létrehozásakor célszerű lehet a fájlokat több kategóriára felosztani. Például az operációs rendszer fájljai és a Program Files mappa fájljai. Ehhez használhat egy szűrőt a kategóriabeállításokban, és kiválaszthat egyedi mappákat.

2. Az Alkalmazásfelügyelő módjának kiválasztása. Meg kell akadályoznia minden kifejezetten nem engedélyezett alkalmazás futtatását. Ehhez válassza ki a *Blokkolt alkalmazások* módot.

3. Alkalmazásfelügyeleti szabályok létrehozása. A szabálybeállításokban válassza ki azt a kategóriát, amelyhez az alapszámítógépről származó futtatható fájlok tartoznak.

Az Alkalmazásfelügyelő konfigurálása egy alapszámítógép alapján a felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
5. Jelölje be az **Alkalmazásfelügyelő** jelölőnégyzetet.
6. **Az Alkalmazásfelügyelő beállításai** részen a **Szabályozási mód** legördülő listából válassza ki **Tiltólista** elemet.
7. A **Művelet** legördülő listából válassza ki az Alkalmazásfelügyelő műveletét:
   - **Tesztszabályok**. Az Alkalmazásfelügyelő nem blokkolja azokat az alkalmazásokat, amelyek futását a szabályok tiltják, de eseményeket generál azokról az alkalmazásokról, amelyek futását egyébként blokkolná.
   - **Szabályok alkalmazása**. Az Alkalmazásfelügyelő blokkolja a tiltott alkalmazásokat, és létrehoz egy megfelelő eseményt.
8. Az Alkalmazásfelügyeleti szabályok listájában kattintson a **Hozzáadás** gombra.

   Ezzel elindul az Alkalmazásfelügyeleti szabály hozzáadására szolgáló varázsló.
9. A **Kategória** legördülő listából válasszon ki egy automatikusan frissülő kategóriát az alapszámítógép alapján.
10. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, amelyekre alkalmazni szeretné az Alkalmazásfelügyeleti szabályt.

11. Konfigurálja az Alkalmazásfelügyeleti szabály speciális beállításait:

    - **Más felhasználók számára megtagadás**. Az alkalmazás a listán nem szereplő összes felhasználó számára megakadályozza a kiválasztott kategóriába tartozó alkalmazások indítását.

    - **Megbízható frissítéstelepítők**. A Kaspersky Endpoint Security a kiválasztott kategóriába tartozó alkalmazásokat megbízható frissítőknek tekinti, amelyek más futtatható fájlokat hozhatnak létre, és amelyek futtatása később engedélyezett lesz.

12. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az Alkalmazásfelügyelő konfigurálása egy alapszámítógép alapján a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **App Control** elemet.

5. Kapcsolja be az **Application Control ENABLED** kapcsolót.

6. A **Operating mode** területen válassza az **Block all except the rules list** opciót.

7. A **Action** területen válassza ki a megfelelő műveletet az Alkalmazásfelügyelőhöz:

    - **Inform**. Az Alkalmazásfelügyelő nem blokkolja azokat az alkalmazásokat, amelyek futását a szabályok tiltják, de eseményeket generál azokról az alkalmazásokról, amelyek futását egyébként blokkolná.

    - **Apply rules**. Az Alkalmazásfelügyelő blokkolja a tiltott alkalmazásokat, és létrehoz egy megfelelő eseményt.

8. Az Alkalmazásfelügyeleti szabályok listájában kattintson a **Add** gombra.

   Ezzel elindul az Alkalmazásfelügyeleti szabály hozzáadására szolgáló varázsló.

9. A **Categories/Applications** részen válasszon ki egy automatikusan frissülő kategóriát az alapszámítógép alapján.

10. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, amelyekre alkalmazni szeretné az Alkalmazásfelügyeleti szabályt.

11. Konfigurálja az Alkalmazásfelügyeleti szabály speciális beállításait:

    - **Users**. Az alkalmazás a listán nem szereplő összes felhasználó számára megakadályozza a kiválasztott kategóriába tartozó alkalmazások indítását.

    - **Trusted Updaters**. A Kaspersky Endpoint Security a kiválasztott kategóriába tartozó alkalmazásokat megbízható frissítőknek tekinti, amelyek más futtatható fájlokat hozhatnak létre, és amelyek futtatása később engedélyezett lesz.

12. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az Alkalmazásfelügyelő konfigurálása egy alapszámítógép alapján az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.
3. Kapcsolja be az **Alkalmazásfelügyelő** kapcsolót.
4. Az **Alkalmazásindítás vezérlésének módja** részen válassza a **Tiltólista elemet. A szabálylistán szereplők kivételével minden alkalmazás engedélyezett**.
5. A **Művelet szabályok által blokkolt alkalmazások indításakor** részen válassza ki az Alkalmazásfelügyelő műveletét:
   - **Információ (teszt üzemmód) és események naplózása jelentésben**. Az Alkalmazásfelügyelő nem blokkolja azokat az alkalmazásokat, amelyek futását a szabályok tiltják, de eseményeket generál azokról az alkalmazásokról, amelyek futását egyébként blokkolná.
   - **Blokkolás**. Az Alkalmazásfelügyelő blokkolja a tiltott alkalmazásokat, és létrehoz egy megfelelő eseményt.
6. Az Alkalmazásfelügyeleti szabályok listájában kattintson a **Hozzáadás** gombra.

   Ezzel elindul az Alkalmazásfelügyeleti szabály hozzáadására szolgáló varázsló.
7. A **Kategória** részen válasszon ki egy automatikusan frissülő kategóriát az alapszámítógép alapján.
8. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, amelyekre alkalmazni szeretné az Alkalmazásfelügyeleti szabályt.
9. Konfigurálja az Alkalmazásfelügyeleti szabály speciális beállításait:
   - **Más felhasználók számára megtagadás**. Az alkalmazás a listán nem szereplő összes felhasználó számára megakadályozza a kiválasztott kategóriába tartozó alkalmazások indítását.
   - **Megbízható frissítéstelepítők**. A Kaspersky Endpoint Security a kiválasztott kategóriába tartozó alkalmazásokat megbízható frissítőknek tekinti, amelyek más futtatható fájlokat hozhatnak létre, és amelyek futtatása később engedélyezett lesz.
10. Mentse el a módosításokat.

Alkalmazásfelügyeleti szabályok kezelése

A Kaspersky Endpoint Security az alkalmazások felhasználók által történő elindítását szabályok révén felügyeli. Az Alkalmazásfelügyeleti szabály megadja az aktiváló feltételeket, valamint a szabály miatti aktiváláskor az Alkalmazásfelügyelő által elvégzett műveleteket (az alkalmazás felhasználók általi elindításának engedélyezését, illetve blokkolását).

A szabálykiváltó feltételek

A szabálykiváltó feltétel a következő korrelációval rendelkezik: „feltétel típusa – feltétel kritériuma – feltételérték”. A szabályt kiváltó feltételek alapján a Kaspersky Endpoint Security egy szabályt alkalmaz (vagy nem alkalmaz) egy alkalmazásra.

A következő típusú feltételek vannak használatban a szabályokban:

- *Belefoglalási feltételek*. A Kaspersky Endpoint Security a szabályt alkalmazza az alkalmazásra, ha az alkalmazás a belefoglalási feltételek közül legalább egynek megfelel.
- *Kizárási feltételek*. A Kaspersky Endpoint Security a szabályt nem alkalmazza az alkalmazásra, ha az alkalmazás a kizárási feltételek közül legalább egynek, a belefoglalási feltételek közül pedig egyiknek sem felel meg.

A szabálykiváltó feltételek kritériumok segítségével készülnek. A szabályok elkészítésére a Kaspersky Endpoint Security alkalmazásban az alábbi kritériumok szolgálnak:

- Az alkalmazás futtatható fájlját tartalmazó mappának vagy az alkalmazás futtatható fájljának elérési útvonala.
- Metaadatok: alkalmazás futtatható fájljának neve, alkalmazás futtatható fájljának verziója, alkalmazásnév, alkalmazás verziója, alkalmazás forgalmazója.
- Alkalmazás futtatható fájljának ellenőrzőösszege.
- Tanúsítvány: kiállító, alany, ujjlenyomat.
- Az alkalmazás szerepeltetése KL kategóriában.
- Az alkalmazás cserélhető meghajtón lévő futtatható fájljának helye.

A feltételben használt összes kritériumnak meg kell adni az értékét. Ha az elindítandó alkalmazások paraméterei megfelelnek a szerepeltetési feltételben megadott kritériumok értékeinek, a szabály kiváltása megtörténik. Ekkor az Alkalmazásfelügyelő elvégzi a szabályban előírt műveletet. Ha az elindítandó alkalmazások paraméterei megfelelnek a kizárási feltételben megadott kritériumok értékeinek, az Alkalmazásfelügyelő nem felügyeli az alkalmazás indítását.

Ha egy tanúsítványt választott szabálykiváltó feltételként, akkor gondoskodnia kell arról, hogy ez a tanúsítvány hozzá legyen adva a számítógép megbízható rendszertárolójához, és ellenőrizze a megbízható rendszertárhasználati beállításokat az alkalmazásban.

Az Alkalmazásfelügyelő által szabály kiváltása esetén hozott döntések

Szabály kiváltásakor az Alkalmazásfelügyelő a szabálynak megfelelően lehetővé teszi, hogy a felhasználók (vagy felhasználói csoportok) elindítsák az alkalmazásokat, illetve blokkolja az indítást. Kiválaszthatja azokat az egyéni felhasználókat vagy felhasználói csoportokat, akik egy adott szabályt kiváltó alkalmazásokat elindíthatnak, illetve nem indíthatnak el.

Az olyan szabályokat, amelyben nincs megadva a szabálynak megfelelő alkalmazások indítására jogosult felhasználó, *blokkoló* szabálynak nevezzük.

Az olyan szabályokat, amelyben nincs megadva a szabálynak megfelelő alkalmazások indítására nem jogosult felhasználó, *engedélyező* szabálynak nevezzük.

A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. Ha például hozzá van rendelve egy Alkalmazásfelügyelő engedélyező szabály egy felhasználói csoporthoz, és emellett hozzá van rendelve egy Alkalmazásfelügyelő blokkoló szabály a felhasználói csoportba tartozó egyik felhasználóhoz, akkor az érintett felhasználó az alkalmazást nem indíthatja el.

Egy szabály műveleti állapota

Az alkalmazásfelügyeleti szabályok a következő állapotokkal rendelkezhetnek:

- **Engedélyezve**. Ez az állapot azt jelenti, hogy a szabály akkor van használatban, ha az Alkalmazásfelügyelő összetevő fut.
- **Letiltva**. Ez az állapot azt jelenti, hogy a szabály akkor van mellőzve, ha az Alkalmazásfelügyelő összetevő fut.
- **Teszt üzemmód**. Ez az állapot azt jelzi, hogy a Kaspersky Endpoint Security engedélyezi az olyan alkalmazások elindítását, melyekre vonatkoznak a szabályok, de az indítások információit jelentésben rögzíti.

Alkalmazásfelügyeleti szabályt kiváltó feltétel hozzáadása

A nagyobb kényelem érdekében az Alkalmazásfelügyeleti szabályok létrehozása során létrehozhat alkalmazáskategóriákat.

Javasoljuk, hogy hozzon létre egy „Munkaalkalmazások” kategóriát, melybe a vállalatnál használt alkalmazások szokásos készletét helyezze. Ha a különböző felhasználói csoportok munkájuk során más-más alkalmazáskészleteket használnak, akkor az egyes csoportok számára külön alkalmazáskategóriákat hozhat létre.

Alkalmazáskategória létrehozása a Felügyeleti konzolon:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Application management** → **Application categories** lehetőséget.
3. Kattintson a munkaterületen az **New category** gombra.

   Elindul a Felhasználói kategóriakészítő varázsló.
4. Kövesse a Felhasználói kategóriakészítő varázsló utasításait.

1. lépés A kategória típusának kiválasztása

Ennél a lépésnél kiválaszthatja az alkalmazáskategóriák következő típusainak egyikét:

- Category with content added manually. Data of executable files is manually added to the category Ha ezt a kategóriatípust választotta, a *Configuring conditions for inclusion of applications in categories* lépésnél és a *Configuring conditions for exclusion of applications from categories* lépésnél meghatározhatja azokat a kritériumokat, amelyek alapján a futtatható fájlok bekerülnek a kategóriába.

- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category Ha ezt a kategóriatípust választotta, a *Settings* lépésnél megadhat egy számítógépet, melynek végrehajtható fájljait a rendszer automatikusan beleveszi a kategóriába.

- Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category Ha ezt a kategóriatípust választotta, a *Repository folder* lépésnél megadhat egy mappát, ahonnan a végrehajtható fájlok automatikusan bekerülnek a kategóriába.

Automatikusan hozzáadott tartalmú kategória létrehozása esetén a Kaspersky Security Center leltározni fogja a következő formátumú fájlokat: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX és SCR.

2. lépés Felhasználói kategórianév megadása

Ennél a lépésnél adja meg az alkalmazáskategória nevét.

3. lépés Az alkalmazások kategóriához való hozzáadásának feltételeinek beállítása

Ha nagyszámú feltételt (például fájlkivonatokat) ad hozzá az Alkalmazásfelügyeleti szabályokhoz, megnő a számítógép erőforrás-használata. Ha a feltételek teljes száma eléri az 50 000-et, teljesítménybeli problémák léphetnek fel. A teljesítmény optimalizálása érdekében javasolt a feltételek felülvizsgálata és csökkentése.

Ez a lépés akkor érhető el, ha a **Category with content added manually** kategóriatípust választotta ki.

Ennél a lépésnél, a **Add** legördülő listán válasszon ki egy feltételt az alkalmazások kategóriába való beemeléséhez:

- **From the list of executable files**. Az ügyfél eszközökön a végrehajtható fájlok listájából hozzáad alkalmazásokat az egyéni kategóriához.

- **From file properties**. A végrehajtható fájlok részletes adatainak megadása, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

- **Metadata from files in folder**. Válassza ki a végrehajtható fájlokat tartalmazó mappát az ügyféleszközön. A Kaspersky Security Center kijelzi a végrehajtható fájlok metaadatait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

- **Checksums of the files in the folder**. Válassza ki a végrehajtható fájlokat tartalmazó mappát az ügyféleszközön. A Kaspersky Security Center kijelzi a végrehajtható fájlok hash-kódjait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

- **Certificates for the files from the folder**. Válassza ki a tanúsítvánnyal aláírt végrehajtható fájlokat tartalmazó mappát az ügyféleszközön. A Kaspersky Security Center kijelzi a végrehajtható fájlok tanúsítványát, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

  Nem ajánlott az olyan feltételek használata, melyek tulajdonságaiban nincs megadva a **Certificate fingerprint** paraméter.

- **MSI installer files metadata**. Válassza ki az MSI-csomagot. A Kaspersky Security Center jelzi az MSI telepítőcsomag végrehajtható fájljainak metaadatait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

- **Checksums of the files from the MSI installer of the application**. Válassza ki az MSI-csomagot. A Kaspersky Security Center jelzi a jelen MSI telepítőcsomag végrehajtható fájljainak hash-kódjait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

- **From KL category**. Adjon meg egy KL kategóriát az alkalmazások egyéni kategóriához való hozzáadásának feltételeként. A *KL category* olyan alkalmazások listája, amelyeknek közösek a témaattribútumaik. A listát a Kaspersky szakértői tartják karban. Az *Office Applications* néven ismert KL kategória többek közt például a Microsoft Office csomag alkalmazásait és az Adobe Acrobat alkalmazást tartalmazza.

  Kiválaszthatja az összes KL kategóriát, hogy létrehozzanak egy kiterjesztett listát a megbízható alkalmazásokról.

- **Specify path to application (masks supported)**. Válasszon ki egy mappát az ügyféleszközön. A Kaspersky Security Center hozzáadja a mappa végrehajtható fájljait az egyéni kategóriához.

- **Select certificate from repository**. Válassza ki a végrehajtható fájlok aláírásához használt tanúsítványokat az egyéni kategóriához történő alkalmazás-hozzáadás feltételeként.

  Nem ajánlott az olyan feltételek használata, melyek tulajdonságaiban nincs megadva a **Certificate fingerprint** paraméter.

  Kiválaszthatja a tanúsítványtárolót. Alapértelmezés szerint az Alkalmazásfelügyelő csak a megbízható rendszertanúsítvány-tárhelyről származó tanúsítvánnyal aláírt alkalmazásokra alkalmaz szabályokat. Ezt a **Szigorú digitális aláírás-ellenőrzés használata** jelölőnégyzet biztosítja.

- **Drive type**. Adja meg a tárolóeszköz típust (minden merevlemez és cserélhető meghajtó vagy csak a cserélhető meghajtók) az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

4. lépés Az alkalmazások kategóriából való kizárásának feltételeinek beállítása

Ez a lépés akkor érhető el, ha a **Category with content added manually** kategóriatípust választotta ki.

Az ennél a lépésnél megadott alkalmazások ki vannak zárva a kategóriából, még akkor is, ha meg lettek adva „Az alkalmazások kategóriához való hozzáadásának feltételeinek beállítása" lépésben.

Ennél a lépésnél, a **Add** legördülő listán válassza ki az alkalmazások kategóriából való kizárásának feltételeit:

- **From the list of executable files**. Az ügyfél eszközökön a végrehajtható fájlok listájából hozzáad alkalmazásokat az egyéni kategóriához.
- **From file properties**. A végrehajtható fájlok részletes adatainak megadása, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.
- **Metadata from files in folder**. Válassza ki a végrehajtható fájlokat tartalmazó mappát az ügyféleszközön. A Kaspersky Security Center kijelzi a végrehajtható fájlok metaadatait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.
- **Checksums of the files in the folder**. Válassza ki a végrehajtható fájlokat tartalmazó mappát az ügyféleszközön. A Kaspersky Security Center kijelzi a végrehajtható fájlok hash-kódjait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.
- **Certificates for the files from the folder**. Válassza ki a tanúsítvánnyal aláírt végrehajtható fájlokat tartalmazó mappát az ügyféleszközön. A Kaspersky Security Center kijelzi a végrehajtható fájlok tanúsítványát, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.
- **MSI installer files metadata**. Válassza ki az MSI-csomagot. A Kaspersky Security Center jelzi az MSI telepítőcsomag végrehajtható fájljainak metaadatait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.
- **Checksums of the files from the MSI installer of the application**. Válassza ki az MSI-csomagot. A Kaspersky Security Center jelzi a jelen MSI telepítőcsomag végrehajtható fájljainak hash-kódjait, az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.
- **From KL category**. Adjon meg egy KL kategóriát az alkalmazások egyéni kategóriához való hozzáadásának feltételeként. A *KL category* olyan alkalmazások listája, amelyeknek közösek a témaattribútumaik. A listát a Kaspersky szakértői tartják karban. Az *Office Applications* néven ismert KL kategória többek közt például a Microsoft Office csomag alkalmazásait és az Adobe Acrobat alkalmazást tartalmazza.

  Kiválaszthatja az összes KL kategóriát, hogy létrehozzanak egy kiterjesztett listát a megbízható alkalmazásokról.
- **Specify path to application (masks supported)**. Válasszon ki egy mappát az ügyféleszközön. A Kaspersky Security Center hozzáadja a mappa végrehajtható fájljait az egyéni kategóriához.
- **Select certificate from repository**. Válassza ki a végrehajtható fájlok aláírásához használt tanúsítványokat az egyéni kategóriához történő alkalmazás-hozzáadás feltételeként.
- **Drive type**. Adja meg a tárolóeszköz típust (minden merevlemez és cserélhető meghajtó vagy csak a cserélhető meghajtók) az alkalmazások egyéni kategóriához való hozzáadásának feltételeként.

5. lépés Beállítások

Ez a lépés akkor érhető el, ha a **Category that includes executable files from selected devices** kategóriatípust választotta ki.

Ennél a lépésnél kattintson a **Add** gombra és adja meg a számítógépeket, melyeknek végrehajtható fájljait a Kaspersky Security Center hozzáadja az alkalmazáskategóriához. Az adott számítógépeknek a **Executable files** mappában található végrehajtható fájljait a Kaspersky Security Center hozzáadja az alkalmazáskategóriához.

Ennél a lépésnél beállíthatja a következő beállításokat is:

- Algoritmus a hash-függvény kiszámításához. Az algoritmus kiválasztásához be kell jelölnie legalább az egyik jelölőnégyzetet:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- A **Synchronize data with Administration Server repository** jelölőnégyzet. Jelölje be ezt a jelölőnégyzetet, ha azt akarja, hogy a Kaspersky Security Center időnként törölje az alkalmazáskategóriát, és hozzáadja ehhez az adott számítógépek végrehajtható fájljait, melyek a **Executable files** mappában találhatóak.

  Ha az **Synchronize data with Administration Server repository** jelölőnégyzet ki van törölve, a Kaspersky Security Center nem hajt végre módosításokat egy alkalmazáskategórián a létrehozása után.

Step 6. Tárhely mappa

Ez a lépés akkor érhető el, ha a **Category that includes executable files from a specific folder** kategóriatípust választotta ki.

Ebben a lépésben adja meg azt a mappát, amelyben a Kaspersky Security Center a futtatható fájlokat keresi, hogy az alkalmazásokat automatikusan hozzáadja az alkalmazáskategóriához.

Ennél a lépésnél beállíthatja a következő beállításokat is:

- A **Include dynamic-link libraries (DLL) in this category** jelölőnégyzet. Jelölje be ezt a jelölőnégyzetet, ha szeretné a dinamikus csatolású könyvtárak (DLL-fájlok) beemelését az alkalmazáskategóriába.

  Ha a DLL fájlok beletartoznak az alkalmazáskategóriába, a Kaspersky Security Center teljesítménye csökkenhet.

- A **Include script data in this category** jelölőnégyzet. Jelölje be ezt a jelölőnégyzetet, ha szeretné beemelni a szkripteket az alkalmazáskategóriába.

  A szkriptfájlok alkalmazáskategóriába történő beemelése visszavetheti a Kaspersky Security Center teljesítményét.

- Algoritmus a hash-függvény kiszámításához. Az algoritmus kiválasztásához be kell jelölnie legalább az egyik jelölőnégyzetet:

  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.

  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- A **Force folder scan for changes** jelölőnégyzet. Jelölje be a jelölőnégyzetet ha azt szeretné, hogy a Kaspersky Security Center időnként keresse az alkalmazáskategóriákhoz való automatikus hozzáadásra használt mappákban lévő végrehajtható fájlokat.

  Ha a **Force folder scan for changes** jelölőnégyzet ki van törölve, a Kaspersky Security Center az alkalmazáskategóriához való automatikus hozzáadásra használt mappákban lévő végrehajtható fájlokat csak akkor keresi meg, ha a mappában módosítások történtek, vagy fájlok lettek hozzáadva vagy törölve.

- A **Scan interval (1–168 hours)** mező. Ebben a mezőben megadhatja az időtartamot (órában), melynek lejárta után a Kaspersky Security Center elindítja az alkalmazáskategóriákhoz való automatikus hozzáadásra használt mappákban a végrehajtható fájlok keresését.

  A mező akkor használható, ha be van jelölve a **Force folder scan for changes** jelölőnégyzet.

7. lépés Egyéni kategória létrehozása

Lépjen ki a varázslóból.

Alkalmazásfelügyeleti szabályt kiváltó új feltétel hozzáadása az alkalmazás felületéhez:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
3. Kattintson a **Blokkolt alkalmazások** vagy az **Engedélyezett alkalmazások** gombra.

   Az Alkalmazásfelügyeleti szabályok listáját nyitja meg.
4. Válassza ki azt a szabályt, amelyhez kiváltó feltételt szeretne konfigurálni.

   Megnyílik az Alkalmazásfelügyelő szabály tulajdonságai ablak.
5. Válassza ki a **Feltételek: N** lapot vagy a **Kizárások** lapot, és kattintson az **Hozzáadás** gombra.

6. Alkalmazásfelügyelő szabályt kiváltó feltétel hozzáadása:

   - **Feltételek az elindított alkalmazások tulajdonságai alapján**. A futó alkalmazások listájában kiválaszthatja azokat az alkalmazásokat, amelyekre az Alkalmazásfelügyeleti szabály vonatkozni fog. A Kaspersky Endpoint Security szintén felsorolja azokat az alkalmazásokat, amelyek korábban futottak a számítógépen. Ki kell választania azt a feltételt, amelyet egy vagy több szabálykiváltó feltétel létrehozására kíván használni: **Fájlkivonat**, **Tanúsítvány**, **KL kategória**, **Metaadatok** vagy **Fájl vagy mappa elérési útja**.

   - **Feltétel(ek) "KL kategória" alapján**. A *KL category* olyan alkalmazások listája, amelyeknek közösek a témaattribútumaik. A listát a Kaspersky szakértői tartják karban. Az „Irodai alkalmazások" néven ismert KL kategória például a Microsoft Office csomag alkalmazásait, az Adobe® Acrobat® alkalmazást és másokat tartalmaz.

   - **Egyedi feltétel**. Kiválaszthatja az alkalmazásfájlt, és kiválaszthatja a szabálykiváltó feltételek egyikét: **Fájlkivonat**, **Tanúsítvány**, **Metaadatok** vagy **Fájl vagy mappa elérési útja**.

   - **Feltétel fájlmeghajtó alapján (cserélhető meghajtó)**. Az Alkamazásfelügyeleti szabály cserélhető meghajtón futó fájlokra vonatkozik.

   - **Feltételek a megadott mappában található fájlok tulajdonságai alapján**. Az Alkamazásfelügyeleti szabály csak a megadott mappában található fájlokra vonatkozik. Az almappákból fájlokat vehet fel vagy zárhat ki. Ki kell választania azt a feltételt, amelyet egy vagy több szabálykiváltó feltétel létrehozására kíván használni: **Fájlkivonat**, **Tanúsítvány**, **KL kategória**, **Metaadatok** vagy **Fájl vagy mappa elérési útja**.

7. Mentse el a módosításokat.

A feltételek hozzáadásakor kérjük, vegye figyelembe az Alkalmazásfelügyelővel kapcsolatos alábbi különleges szempontokat:

- A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket maszk metaadatokban való megadásához: **File name**, **Application name**, **Vendor**.

- A Kaspersky Endpoint Security nem támogatja az MD5 ellenőrzőösszeget, és MD5 ellenőrzőösszeg alapján nem felügyeli az alkalmazások indítását. Szabálykiváltó feltételként SHA256 ellenőrzőösszeg szolgál.

- Szabálykiváltó feltételként nem javasolt csak a **Kiállító** és a **Tanúsítvány alanya** kritériumokat használni. E kritériumok használata megbízhatatlan.

- Ha szimbolikus hivatkozást használ a **Fájl vagy mappa elérési útja** mezőben, akkor az Alkalmazásfelügyeleti szabály helyes működése érdekében javasoljuk, hogy oldja fel a szimbolikus hivatkozást. Ehhez kattintson a **Szimbolikus hivatkozás megoldása** gombra.

Futtatható fájlok hozzáadása a Futtatható fájlok mappából az alkalmazáskategóriákba

Az **Executable files** mappában megjelenik a számítógépeken észlelt végrehajtható fájlok listája. A Kaspersky Endpoint Security létrehoz egy listát a végrehajtható fájlokról, miután végre lett hajtva a Leltárfeladat.

A Executable files mappából futtatható fájlok hozzáadása az alkalmazáskategóriához:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Application management** → **Executable files** lehetőséget.

3. A munkaterületen válassza ki az alkalmazáskategóriákhoz hozzáadni kívánt végrehajtható fájlokat.

4. Nyissa meg jobb kattintással a helyi menüt a kiválasztott végrehajtott fájlokhoz, majd válassza ki a **Add to category** lehetőséget.

5. A megnyíló ablakban tegye a következőket:

   - Az ablak felső részén válassza az alábbi lehetőségek egyikét:

     - **Add to a new application category**. Válassza ezt a lehetőséget, ha új alkalmazáskategóriát akar létrehozni, és végrehajtható fájlokat akar hozzáadni.

     - **Add to an existing application category**. Válassza ezt a lehetőséget, ha egy meglévő alkalmazáskategóriát akar kiválasztani, és végrehajtható fájlokat akar hozzáadni.

   - A **Rule type** blokkban válassza ki a következő opciók egyikét:

     - **Rules for adding to inclusions**. Válassza ezt a lehetőséget, ha egy olyan feltételt akar létrehozni, amely végrehajtható fájlokat ad hozzá az alkalmazáskategóriához.

     - **Rules for adding to exclusions**. Válassza ezt a lehetőséget, ha egy olyan feltételt akar létrehozni, amely végrehajtható fájlokat zár ki az alkalmazáskategóriákból.

   - A **Parameter used as a condition** blokkban válassza ki a következő opciók egyikét:

     - **Certificate details (or SHA256 hashes for files without a certificate)**.

     - **Certificate details (files without a certificate will be skipped)**.

     - **Only SHA256 (files without a hash will be skipped)**.

     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

6. Mentse el a módosításokat.

Eseményhez kapcsolódó végrehajtható fájlok hozzáadása az alkalmazáskategóriához

Az Alkalmazásfelügyelő eseményeiből eredő végrehajtható fájlok hozzáadásához az alkalmazáskategóriához:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Events** lapot.

3. Válassza ki az Alkalmazásfelügyelő összetevő működéséhez köthető eseményeket (Az Alkalmazásfelügyelő összetevő működéséből eredő események megtekintése, Az Alkalmazásfelügyelő összetevő tesztműködéséből eredő események megtekintése) az **Event selections** legördülő listából.

4. Kattintson az **Run selection** gombra.

5. Válassza ki az alkalmazáskategóriákhoz hozzáadni kívánt eseményekhez köthető végrehajtható fájlokat.

6. Nyissa meg jobb kattintással a helyi menüt a kiválasztott eseményekért, majd válassza ki a **Add to category** lehetőséget.

7. A megnyíló ablakban konfigurálja az alkalmazáskategória beállításait:

   - Az ablak felső részén válassza az alábbi lehetőségek egyikét:

     - **Add to a new application category**. Válassza ezt a lehetőséget, ha új alkalmazáskategóriát akar létrehozni, és végrehajtható fájlokat akar hozzáadni.

     - **Add to an existing application category**. Válassza ezt a lehetőséget, ha egy meglévő alkalmazáskategóriát akar kiválasztani, és végrehajtható fájlokat akar hozzáadni.

   - A **Rule type** blokkban válassza ki a következő opciók egyikét:

     - **Rules for adding to inclusions**. Válassza ezt a lehetőséget, ha egy olyan feltételt akar létrehozni, amely végrehajtható fájlokat ad hozzá az alkalmazáskategóriához.

     - **Rules for adding to exclusions**. Válassza ezt a lehetőséget, ha egy olyan feltételt akar létrehozni, amely végrehajtható fájlokat zár ki az alkalmazáskategóriákból.

   - A **Parameter used as a condition** blokkban válassza ki a következő opciók egyikét:

     - **Certificate details (or SHA-256 hashes for files without a certificate)**.

     - **Certificate details (files without a certificate will be skipped)**.

     - **Only SHA-256 (files without a hash will be skipped)**.

     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

8. Mentse el a módosításokat.

Alkalmazásfelügyeleti szabály hozzáadása

Alkalmazásfelügyeleti szabály hozzáadása a Kaspersky Security Center segítségével:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.
   Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.

4. Kattintson **Hozzáadás** gombra.
   Megnyílik az **Alkalmazásfelügyeleti szabály** ablak.

5. Végezze el az alábbiak egyikét:

   - Ha létre akar hozni egy új kategóriát:

     a. Kattintson a **Kategória létrehozása** gombra.
        Elindul a Felhasználói kategóriakészítő varázsló.

b. Kövesse a Felhasználói kategóriakészítő varázsló utasításait.

c. A **Kategória** legördülő listából válassza ki a létrehozott alkalmazáskategóriát.

- Ha egy meglévő alkalmazáskategóriát kíván szerkeszteni:

  a. A **Kategória** legördülő listából válassza ki azt a létrehozott alkalmazáskategóriát, amit szerkeszteni kíván.

  b. Kattintson a **Tulajdonságok** gombra.

  c. Módosítsa a kiválasztott alkalmazáskategória beállításait.

  d. Mentse el a módosításokat.

  e. Válassza ki a **Kategória** legördülő listán azt a létrehozott alkalmazáskategóriát, amelynek alapján szabályt szeretne létrehozni.

6. Kattintson az **Felhasználók és jogaik** táblázatban a **Hozzáadás** gombra.

   A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

7. Az **Felhasználók és jogaik** táblázatban tegye a következőt:

   - Ha engedélyezni szeretné, hogy a kiválasztott kategóriába tartozó alkalmazásokat a felhasználók és / vagy felhasználói csoportok elindíthassák, jelölje be az érintett sorokban lévő **Engedélyezés** jelölőnégyzetet.

   - Ha blokkolni szeretné, hogy a kiválasztott kategóriába tartozó alkalmazásokat a felhasználók és / vagy felhasználói csoportok elindíthassák, jelölje be az érintett sorokban lévő **Blokkolás** jelölőnégyzetet.

8. Jelölje be a **Más felhasználók számára megtagadás** jelölőnégyzetet, ha azt szeretné, hogy a kiválasztott kategóriába tartozó alkalmazások indítása minden olyan felhasználó számára blokkolva legyen, aki nem szerepel a **Felhasználó vagy csoport** oszlopban, és nem is tartozik a **Felhasználó vagy csoport** oszlopban megadott felhasználói csoportok valamelyikébe.

9. Ha azt szeretné, hogy a Kaspersky Endpoint Security a kiválasztott alkalmazáskategóriákban lévő alkalmazásokat olyan megbízható frissítőknek tekintse, melyek más utólag futtatható végrehajtható fájlokat hoznak létre, jelölje be a **Megbízható frissítéstelepítők** jelölőnégyzetet.

   A Kaspersky Endpoint Security beállításainak áttelepítésekor a megbízható frissítéstelepítők által létrehozott végrehajtható fájlok listája is át lesz telepítve.

10. Mentse el a módosításokat.

Alkalmazásfelügyeleti szabály megadása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.

3. Kattintson a **Blokkolt alkalmazások** vagy az **Engedélyezett alkalmazások** gombra.

   Az Alkalmazásfelügyeleti szabályok listáját nyitja meg.

4. Kattintson **Hozzáadás** gombra.

   Ezután megnyílik az Alkalmazásfelügyeleti szabály beállításainak ablaka.

5. Az **Általános beállítások** lapon határozza meg a szabály főbeállításait:

   a. A **Szabály neve** mezőben adja meg a szabály nevét.

   b. A **Leírás** mezőben adja meg a szabály leírását.

   c. Kattintson az **Felhasználók és jogaik** táblázatban a **Hozzáadás** gombra.

   A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.

   A szabály minden felhasználóra vonatkozik alapértelmezés szerint.

   > Ha a táblázatban nincs megadva felhasználó, a szabályt nem lehet menteni.

   d. Az **Felhasználók és jogaik** táblázatban a kapcsolóval határozza meg a felhasználók jogait az alkalmazások elindításához.

   e. Jelölje be a **Más felhasználók számára megtagadás** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás megakadályozza a szabálykiváltó feltételeknek megfelelő alkalmazások futtatását az olyan felhasználóknál, akik nem szerepelnek az **Felhasználók és jogaik** táblázatban, és nem tagjai az **Felhasználók és jogaik** táblázatban szereplő felhasználói csoportoknak.

   > Ha a **Más felhasználók számára megtagadás** jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem szabályozza az olyan felhasználók által kezdeményezett alkalmazásindításokat, akik nincsenek megadva az **Felhasználók és jogaik** táblázatban, és nem is tartoznak az **Felhasználók és jogaik** táblázatban megadott felhasználói csoportok valamelyikébe.

   f. Jelölje be a **Megbízható frissítéstelepítők** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security megbízható frissítéstelepítőnek tekintse a szabálykiváltó feltételeknek megfelelő alkalmazásokat. A *megbízható frissítéstelepítők* olyan alkalmazások, amelyek olyan más futtatható fájlokat hozhatnak létre, amelyek a későbbiekben futhatnak.

   Amennyiben egy alkalmazás több szabályt is aktivál, a Kaspersky Endpoint Security beállítja a *Megbízható frissítéstelepítők* jelölőt, ha a következő feltételek teljesülnek:

   - Minden szabály lehetővé teszi az alkalmazás futtatását.
   - Legalább egy szabálynál be van jelölve a **Megbízható frissítéstelepítők** jelölőnégyzet.

6. A **Feltételek: N** lapon hozza létre vagy módosítsa a befogadási feltételeket a szabály kioldásához.

7. A **Kizárások: N** lapon hozza létre vagy módosítsa a kizárási feltételeket a szabály kioldásához.

   A Kaspersky Endpoint Security beállításainak áttelepítésekor a megbízható frissítéstelepítők által létrehozott végrehajtható fájlok listája is át lesz telepítve.

8. Mentse el a módosításokat.

Az Alkalmazásfelügyeleti szabályok állapotának módosítása a Kaspersky Security Center segítségével

Alkalmazásfelügyeleti szabály állapotának módosítása a Felügyeleti konzolon:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.

   Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.
4. Kattintson a bal egérgombbal a **Státusz** oszlopban a helyi menü megjelenítéséhez, majd válassza ki az alábbiak egyikét:
   - **Be**. Ez az állapot azt jelenti, hogy a szabály akkor van használatban, ha az Alkalmazásfelügyelő összetevő fut.
   - **Ki**. Ez az állapot azt jelenti, hogy a szabály akkor van mellőzve, ha az Alkalmazásfelügyelő összetevő fut.
   - **Teszt** Ez az állapot azt jelenti, hogy a Kaspersky Endpoint Security mindig engedélyezi az olyan alkalmazások elindítását, melyekre vonatkozik a szabály, de az indítások információit jelentésben rögzíti.
5. Mentse el a módosításokat.

Alkalmazásfelügyeleti szabály állapotának módosítása az alkalmazás felületén:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.
3. Kattintson a **Blokkolt alkalmazások** vagy az **Engedélyezett alkalmazások** gombra.

   Az Alkalmazásfelügyeleti szabályok listáját nyitja meg.
4. A **Státusz** oszlopban nyissa meg a helyi menüt, és válassza ki az alábbiak egyikét:
   - **Engedélyezve**. Ez az állapot azt jelenti, hogy a szabály akkor van használatban, ha az Alkalmazásfelügyelő összetevő fut.
   - **Letiltva**. Ez az állapot azt jelenti, hogy a szabály akkor van mellőzve, ha az Alkalmazásfelügyelő összetevő fut.
   - **Teszt üzemmód**. Ez az állapot azt jelenti, hogy a Kaspersky Endpoint Security mindig engedélyezi az olyan alkalmazások elindítását, melyekre vonatkozik ez a szabály, de az indítások információit jelentésben rögzíti.
5. Mentse el a módosításokat.

Alkalmazásfelügyeleti szabályok exportálása és importálása

Az Alkalmazásfelügyeleti szabályok listáját exportálhatja egy XML-fájlba. Használhatja az exportálás/importálás funkciót az Alkalmazásfelügyeleti szabályok biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

Alkalmazásfelügyeleti szabályok exportálása és importálása esetén gondoljon az alábbi különleges szempontokra:

- A Kaspersky Endpoint Security a szabályok listáját csak aktív alkalmazásfelügyeleti módban exportálja. Más szavakkal, ha az Alkalmazásfelügyelő tiltólista módban működik, a Kaspersky Endpoint Security csak az ebben a módban érvényes szabályokat exportálja. Az engedélyezési lista módban érvényes szabályok listájának exportálásához át kell kapcsolni az üzemmódot, és újra le kell futtatni az exportálást.

- A Kaspersky Endpoint Security az alkalmazásfelügyeleti szabályok működéséhez alkalmazás-kategóriákat használ. Amikor az alkalmazásfelügyeleti szabályokat másik szerverre költözteti, az alkalmazás-kategóriákat is át kell költöztetnie. Az alkalmazás-kategóriák exportálásával és importálásával kapcsolatban további tájékoztatásért lásd a Kaspersky Security Center súgóját.

Az Alkalmazásfelügyeleti szabályok listájának exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.
4. Az Alkalmazásfelügyeleti szabályok listájának exportálása:
   a. Jelölje ki az exportálni kívánt szabályokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
      Ha nem jelölt ki szabályt, a Kaspersky Endpoint Security az összes szabályt exportálja.
   b. Kattintson az **Exportálás** hivatkozásra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a szabályok listáját, és válassza a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security exportálja a szabályok listáját az XML-fájlba.
5. Az Alkalmazásfelügyeleti szabályok listájának importálása:
   a. Kattintson az **Import** hivatkozásra.
      A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.
   b. Nyissa meg a fájlt.
      Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
6. Mentse el a módosításokat.

Az Alkalmazásfelügyeleti szabályok listájának exportálása és importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **App Control** elemet.

5. A(z) **Operating mode** területen válassza ki a szabályok listáját: alkalmazás tiltólista vagy engedélyezési lista.

6. A szabályok listájának exportálása:

   a. Jelölje ki az exportálni kívánt szabályokat.

   b. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a szabályok listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

7. A szabályok listájának importálása:

   a. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a szabályok listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.

8. Mentse el a módosításokat.

Az Alkalmazásfelügyelő összetevő működéséből eredő események megtekintése

A Kaspersky Security Center által fogadott, Alkalmazásfelügyelő összetevő működéséből eredő események megtekintéséhez:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Events** lapot.

3. Kattintson az **Create a selection** gombra.

4. A megnyíló ablakban válassza az **Events** szakaszt.

5. Kattintson az **Clear all** gombra.

6. Az **Events** táblázatban jelölje be az **Alkalmazásindítás letiltva** jelölőnégyzetet.

7. Mentse el a módosításokat.

8. Az **Event selections** legördülő listán válassza ki a létrehozott választást.

9. Kattintson az **Run selection** gombra.

A blokkolt alkalmazásokra vonatkozó jelentés megtekintése

A blokkolt alkalmazások jelentéseinek megtekintéséhez:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Reports** lapot.
3. Kattintson az **New report template** gombra.

   Ekkor elindul az új Jelentéssablon varázsló.
4. Kövesse a Jelentéssablon-varázsló utasításait. A **Selecting the report template type** lépésben válassza az **Other** → **Report on prohibited applications** lehetőséget.

   Miután végzett az Új jelentéssablon varázslóval, az új jelentéssablon megjelenik a **Reports** lapon lévő táblázatban.
5. Nyissa meg a jelentést dupla kattintással.

Megkezdődik a jelentés előállítási folyamata. A jelentés egy új ablakban jelenik meg.

Az Alkalmazásfelügyeleti szabályok tesztelése

Annak biztosítása érdekében, hogy az Alkalmazásfelügyeleti szabályok ne blokkoljanak a munkához szükséges alkalmazásokat, javasoljuk, hogy engedélyezze az Alkalmazásfelügyeleti szabályok tesztelését, és elemezze a működésüket az új szabályok létrehozása után. Ha az Alkalmazásfelügyeleti szabályok tesztelése be van kapcsolva, a Kaspersky Endpoint Security nem blokkolja azokat az alkalmazásokat, amelyeknek indítását tiltja az Alkalmazásfelügyelő, hanem értesítéseket küld indításukról az Adminisztrációs kiszolgáló részére.

Az Alkalmazásfelügyeleti szabályok működésének elemzéséhez át kell tekinteni a belőlük eredő, a Kaspersky Security Center részére jelentett Alkalmazásfelügyelő eseményeket. Ha a tesztmód nem blokkolja a számítógép alkalmazásainak elindítását, akkor a szabályok megfelelően lettek létrehozva. Egyéb esetben ajánlott frissíteni a létrehozott szabályok beállításait, további szabályokat létrehozni vagy törölni a meglévőket.

Alapértelmezés szerint a Kaspersky Endpoint Security lehetővé teszi az összes olyan alkalmazás indítását rendszerindításkor, amelyet nem tiltanak a szabályok.

Az Alkalmazásfelügyelő szabály tesztelés engedélyezése és letiltása

Az Alkalmazásfelügyelő-szabályok tesztelésének be- és kikapcsolása a Kaspersky Security Centerben:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.

   Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.

4. Válassza ki az **Felügyeleti mód** legördülő listán valamelyiket az alábbi elemek közül:

   - **Tiltólista**. Ha ez az opció van kiválasztva, az Alkalmazásfelügyelő az összes felhasználó számára engedélyezi bármely alkalmazás elindítását, kivéve, ha teljesülnek az Alkalmazásfelügyelő blokkolási szabályainak feltételei.

   - **Engedélyezési lista**. Ha ez az opció van kiválasztva, az Alkalmazásfelügyelő az összes felhasználó számára blokkolja bármely alkalmazás elindítását, kivéve, ha teljesülnek az Alkalmazásfelügyelő engedélyezési szabályainak feltételei.

5. Végezze el az alábbiak egyikét:

   - Ha szeretné engedélyezni az Alkalmazásfelügyeleti szabályainak tesztelését, válassza a **Tesztszabályok** lehetőséget a **Művelet** legördülő listában.

   - Ha engedélyezni szeretné, hogy az Alkalmazásfelügyelő kezelje az alkalmazások indítását a felhasználói számítógépeken, a legördülő listában válassza a **Szabályok alkalmazása** lehetőséget.

6. Mentse el a módosításokat.

Az Alkalmazásfelügyeleti szabályok tesztelésének engedélyezéséhez, vagy az Alkalmazásfelügyelő blokkoló tevékenységének kiválasztásához:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.

3. Kattintson a **Blokkolt alkalmazások** vagy az **Engedélyezett alkalmazások** gombra.

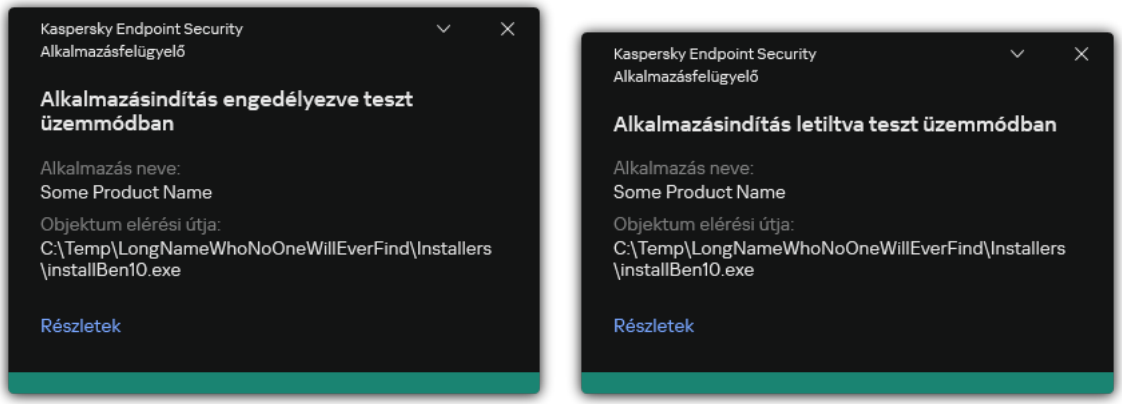
   Az Alkalmazásfelügyeleti szabályok listáját nyitja meg.

4. A **Státusz** részben válassza a **Teszt üzemmód** lehetőséget.

   Ez az állapot azt jelenti, hogy a Kaspersky Endpoint Security mindig engedélyezi az olyan alkalmazások elindítását, melyekre vonatkozik ez a szabály, de az indítások információit jelentésben rögzíti.

5. Mentse el a módosításokat.

A Kaspersky Endpoint Security nem blokkolja azokat az alkalmazásokat, amelyeknek indítását Alkalmazásfelügyelő összetevő tiltja, hanem értesítéseket küld indításukról az Adminisztrációs kiszolgáló részére. A szabályok felhasználói számítógépen történő teszteléséről szóló értesítések megjelenítését is beállíthatja (lásd az alábbi ábrát).



Alkalmazásfelügyelői értesítések teszt üzemmódban

A teszt módban blokkolt alkalmazások jelentéseinek megtekintése

A teszt módban letiltott alkalmazások jelentéseinek megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Reports** lapot.
3. Kattintson az **New report template** gombra.

   Ekkor elindul az új Jelentéssablon varázsló.
4. Kövesse a Jelentéssablon-varázsló utasításait. A **Selecting the report template type** lépésben válassza az **Other → Report on prohibited applications in test mode** lehetőséget.

   Miután végzett az Új jelentéssablon varázslóval, az új jelentéssablon megjelenik a **Reports** lapon lévő táblázatban.
5. Nyissa meg a jelentést dupla kattintással.

Megkezdődik a jelentés előállítási folyamata. A jelentés egy új ablakban jelenik meg.

Az Alkalmazásfelügyelő összetevő tesztműködéséből eredő események megtekintése

A Kaspersky Security Center által fogadott Alkalmazásfelügyelő tesztesemények megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Events** lapot.
3. Kattintson az **Create a selection** gombra.
4. A megnyíló ablakban válassza az **Events** szakaszt.
5. Kattintson az **Clear all** gombra.
6. Az **Events** táblázatban jelölje be az **Alkalmazásindítás letiltva teszt üzemmódban** és az **Alkalmazásindítás engedélyezve teszt üzemmódban** jelölőnégyzetet.
7. Mentse el a módosításokat.
8. Az **Event selections** legördülő listán válassza ki a létrehozott választást.
9. Kattintson az **Run selection** gombra.

Alkalmazástevékenység-figyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

Az *Alkalmazástevékenység-figyelő* egy olyan eszköz, amellyel valós időben tekinthetők meg a felhasználó számítógépén futó alkalmazások tevékenységével kapcsolatos információk.

Az Alkalmazástevékenység-figyelő használatához telepíteni kell az Alkalmazásfelügyelő és a Behatolásmegelőző rendszer összetevőket. Ha ezek az összetevők nincsenek telepítve, az Alkalmazástevékenység-figyelő szakasz az alkalmazás főablakában rejtve van.

Az Alkalmazástevékenység-figyelő indítása:

Az alkalmazás főablakának **Figyelés** részén kattintson az **Alkalmazástevékenység-figyelő** csempére.

Ebben az ablakban három fülön jelennek meg a felhasználó számítógépén futó alkalmazások tevékenységével kapcsolatos információk:

- A **Minden alkalmazás** fül a számítógépre telepített összes alkalmazásról nyújt információt.
- A **Fut** fül azt mutatja meg, hogy a számítógép mennyi erőforrását használják az egyes alkalmazások valós időben. Erről a fülről továbbléphet az egyes alkalmazások engedélyeinek konfigurálására.
- A **Futtatás indításkor** fül azoknak az alkalmazásoknak a listáját jeleníti meg, amelyek az operációs rendszer indulásakor szintén beindulnak.

Ha el szeretné rejteni az alkalmazástevékenység adatait a felhasználó számítógépén, korlátozhatja a felhasználók hozzáférését az Alkalmazástevékenység-figyelő eszközhöz.

Az Alkalmazástevékenység-figyelő elrejtése az alkalmazás felületén az Adminisztrációs Konzol (MMC) használatával

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.
4. Használja **Hide Application Activity Monitor section** jelölőnégyzetet az eszközhöz való hozzáférés engedélyezéséhez vagy visszavonásához.
5. Mentse el a módosításokat.

Az Alkalmazástevékenység-figyelő elrejtése az alkalmazás felületén a Web Console és a Cloud Console segítségével

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **User Interaction** elemet.
5. A(z) **Hide Application Activity Monitor section** jelölőnégyzettel engedélyezheti vagy tilthatja le az eszközhöz való hozzáférést.
6. Mentse el a módosításokat.

Fájlok vagy mappák névmaszkjainak létrehozási szabályai

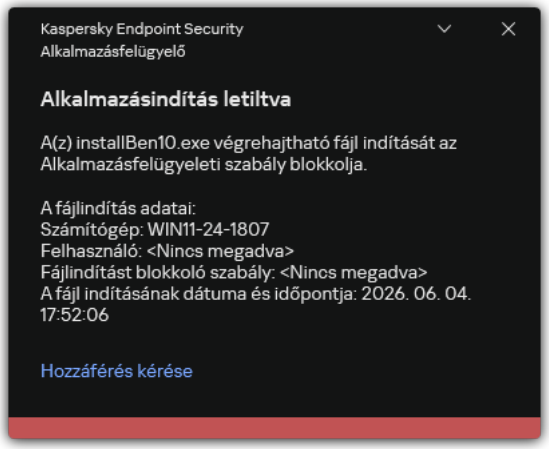
A *fájl vagy mappa névmaszkja* a fájl vagy mappa nevének ábrázolása, valamint a fájl gyakori karakterekkel történő kiterjesztése.

A következő szokványos karaktereket használhatja fájl vagy mappa névmaszkjának létrehozásához:

- A `*` (csillag) karakter, amely bármely karakterkészletet (beleértve az üres készletet is) helyettesíthet. Például a `C:\*.txt` maszk minden olyan `txt` kiterjesztésű fájlhoz vezető útvonalat magában foglal, amely a (C:) meghajtón lévő mappákban és almappákban található.
- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

Az Alkalmazásfelügyelő üzenetsablonjainak szerkesztése

Ha egy felhasználó megpróbálja az Alkalmazásfelügyeleti szabályok által blokkolt valamelyik alkalmazást elindítani, a Kaspersky Endpoint Security megjelenít egy üzenetet arról, hogy az alkalmazás indítása blokkolva van. A Kaspersky szakértői egy üzenetsablont biztosítanak a felhasználónak, amely ismerteti az alkalmazás blokkolásának okait (lásd az alábbi ábrát). Az üzenetsablonok kezeléséhez speciális változók állnak rendelkezésre (pl. `%USER_NAME%`). A változók lehetővé teszik egyetlen üzenetsablon használatát a különböző számítógépeken. Üzenet generálásakor a Kaspersky Endpoint Security lekéri a változó értékét az operációs rendszer beállításaiból, és beilleszti azt az adott számítógéphez, felhasználóhoz és eseményhez tartozó üzenetbe.



Az Alkalmazásfelügyelő értesítései

Ha a felhasználó úgy véli, hogy az alkalmazás indítása tévedésből van blokkolva, akkor az üzenet szövegében lévő hivatkozás segítségével üzenetet küldhet a helyi vállalati hálózati rendszergazdának. Ehhez a felhasználónak a **Hozzáférés kérése** gombra kell kattintania, és üzenetet kell küldenie a rendszergazdának, amelyben leírja a helyzetet. Készíthet egy sablont is a rendszergazdának küldött üzenetről, és hozzáadhat olyan adatokat, amelyek alapján dönthet az alkalmazáshoz való hozzáférés engedélyezéséről vagy letiltásáról. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Alkalmazásindítás hozzáférésének blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

Az Alkalmazásfelügyelő üzenetsablonjának módosítása az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza a **Biztonsági felügyelet → Alkalmazásfelügyelő** lehetőséget.
4. A megnyíló **Sablonok** részen kattintson az **Üzenetsablon beállításai** gombra.

5. Ekkor megnyílik egy ablak, amelyben konfigurálhatja az Alkalmazásfelügyelő sablonjait:

   - **Üzenet a blokkolásról**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.

     Nem konfigurálhat üzenetsablonokat az Alkalmazásfelügyelő esetében teszt üzemmódban. Az Alkalmazásfelügyelő teszt üzemmódban előre beállított értesítéseket jelenít meg.

   - **Üzenet a rendszergazdának**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Az alapértelmezett sablonszöveget az **Alapértelmezés szerint** gombra kattintva is visszaállíthatja.

6. Mentse el a módosításokat.

Az Alkalmazásfelügyelő üzenetsablonjának módosítása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **App Control** elemet.

5. A(z) **Message templates** blokkban kattintson a(z) **Messages about application startup block** hivatkozásra, és konfigurálja a sablonokat az Alkalmazásfelügyeleti üzenetekhez:

   - **Message to user**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.

     Nem konfigurálhat üzenetsablonokat az Alkalmazásfelügyelő esetében teszt üzemmódban. Az Alkalmazásfelügyelő teszt üzemmódban előre beállított értesítéseket jelenít meg.

   - **Message to administrator**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Add variable** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Az alapértelmezett sablonszöveget a(z) **Reset to default** gombra kattintva is visszaállíthatja.

6. Mentse el a módosításokat.

Az Alkalmazásfelügyelő üzenetsablonjának módosítása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.

3. Az **Alkalmazás blokkolásáról szóló üzenetek sablonjai** részen konfigurálja az Alkalmazásfelügyelő üzenetsablonjait:

   - **Üzenet a blokkolásról**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.

     Nem konfigurálhat üzenetsablonokat az Alkalmazásfelügyelő esetében teszt üzemmódban. Az Alkalmazásfelügyelő teszt üzemmódban előre beállított értesítéseket jelenít meg.

   - **Üzenet a rendszergazdának**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó hozzáadása** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Az alapértelmezett sablonszöveget a **Visszaállítás** gombra kattintva is visszaállíthatja.

4. Mentse el a módosításokat.

Változók az Alkalmazásfelügyeleti üzenetsablonokban

A következő változókat használhatja a felhasználói és a rendszergazdai üzenetsablonokban:

- **A kiváltott szabály neve** – `%RULE%`.

  A fájl futtatását blokkoló szabály neve.

- **Aktuális dátum** – `%DATE%`.

  Az a dátum, amikor a fájl futtatását blokkolták (NN.HH.ÉÉÉÉ formátumban).

- **Aktuális idő** – `%TIME%`.

  Az az időpont, amikor a fájlok futtatását blokkolták (ÓÓ:PP formátumban).

- **Felhasználónév** - `%USER_NAME%`.

  Azon a számítógépen lévő aktuális felhasználói fiók neve, amelyen a fájlok futtatását blokkolták (`<device name>\<user alias>` formátumban, például: `DESKTOP-123\John.Smith`).

- **Számítógép neve** - `%COMPUTER_NAME%`.

  Annak a számítógépnek a neve, amelyen a fájlok futtatását blokkolták.

- **Futtatható fájl neve** – `%FILE_NAME%`.

  A blokkolt alkalmazás futtatható fájljának neve.

- **Futtatható fájl KL kategóriája** – `%KL_CAT%`.

  KL kategória, amelybe a blokkolt alkalmazás tartozik (például *Böngészők* vagy más kategória).

- **Futtatható fájl elérési útja** – `%FILE_PATH%`.

  A blokkolt alkalmazás futtatható fájljának teljes elérési útja.

- **Futtatható fájl verziója** – `%FILE_VERSION%`.

  A blokkolt alkalmazás futtatható fájljának verziója.

- **Futtatható fájl eredeti neve** – `%ORIGINAL_FILE_NAME%`.

  A blokkolt alkalmazás futtatható fájljának eredeti neve. A fájlnév az alkalmazás futtatható fájljának tulajdonságaiban van megadva.

- **Forgalmazó** – `%FILE_PUBLISHER%`.

  A blokkolt alkalmazás forgalmazója.

- **Alkalmazásnév** - `%FILE_PRODUCT_NAME%`.

  A blokkolt alkalmazás neve.

- **Alkalmazás verziója** – `%PRODUCT_VERSION%`.

  A blokkolt alkalmazás verziója.

- **Futtatható fájl kivonata** – `%FILE_HASH%`.

  Az alkalmazás futtatható fájljának ellenőrzőösszege.

- **Tanúsítvány kibocsátója** - `%CERT_ISSUER%`.

  A tanúsítvány kibocsátója, amellyel a futtatható fájl alá van írva.

- **Tanúsítvány tulajdonosa** – `%CERT_SUBJECT%`.

  A tanúsítvány tulajdonosa, amellyel a futtatható fájl aláírva van.

- **Tanúsítvány ujjlenyomata** – `%CERT_THUMBPRINT%`.

  A tanúsítvány ujjlenyomata, amellyel a futtatható fájl aláírva van.

A legjobb gyakorlat az engedélyezett alkalmazások listájának megvalósításához

Az engedélyezett alkalmazások listájának megvalósításának tervezésekor ajánlott elvégezni a következő műveleteket:

1. Alakítsa ki a következő csoporttípusokat:

   - Felhasználói csoportok. A felhasználói csoportok, akiknek engedélyeznie kell a különböző alkalmazáskészletek használatát.

   - Adminisztrációs csoportok. Számítógépek egy vagy több csoportja, melyeken a Kaspersky Security Center alkalmazni fogja az engedélyezett alkalmazások listáját. Több számítógépcsoportot kell létrehoznia, ha ezekhez a csoportokhoz az engedélyezési listák különböző beállításait használja.

2. Lista létrehozása olyan alkalmazásokról, melyeknek elindíthatónak kell lenniük.

   A lista létrehozása előtt ajánlott a következőt tenni:

   a. Leltárfeladatfuttatása.

      A leltárfeladat létrehozásával, rekonfigurációjával és elindulásával kapcsolatos információk elérhetőek a Feladatkezelés részben.

   b. Tekintse meg a végrehajtható fájlok listáját.

Engedélyezési lista mód konfigurálása az alkalmazásokhoz

Az engedélyezési lista mód konfigurálásakor ajánlott elvégezni a következő műveleteket:

1. Olyan alkalmazáskategóriák létrehozása, melyek azokat az alkalmazásokat tartalmazzák, amiknek az indításhoz engedélyezve kell lenniük.

   Kiválaszthatja az alkalmazáskategória-létrehozás következő módszereinek egyikét:

   - **Category with content added manually**. A következő feltételek használatával manuális hozzáadás is lehetséges:

     - Fájl metaadatok. A Kaspersky Security Center minden olyan végrehajtható fájlt hozzáad az alkalmazáskategóriához, amelyhez a megadott metaadatok tartoznak.

     - Fájl hash-kód. A Kaspersky Security Center minden olyan végrehajtható fájlt hozzáad az alkalmazáskategóriához, amelyhez a megadott hash-kód tartozik.

       Ennek a feltételnek a használata kizárja a frissítések automatikus telepítésének lehetőségét, mivel a fájlok különböző verzióinak különböző has-kódjaik lesznek.

     - Fájl tanúsítvány. A Kaspersky Security Center minden olyan végrehajtható fájlt hozzáad az alkalmazáskategóriához, amely a megadott tanúsítvánnyal van aláírva.

     - KL kategória. A Kaspersky Security Center minden olyan végrehajtható fájlt hozzáad az alkalmazáskategóriához, amely a megadott KL kategóriába tartozik.

     - Alkalmazásmappa. A Kaspersky Security Center minden olyan végrehajtható fájlt hozzáad az alkalmazáskategóriához, amely ebben a mappában található.

       Ennek az **Application folder** feltételnek a használata kockázatos lehet, mivel a megadott mappában lévő összes alkalmazás elindítható lesz. Ajánlott alkalmazni a szabályokat – amik az **Application folder** feltétellel bíró alkalmazáskategóriákat használják – azon felhasználók számára, akiknek a frissítések automatikus telepítése engedélyezve kell legyen.

   - **Kategória a megadott mappák végrehajtható fájljaival**. Megadhatja a mappát, melyből a végrehajtható fájlok automatikusan hozzá lesznek rendelve a létrehozott alkalmazáskategóriához.

   - **Category that includes executable files from selected devices**. Megadhat egy számítógépet, melyből az összes végrehajtható fájl automatikusan hozzá lesz rendelve a létrehozott alkalmazáskategóriához.

     Ha az alkalmazáskategóriák létrehozásának ezt a módszerét követi, a Kaspersky Security Center a számítógépen található alkalmazásokra vonatkozó információkat a **Executable files** mappából olvassa be.

2. Az engedélyezési lista mód kiválasztása az Alkalmazásfelügyelő összetevő számára.

3. Alkalmazásfelügyeleti szabályok létrehozása a létrehozott alkalmazáskategóriák használatával.

   Az **Golden Image** szabály és a **Megbízható frissítéstelepítők** szabály kezdetben az Engedélyezési lista módhoz van meghatározva. Ezek az Alkalmazásfelügyeleti szabályok KL kategóriáknak felelnek meg. A *Golden Image* KL kategória azokat a programokat foglalja magába, melyek biztosítják az operációs rendszer normális működését. A *Megbízható frissítéstelepítők* KL kategória a legjobb hírnevű szoftverforgalmazók frissítéseit tartalmazza. Ezeket a szabályokat nem lehet törölni. E szabályok beállításai nem szerkeszthetők. Alapértelmezés szerint az **Golden Image** szabály be, a **Megbízható frissítéstelepítők** szabály pedig ki van kapcsolva. Minden felhasználó elindíthatja a szabályok kiváltó feltételeinek megfelelő alkalmazásokat.

4. Határozza meg az alkalmazásokat, amelyek számára a frissítések automatikus telepítése engedélyezve kell legyen.

   A következő módokon engedélyezheti a frissítések automatikus telepítését:

   - Adjon meg egy kibővített listát az engedélyezett alkalmazásokról a KL kategóriák alá tartozó alkalmazások indításának engedélyezésével.
   - Adjon meg egy kibővített listát az engedélyezett alkalmazásokról a tanúsítvánnyal rendelkező alkalmazások indításának engedélyezésével.

     A tanúsítvánnyal aláírt alkalmazások elindításának engedélyezéséhez létrehozhat egy tanúsítványalapú feltétellel rendelkező kategóriát, mely csak a **Subject** paramétert használja a `*` értékkel.
   - Az Alkalmazásfelügyeleti szabályhoz válassza ki a **Megbízható frissítéstelepítők** paramétert. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a szabályban megadott alkalmazásokat Megbízható frissítőnek tekint. A Kaspersky Endpoint Security engedélyezi az olyan alkalmazások elindítását, amelyek a kategóriaszabályokban megadott alkalmazások által lettek telepítve vagy frissítve, amennyiben nem érvényes rájuk blokkoló szabály.

     A Kaspersky Endpoint Security beállításainak áttelepítésekor a megbízható frissítéstelepítők által létrehozott végrehajtható fájlok listája is át lesz telepítve.
   - Hozzon létre egy mappát, és helyezze el az alkalmazások végrehajtható fájljaiban, amelyek automatikus frissítésének telepítését engedélyezni akarja. Ezután hozzon létre egy alkalmazáskategóriát az **Application folder** feltétellel, és adja meg az adott mappa elérési útját. Ezután hozzon létre egy engedélyezőszabályt, és válassza ki ezt a kategóriát.

     Ennek az **Application folder** feltételnek a használata kockázatos lehet, mivel a megadott mappában lévő összes alkalmazás elindítható lesz. Ajánlott alkalmazni a szabályokat – amik az **Application folder** feltétellel bíró alkalmazáskategóriákat használják – azon felhasználók számára, akiknek a frissítések automatikus telepítése engedélyezve kell legyen.

Engedélyezési lista mód tesztelése

Annak biztosítása érdekében, hogy az Alkalmazásfelügyeleti szabályok ne blokkoljanak a munkához szükséges alkalmazásokat, javasoljuk, hogy engedélyezze az Alkalmazásfelügyeleti szabályok tesztelését, és elemezze a működésüket az új szabályok létrehozása után. Ha a tesztelés engedélyezve van, a Kaspersky Endpoint Security nem blokkolja azokat az alkalmazásokat, amelyeknek indítását Alkalmazásfelügyeleti szabályok tiltják, hanem értesítéseket küld indításukról az Adminisztrációs kiszolgáló részére.

Az engedélyezési lista mód tesztelésekor ajánlott elvégezni a következő műveleteket:

1. A tesztelés időtartamának meghatározása (pár naptól két hónapig).
2. Kapcsolja be az Alkalmazásfelügyeleti szabályok tesztelését.
3. Vizsgálja meg az Alkalmazásfelügyelő összetevő működésének tesztéléséből eredő eseményeket és a teszt módban letiltott alkalmazásokról szóló jelentések a tesztelés eredményeinek elemzéséhez.
4. Az elemzés eredményeitől függően módosítson az engedélyezési lista mód beállításain.

   Tételesen: a teszteredmények alapján lehetősége van felvenni eseményekhez kapcsolódó, végrehajtható fájlokat egy alkalmazáskategóriába.

Engedélyezési lista mód támogatása

A blokkolási művelet kiválasztása az Alkalmazásfelügyelőhöz után ajánlott folytatni az engedélyezési lista mód támogatását a következő műveletek elvégzésével:

- Vizsgálja meg az Alkalmazásfelügyelő összetevő működéséből eredő eseményeket és a blokkolt futtatások jelentéseit az Alkalmazásfelügyelő hatékonyságának elemzéséhez.
- Elemezze a felhasználók kérelmeit az alkalmazások eléréséhez.
- Elemezze az ismeretlen futtatható fájlokat a megbízhatóságuk Kaspersky Security Network ben való ellenőrzésével.
- Az operációsrendszer vagy a szoftver frissítéseinek telepítése előtt telepítse a számítógépek tesztcsoportjainak frissítéseit, hogy ellenőrizze, miképp dolgozzák fel ezeket az Alkalmazásfelügyeleti szabályok.
- Adja hozzá a szükséges alkalmazásokat az Alkalmazásfelügyeleti szabályokban használt kategóriákhoz.

Hálózati portok megfigyelése

A Kaspersky Endpoint Security működése során a Webfelügyelő, a Levelezés védelem, a Web védelem, a Viselkedésészlelés és a Biztonsági rések kihasználásának megelőzése összetevő figyeli a számítógépen a bizonyos protokollokkal továbbított és a megadott nyitott TCP és UDP portokon átmenő adatforgalmat. A Levelezés védelem összetevő például az SMTP-n keresztül továbbított adatokat elemzi, a Web védelem összetevő pedig a HTTP-n és FTP-n keresztül továbbított adatokat elemzi.

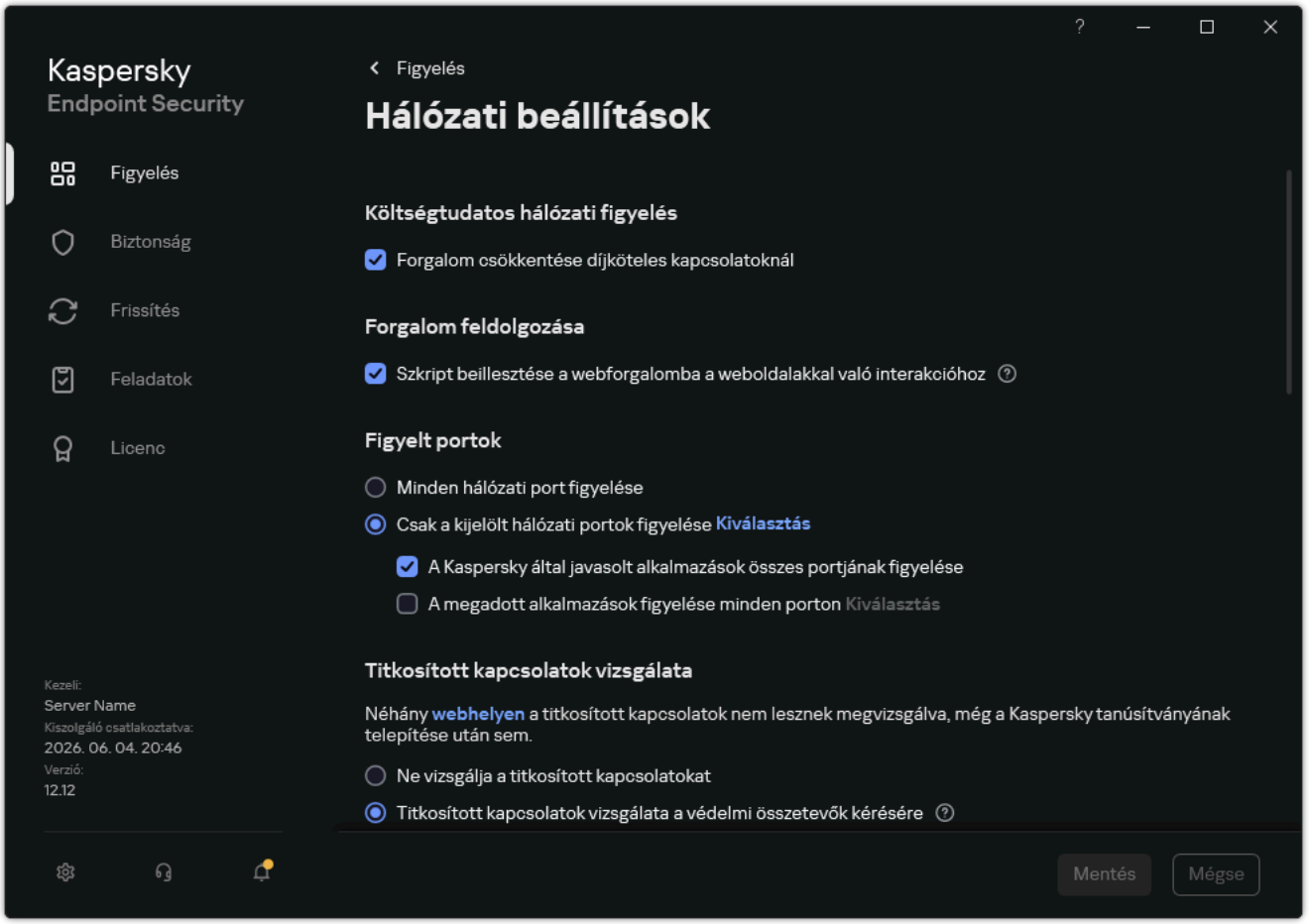
A Kaspersky Endpoint Security a felhasználó számítógépének TCP és UDP portjait több csoportra osztja aszerint, hogy mekkora a valószínűsége a feltörésüknek. Egyes hálózati portok a sebezhető szolgáltatásokhoz vannak fenntartva. Javasolt alaposabban megfigyelni ezeket a portokat, mivel nagyobb eséllyel célozhatják meg őket hálózati támadások. Ha nem szabványos hálózati portokra támaszkodó nem szabványos szolgáltatásokat használ, akkor ezeket a portokat is megcélozhatják a támadó számítógépek. Megadhatja a hálózati portok listáját és a hálózati hozzáférést kérő alkalmazások listáját. Ezekre a portokra és alkalmazásokra a Levelezés védelem és a Web védelem összetevők a hálózati forgalom megfigyelése közben különösen odafigyelnek.

A számítógép biztonsága érdekében a Viselkedésészlelés és a Biztonsági rések kihasználásának megelőzése összetevők a hálózati portokon áthaladó adatfolyamokat is figyelik. Az összetevők folyamatosan figyelik a hálózati forgalmat, hogy felismerjék az egyes fenyegető folyamatokat.

Minden hálózati port figyelésének bekapcsolása

Minden hálózati port figyelésének bekapcsolása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.



Hálózati portok figyelésének beállításai

3. A **Figyelt portok** részben válassza ki a **Minden hálózati port figyelése** elemet.
4. Mentse el a módosításokat.

A figyelt hálózati portok listájának létrehozása

A felügyelt hálózati portok listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

A figyelt hálózati portok listájának létrehozása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Monitored ports** részben válassza ki a **Monitor selected network ports only** elemet.
4. Kattintson **Kijelölés** gombra.

   Ez megnyitja az e-mailekhez és a hálózati forgalomhoz általában használt hálózati portok listáját. A hálózati portok listája megtalálható a Kaspersky Endpoint Security csomagjában.
5. A **Státusz** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le a hálózati portok figyelését.
6. Ha a lista nem tartalmaz egy hálózati portot, az alábbi módon veheti fel rá:
   a. Kattintson **Hozzáadás** gombra.
   b. A megnyíló ablakban adja meg a hálózati port számát és a rövid leírását.
   c. Állítsa be az **Aktív** vagy **Inaktív** állapotot a hálózati port figyeléséhez.
7. Mentse el a módosításokat.

Ha az FTP protokoll passzív módban fut, a kapcsolat a figyelemmel kísért hálózati portok listáján nem szereplő véletlenszerű hálózati porton jöhet létre. Az ilyen kapcsolatok védelme érdekében engedélyezze az összes hálózati port felügyeletét, vagy konfigurálja a hálózati portok vezérlését az FTP-kapcsolatokat létrehozó alkalmazások számára.

Azon alkalmazások listájának létrehozása, amelyeknél minden hálózati portot figyelni szeretne

Létrehozhatja azon alkalmazások táblázatát, amelyeknél a Kaspersky Endpoint Security az összes hálózati portot figyeli.

Javasoljuk, hogy az FTP protokollon keresztül adatokat fogadó, illetve küldő alkalmazásokat vegye fel azon alkalmazások listájára, amelyeknél a Kaspersky Endpoint Security az összes hálózati portot figyelemmel kíséri.

Azon alkalmazások listájának létrehozása, amelyeknél minden hálózati portot figyelni szeretne:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Monitored ports** részben válassza ki a **Monitor selected network ports only** elemet.
4. Jelölje be **A Kaspersky által javasolt alkalmazások összes portjának figyelése** négyzetet.

   Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security az összes hálózati portot felügyeli a következő alkalmazásoknál:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.
   - Microsoft Edge.
   - Mozilla Firefox.
   - Internet Explorer.
   - Java.
   - mIRC.
   - Opera.
   - Pidgin.
   - Safari.
   - Mail.ru Agent.
   - Yandex Browser.
5. Jelölje be **A megadott alkalmazások figyelése minden porton** jelölőnégyzetet.

6. Kattintson **Kijelölés** gombra.

   Ez megnyitja az alkalmazások listáját, amelyeknél a Kaspersky Endpoint Security a hálózati portot figyeli.

7. A **Státusz** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le a hálózati portok figyelését.

8. Ha az alkalmazáslista nem tartalmaz egy alkalmazást, az alábbi módon veheti fel rá:

   a. Kattintson **Hozzáadás** gombra.

   b. A megnyíló ablakban írja be az alkalmazás futtatható fájljának elérési útját és egy rövid leírást.

   c. Állítsa be az **Aktív** vagy **Inaktív** állapotot a hálózati portok figyeléshez.

9. Mentse el a módosításokat.

Figyelt portok listájának exportálása és importálása

A Kaspersky Endpoint Security a következő listákat használja a hálózati portok figyeléséhez: hálózati portok listája és azon alkalmazások listája, amelyek portjait a Kaspersky Endpoint Security figyeli. Exportálhatja a megfigyelt portok listáját egy XML-fájlba. Ezután módosíthatja a fájlt, például nagy számú azonos leírású port hozzáadásával. Az exportálás/importálás funkciót használhatja biztonsági mentés létrehozására a figyelt portok listáiról, vagy a listák egy másik kiszolgálóra való áttelepítéséhez is.

A figyelt portok listáinak exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Network Settings** elemet.

5. Hálózati portok listájának exportálása:

   a. A **Monitored ports** területen válassza az **Monitor selected network ports only** opciót.

   b. Kattintson a **selected N ports** hivatkozásra.

      Megnyílik a **Network ports** ablak. A **Network ports** ablakban megjelenik az e-mailekhez és a hálózati forgalomhoz általában használt hálózati portok listája. A hálózati portok listája megtalálható a Kaspersky Endpoint Security csomagjában.

   c. A hálózati portok listájában válassza ki az exportálni kívánt portokat.

   d. Kattintson az **Export** gombra.

   e. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a hálózati portok listáját, és válassza a fájl mentésére kiszemelt mappát.

   f. Mentse a fájlt.

      A Kaspersky Endpoint Security a hálózati portok teljes listáját exportálja az XML-fájlba.

6. Azon alkalmazások listájának exportálása, amelyek portjait a Kaspersky Endpoint Security figyeli:

   a. A **Monitored ports** részen jelölje be az **Monitor all ports for specified applications** jelölőnégyzetet.

   b. Kattintson a **selected N applications** hivatkozásra.

   c. Az alkalmazások listájában válassza ki az exportálni kívánt alkalmazásokat.

   d. Kattintson az **Export** gombra.

   e. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné az alkalmazások listáját, és válassza ki a fájl mentésére kiszemelt mappát.

   f. Mentse a fájlt.

   A Kaspersky Endpoint Security az alkalmazások teljes listáját exportálja az XML-fájlba.

7. Hálózati portok listájának importálása:

   a. A hálózati portok listájában kattintson az **Import** gombra.

   A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a hálózati portok listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a hálózati portokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

8. Azon alkalmazások listájának importálása, amelyek portjait a Kaspersky Endpoint Security figyeli:

   a. Az alkalmazások listájában kattintson az **Import** gombra.

   A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné az alkalmazások listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista az alkalmazásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

9. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza az **Általános beállítások → Hálózati beállítások** lehetőséget.

4. A **Monitored ports** részben válassza ki a **Monitor selected network ports only** elemet.

5. Kattintson a **Beállítások** gombra.

   Megnyílik a **Network ports** ablak. A **Network ports** ablakban megjelenik az e-mailekhez és a hálózati forgalomhoz általában használt hálózati portok listája. A hálózati portok listája megtalálható a Kaspersky Endpoint Security csomagjában.

6. Hálózati portok listájának exportálása:

   a. A hálózati portok listájában válassza ki az exportálni kívánt portokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.

      Ha nem jelölt ki portot, a Kaspersky Endpoint Security az összes portot exportálja.

   b. Kattintson az **Export** gombra.

   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a hálózati portok listáját, és válassza a fájl mentésére kiszemelt mappát.

   d. Mentse a fájlt.

      A Kaspersky Endpoint Security a hálózati portok teljes listáját exportálja az XML-fájlba.

7. Azon alkalmazások listájának exportálása, amelyek portjait a Kaspersky Endpoint Security figyeli:

   a. Jelölje be **A megadott alkalmazások figyelése minden porton** jelölőnégyzetet.

   b. Az alkalmazások listájában válassza ki az exportálni kívánt alkalmazásokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.

      Ha nem jelölt ki alkalmazást, a Kaspersky Endpoint Security az összes alkalmazást exportálja.

   c. Kattintson az **Export** gombra.

   d. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné az alkalmazások listáját, és válassza ki a fájl mentésére kiszemelt mappát.

   e. Mentse a fájlt.

      A Kaspersky Endpoint Security az alkalmazások teljes listáját exportálja az XML-fájlba.

8. Hálózati portok listájának importálása:

   a. A hálózati portok listájában kattintson az **Importálás** gombra.

      A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a hálózati portok listáját.

   b. Nyissa meg a fájlt.

      Ha a számítógépen már létezik egy lista a hálózati portokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

9. Azon alkalmazások listájának importálása, amelyek portjait a Kaspersky Endpoint Security figyeli:

   a. Az alkalmazások listájában kattintson az **Importálás** gombra.

      A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné az alkalmazások listáját.

   b. Nyissa meg a fájlt.

      Ha a számítógépen már létezik egy lista az alkalmazásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

10. Mentse el a módosításokat.

Naplóvizsgálat

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt.

A 11.11.0 verziótól kezdődően a Kaspersky Endpoint Security for Windows tartalmazza a Napló vizsgálata összetevőt. A Napló vizsgálata figyelemmel kíséri a védett környezetek integritását a Windows eseménynapló-elemzése alapján. Ha az alkalmazás szokatlan magatartást érzékel a rendszerben, jelzi a rendszergazdának, mert ez a magatartás kibertámadásra tett kísérlet jele is lehet.

A Kaspersky Endpoint Security elemzi a Windows eseménynaplóit, és észleli a szabálysértéseket. Az összetevő előre definiált szabályokat tartalmaz. Az előre definiált szabályok heurisztikus elemzésen alapulnak. Saját szabályokat (egyéni szabályokat) is hozzáadhat. Egy szabály aktiválódásakor az alkalmazás *Critical* állapotú eseményt hoz létre (lásd az alábbi ábrát).

Ha a Naplóvizsgálatot szeretné használni, győződjön meg arról, hogy az auditálási házirend biztonsági beállításai megfelelően vannak konfigurálva, és a rendszer naplózza a vonatkozó eseményeket (részleteket a Microsoft terméktámogatási webhelyén találhat).



Naplóvizsgálati értesítés

Előre definiált szabályok konfigurálása

Az előre definiált szabályok a védett számítógépeken előforduló rendellenes tevékenységek sablonjait tartalmazzák. A rendellenes tevékenységek támadási kísérletet jelezhetnek. Az előre definiált szabályok heurisztikus elemzésen alapulnak. A Naplóvizsgálathoz hét előre definiált szabály érhető el. Bármelyik szabályt engedélyezheti vagy letilthatja. Az előre definiált szabályokat nem lehet törölni.

A következő műveletek eseményeinek megfigyelésére szolgáló szabályok kiváltási feltételeit konfigurálhatja:

- Jelszó találgatásos támadásainak észlelése
- Hálózati bejelentkezés észlelése

Előre definiált szabályok konfigurálása az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakában válassza a **Biztonsági felügyelet → Naplóvizsgálat** lehetőséget.
4. Győződjön meg arról, hogy a **Naplóvizsgálat** jelölőnégyzet be van jelölve.
5. Az **Előre definiált szabályok** részen kattintson a **Beállítások** gombra.
6. Az előre definiált szabályok konfigurálásához jelölje be vagy törölje a jelölőnégyzeteket:
   - **A rendszerben lehetséges találgatásos támadásra utaló mintázatok találhatók**.
   - **A hálózati bejelentkezési munkamenet során szokatlan tevékenység észlelhető**.
   - **Windows eseménynaplóval való lehetséges visszaélésre utaló minták találhatók**.
   - **Újonnan telepített szolgáltatás nevében észlelt szokatlan műveletek**.
   - **Explicit hitelesítő adatokat használó szokatlan bejelentkezés észlelve**.
   - **Lehetséges Kerberos hamisított PAC-s (MS14-068) támadás mintái észlelhetők a rendszerben**.
   - **Gyanús módosítások észlelhetők az emelt szintű beépített Rendszergazdák csoportban**.
7. Szükség esetén konfigurálja a **rendszerben lehetséges találgatásos támadásra utaló mintázatok találhatók** szabályt:
   a. Kattintson a szabály alatti **Beállítások** gombra.
   b. A megnyíló ablakban adja meg a kísérletek számát és az időszakot, amelyen belül el kell végezni a jelszóbeírási kísérleteket a szabály aktiválásához.
   c. Kattintson az **OK** gombra.
8. Ha kiválasztotta **A rendszer szokatlan tevékenységet észlel egy hálózati bejelentkezési munkamenet során** szabályt, konfigurálnia kell a beállításait:
   a. Kattintson a szabály alatti **Beállítások** gombra.
   b. A **Hálózati bejelentkezés észlelése** részen adja meg az időszak kezdetét és végét.

      A Kaspersky Endpoint Security a meghatározott időszakban végzett bejelentkezési kísérleteket rendellenes tevékenységnek tekinti.

      Alapértelmezés szerint az időszak nincs beállítva, és az alkalmazás nem figyeli a bejelentkezési kísérleteket. Ahhoz, hogy az alkalmazás folyamatosan figyelje a bejelentkezési kísérleteket, állítsa be az időszakot 0:00 – 23:59 értékre. Az időszak kezdete és vége nem eshet egybe. Ha megegyeznek, az alkalmazás nem figyeli a bejelentkezési kísérleteket.

c. Hozza létre a megbízható felhasználók és a megbízható IP-címek (IPv4 és IPv6) listáját.

A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata. A Kaspersky Endpoint Security nem figyeli ezen felhasználók és számítógépek bejelentkezési kísérleteit.

d. Kattintson az **OK** gombra.

9. Mentse el a módosításokat.

Előre definiált szabályok konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Log Inspection** elemet.
5. Győződjön meg arról, hogy a **Log Inspection ENABLED** kapcsoló be van kapcsolva.
6. Az **Predefined rules** részen engedélyezze vagy tiltsa le az előre definiált szabályokat a kapcsolókkal:
   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.

   a. **Suspicious changes detected in the privileged built-in Administrators group**.
7. Ha szükséges, konfigurálja a(z) **There are patterns of a possible brute-force attack in the system** szabályt:

   a. Kattintson a szabály alatti **Settings** lehetőségre.

   b. A megnyíló ablakban adja meg a kísérletek számát és az időszakot, amelyen belül el kell végezni a jelszóbeírási kísérleteket a szabály aktiválásához.

   c. Kattintson az **OK** gombra.
8. Ha kiválasztotta a(z) **There is an atypical activity detected during a network logon session** szabályt, konfigurálnia kell a beállításait:

   a. Kattintson a szabály alatti **Settings** lehetőségre.

   b. A **Network logon detection** területen adja meg az időszak kezdetét és végét.

A Kaspersky Endpoint Security a meghatározott időszakban végzett bejelentkezési kísérleteket rendellenes tevékenységnek tekinti.

Alapértelmezés szerint az időszak nincs beállítva, és az alkalmazás nem figyeli a bejelentkezési kísérleteket. Ahhoz, hogy az alkalmazás folyamatosan figyelje a bejelentkezési kísérleteket, állítsa be az időszakot 0:00 – 23:59 értékre. Az időszak kezdete és vége nem eshet egybe. Ha megegyeznek, az alkalmazás nem figyeli a bejelentkezési kísérleteket.

c. A **Exclusions** területen adja meg a megbízható felhasználókat és a megbízható IP-címeket (IPv4 és IPv6).

A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata. A Kaspersky Endpoint Security nem figyeli ezen felhasználók és számítógépek bejelentkezési kísérleteit.

d. Kattintson az **OK** gombra.

9. Mentse el a módosításokat.

Előre definiált szabályok konfigurálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Naplóvizsgálat** lehetőséget.
3. Győződjön meg arról, hogy a **Naplóvizsgálat** kapcsoló be van kapcsolva.
4. Az **Előre definiált szabályok** részben kattintson a **Konfigurálás** gombra.
5. Az előre definiált szabályok konfigurálásához jelölje be vagy törölje a jelölőnégyzeteket:
   - **A rendszerben lehetséges találgatásos támadásra utaló mintázatok találhatók**.
   - **A hálózati bejelentkezési munkamenet során szokatlan tevékenység észlelhető**.
   - **Windows eseménynaplóval való lehetséges visszaélésre utaló minták találhatók**.
   - **Újonnan telepített szolgáltatás nevében észlelt szokatlan műveletek**.
   - **Explicit hitelesítő adatokat használó szokatlan bejelentkezés észlelve**.
   - **Lehetséges Kerberos hamisított PAC-s (MS14-068) támadás mintái észlelhetők a rendszerben**.

   a. **Gyanús módosítások észlelhetők az emelt szintű beépített Rendszergazdák csoportban**.

6. Szükség esetén konfigurálja a **rendszerben lehetséges találgatásos támadásra utaló mintázatok találhatók** szabályt:

   a. Kattintson a szabály alatti **Beállítások** lehetőségre.

   b. A megnyíló ablakban adja meg a kísérletek számát és az időszakot, amelyen belül el kell végezni a jelszóbeírási kísérleteket a szabály aktiválásához.

7. Ha kiválasztotta **A rendszer szokatlan tevékenységet észlel egy hálózati bejelentkezési munkamenet során** szabályt, konfigurálnia kell a beállításait:

   a. Kattintson a szabály alatti **Beállítások** lehetőségre.

   b. A **Hálózati bejelentkezés észlelése** részen adja meg az időszak kezdetét és végét.

   A Kaspersky Endpoint Security a meghatározott időszakban végzett bejelentkezési kísérleteket rendellenes tevékenységnek tekinti.

   Alapértelmezés szerint az időszak nincs beállítva, és az alkalmazás nem figyeli a bejelentkezési kísérleteket. Ahhoz, hogy az alkalmazás folyamatosan figyelje a bejelentkezési kísérleteket, állítsa be az időszakot 0:00 – 23:59 értékre. Az időszak kezdete és vége nem eshet egybe. Ha megegyeznek, az alkalmazás nem figyeli a bejelentkezési kísérleteket.

   c. A **Kizárások** részben adja meg a megbízható felhasználókat és a megbízható IP-címeket (IPv4 és IPv6).

   A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata. A Kaspersky Endpoint Security nem figyeli ezen felhasználók és számítógépek bejelentkezési kísérleteit.

8. Mentse el a módosításokat.

Ennek eredményeként, amikor a szabály aktiválódik, a Kaspersky Endpoint Security egy *kritikus esemény*hez létre.

Egyéni szabályok hozzáadása

Saját feltételeit is beállíthatja a naplóvizsgálati szabály kiváltásához. Ehhez meg kell adnia egy eseményazonosítót, és ki kell választania egy eseményforrást. Az eseményazonosítót megkeresheti a Microsoft terméktámogatási webhelyén. Az eseményforrást kiválaszthatja a standard naplók közül: *Application*, *Security* vagy *System*. Egy harmadik féltől származó alkalmazás naplóját is megadhatja. A harmadik féltől származó alkalmazásnapló nevét megkeresheti az Eseménymegtekintő eszköz segítségével. A rendszer a harmadik felektől származó alkalmazásnaplókat az Alkalmazás- és szolgáltatásnaplók mappában tárolja (például a *Windows PowerShell* naplót).

> Az alkalmazás nem ellenőrzi, hogy a megadott napló ténylegesen létezik-e a Windows eseménynaplójában. Ha hibás a napló neve, az alkalmazás nem követi figyelemmel a naplóeseményeket.

Az egyéni szabályok listája már tartalmaz három szabályt, amelyet a Kaspersky szakértői hoztak létre.

Egyéni szabály hozzáadása az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakában válassza a **Biztonsági felügyelet → Naplóvizsgálat** lehetőséget.
4. Győződjön meg arról, hogy a **Naplóvizsgálat** jelölőnégyzet be van jelölve.
5. Az **Egyéni szabályok** részben kattintson a **Beállítások** gombra.
6. A megjelenő ablakban jelölje be azon egyéni szabályok mellett található jelölőnégyzeteket, amelyeket engedélyezni szeretne.

7. Szükség esetén kattintson a **Hozzáadás** gombra, hogy létrehozza a saját egyéni szabályait.

8. Ekkor megnyílik egy ablak, amelyben konfigurálhatja az egyéni szabályt:

   - **Szabály neve**.
   - **Napló neve**. Windows-eseménynaplók. A következő naplók érhetők el: *Application*, *Security*, *System*.
   - **Forrás**. Harmadik felektől származó alkalmazásnaplók. A harmadik féltől származó alkalmazásnapló nevét megkeresheti az Eseménymegtekintő eszköz segítségével. A rendszer a harmadik felektől származó alkalmazásnaplókat az Alkalmazás- és szolgáltatásnaplók mappában tárolja (például a *Windows PowerShell* naplót).
   - **Eseményazonosítók**. Eseményazonosítók a Windows eseménynaplójában. Az eseményazonosítókat megkeresheti a Microsoft műszaki dokumentációjában.

9. Mentse el a módosításokat.

Egyéni szabály hozzáadása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **Log Inspection** elemet.
5. Győződjön meg arról, hogy a **Log Inspection ENABLED** kapcsoló be van kapcsolva.
6. Az **Custom rules** részben válassza ki az engedélyezni kívánt egyéni szabályokat.
7. Szükség esetén kattintson a **Add** gombra, hogy létrehozza a saját egyéni szabályait.
8. Ekkor megnyílik egy ablak, amelyben konfigurálhatja az egyéni szabályt:

   - **Rule name**.
   - **Custom log name**. Windows-eseménynaplók. A következő naplók érhetők el: *Application*, *Security*, *System*.
   - **Origin**. Harmadik felektől származó alkalmazásnaplók. A harmadik féltől származó alkalmazásnapló nevét megkeresheti az Eseménymegtekintő eszköz segítségével. A rendszer a harmadik felektől származó alkalmazásnaplókat az Alkalmazás- és szolgáltatásnaplók mappában tárolja (például a *Windows PowerShell* naplót).
   - **Event Identifiers**. Eseményazonosítók a Windows eseménynaplójában. Az eseményazonosítókat megkeresheti a Microsoft műszaki dokumentációjában.

9. Mentse el a módosításokat.

Egyéni szabály hozzáadása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Naplóvizsgálat** lehetőséget.

3. Győződjön meg arról, hogy a **Naplóvizsgálat** kapcsoló be van kapcsolva.

4. Az **Egyéni szabályok** részben kattintson a **Konfigurálás** gombra.

5. A megjelenő ablakban jelölje be azon egyéni szabályok mellett található jelölőnégyzeteket, amelyeket engedélyezni szeretne.

6. Szükség esetén kattintson a **Hozzáadás** gombra, hogy létrehozza a saját egyéni szabályait.

7. Ekkor megnyílik egy ablak, amelyben konfigurálhatja az egyéni szabályt:

   - **Szabály neve**.
   - **Napló neve**. Windows-eseménynaplók. A következő naplók érhetők el: *Application*, *Security*, *System*.
   - **Forrás**. Harmadik felektől származó alkalmazásnaplók. A harmadik féltől származó alkalmazásnapló nevét megkeresheti az Eseménymegtekintő eszköz segítségével. A rendszer a harmadik felektől származó alkalmazásnaplókat az Alkalmazás- és szolgáltatásnaplók mappában tárolja (például a *Windows PowerShell* naplót).
   - **Eseményazonosító**. Eseményazonosítók a Windows eseménynaplójában. Az eseményazonosítókat megkeresheti a Microsoft műszaki dokumentációjában.

8. Mentse el a módosításokat.

A művelet eredményeként a Kaspersky Endpoint Security a szabály kiváltásakor létrehoz egy *Critical* eseményt.

Rendszerintegritás-figyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt.

A 12.6-os verziótól kezdve a Kaspersky Endpoint Security for Windows a Fájlintegritás-figyelő összetevő helyett a Rendszerintegritás-felügyelet összetevőt tartalmazza. A Rendszerintegritás-figyelő összetevő a Fájlintegritás-figyelő összes funkcióját tartalmazza, és lehetővé teszi a beállításjegyzék-változások és a külső eszközök csatlakoztatásának figyelését.

A Rendszerintegritás-figyelő figyeli az operációs rendszerben bekövetkező olyan változásokat, amelyek a számítógépes biztonság sérülésére utalhatnak. Ilyen változások észlelésekor a Kaspersky Endpoint Security megfelelő eseményeket generál, és figyelmezteti a rendszergazdát. A Rendszerintegritás-figyelő valós idejű üzemmódban működhet, és kérésre rendszerintegritás-ellenőrzéseket is végezhet.

Valós idejű rendszerintegritás-figyelő

Valós idejű üzemmódban a Rendszerintegritás-figyelő nyomon követi az összetevő hatókörébe tartozó objektumok változásait (a *figyelési hatókör*). A Rendszerintegritás-figyelő lehetővé teszi az ilyen objektumokhoz való illetéktelen hozzáférés valós idejű blokkolását is.

Igény szerinti rendszerintegritás-ellenőrzés

Az igény szerinti rendszerintegritás-ellenőrzés egy manuálisan vagy ütemezetten futtatható feladat. A *Rendszerintegritás-ellenőrzés* feladat futtatásához konfigurálnia kell az összetevő hatókörét (a *figyelési hatókör*), és létre kell hoznia egy alapszintet. Az *alapszint* a rendszerben lévő objektumok rögzített állapota, amelyet az alkalmazás referenciaként használ az aktuális állapottal való összehasonlításkor.

Fájlintegritás-figyelő beállításainak migrálása

Amikor a Kaspersky Endpoint Security 12.6 verziójára frissíti, a Fájlintegritás-figyelő beállításai automatikusan migrálásra kerülnek. A migrálás részeként az alkalmazás a figyelési szabályokat áthelyezi a Rendszerintegritás-figyelőbe. A Fájlintegritás-figyelő szabályokat a rendszer akkor is migrálja a Rendszerintegritás-figyelőbe, amikor a migráció a KSWS megoldásból a KES megoldásba kerül.

A Rendszerintegritás-figyelő megfelelő működésének biztosítása érdekében a Kaspersky Endpoint Security alkalmazást és az adminisztrációs bővítményt frissíteni kell a 12.6-os verzióra. Ha az adminisztrációs bővítmény korábbi verziója van telepítve, akkor nem konfigurálhatja a Rendszerintegritás-figyelőt, mert az adminisztrációs bővítmény nem rendelkezik **Rendszerintegritás-figyelő** szakasszal.

A Rendszerintegritás-figyelő szabályairól

A Rendszerintegritás-figyelő működéséhez hozzá kell adni legalább egy szabályt. A *Rendszerintegritás-figyelői szabály* egy olyan feltételkészlet, amely meghatározza a felhasználók fájlokhoz és beállításjegyzékhez való hozzáférését. A Rendszerintegritás-figyelő észleli a fájlok és a beállításjegyzék módosításait a megadott *figyelési hatókörben*. A figyelési hatókör a Rendszerintegritás-figyelő szabályainak egyik feltétele.

A Rendszerintegritás-figyelő a következő objektumok megfigyelését teszi lehetővé:

- Fájlok
- Beállításjegyzék
- Külső eszközök

A fájlfigyeléssel kapcsolatos különleges szempontok

A Rendszerintegritás-figyelő figyeli a fájlok és mappák változásait, valamint a figyelési hatókörhöz hozzáadott vagy onnan eltávolított fájlokat. Ezek a változtatások arra utalhatnak, hogy egy támadó sikeresen átjutott a számítógép védelmén. Javasoljuk, hogy olyan objektumokat adjon meg, amelyeket ritkán módosítanak, vagy amelyekhez kizárólag a rendszergazdának van hozzáférése. Ez segít csökkenteni a Rendszerintegritás-figyelő eseményeinek számát.

> A Rendszerintegritás-felügyelet nem figyeli a kiszolgáló megosztott mappáiban lévő fájlok változásait. A Rendszerintegritás-felügyelet csak helyileg használható.

A Kaspersky Endpoint Security csak azokon a lemezeken figyeli a fájlok és mappák változásait, amelyek a valós idejű Rendszerintegritás-figyelő működésének megkezdésekor csatlakoztatva voltak. Ha nem volt lemez csatlakoztatva, amikor a valós idejű Rendszerintegritás-figyelő működése megkezdődött, az alkalmazás akkor sem figyeli a fájlok és mappák változásait a lemezen, ha a fájlok és mappák hozzá vannak adva a figyelési hatókörhöz.

A beállításjegyzék-figyeléssel kapcsolatos különleges szempontok

A Rendszerintegritás-figyelő figyeli a beállításjegyzéket. Ezek a változtatások arra utalhatnak, hogy egy támadó sikeresen átjutott a számítógép védelmén.

A Rendszerintegritás-figyelő a beállításjegyzék következő fő kulcsait figyeli:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`

- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG (csak a Valós idejű rendszerintegritás-felügyeletben érhető el)
- HKEY_CURRENT_USER (csak a Valós idejű rendszerintegritás-felügyeletben érhető el)

> A *Rendszerintegritás-ellenőrzés* nem támogatja a HKEY_CURRENT_USER kulcsot. Megadhat egy kulcsot a HKEY_USERS alatt mint HKEY_USERS\<user profile ID>\<key>.

Külső eszközök figyelésével kapcsolatos különleges szempontok

A Rendszerintegritás-figyelő figyeli a külső eszközök csatlakoztatását és leválasztását. Erre azért van szükség, hogy megvédje a számítógépet az ilyen eszközökkel való fájlcseréből eredő biztonsági fenyegetésektől. A Rendszerintegritás-figyelő nem figyeli a külső eszközökhöz való hozzáférést, és nem blokkolja a fájlcserét. Az eszközök elérését egy másik alkalmazásösszetevő, a Eszközfelügyelő használatával is konfigurálhatja.

> Amikor fut az *Alapszintű Rendszerintegritás-felügyelet* feladat, az alkalmazás figyelmen kívül hagyja a külső eszközök újracsatlakoztatását, ha az operációs rendszerben az eszközök meghajtóbetűjele megegyezik. A naplózáshoz az újra csatlakoztatott eszközöknek eltérő meghajtóbetűjellel kell rendelkezniük.

A Rendszerintegritás-figyelő az alábbi típusú külső eszközök csatlakoztatását figyeli:

- Cserélhető meghajtó (beleértve az USB cserélhető meghajtókat is)
- Merevlemez
- Külső hálózati adapter
- CD-/DVD-/Blu-ray-meghajtó
- Szkenner/kamera

Valós idejű rendszerintegritás-figyelő

A Rendszerintegritás-figyelő lehetővé teszi az operációs rendszer változásainak valós idejű követését. Nyomon követheti azokat a módosításokat, amelyek a számítógép biztonságának sérülésére utalhatnak. Az összetevő lehetővé teszi ezen módosítások blokkolását vagy pusztán a változási események naplózását.

A Rendszerintegritás-figyelő működéséhez hozzá kell adni legalább egy szabályt. A *Rendszerintegritás-figyelői szabály* egy olyan feltételkészlet, amely meghatározza a felhasználók fájlokhoz és beállításjegyzékhez való hozzáférését. A Rendszerintegritás-figyelő észleli a fájlok és a beállításjegyzék módosításait a megadott *figyelési hatókörben*. A figyelési hatókör a Rendszerintegritás-figyelő szabályainak egyik feltétele.

Valós idejű Rendszerintegritás-figyelői módok

Annak érdekében, hogy a Rendszerintegritás-figyelői szabályok ne blokkoljanak az operációs rendszer vagy más szolgáltatások működése szempontjából kritikus erőforrásokkal végzett műveleteket, javasoljuk a Teszt mód engedélyezését, és annak elemzését, hogy az összetevő milyen hatással van a rendszerre. Bekapcsolt Teszt mód mellett a Kaspersky Endpoint Security nem blokkolja a szabályok által tiltott felhasználói tevékenységeket, hanem *Figyelmeztetés* ⚠ típusú eseményeket generál.

A Valós idejű Rendszerintegritás-figyelő összetevőnek két módja van:

- Blokkolás

  Ebben a módban a Rendszerintegritás-figyelő nyomon követi a rendszerben bekövetkezett változásokat, és a szabályoknak megfelelően végrehajt egy műveletet: **Engedélyezés** vagy **Blokkolás**. A Rendszerintegritás-figyelő is generál egy megfelelő eseményt, és módosítja az eszköz állapotát a Kaspersky Security Center konzolon.

- Értesítés

  Ebben a módban a Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket. Ha a fájlokkal vagy a beállításjegyzékkel végzett művelet le van tiltva, az alkalmazás egy eseményt generál: *A tiltott műveletet teszt módban engedélyezték*. A szabályok rendszerre gyakorolt hatásának elemzéséhez tekintse meg a jelentéseket.

Valós idejű Rendszerintegritás-figyelő engedélyezése

A valós idejű rendszerintegritás-figyelő engedélyezése a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakában válassza a **Biztonsági felügyelet** → **Rendszerintegritás-figyelő** lehetőséget.
4. Jelölje be a **Rendszerintegritás-figyelő** jelölőnégyzetet.
5. A **Blokkolási szabályok működési módja** részen válasszon egy üzemmódot a Valós idejű rendszerintegritás-felügyelethez:
   - **Blokkolás**. Ebben a módban a Rendszerintegritás-figyelő blokkolja a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.
   - **Tájékoztatás**. Ebben a módban a Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.
6. A **Valós idejű rendszerintegritás-figyelő** részen jelölje be a **Valós idejű rendszerintegritás-figyelő** jelölőnégyzetet.

7. Külső eszköz figyelésének konfigurálása:

   a. Jelölje be az **Eszközök figyelése** jelölőnégyzetet.

   b. Az **Esemény súlyossági szintje** legördülő listából válassza ki a külső eszköz figyelési eseményeinek fontossági szintjét: *Információs*, *Figyelmeztetés*, *Kritikus*.

   A Rendszerintegritás-figyelő rögzíti a külső eszközök aktuális csatlakoztatását. Az alkalmazás azután kezdi el figyelni a külső eszközök csatlakoztatását és leválasztását, miután az összetevő engedélyezve lett az alkalmazás beállításaiban. Ezt követően egy külső eszköz csatlakoztatásakor vagy leválasztásakor az alkalmazás létrehoz egy megfelelő eseményt.

8. A fájl- és beállításjegyzék-figyelés konfigurálása:

   a. Jelölje be a **Fájlok és a beállításjegyzék figyelése** jelölőnégyzetet.

   b. Kattintson a **Beállítások** gombra.

   Ezzel megnyílik a Rendszerintegritás-figyelő szabályainak listája.

   c. Kattintson **Hozzáadás** gombra.

   Azt is megteheti, hogy más forrásból importál szabályokat.

   d. Konfigurálja a Rendszerintegritás-felügyelet szabályát (lásd az alábbi táblázatot).

9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Valós idejű rendszerintegritás-figyelő engedélyezése a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **System Integrity Monitoring** elemet.
5. Kapcsolja be az **System Integrity Monitoring ENABLED** kapcsolót.
6. Válassza ki az **Windows** lapot.
7. A **Real-Time System Integrity Monitoring** területen válasszon egy módot a Valós idejű rendszerintegritás-felügyelethez:

   - **Apply rules**. Ebben a módban a Rendszerintegritás-figyelő blokkolja a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.
   - **Test rules (Inform)**. Ebben a módban a Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.

8. A fájl- és beállításjegyzék-figyelés konfigurálása:

   a. Tegyen jelölést a **Monitor files and the registry** jelölőnégyzetbe.

   b. Kattintson az **Rules** gombra.

   Ezzel megnyílik a Rendszerintegritás-figyelő szabályainak listája.

   c. Kattintson az **Add** gombra.

   Azt is megteheti, hogy más forrásból importál szabályokat.

   d. Konfigurálja a Rendszerintegritás-felügyelet szabályát (lásd az alábbi táblázatot).

9. Külső eszköz figyelésének konfigurálása:

   a. Tegyen jelölést a **Monitor devices** jelölőnégyzetbe.

   b. Az **Event severity level** legördülő listából válassza ki a külső eszköz figyelési eseményeinek fontossági szintjét: *Informational* ⓘ, *Warning* ⚠, *Critical* ⓘ.

   A Rendszerintegritás-figyelő rögzíti a külső eszközök aktuális csatlakoztatását. Az alkalmazás azután kezdi el figyelni a külső eszközök csatlakoztatását és leválasztását, miután az összetevő engedélyezve lett az alkalmazás beállításaiban. Ezt követően egy külső eszköz csatlakoztatásakor vagy leválasztásakor az alkalmazás létrehoz egy megfelelő eseményt.

10. A szabályzat számítógépekre való alkalmazásához zárja le a 🔒 lakat ikonokat, és mentse a módosításokat.

A valós idejű Rendszerintegritás-figyelő engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Rendszerintegritás-figyelő** lehetőséget.

3. Kapcsolja be a **Rendszerintegritás-figyelő** billenőkapcsolót.

4. A **Blokkolási szabályok működési módja** részen válasszon egy üzemmódot a Valós idejű rendszerintegritás-felügyelethez:

   - **Blokkolás**. Ebben a módban a Rendszerintegritás-figyelő blokkolja a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.

   - **Tájékoztatás**. Ebben a módban a Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.

5. A **Valós idejű rendszerintegritás-figyelő** részen jelölje be a **Valós idejű rendszerintegritás-figyelő** jelölőnégyzetet.

6. Külső eszköz figyelésének konfigurálása:

   a. Jelölje be az **Eszközök figyelése** jelölőnégyzetet.

   b. Az **Esemény súlyossági szintje** legördülő listából válassza ki a külső eszköz figyelési eseményeinek fontossági szintjét: *Információs* ⓘ, *Figyelmeztetés* ⚠, *Kritikus* ⓘ.

A Rendszerintegritás-figyelő rögzíti a külső eszközök aktuális csatlakoztatását. Az alkalmazás azután kezdi el figyelni a külső eszközök csatlakoztatását és leválasztását, miután az összetevő engedélyezve lett az alkalmazás beállításaiban. Ezt követően egy külső eszköz csatlakoztatásakor vagy leválasztásakor az alkalmazás létrehoz egy megfelelő eseményt.

7. A fájl- és beállításjegyzék-figyelés konfigurálása:

   a. Jelölje be a **Fájlok és a beállításjegyzék figyelése** jelölőnégyzetet.

   b. Kattintson a **Beállítás** gombra.

   Ezzel megnyílik a Rendszerintegritás-figyelő szabályainak listája.

   c. Kattintson **Hozzáadás** gombra.

   Azt is megteheti, hogy más forrásból importál szabályokat.

8. Konfigurálja a Rendszerintegritás-felügyelet szabályát (lásd az alábbi táblázatot).

9. Mentse el a módosításokat.

A valós idejű Rendszerintegritás-figyelő szabálybeállításai

Paraméter	Leírás
Szabály neve	A valós idejű Rendszerintegritás-figyelő szabályneve
Műveletek fájlokkal és a beállításjegyzékkel	• **Engedélyezés**. A Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket. • **Blokkolás**. A Rendszerintegritás-figyelő viselkedése a kiválasztott módtól függ. Ha kiválasztotta a *Rendszervédelem módot*, a Rendszerintegritás-figyelő blokkolja a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal végzett műveleteket, létrehoz egy megfelelő eseményt, és módosítja az eszköz állapotát a Kaspersky Security Center konzolon. Ha kiválasztotta a *Teszt módot*, a Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket.

Paraméter	Leírás
Esemény súlyossági szintje	A Kaspersky Endpoint Security naplózza a fájlmódosítási eseményeket, amikor egy figyelési hatókörben lévő fájl vagy beállításkulcs módosul. A következő súlyossági szintek érhetők el az eseményekhez: *Tájékoztatás*, *Figyelmeztetés*, *Kritikus*.

Figyelés hatóköre	• **File**. Az összetevő által felügyelt fájlok és mappák listája. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.
	maszkok használata:
	  • A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
	  • Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
	  • A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.
	• **Beállításjegyzék**. Az összetevő által figyelt beállításkulcsok és értékek listája. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

Kizárások	• **File**. A figyelési hatókörből való kizárások listája. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. Például: `C:\Folder\Application\*.log`. A kizárási bejegyzések prioritása magasabb, mint a figyelési hatókör bejegyzéseinek.
	maszkok használata:
	  • A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
	  • Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
	  • A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.
	• **Beállításjegyzék**. A figyelési hatókörből való kizárások listája. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor. A kizárási bejegyzések prioritása magasabb, mint a figyelési hatókör bejegyzéseinek.

Megbízható felhasználók és/vagy felhasználói csoportok	A *megbízható felhasználó* olyan felhasználó, aki műveleteket hajthat végre a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal. Ha a Kaspersky Endpoint Security megbízható felhasználó által végrehajtott műveletet észlel, a Rendszerintegritás-figyelő létrehoz egy *Információs* típusú eseményt. A felhasználókat kiválaszthatja az Active Directoryban, a Kaspersky Security Center fióklistájában, vagy a helyi felhasználónév manuális megadásával. A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata.
Fájlműveleti jelölők / felügyelt műveletek	Az alkalmazás által felügyelt fájlokkal vagy beállításkulcsokkal végzett műveleteket jellemző jelölők.
Kivonatolás	Fájlkivonat kiszámításaa módosításkor. A Kaspersky Endpoint Security az esemény generálásakor információkat ad hozzá a fájl kivonatáról.

Igény szerinti rendszerintegritás-ellenőrzés

Az igény szerinti rendszerintegritás-ellenőrzés egy manuálisan vagy ütemezetten futtatható feladat. Amikor fut a *Rendszerintegritás-ellenőrzés* feladat, az alkalmazás összehasonlítja a figyelési hatókörbe tartozó objektumok aktuális állapotát az *alapszint* állapotával. A valós idejű Rendszerintegritás-figyelővel ellentétben a *Rendszerintegritás-ellenőrzés* feladat segít korlátozni az események számát, és átfogó jelentést készít az operációs rendszer változásairól.

A Rendszerintegritás-figyelő működéséhez hozzá kell adni legalább egy szabályt. A *Rendszerintegritás-figyelői szabály* egy olyan feltételkészlet, amely meghatározza a felhasználók fájlokhoz és beállításjegyzékhez való hozzáférését. A Rendszerintegritás-figyelő észleli a fájlok és a beállításjegyzék módosításait a megadott *figyelési hatókörben*. A figyelési hatókör a Rendszerintegritás-figyelő szabályainak egyik feltétele. Konfigurálhat olyan szabályokat, amelyeket a valós idejű Rendszerintegritás-figyelő és a *Rendszerintegritás-ellenőrzés* feladat megoszt, vagy létrehozhat külön szabályokat a feladathoz. Az alapszint létrehozásához a Kaspersky Endpoint Security alkalmazza a figyelési hatókört a *Rendszerintegritás-ellenőrzés* feladatból az *Alapszint frissítése* feladatra.

Alapszint létrehozása és frissítése

A *Rendszerintegritás-ellenőrzés* feladatnak alapszintre van szüksége a működéséhez. Az *alapszint* a rendszerben lévő objektumok rögzített állapota, amelyet az alkalmazás referenciaként használ az aktuális állapottal való összehasonlításkor. Ha a rendszer jelenlegi állapota eltér az alapszintben rögzített állapottól, a Kaspersky Endpoint Security generálja a megfelelő eseményt. Alapszintet az *Alapszint frissítése* feladattal hozhat létre vagy frissíthet.

Az alapszintet a következő módokban frissítheti:

- Teljes frissítés.

  Az alkalmazás a figyelési hatókörben lévő összes objektumot frissíti.

- Növekményes frissítés.

  Az alkalmazás csak a módosított vagy új objektumokat észleli és frissíti.

Alapszint létrehozásának vagy frissítésének menete az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza a **Kaspersky Endpoint Security for Windows (14.1)** → **Alapverzió frissítése**lehetőséget.

2. lépés: Az alapszint frissítése mód kiválasztása

Válasszon ki az alapszint frissítési módját:

- **Teljes frissítés**. Az alkalmazás a figyelési hatókörben lévő összes objektumot frissíti.
- **Növekményes frissítés**. Az alkalmazás csak a módosított vagy új objektumokat észleli és frissíti.

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés A feladat nevének megadása

Írja be a feladat nevét, például *2024-es alapszint*.

5. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Alapszint létrehozásának vagy frissítésének menete a Web Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Baseline update** lehetőséget.

c. A **Task name** mezőben adjon meg egy rövid leírást, például *2024-es alapszint*.

d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. Válasszon ki az alapszint frissítési módját:

   - **Full update**. Az alkalmazás a figyelési hatókörben lévő összes objektumot frissíti.
   - **Incremental update**. Az alkalmazás csak a módosított vagy új objektumokat észleli és frissíti.

10. Mentse el a módosításokat.

11. Válassza ki a feladat melletti jelölőnégyzetet.

12. Kattintson az **Start** gombra.

A figyelési hatókör konfigurálása a Rendszerintegritás-ellenőrzés feladathoz

Alapértelmezés szerint a *Rendszerintegritás-ellenőrzés* feladat figyelési hatóköre megegyezik a valós idejű Rendszerintegritás-figyelő figyelési hatókörével. Más figyelési hatókört is beállíthat a feladathoz.

A Rendszerintegritás-felügyelet nem támogatja a `HKEY_CURRENT_USER` és a `HKEY_CURRENT_CONFIG` kulcsok importálását a *Rendszerintegritás-ellenőrzés* feladatba. Ha a feladat figyelési hatóköre tartalmazza ezeket a kulcsokat, az alkalmazás létrehozza *A figyelési hatókör helytelen objektumokat tartalmaz* eseményt.

Más figyelési hatókör konfigurálása a Rendszerintegritás-ellenőrzés feladathoz a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A szabályzat ablakában válassza a **Biztonsági felügyelet** → **Rendszerintegritás-figyelő** lehetőséget.

4. Jelölje be a **Rendszerintegritás-figyelő** jelölőnégyzetet.

5. A **Rendszerintegritás-ellenőrzés** alatt válassza ki a feladat konfigurációs módját: **Egyéni beállítások**.

6. Külső eszköz figyelésének konfigurálása:

   a. Jelölje be az **Eszközök figyelése** jelölőnégyzetet.

   b. Az **Esemény súlyossági szintje** legördülő listából válassza ki a külső eszköz figyelési eseményeinek fontossági szintjét: *Információs*, *Figyelmeztetés*, *Kritikus*.

   A Rendszerintegritás-figyelő az alapszint létrehozásakor rögzíti az információkat a csatlakoztatott külső eszközökről. Ezt követően egy külső eszköz csatlakoztatásakor az alkalmazás létrehoz egy megfelelő eseményt. Amikor fut a *Rendszerintegritás-ellenőrzés* feladat, az alkalmazás nem figyeli a külső eszközök leválasztását.

7. A fájl- és beállításjegyzék-figyelés konfigurálása:

   a. Jelölje be a **Fájlok és a beállításjegyzék figyelése** jelölőnégyzetet.

   b. Kattintson a **Beállítások** gombra.

   Ezzel megnyílik a Rendszerintegritás-figyelő szabályainak listája.

   c. Kattintson **Hozzáadás** gombra.

   Azt is megteheti, hogy más forrásból importál szabályokat.

   d. Konfigurálja a Rendszerintegritás-felügyelet szabályát (lásd az alábbi táblázatot).

8. Mentse el a módosításokat.

Más figyelési hatókör konfigurálása a System Integrity Check feladathoz a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Security Controls** → **System Integrity Monitoring** elemet.

5. Válassza ki az **Windows** lapot.

6. Kapcsolja be az **System Integrity Monitoring ENABLED** kapcsolót.

7. A **System Integrity Check** területen válassza ki a feladat konfigurációs módját: **Custom settings**.

8. Külső eszköz figyelésének konfigurálása:

   a. Tegyen jelölést a **Monitor devices** jelölőnégyzetbe.

   b. Az **Event severity level** legördülő listából válassza ki a külső eszköz figyelési eseményeinek fontossági szintjét: *Informational*, *Warning*, *Critical*.

   A Rendszerintegritás-figyelő az alapszint létrehozásakor rögzíti az információkat a csatlakoztatott külső eszközökről. Ezt követően egy külső eszköz csatlakoztatásakor az alkalmazás létrehoz egy megfelelő eseményt. Amikor fut a *Rendszerintegritás-ellenőrzés* feladat, az alkalmazás nem figyeli a külső eszközök leválasztását.

9. A fájl- és beállításjegyzék-figyelés konfigurálása:

    a. Tegyen jelölést a **Monitor files and the registry** jelölőnégyzetbe.

    b. Kattintson az **Rules** gombra.

    Ezzel megnyílik a Rendszerintegritás-figyelő szabályainak listája.

    c. Kattintson az **Add** gombra.

    Azt is megteheti, hogy más forrásból importál szabályokat.

    d. Konfigurálja a Rendszerintegritás-felügyelet szabályát (lásd az alábbi táblázatot).

10. Mentse el a módosításokat.

Más figyelési hatókör konfigurálása a Rendszerintegritás-ellenőrzés feladathoz az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet → Rendszerintegritás-figyelő** lehetőséget.
3. Kapcsolja be a **Rendszerintegritás-figyelő** billenőkapcsolót.
4. A **Rendszerintegritás-ellenőrzés** alatt válassza ki a feladat konfigurációs módját: **Egyéni beállítások**.
5. Külső eszköz figyelésének konfigurálása:

    a. Jelölje be az **Eszközök figyelése** jelölőnégyzetet.

    b. Az **Esemény súlyossági szintje** legördülő listából válassza ki a külső eszköz figyelési eseményeinek fontossági szintjét: *Információs* ⓘ, *Figyelmeztetés* ⚠, *Kritikus* ⓘ.

    A Rendszerintegritás-figyelő az alapszint létrehozásakor rögzíti az információkat a csatlakoztatott külső eszközökről. Ezt követően egy külső eszköz csatlakoztatásakor az alkalmazás létrehoz egy megfelelő eseményt. Amikor fut a *Rendszerintegritás-ellenőrzés* feladat, az alkalmazás nem figyeli a külső eszközök leválasztását.

6. A fájl- és beállításjegyzék-figyelés konfigurálása:

    a. Jelölje be a **Fájlok és a beállításjegyzék figyelése** jelölőnégyzetet.

    b. Kattintson a **Beállítás** gombra.

    Ezzel megnyílik a Rendszerintegritás-figyelő szabályainak listája.

    c. Kattintson **Hozzáadás** gombra.

    Azt is megteheti, hogy más forrásból importál szabályokat.

    d. Konfigurálja a Rendszerintegritás-felügyelet szabályát (lásd az alábbi táblázatot).

7. Mentse el a módosításokat.

A Rendszerintegritás-ellenőrzés feladat szabályának beállításai

Paraméter	Leírás
Szabály neve	A *Rendszerintegritás-ellenőrzés* feladat szabályának neve.
Esemény súlyossági szintje	A Kaspersky Endpoint Security naplózza a fájlmódosítási eseményeket, amikor egy figyelési hatókörben lévő fájl vagy beállításkulcs módosul. A következő súlyossági szintek érhetők el az eseményekhez: *Tájékoztatás*, *Figyelmeztetés*, *Kritikus*.

Figyelés hatóköre	• **File**. Az összetevő által felügyelt fájlok és mappák listája. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.
	maszkok használata:
	  • A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
	  • Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
	  • A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.
	• **Beállításjegyzék**. Az összetevő által figyelt beállításkulcsok és értékek listája. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor.

Kizárások	• **File**. A figyelési hatókörből való kizárások listája. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. Például: `C:\Folder\Application\*.log`. A kizárási bejegyzések prioritása magasabb, mint a figyelési hatókör bejegyzéseinek.
	maszkok használata:
	  • A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
	  • Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
	  • A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.
	• **Beállításjegyzék**. A figyelési hatókörből való kizárások listája. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor. A kizárási bejegyzések prioritása magasabb, mint a figyelési hatókör bejegyzéseinek.

A Rendszerintegritás-ellenőrzés feladat futtatása

A *Rendszerintegritás-ellenőrzés* feladat lehetővé teszi a fájlok és beállításkulcsok módosításának ellenőrzését, valamint a külső eszközök csatlakoztatásának ellenőrzését. A fájlok módosításának ellenőrzéséhez futtassa a *Rendszerintegritás-ellenőrzés* feladatot a következő módokban:

- Gyors vizsgálat.

  A fájlok módosításának ellenőrzésekor az alkalmazások csak a fájlattribútumokat ellenőrzik. Az alkalmazás nem ellenőrzi a fájlok tartalmát.

- Teljes vizsgálat.

  A fájlok módosításának ellenőrzésekor az alkalmazások ellenőrzik az összes fájlattribútumot és a fájlok tartalmát.

Az, hogy a feladat milyen üzemmódban fut, nincs hatással a beállításjegyzék vagy a külső eszközök ellenőrzésére.

A Rendszerintegritás-ellenőrzés feladat futtatása a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.
3. Kattintson az **New task** gombra.

   Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.
4. Válassza ki a **Kaspersky Endpoint Security → Alapszintű rendszerintegritás-felügyelet** elemet. Válasszon ki egy Rendszerintegritás-felügyelet módot:

   - **Teljes vizsgálat**. Ebben a módban az alkalmazás a fájlok összes attribútumát és kivonatát ellenőrzi.
   - **Gyors vizsgálat**. Ebben a módban az alkalmazás csak a fájlattribútumokat ellenőrzi.
5. Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

   - Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket: hozzá nem rendelt eszközök. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
   - Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.
   - Adja meg azon eszközök listáját, amelyeken a feladatot futtatni kívánja.
   - Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
6. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.
7. A feladat indításának ütemezése, például manuálisan vagy a hét egy adott napján.
8. Adja meg a feladat nevét.
9. Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

A System Integrity Check feladat futtatása a Web Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.
2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **System Integrity Check** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *Heti rendszerintegritás-ellenőrzés*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. Válasszon ki egy Rendszerintegritás-ellenőrzési módot:

   - **Quick Scan**. Az alkalmazás csak a fájlattribútumokat ellenőrzi. Az alkalmazás nem ellenőrzi a fájlok tartalmát.
   - **Full Scan**. Az alkalmazás a fájlok összes attribútumát és tartalmát ellenőrzi.

10. Mentse el a módosításokat.

11. Válassza ki a feladat melletti jelölőnégyzetet.

12. Kattintson az **Start** gombra.

A *Rendszerintegritás-ellenőrzés* feladat sikeres befejezéséhez a *Rendszerintegritás-ellenőrzés* feladat figyelési hatókörének teljesen meg kell egyeznie az alapszinttel. Ha a figyelési hatókör eltérő, a feladat hibával fejeződik be. A figyelési hatókörök szinkronizálásához futtassa az *Alapszint frissítése* feladatot új felügyeleti körrel.

Rendszerintegritás-figyelői szabályok exportálása és importálása

A Rendszerintegritás-figyelői szabályok listáját exportálhatja egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú rekord hozzáadásával. Használhatja az exportálás/importálás funkciót a Rendszerintegritás-figyelői szabályok biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

A Rendszerintegritás-felügyelet nem támogatja a `HKEY_CURRENT_USER` és a `HKEY_CURRENT_CONFIG` kulcsok importálását a *Rendszerintegritás-ellenőrzés* feladatba. Ha a feladat figyelési hatóköre tartalmazza ezeket a kulcsokat, az alkalmazás létrehozza *A figyelési hatókör helytelen objektumokat tartalmaz* eseményt.

A Rendszerintegritás-figyelő szabályait tartalmazó lista exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakában válassza a **Biztonsági felügyelet → Rendszerintegritás-figyelő** lehetőséget.
4. A *Valós idejű rendszerintegritás-figyelő* szabályainak exportálása vagy importálása:
   a. A **Valós idejű rendszerintegritás-figyelő** részen kattintson a **Beállítások** gombra.
   b. A Valós idejű rendszerintegritás-figyelő szabályait tartalmazó lista exportálása:
      1. Jelölje ki az exportálni kívánt szabályokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
         Ha nem jelölt ki szabályt, a Kaspersky Endpoint Security az összes szabályt exportálja.
      2. Kattintson az **Exportálás** hivatkozásra.
      3. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a szabályok listáját, és válassza a fájl mentésére kiszemelt mappát.
      4. Mentse a fájlt.
         A Kaspersky Endpoint Security exportálja a szabályok listáját az XML-fájlba.
   c. A Valós idejű rendszerintegritás-figyelő szabályait tartalmazó lista importálása:
      1. Kattintson az **Import** hivatkozásra.
         A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.
      2. Nyissa meg a fájlt.
         Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
5. A *Rendszerintegritás-ellenőrzés* szabályainak exportálása vagy importálása:
   a. A **Rendszerintegritás-ellenőrzés** részen válassza az **Egyéni beállítások** elemet.
   b. Kattintson a **Beállítások** gombra.
   c. A Rendszerintegritás-ellenőrzés szabályait tartalmazó lista exportálása:
      1. Jelölje ki az exportálni kívánt szabályokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
         Ha nem jelölt ki szabályt, a Kaspersky Endpoint Security az összes szabályt exportálja.
      2. Kattintson az **Exportálás** hivatkozásra.
      3. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a szabályok listáját, és válassza a fájl mentésére kiszemelt mappát.
      4. Mentse a fájlt.

A Kaspersky Endpoint Security exportálja a szabályok listáját az XML-fájlba.

d. A Rendszerintegritás-ellenőrzés szabályait tartalmazó lista importálása:

1. Kattintson az **Import** hivatkozásra.

   A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.

2. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

6. Mentse el a módosításokat.

A Rendszerintegritás-ellenőrzés szabályait tartalmazó lista exportálása és importálása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Security Controls** → **System Integrity Monitoring** elemet.
5. Válassza ki az **Windows** lapot.
6. A *Valós idejű rendszerintegritás-figyelő* szabályainak exportálása vagy importálása:

   a. A **Real-Time System Integrity Monitoring** részen kattintson a **Rules** hivatkozásra.

   b. A Valós idejű rendszerintegritás-figyelő szabályait tartalmazó lista exportálása:

   1. Jelölje ki az exportálni kívánt szabályokat.
   2. Kattintson az → **Export** gombra.

      A Kaspersky Endpoint Security a szabályok listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

   c. A Valós idejű rendszerintegritás-figyelő szabályait tartalmazó lista importálása:

   1. Kattintson az → **Import** gombra.

      A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a megbízható címek listáját.
   2. Nyissa meg a fájlt.

      Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.
7. A *Rendszerintegritás-ellenőrzés* szabályainak exportálása vagy importálása:

   a. A **On-Demand System Integrity Check** területen válassza az **Custom settings** opciót.

   b. Kattintson a **Rules** hivatkozásra.

c. A Rendszerintegritás-ellenőrzés szabályait tartalmazó lista exportálása:

1. Jelölje ki az exportálni kívánt szabályokat.
2. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a szabályok listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

d. A Rendszerintegritás-ellenőrzés szabályait tartalmazó lista importálása:

1. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a megbízható címek listáját.
2. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.

8. Mentse el a módosításokat.

A Rendszerintegritás-figyelői jelentések megtekintése

A Rendszerintegritás-figyelői szabályok teljesítményének elemzéséhez megtekintheti az alkalmazás által generált jelentéseket és eseményeket. A Kaspersky Endpoint Security a következő jelentéseket készíti az összetevővel kapcsolatban:

- Az alkalmazás felületén:
  - A Rendszerintegritás-figyelői jelentés
  - A Rendszerintegritás-ellenőrzési jelentés
  - Az Alapszintre vonatkozó frissítési jelentés

  A jelentések rendszerintegritás-figyelő eseményeket tartalmaznak.
- A Kaspersky Security Center konzolon:
  - Azokról a számítógépekről készült jelentés, amelyeken a figyelési szabályok a legtöbbször aktiválódtak
  - Jelentés a leggyakrabban kiváltott figyelési szabályokról

  Alapértelmezés szerint a jelentés az előző 30 napra vonatkozik, beleértve a létrehozás dátumát is.

A Rendszerintegritás-figyelői jelentések megtekintése a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Reports** lapot.
3. Kattintson az **New report template** gombra.

   Ekkor elindul az új Jelentéssablon varázsló.

4. Kövesse a Jelentéssablon-varázsló utasításait. A **Selecting the report template type** lépésben válassza ki a Rendszerintegritás-figyelői jelentést (az **Other** szakasz):

   - **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   Miután végzett az Új jelentéssablon varázslóval, az új jelentéssablon megjelenik a **Reports** lapon lévő táblázatban.

5. Nyissa meg a jelentést dupla kattintással.

   Megkezdődik a jelentés előállítási folyamata. A jelentés egy új ablakban jelenik meg.

A Rendszerintegritás-figyelői jelentések megtekintése a Web Console-on

1. A Web Console fő ablakában válassza a **Monitoring** → **Reports** lehetőséget.
2. Kattintson az **Add** gombra.

   Ekkor elindul az új Jelentéssablon varázsló.

3. A **Template type** alatt az **Other** részen válasszon ki egy Rendszerintegritás-figyelői jelentést:

   - **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   Miután végzett az Új jelentéssablon varázslóval, az új jelentéssablon megjelenik a táblázatban.

4. Válassza ki és futtassa a jelentést.

   Megkezdődik a jelentés előállítási folyamata. A jelentés egy új ablakban jelenik meg.

Az alkalmazás által generált események megtekintéséhez a Kaspersky Security Center konzol eseménykijelöléseit is használhatja.

Rendszerintegritási állapot visszaállítása

A Kaspersky Security Center konzolon lévő számítógépek állapota a következők valamelyikével rendelkezik: *OK*, *Warning*, vagy *Critical*. Ha a Rendszerintegritás-figyelő a figyelési hatókörben lévő fájlok vagy beállításkulcsok módosítását észleli, a számítógép állapota a következőre módosul. *Warning* vagy *Critical*. A Rendszerintegritás-figyelő által hozzárendelt állapot a *rendszerintegritás állapota*. Visszaállíthatja a rendszerintegritás állapotát, például ha az elemzés során meggyőződött arról, hogy az objektumok észlelt módosítása nincs hatással a számítógép biztonságára.

A rendszer integritási állapotának visszaállítása a Felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **A rendszer integritási állapotának visszaállítása** elemet.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. lépés Feladatindítási ütemezés konfigurálása

Konfigurálja a feladat ütemezését, például manuálisan.

4. lépés A feladat nevének megadása

Adja meg a feladat nevét, például *Az állapot visszaállítása a figyelési hatókör módosítása után*.

5. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

A rendszer integritási állapotának visszaállítása a Web Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **System integrity status reset** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például *Az állapot visszaállítása a figyelési hatókör módosítása után*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon fiókot a feladat futtatásához. A Kaspersky Endpoint Security alapértelmezés szerint a helyi felhasználói fiók jogaival kezdi meg a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. Válassza ki a feladat melletti jelölőnégyzetet.

8. Kattintson az **Start** gombra.

Ennek eredményeként, ha a számítógép állapota a *Warning* vagy *Critical* értékre módosul, a Rendszerintegritás-figyelő eseményei miatt a számítógép állapota visszaáll az *OK* állapotra. Ha a számítógép állapota más események miatt is megváltozott, a számítógép állapota változatlan marad.

Cloud Discovery

A Cloud Discovery kezeli a felhasználók felhőszolgáltatásokhoz való hozzáférését. A felhőszolgáltatások közé tartozik például a Microsoft Teams, a Salesforce és a Microsoft Office 365. A felhőszolgáltatások kategóriákba vannak csoportosítva, például *fájlmegosztás*, *üzenetküldés*, *e-mail*. A Kaspersky szakértői rendszeresen frissítik a Cloud Discovery kategóriákat és a kategóriákba sorolt felhőszolgáltatásokat. A Kaspersky Endpoint Security az alkalmazás adatbázisával együtt frissíti a kategóriák és a felhőszolgáltatások készletét. Ez azt jelenti, hogy a Cloud Discovery nem használja a Kaspersky Security Network megoldást a felhőszolgáltatások kategorizálására.

A Cloud Discovery a következő funkciókat biztosítja:

- Felhőszolgáltatás használatának nyomon követése
- A felhőszolgáltatásokhoz való felhasználói hozzáférés blokkolása

Rendszerkövetelmények

A Cloud Discovery a következő feltételek teljesülése esetén érhető el:

- Az alkalmazás olyan számítógépre van telepítve, amelyen munkaállomásokhoz készült Windows fut.

  Az összetevő nem érhető el kiszolgálókhoz.

- Kaspersky Security Center 15.1 vagy újabb verzió.

  Az összetevő nem érhető el az Adminisztrációs konzolon (MMC). A Cloud Discoveryt a Kaspersky Security Center Web Console-on és a Kaspersky Security Center Cloud Console-on konfigurálhatja.

- Kaspersky Next licenc.

Engedélyezze a Cloud Discovery összetevő által igényelt alkalmazásfunkciókat:

1. **Titkosított kapcsolatok vizsgálata**. Erre a HTTPS-forgalom figyeléséhez van szükség. Ezt a funkciót a **Hálózati beállítások** részen kezelheti.

2. **Szkript beillesztése a webforgalomba a weboldalakkal való interakcióhoz**. A parancsfájl lehetővé teszi a Cloud Discovery események regisztrációját. A parancsfájl emellett a felhőszolgáltatásokhoz való hozzáférés teljes körű blokkolását is biztosítja. A parancsfájl nélkül az alkalmazás csak a felhőszolgáltatási tartományok hozzáférését blokkolja. Ezt a funkciót a **Hálózati beállítások** részen kezelheti.

Engedélyezheti **Az engedélyezett oldalak megnyitásának naplózása** funkciót is. A funkció magában foglalja az események csoportosítását, amikor a felhasználó olyan weboldalakat látogat meg, amelyek ugyanahhoz a tartományhoz tartoznak. Ily módon, amikor a felhasználó felhőszolgáltatást használ, a Cloud Discovery csak egy eseményt naplóz, nem pedig több eseményt minden egyes weboldalhoz. Ezt a funkciót a **Webfelügyelő** részen kezelheti.

Felhőszolgáltatások figyelése

Amikor egy felhasználó elkezd használni egy felhőszolgáltatást, a Kaspersky Endpoint Security regisztrálja az eseményt, és létrehoz egy bejegyzést a jelentésben. A Cloud Discovery ellenőrzi a felhőszolgáltatások használatát a böngészőben és a megfelelő alkalmazásokban. A Cloud Discovery a felhőszolgáltatások használatát HTTP és HTTPS protokollokon keresztül ellenőrzi.

A felhőszolgáltatások felügyeletének engedélyezése a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Communication & Web Protection** → **Cloud Discovery** elemet.

5. Kapcsolja be az **Cloud Discovery ENABLED** kapcsolót.

6. Mentse el a módosításokat.

Ennek eredményeképpen az alkalmazás továbbítja a Kaspersky Security Center felé a használt felhőszolgáltatásokról szóló információkat. A felhőszolgáltatások használatára vonatkozó információkat a jelentésekben tekintheti meg. Szükség esetén letilthatja a felhőszolgáltatásokhoz való hozzáférést.

A felhőszolgáltatásokhoz való hozzáférés blokkolása

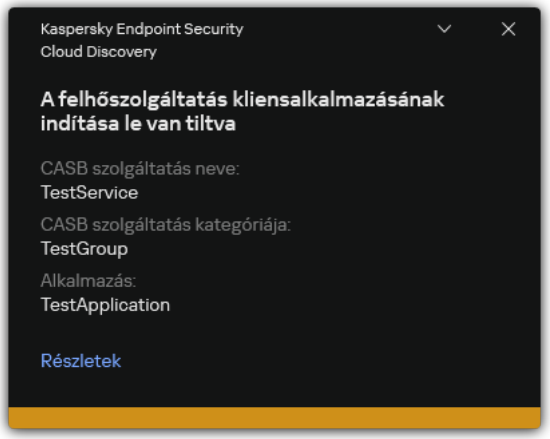
A felhőszolgáltatásokhoz való hozzáférés blokkolása csak a Kaspersky Next EDR Optimum és XDR Expert licenc esetében érhető el. Ez a funkció nem érhető el a Kaspersky Next EDR Foundations licenc esetében. Az alkalmazás funkcióinak összehasonlítását a Kaspersky Next licenc típusától függően a Kaspersky Next Súgóban találja.

A rendszergazda korlátozhatja a felhasználók hozzáférését a Cloud Discovery-kategóriákhoz vagy egyes felhőszolgáltatásokhoz. Így az adminisztrátor csak biztonságos felhőszolgáltatásokat engedélyezhet, és elkerülheti az adatszivárgást. A Cloud Discoveryben minden egyes felhőszolgáltatáshoz megjelenik a *kockázati szintre vonatkozó információ*. A kockázati szint segít kiszűrni azokat a szolgáltatásokat, amelyek nem felelnek meg a vállalat biztonsági követelményeinek.

A kockázati szint egy becslés, és nem minősíti a felhőszolgáltatás minőségét vagy annak szállítóját. A kockázati szint egyszerűen a Kaspersky szakértőinek ajánlása.

A felhőszolgáltatások kockázati szintjei a házirend **Cloud Discovery** szakaszában jelennek meg az összes ellenőrzött felhőszolgáltatás listájában.

A Kaspersky Endpoint Security egyéb összetevői védelmet nyújtanak a fenyegetésekkel szemben, és nyomon követik a gyanús felhasználói tevékenységeket a felhőszolgáltatások használata során.



Cloud Discovery értesítés

A Cloud Discovery nem blokkolja a Kaspersky Endpoint Security előtt indított felhőalkalmazásokat.

A felhőszolgáltatásokhoz való hozzáférés blokkolása a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Communication & Web Protection** → **Cloud Discovery** elemet.
5. Kapcsolja be az **Cloud Discovery ENABLED** kapcsolót.

   Megjelenik az összes felhőszolgáltatás listája. A felhőszolgáltatások kategóriákba vannak csoportosítva, például: *File sharing*, *Messengers*, *Email*. A Kaspersky szakértői rendszeresen frissítik a Cloud Discovery kategóriákat és a kategóriákba sorolt felhőszolgáltatásokat. A Kaspersky Endpoint Security az alkalmazás adatbázisával együtt frissíti a kategóriák és a felhőszolgáltatások készletét.
6. A(z) **Access** oszlopban található kapcsoló segítségével konfigurálhatja a felhőszolgáltatásokhoz való hozzáférést.
7. Mentse el a módosításokat.

Ennek eredményeképpen az alkalmazás ellenőrzi a felhőszolgáltatások használatát a böngészőben és a megfelelő alkalmazásokban.

Megbízható zóna

A *megbízható zóna* olyan, a rendszergazda által beállított objektumok és alkalmazások listája, melyeket a Kaspersky Endpoint Security aktív módban nem figyel.

A megbízható zónát a rendszergazda függetlenül, a kezelt objektumok tulajdonságai és a számítógépen telepített alkalmazások alapján hozhatja létre. Akkor válhat szükségessé objektumok és alkalmazások felvétele a megbízható zónába, ha a Kaspersky Endpoint Security egy olyan objektumhoz vagy alkalmazáshoz való hozzáférést blokkol, amelyről biztosan tudja, hogy ártalmatlan. A rendszergazda engedélyezheti a felhasználónak, hogy létrehozza a saját helyi megbízható zónáját egy adott számítógéphez. Így a felhasználók a házirendben található általános megbízható zóna mellett létrehozhatják a kizárásokra és megbízható alkalmazásokra vonatkozó saját listájukat is.

A Kaspersky Endpoint Security 12.5 for Windowstól kezdve lehetőség van az EDR telemetria hozzáadására a megbízható zónához. Ez lehetővé teszi az alkalmazás által a telemetriagyűjtő kiszolgálónak küldött adatok optimalizálását a Kaspersky Anti Targeted Attack Platform (EDR) megoldás számára.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon.

A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazást Light Agent üzemmódban is telepítheti a virtuális környezetek védelme céljából. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben.

Kizárás a vizsgálatból létrehozása

A *vizsgálatból való kizárás* olyan feltételkészlet, amelyet teljesíteni kell, hogy a Kaspersky Endpoint Security ne vizsgálja a vírusok és egyéb fenyegetések jelenlétét. A vizsgálatból való kizárások révén biztonsággal használhatók az olyan jogszerű szoftverek, amelyekkel a bűnözők károsíthatják a számítógépet vagy a személyes adatokat. Miközben ezeknek az alkalmazásoknak nincs rosszindulatú funkciója, a behatolók felhasználhatják őket rosszindulatú eljárásaik során. A betolakodók által a számítógép vagy a személyes adatok károsítására használható legitim szoftverekről részletes információkat a Kaspersky IT Encyclopedia webhelyen találhat.

Az ilyen alkalmazásokat a Kaspersky Endpoint Security blokkolhatja. A blokkolás megelőzése érdekében a használatban lévő alkalmazásoknál vizsgálatból való kizárásokat adhat meg. Ehhez fel kell venni a megbízható zónába a Kaspersky IT Encyclopedia által felsorolt nevet vagy névmaszkot. Például gyakran használhatja a Radmin alkalmazást a számítógépek távoli adminisztrációjához. A Kaspersky Endpoint Security az ilyen tevékenységet gyanúsnak tekinti, és előfordulhat, hogy blokkolja. Az alkalmazás blokkolásának megelőzése érdekében készítsen vizsgálatból való kizárást a Kaspersky IT Encyclopedia által megadott névvel vagy névmaszkkal.

Ha a számítógépre egy adatokat gyűjtő és azokat feldolgozásra továbbító alkalmazás van telepítve, a Kaspersky Endpoint Security rosszindulatú programként sorolhatja be ezt az alkalmazást. Ennek elkerülésére a Kaspersky Endpoint Security jelen dokumentumban leírt módon való konfigurálásával kizárhatja az alkalmazást a vizsgálatból.

A vizsgálatból való kizárásokat az alábbi alkalmazásösszetevők, valamint a rendszergazda által beállított feladatok használhatnak:

- Viselkedésészlelés
- Biztonsági rések kihasználásának megelőzése
- Behatolásmegelőző rendszer
- Fájl védelem
- Web védelem
- Levelezés védelem
- *Kártevő vizsgálata* feladat

A Kaspersky Endpoint Security nem vizsgálja az objektumokat, ha az azokat tartalmazó meghajtó vagy mappa valamelyik vizsgálati feladat megkezdésekor megtalálható a vizsgálat hatókörében. A vizsgálatból való kizárás azonban nem érvényes, ha az adott objektum egyéni vizsgálatára kerül sor.

A vizsgálati kizárások listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Vizsgálatból való kizárások létrehozásának menete az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.
4. A **Kizárások a vizsgálatból és megbízható alkalmazások → Kizárások a vizsgálatból** részen kattintson a **Beállítások** gombra.

   Ez megnyitja a kizárások listáját tartalmazó ablakot.
5. Válassza az **Merge values when inheriting** jelölőnégyzetet, ha egy összesített listát szeretne létrehozni a vállalat összes számítógépén lévő kizárásokról. A szülő és gyermek házirendjeiben lévő kizárási listák egyesítve lesznek. A lista egyesítve lesz, ha öröklésкor az értékek egyesítése öröklésкor engedélyezve van. A szülő házirendjében lévő kizárások a gyermek házirendjében csak olvasható nézetben jelennek meg. A szülő házirendjében lévő kizárásokat nem lehet módosítani vagy törölni.

6. Jelölje be a **Allow use of local exclusions** jelölőnégyzetet, ha szeretné engedélyezni a felhasználó számára a kizárások helyi listájának létrehozását. Így a felhasználó létrehozhatja a kizárások saját listáját, a házirendben létrehozott kizárások általános listája mellett. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.

   Ha a jelölőnégyzet nincs bejelölve, a felhasználó a kizárásoknak csak a házirendben létrehozott általános listájához férhet hozzá. Ezenkívül, ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security elrejti a vizsgálati kizárások összevont listáját az alkalmazás felhasználói felületén.

7. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

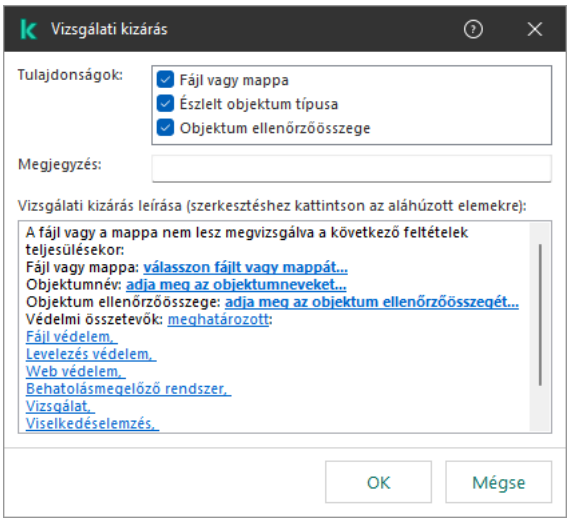
   - **Kategória**. A vizsgálati kizárásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy vizsgálati kizárást a kategóriához.

   - **Új kizárás**. A Kaspersky Endpoint Security egy új vizsgálati kizárást ad hozzá a lista gyökeréhez.

   - **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált vizsgálati kizárásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált vizsgálati kizárások is hozzá lettek adva. Előre definiált vizsgálati kizárásokat kell kiválasztania a védett kiszolgáló céljától függően.

   - **Új kizárás a kiválasztott kategóriában**. Ha új vizsgálati kizárást szeretne hozzáadni egy adott kategóriához, válassza ki a kategóriát.

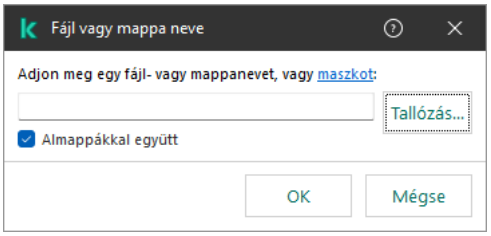
8. Fájl vagy mappa vizsgálatból való kizárása:



Kizárási beállítások

a. A **Properties** részben jelölje be a **File or folder** jelölőnégyzetet.

b. Kattintson a hivatkozásra az alábbi részen a **Fájl vagy mappa neve** ablak megnyitásához.



Válasszon fájlt vagy mappát

a. Adja meg a fájl vagy mappa nevét, illetve nevének a maszkját, vagy válassza ki a fájlt vagy mappát a mappaszerkezetben a **Tallózás** gombra kattintva.

maszkok használata:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `?:\Users\*\Folder\` maszkot.

A Kaspersky Endpoint Security támogatja a környezeti változókat

Kizárhatja a hálózati mappákat. Ehhez manuálisan adja meg a hálózati mappa elérési útját (például `\\Network Share\*`).

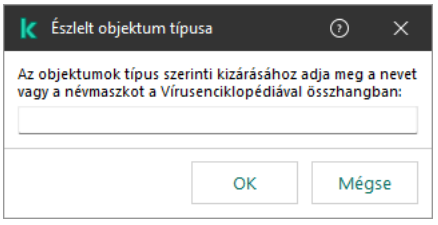
> A Kaspersky Endpoint Security nem támogatja a `%userprofile%` környezeti változót, amikor a Kaspersky Security Center konzol segítségével hozza létre a kizárások listáját. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a `*` karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást.

b. Mentse el a módosításokat.

9. Adott nevű objektumok kizárása a vizsgálatból:

a. A **Tulajdonságok** részben jelölje be az **Észlelt objektum típusa** jelölőnégyzetet.

b. Kattintson a hivatkozásra az alábbi részen az **Észlelt objektum típusa** ablak megnyitásához.



Objektum kiválasztása

a. Adja meg az objektumtípus nevét a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például `Email-Worm`, `Rootkit` vagy `RemoteAdmin`).

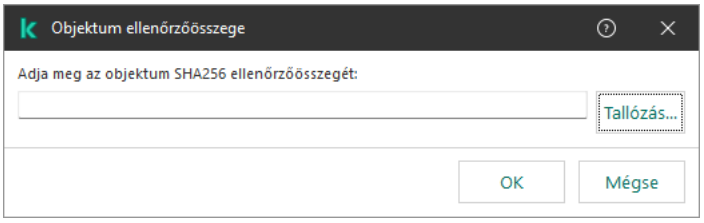
Használhat maszkokat a `?` karakterrel (bármely karaktert helyettesíti) és a `*` karakterrel (tetszőleges számú karaktert helyettesít). Például, ha a `Client*` maszk van megadva, a Kaspersky Endpoint Security kizárja a `Client-IRC`, `Client-P2P` és a `Client-SMTP` objektumokat is a vizsgálatokból.

b. Mentse el a módosításokat.

10. Ha ki szeretne zárni egy fájlt a vizsgálatokból:

a. A **Tulajdonságok** részben jelölje be az **Objektum ellenőrzőösszege** jelölőnégyzetet.

b. Kattintson a hivatkozásra az alábbi részen az **Objektum ellenőrzőösszege** ablak megnyitásához.



Fájl választása

a. Adja meg a fájl ellenőrzőösszeget vagy válassza ki a fájlt a **Tallózás** gombra kattintással.

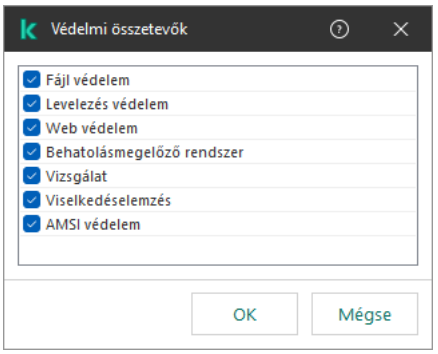
Ha a fájl megváltozik, a fájl ellenőrzőösszege is megváltozik. Ebben az esetben a módosított fájl nem lesz hozzáadva a kizárásokhoz.

b. Mentse el a módosításokat.

11. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

12. Adja meg, mely Kaspersky Endpoint Security összetevők használják a vizsgálatból való kizárást:

    a. Kattintson a hivatkozásra az alábbi részen a **Védelmi összetevők** ablak megnyitásához.



Védelmi összetevők kiválasztása

    a. Jelölje be a jelölőnégyzeteket azokkal az összetevőkkel szemben, amelyekben alkalmazni szeretné a vizsgálatból való kizárást.

    Ha a vizsgálatból való kizárás beállításaiban meg vannak adva összetevők, akkor a kizárás csak akkor jut érvényre, ha a Kaspersky Endpoint Security megadott összetevői végeznek vizsgálatot.

    Ha a vizsgálatból való kizárás beállításaiban nincsenek megadva összetevők, akkor a kizárás a Kaspersky Endpoint Security összes összetevője által végzett vizsgálat során érvényre jut.

13. Kattintson az **OK** gombra.

    Az új kizárás bekerül a listába. A kizárást bármikor letilthatja az objektum melletti jelölőnégyzet segítségével.

14. Mentse el a módosításokat.

Vizsgálatból kizárás létrehozásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Trusted Zone** szakaszt.

5. Az ablakban kattintson a **Malware Scan exclusions** hivatkozásra.

6. Válassza a **Merge values when inheriting** jelölőnégyzetet, ha egy összesített listát szeretne létrehozni a vállalat összes számítógépén lévő kizárásokról. A szülő és gyermek házirendjeiben lévő kizárási listák egyesítve lesznek. A lista egyesítve lesz, ha öröklésekor az értékek egyesítése öröklésekor engedélyezve van. A szülő házirendjében lévő kizárások a gyermek házirendjében csak olvasható nézetben jelennek meg. A szülő házirendjében lévő kizárásokat nem lehet módosítani vagy törölni.

7. Jelölje be a **Allow use of local exclusions** jelölőnégyzetet, ha szeretné engedélyezni a felhasználó számára a kizárások helyi listájának létrehozását. Így a felhasználó létrehozhatja a kizárások saját listáját, a házirendben létrehozott kizárások általános listája mellett. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.

   Ha a jelölőnégyzet nincs bejelölve, a felhasználó a kizárásoknak csak a házirendben létrehozott általános listájához férhet hozzá. Ezenkívül, ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security elrejti a vizsgálati kizárások összevont listáját az alkalmazás felhasználói felületén.

8. Kattintson a **Add** gombra, és válasszon ki egy műveletet:

   - **Category**. A vizsgálati kizárásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy vizsgálati kizárást a kategóriához.
   - **New exclusion**. A Kaspersky Endpoint Security egy új vizsgálati kizárást ad hozzá a lista gyökeréhez.
   - **Select exclusion from list**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált vizsgálati kizárásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált vizsgálati kizárások is hozzá lettek adva. Előre definiált vizsgálati kizárásokat kell kiválasztania a védett kiszolgáló céljától függően.

   Ha új vizsgálati kizárást szeretne hozzáadni egy adott kategóriához, jelölje be a kategória melletti jelölőnégyzetet, és válassza a **New exclusion** lehetőséget.

9. Válassza ki, hogyan kíván kizárást hozzáadni: **Path to the file or folder**, **Object type** vagy **Object hash**.

10. Ha ki szeretne zárni egy fájlt vagy mappát a vizsgálatból, adja meg manuálisan az elérési utat. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor:

    - A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
    - Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
    - A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

      Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `?:\Users\*\Folder\` maszkot.

      Kizárhatja a hálózati mappákat. Ehhez manuálisan adja meg a hálózati mappa elérési útját (például `\\Network Share\*`).

11. Ha egy adott típusú objektumot szeretne kizárni a vizsgálatokból, a(z) **Object type** mezőben adja meg az objektumtípus nevét a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például: `Email-Worm`, `Rootkit` vagy `RemoteAdmin`).

    Használhat maszkokat a `?` karakterrel (bármely karaktert helyettesíti) és a `*` karakterrel (tetszőleges számú karaktert helyettesít). Például, ha a `Client*` maszk van megadva, a Kaspersky Endpoint Security kizárja a `Client-IRC`, `Client-P2P` és a `Client-SMTP` objektumokat is a vizsgálatokból.

12. Ha ki szeretne zárni egy fájlt a vizsgálatokból, adja meg a fájl ellenőrzőösszeget a(z) **Object hash** mezőben.

    Ha a fájl megváltozik, a fájl ellenőrzőösszege is megváltozik. Ebben az esetben a módosított fájl nem lesz hozzáadva a kizárásokhoz.

13. A(z) **Apply exclusion to** blokkban válassza ki az összetevőket, amelyekre alkalmazni szeretné a kizárást a vizsgálatból.

14. Szükség esetén adjon meg rövid megjegyzést a **Comment** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

15. Kattintson az **OK** gombra.

    Az új kizárás bekerül a listába. Bármikor használhatja a kapcsolót egy kizárás megszüntetéséhez.

16. Mentse el a módosításokat.

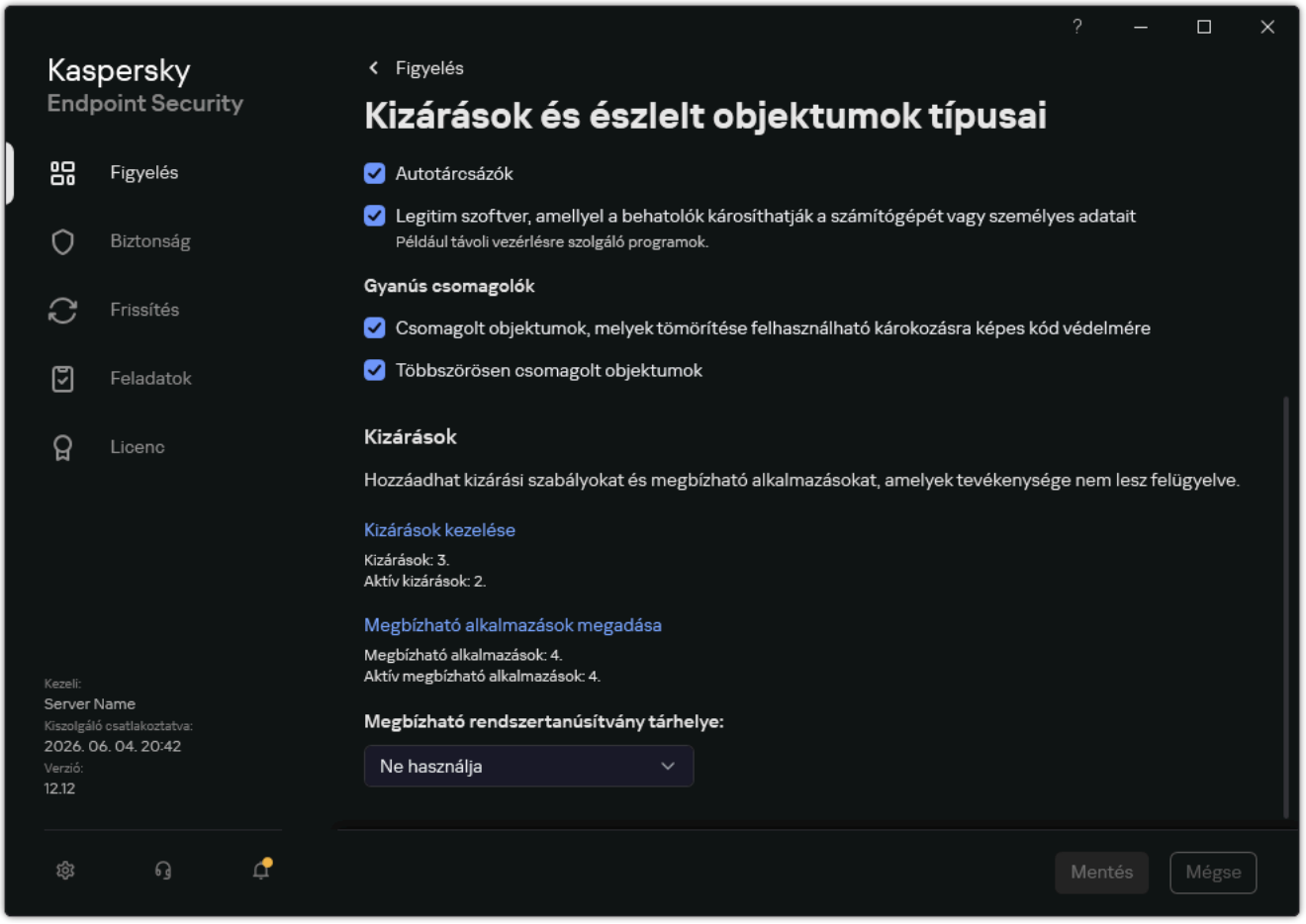
Vizsgálatból kizárás létrehozásának menete az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.

3. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

A Kaspersky Endpoint Security elrejti a vizsgálati kizárások listáját az alkalmazás felhasználói felületén, ha a konzolon a rendszergazda letiltotta a vizsgálati kizárások konfigurálását („zárt lakat" szimbólum), és a helyi vizsgálati kizárások tiltva vannak (a **Helyi kizárások használatának engedélyezése** jelölőnégyzet nincs bejelölve).



Kizárások beállításai

4. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

   - **Kategória**. A vizsgálati kizárásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy vizsgálati kizárást a kategóriához.
   - **Új kizárás**. A Kaspersky Endpoint Security egy új vizsgálati kizárást ad hozzá a lista gyökeréhez.
   - **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált vizsgálati kizárásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált vizsgálati kizárások is hozzá lettek adva. Előre definiált vizsgálati kizárásokat kell kiválasztania a védett kiszolgáló céljától függően.

   Ha új vizsgálati kizárást szeretne hozzáadni egy adott kategóriához, jelölje be a kategória melletti jelölőnégyzetet, és válassza az **Új kizárás** lehetőséget.

5. Ha ki szeretne zárni egy fájlt vagy mappát a vizsgálatokból, válassza ki a fájlt vagy mappát a **Tallózás** gombra kattintással.

Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

  Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `?:\Users\*\Folder\` maszkot.

  Kizárhatja a hálózati mappákat. Ehhez manuálisan adja meg a hálózati mappa elérési útját (például `\\Network Share\*`).

6. Ha egy adott típusú objektumot szeretne kizárni a vizsgálatokból, az **Észlelt objektum típusa** mezőben adja meg az objektumtípus nevét a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például: `Email-Worm`, `Rootkit` vagy `RemoteAdmin`).

   Használhat maszkokat a `?` karakterrel (bármely karaktert helyettesíti) és a `*` karakterrel (tetszőleges számú karaktert helyettesít). Például, ha a `Client*` maszk van megadva, a Kaspersky Endpoint Security kizárja a `Client-IRC`, `Client-P2P` és a `Client-SMTP` objektumokat is a vizsgálatokból.

7. Ha ki szeretne zárni egy fájlt a vizsgálatokból, adja meg a fájl ellenőrzőösszeget az **Objektumkivonat** mezőben.

   Ha a fájl megváltozik, a fájl ellenőrzőösszege is megváltozik. Ebben az esetben a módosított fájl nem lesz hozzáadva a kizárásokhoz.

8. A **Védelmi összetevők** blokkban válassza ki az összetevőket, amelyekre alkalmazni szeretné a kizárást a vizsgálatból.

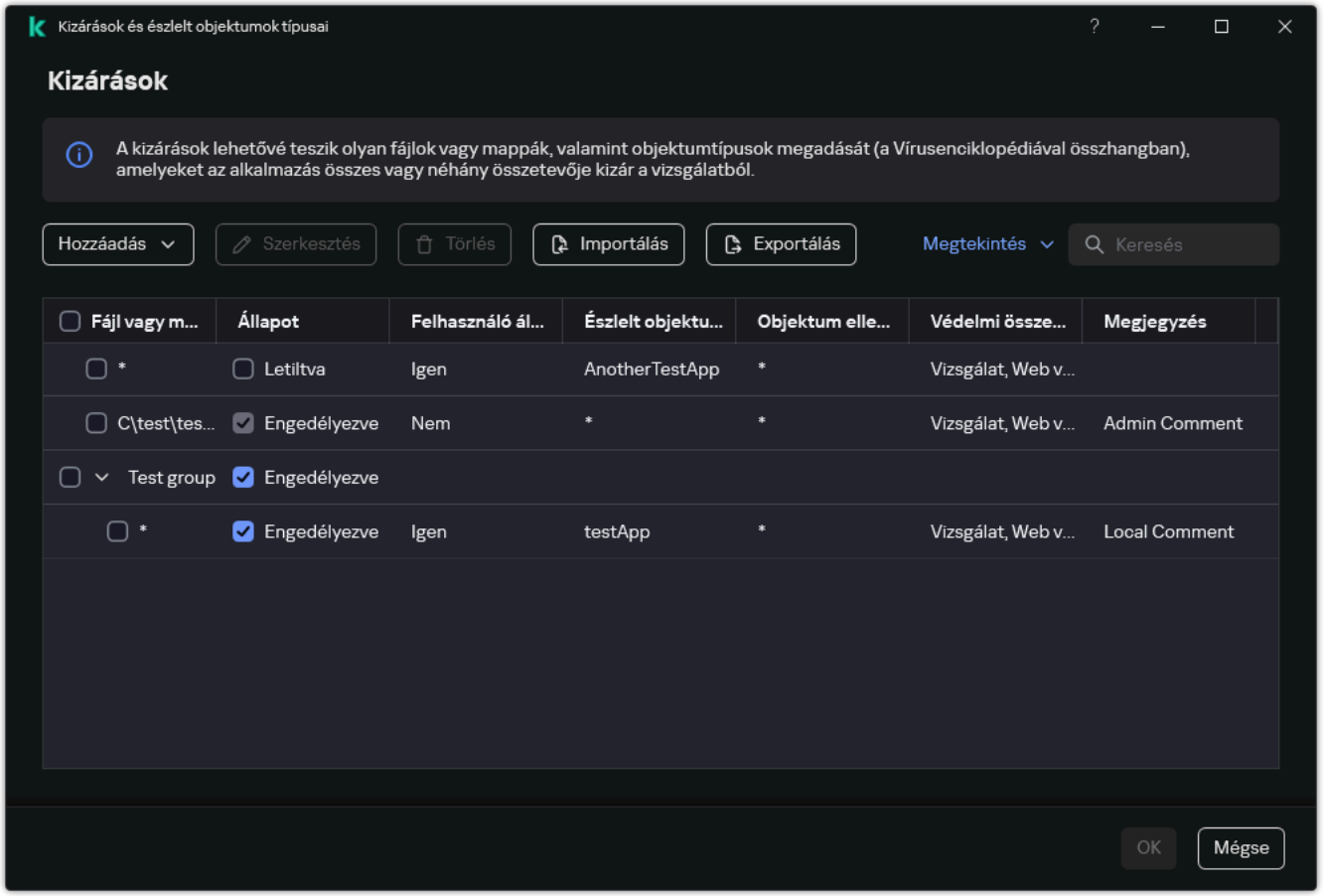
9. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

10. Válassza ki az **Aktív** állapotot a kizáráshoz.

11. Kattintson **Hozzáadás** gombra.

    Az új kizárás bekerül a listába. A kizárást bármikor letilthatja az **Állapot** oszlopban található jelölőnégyzet segítségével.

12. Mentse el a módosításokat.



Kizárások listája

Elérési út maszk példák:

Javasoljuk, hogy abszolút elérési utak helyett relatív útvonalakat adjon meg. Ez lehetővé teszi nemcsak a fájlrendszer-objektumok, hanem a fájl nélküli objektumok kizárását is. Például: `*\Program Files (x86)\Folder\Subfolder`.

Elérési utak a mappákban található fájlokhoz:

- A `*.exe` maszk tartalmazza az exe kiterjesztésű fájlok elérési útvonalait.
- A `example*` maszk tartalmazza a EXAMPLE nevű fájlok elérési útvonalát.

Elérési útvonalak a megadott mappákban található fájlokhoz:

- A `C:\dir\*.*` maszk tartalmazza a `C:\dir\` mappában található fájlok elérési útvonalát, azonban a `C:\dir\` almappa fájljaiét nem.
- A `C:\dir\*` maszk a `C:\dir\` mappában található összes fájl elérési útvonalát tartalmazza, beleértve az almappákat is.
- A `C:\dir\` maszk a `C:\dir\` mappában található összes fájl elérési útvonalát tartalmazza, beleértve az almappákat is.
- A `C:\dir\*.exe` maszk tartalmazza a `C:\dir\` mappában található, EXE kiterjesztésű fájlok elérési útvonalát, azonban a `C:\dir\` almappa fájljaiét nem.
- A `C:\dir\test` maszk tartalmazza a `C:\dir\` mappában található, „test” nevű fájlok elérési útvonalát, azonban a `C:\dir\` almappa fájljaiét nem.
- A `C:\dir\*\test` maszk a `C:\dir\` mappában és a `C:\dir\` almappáiban található összes „test” nevű fájl elérési útját tartalmazza.
- A `C:\dir1\*\dir3\` maszk tartalmazza a `C:\dir1\` mappában található első szintű dir3 almappák fájljainak elérési útvonalát.
- A `C:\dir1\**\dirN\` maszk tartalmazza a `C:\dir1\` mappában található bármilyen szintű dirN almappák fájljainak elérési útvonalát.

Elérési útvonalak a megadott nevű mappákban található fájlokhoz:

- A `dir\*.*` maszk tartalmazza a "dir" mappában található fájlok elérési útvonalát, azonban az almappák fájljaiét nem.
- A `dir\*` maszk tartalmazza a "dir" mappában található fájlok elérési útvonalát, azonban az almappák fájljaiét nem.
- A `dir\` maszk tartalmazza a "dir" mappában található fájlok elérési útvonalát, azonban az almappák fájljaiét nem.
- A `dir\*.exe` maszk tartalmazza a "dir" mappában található, EXE kiterjesztésű fájlok elérési útvonalát, azonban az almappák fájljaiét nem.
- A `dir\test` maszk tartalmazza a „dir” mappában található „test” nevű fájlok elérési útvonalát, azonban az almappák fájljaiét nem.

Kizárás létrehozása az észlelt objektumok típusa szerint

A Kaspersky Endpoint Security az észlelt objektumokat a következők szerint sorolja be:

- **Vírusok és férgek**

  Alkategória: vírusok és férgek (Viruses_and_Worms)

  Veszély szintje: magas

  A klasszikus vírusok és férgek a felhasználó által nem jóváhagyott műveleteket végeznek. Olyan másolatokat hozhatnak létre önmagukról, amelyek szintén képesek önmaguk másolására.

  Klasszikus vírus

  Miután egy klasszikus vírus a számítógépbe jut, megfertőz egy fájlt, aktiválódik, rosszindulatú műveleteket hajt végre, és önmaga másolataival lát el további fájlokat.

A klasszikus vírus csak a számítógép helyi erőforrásaiban sokszorozódik meg, saját magától másik számítógépre nem tud átjutni. Csak akkor kerül át másik számítógépre, ha saját magát bemásolja egy megosztott könyvtárba, egy behelyezett CD-re, vagy, ha a felhasználó továbbít egy email üzenetet, amelynek a csatolt fájlja fertőzött.

A klasszikus vírus kódja a számítógépek, operációs rendszerek vagy alkalmazások számos területét elérheti. A környezettől függően a vírusok lehetnek *fájl vírusok*, *boot vírusok*, *script vírusok* vagy *makróvírusok*.

A vírusok rendkívül sokféle módon fertőzhetnek fájlokat. A(z) *Overwriting* vírusok saját kódjukkal felülírják a fertőzött fájlt, így törölve annak tartalmát. A fertőzött fájl működése leáll, így nem lehet helyreállítani. A(z) *Parasitic* vírusok csak módosítják a fájlokat, azokat teljesen vagy részlegesen működőképes állapotban hagyva. A(z) *Companion* nem módosítják a fájlokat, csak másolatot készítenek róluk. Egy fertőzött fájlt megnyitva annak másolata (azaz tulajdonképpen a vírus) indul el. Az alábbi vírusok szintén megtalálhatók: *Link vírusok*, *OBJ-vírusok*, *LIB-vírusok*, *forráskódú* vírusok és számos egyéb.

Worm

A klasszikus vírusokhoz hasonlóan a férgek kódja akkor aktiválódik és hajt végre rosszindulatú műveleteket, ha már elterjedt a rendszerben. Azért féreg a neve, mert képes „átmászni” az egyik számítógépről a másikra a felhasználó engedélye nélkül, hogy számos adatcsatornán keresztül elterjessze a másolatait.

A különböző férgeket megkülönböztető fő tulajdonság az elterjedésük módja. Az alábbi táblázat áttekintést nyújt a férgek különféle típusairól, azok terjedésének módja alapján.

A férgek terjedésének módjai

Típus	Name	Leírás
E-mail-féreg	E-mail-féreg	Ezek e-mailen keresztül terjednek. A fertőzött e-mail tartalmaz egy a féreg másolatát tartalmazó csatolt fájlt, vagy egy hivatkozást egy webhelyre feltöltött, kifejezetten erre a célra feltört vagy létrehozott fájlhoz. Ha a felhasználó megnyitja a csatolt fájlt, a féreg aktiválódik. A hivatkozásra kattintva a fájlt letöltve, majd megnyitva a féreg szintén megkezdi a rosszindulatú műveleteket. Ezután megkezdi lemásolni saját magát, újabb e-mail címek keresésébe kezd, és terjeszteni kezdi a fertőzött üzeneteket.
IM-Worm	IM kliens férgek	Azonnali üzenetküldőkön keresztül terjednek. Az ilyen férgek rendszerint a felhasználó partnerlistáját felhasználva üzenetet küldenek, benne egy adott webhelyen, a féreg másolatát tartalmazó fájlra mutató hivatkozással. Amikor a felhasználó letölti és megnyitja a fájlt, a féreg aktiválódik.
IRC-Worm	Internetes csevegési férgek	Ezek olyan Internet Relay Chats szolgáltatásokon keresztül terjednek, amelyek valós idejű kommunikációt biztosítanak az interneten keresztül. Az ilyen férgek az internetes csevegésben egy önmagukat tartalmazó fájlt adnak közre, vagy egy hivatkozást a fájlra. Amikor a felhasználó letölti és megnyitja a fájlt, a féreg aktiválódik.
Net-Worm	Hálózati férgek	Ezek a férgek számítógépes hálózatokon terjednek. A többi féreggel ellentétben a tipikus hálózati féreg a felhasználó beavatkozása nélkül terjed. A féreg átvizsgálja a helyi hálózaton található számítógépeket, és sebezhetőséget jelentő programokat keres. Ehhez erre a célra létrehozott hálózati programcsomagokat küld szét (amik a biztonsági rések kiaknázását végzik), benne a féreg kódjával. Ha egy „sebezhető” számítógép található a hálózaton, az megkapja az ilyen hálózati csomagot. Amint a féreg teljesen bejutott a számítógépbe, azonnal aktiválódik.
P2P-Worm	Fájlcserélő hálózati férgek	Fájlcserélő (Peer-to-Peer) hálózatokon keresztül terjednek. A P2P hálózatba való bejutáshoz a féreg bemásolja magát a fájlcsere mappába, amely rendszerint a felhasználó számítógépén található. A P2P hálózat információkat jelenít meg a fájlról, így a felhasználó a többi fájlhoz hasonlóan „megtalálja” a fertőzött fájlt a hálózaton, majd letölti és megnyitja. A kifinomultabb férgek adott P2P-hálózat protokollját is képesek emulálni: ezek pozitív válaszokat küldenek a keresésekre, majd felajánlják saját másolatukat letöltésre.
Worm	Egyéb típusú férgek	Az egyéb típusú férgek a következők lehetnek: • Saját másolataikat hálózati erőforrásokon át terjesztő férgek. Az operációs rendszer funkcióit kihasználva ezek megvizsgálják az elérhető hálózati mappákat, más számítógépekhez kapcsolódnak az interneten keresztül, és megkísérlik azok lemezmeghajtói felett átvenni a teljes uralmat. A fent ismertetett férgekkel ellentétben mások maguktól nem aktiválódnak, csak akkor, ha a felhasználó megnyitja a féreg egy másolatát tartalmazó fájlt. • Olyan férgek, amelyek a táblázatban ismertetett módok egyikét sem használják az elterjedésre (pl. a mobiltelefonokon terjedő férgek).

- **Trójai programok (köztük zsarolóprogramok)**

  Alkategória: Trójai programok

  Veszély szintje: magas

  A férgekkel és vírusokkal ellentétben a trójai programok nem szaporítják magukat. A számítógépet például e-mailen vagy böngészőn át szállják meg, amikor a felhasználó fertőzött weboldalt látogat meg. A trójai programok a felhasználó közreműködésével indulnak el. Rosszindulatú működésüket közvetlenül az elindulásukat követően kezdik meg.

  A különböző trójai programok eltérően viselkednek a fertőzött számítógépeken. A „trójai" fő funkciói az információk blokkolása, módosítása vagy megsemmisítése, leállítva ezzel számítógépeket, hálózatokat. Ezen kívül a trójai programok fájlokat fogadnak és küldenek, futtatják azokat, üzeneteket jelenítenek meg a képernyőn, weboldalaknak küldenek kérést, programokat töltenek le és telepítenek, valamint újraindítják a számítógépet.

  A hackerek gyakran különböző trójai programok „készletét" alkalmazzák.

  Az alábbi táblázat a trójai programok viselkedéstípusait ismerteti.

  Trójai programok viselkedése fertőzött számítógépen

Típus	Name	Leírás
Trojan-ArcBomb	Trójai programok – „archívumbombák"	Kicsomagoláskor az archívumok mérete megnő, ami kihat a számítógép működésére. Az ilyen archívum kicsomagolásakor a számítógép működése lelassul, esetleg lefagy és a merevlemez megtelhet „üres" adatokkal. Az „archívumbombák" különösen nagy veszélyt jelentenek fájl és levelező kiszolgálókra. Ha a kiszolgáló automatikus rendszert használ a beérkező információk feldolgozására, az „archívumbomba" leállíthatja a működését.
Backdoor	Távoli rendszerfelügyeletet lehetővé tevő trójai programok	Az összes közül ezek a legveszélyesebb trójai programok. Funkciójuk alapján hasonlítanak a számítógépre telepített rendszerfelügyeleti alkalmazásokhoz. Ezek a programok a felhasználó tudtán kívül telepítik magukat a számítógépre, lehetővé téve, hogy a betolakodó távolról átvegye az uralmat a gép felett.
Trojan	Trójai programok	Ez a kategória az alábbi rosszindulatú alkalmazásokat tartalmazza: • **Klasszikus trójai programok**. Ezek a programok csak a trójai programok fő funkcióit látják el, melyek a következők: az információk blokkolása, módosítása vagy megsemmisítése és a számítógépek, hálózatok leállítása. Nem rendelkeznek olyan speciális funkciókkal, mint a táblázatban szereplő más típusok. • **Sokoldalú trójai programok**. Ezek a programok számos trójai programra jellemző speciális funkcióval rendelkeznek.
Trojan-Ransom	Váltságdíj trójai	Ezek a felhasználó adatait „túszul ejtik", módosítva vagy blokkolva azt, esetleg meggátolják a számítógép működését, hogy a felhasználó számára elvesszenek az adatok. A betolakodó váltságdíjat követel a felhasználótól, azt ígérve, hogy küld egy alkalmazást, amellyel visszaállítható a számítógép normál állapota az elveszett adatokkal együtt.
Trojan-Clicker	Trójai kattintók	Ezek a felhasználó számítógépéről weboldalakat látogatnak meg, saját maguk utasítva a webböngészőt, vagy módosítva az operációs rendszer fájljaiban megadott webcímet. Az ilyen programokkal a betolakodó hálózati támadást indíthat, valamint webhelyek látogatottságát növelheti, hogy a reklámcsíkhirdetések megjelenítésének a száma növekedjen.
Trojan-Downloader	Trójai-letöltők	Ezek a betolakodó weboldaláról további rosszindulatú alkalmazásokat töltenek le és telepítenek a felhasználó számítógépére. A letöltendő rosszindulatú alkalmazás fájlnevét tartalmazhatják, illetve megkaphatják a meglátogatott weboldalról is.
Trojan-Dropper	Trójaitelepítők	Más trójai programokat tartalmaznak, melyeket a számítógép merevlemezére mentenek, majd telepítenek. A betolakodók a telepítő típusú trójai programokat az alábbi célokból használhatják: • Rosszindulatú alkalmazás telepítése a felhasználó tudtán kívül: A trójai telepítőprogramok nem jelenítenek meg rendszerüzeneteket, vagy hamis információkat jelenítenek meg például tömörített fájl hibájáról, esetleg az operációs rendszer inkompatibilis verziójáról. • Más ismert rosszindulatú alkalmazások megvédése a felfedezéstől: nem minden vírusirtó szoftver képes felismerni a trójai telepítőprogramon belül a rosszindulatú alkalmazást.

Típus	Name	Leírás
Trojan-Notifier	Trójai-értesítők	Tájékoztatják a betolakodót, hogy a fertőzött számítógép hozzáférhető, és elküldik neki a számítógép adatait: az IP-címet, a megnyitott port számát, illetve az e-mail-címet. Kapcsolatba lépnek a betolakodóval e-mailben vagy FTP-n, weboldalának meglátogatásával vagy más módon. Ezek a programok gyakran több trójai programból álló programcsomag részét képezik. Ezek értesítik a betolakodót a többi trójai program sikeres telepítéséről.
Trojan-Proxy	Trójai-proxyk	Segítségükkel a betolakodó névtelenül érhet el weboldalakat a felhasználó számítógépéről; gyakran alkalmazzák őket levélszemét küldésére.
Trojan-PSW	Jelszólopó programok	A jelszólopók olyan típusú trójai programok, amelyek felhasználói fiókokat törnek fel, például szoftver regisztrációs adatait szerzik meg. A bizalmas adatokat a rendszerfájlokban és a regisztrációs adatbázisban érik el, majd elküldik azokat a „támadónak” e-mail, FTP útján, meglátogatva a weboldalát, esetleg más módon. Néhány ilyen trójai program a táblázat által tárgyalt külön kategóriába sorolható. Ezek a bankfiók adatokat lopó trójai programok (Trojan-Banker), az azonnali üzenetküldő programok felhasználóitól adatokat lopó trójai programok (Trójai-IM) valamint online játékok felhasználóitól adatokat lopó trójai programok (Trojan-GameThief).
Trojan-Spy	Trójai-kémek	Ezek kémkednek a felhasználó után, információkat gyűjtenek az általa a számítógépen végzett műveletekről. Eltéríthetik a felhasználó által a billentyűzeten begépelt adatokat, képernyőképet készíthetnek, vagy elkészíthetik az aktív alkalmazások teljes listáját. Miután megszerezték az információkat, eljuttatták azokat a betolakodónak e-mail, FTP útján, a weboldalát meglátogatva vagy más módon.
Trojan-DDoS	Trójai hálózattámadók	Az ilyen programok a felhasználó számítógépéről rengeteg kérést küldenek egy távoli kiszolgálóra. A kiszolgáló az összes kérésre reagálva kifogy az erőforrásaiból, és leáll (Denial-of-Service, vagy DoS). A hackerek gyakran több számítógépet is megfertőznek ilyen programokkal, hogy több párhuzamos támadást indíthassanak egyetlen kiszolgáló ellen. A DoS programok egy számítógépről a felhasználó tudtával indítanak támadást. A DDoS (elosztott DoS) programok több számítógépről a fertőzött számítógép felhasználójának a tudta nélkül indítanak elosztott támadást.
Trojan-IM	Azonnali üzenetküldő ügyfelek felhasználóitól adatokat lopó trójai programok	Ellopják az azonnali üzenetküldők felhasználóinak számlaszámait és jelszavait. Az információkat eljuttatják a betolakodónak e-mail, FTP útján, a weboldalát meglátogatva vagy más módon.
Rootkit	Rootkitek	Ezek más rosszindulatú alkalmazásokat és azok tevékenységét maszkolják, így meghosszabbítva azok jelenlétét az operációs rendszerben. Emellett a fertőzött számítógép memóriájában olyan fájlokat, folyamatokat vagy beállításkulcsokat rejtenek el, amelyek rosszindulatú alkalmazásokat futtatnak. A rootkitek maszkolhatnak adatcserét alkalmazások között a felhasználó számítógépén és a hálózaton található számítógépek között.
Trojan-SMS	SMS-üzenetek formájában megjelenő trójai programok	Ezek mobiltelefonokat fertőznek meg, SMS-üzeneteket küldve fizetős telefonszámokra.
Trojan-GameThief	Online játékok felhasználóitól adatokat lopó trójai programok	Ezek online játékok résztvevőitől lopnak fiókbejelentkezéseket, aztán eljuttatják a betolakodónak e-mailben, FTP-n, a weboldala meglátogatásával vagy más módon.
Trojan-Banker	Bankszámlaadatokat lopó trójai programok	Ezek bankszámlaadatokat vagy elektronikus fizetési rendszeradatokat lopnak, aztán → eljuttatják a hackernek e-mailben, FTP-n, a weboldala meglátogatásával vagy más módon.
Trojan-Mailfinder	E-mail címeket gyűjtő trójai programok	Ezek a számítógépen található e-mail címeket gyűjtik össze, aztán eljuttatják a betolakodónak e-mail, FTP útján, a weboldalát meglátogatva vagy más módon. A betolakodók az összegyűjtött címekre aztán levélszemetet küldenek.

- **Rosszindulatú eszközök**

  Alkategória: Rosszindulatú eszközök

  Veszély szintje: közepes

  A többi rosszindulatú programmal ellentétben a rosszindulatú eszközök az elindítás után közvetlenül nem kezdik el a működésüket. Ily módon biztonságosan menthetők és elindíthatók a felhasználó számítógépén. A betolakodók az ilyen programok funkcióit gyakran használják vírusok, férgek és trójai programok létrehozására, hálózati támadások indítására távoli kiszolgálók ellen, számítógépek feletti uralom átvételére vagy más rosszindulatú műveletek végrehajtására.

  A rosszindulatú eszközök különböző funkciói az alábbi táblázat szerint csoportosíthatók.

Típus	Name	Leírás
Constructor	Konstruktorok	Ezek segítségével hozhatók létre új vírusok, férgek és trójai programok. Néhány konstruktor szabványos ablakalapú felülettel rendelkezik, ahol a felhasználó kiválaszthatja a létrehozni kívánt rosszindulatú alkalmazás típusát, a hibakeresésre adandó választ és egyéb tulajdonságokat.
Dos	Hálózati támadások	Az ilyen programok a felhasználó számítógépéről rengeteg kérést küldenek egy távoli kiszolgálóra. A kiszolgáló az összes kérésre reagálva kifogy az erőforrásaiból, és leáll (Denial-of-Service, vagy DoS).
Exploit	Biztonsági rések	Az *exploit* olyan adatcsomag vagy programkód, amely az alkalmazás sebezhetőségét megkeresve, azt kihasználva rosszindulatú műveletbe kezd a számítógépen. Például az exploit fájlokat ír és olvas, vagy kérést küld „fertőzött" weboldalaknak. A különböző exploitok különböző alkalmazások vagy hálózati szolgáltatások sebezhetőségét használják ki. Az exploit hálózati csomagnak álcázva magát a hálózaton keresztül számos számítógépbe eljut, sebezhető hálózati szolgáltatásokkal rendelkező számítógépeket keresve. A DOC fájlban működő exploit a szövegszerkesztő program sebezhetőségét használja ki. A készítője által beprogramozott műveletet akkor kezdi végrehajtani, amikor a felhasználó megnyitja a fertőzött fájlt. Az e-mail üzenetbe ágyazott exploit az e-mail kliens sebezhetőségeit keresi. A rosszindulatú műveletet akkor kezdi végrehajtani, amikor a felhasználó megnyitja a fertőzött üzenetet az e-mail kliensben. A hálózati férgek a hálózaton exploitok segítségével terjednek. A Nuker exploitok számítógépeket leállító hálózati csomagok.
FileCryptor	Titkosítók	Ezek más rosszindulatú alkalmazásokat titkosítanak, hogy elrejtsék azokat a víruskereső alkalmazások elől.
Flooder	Hálózatokat „szennyező" programok	Ezek nagy mennyiségű üzenetet küldenek hálózati csatornákon. Az ilyen eszközök között találhatók az internetes csevegéseket szennyező programok is. Az elárasztó eszközök nem tartalmaznak e-mail, IM-kliens és mobilkommunikációs rendszerek csatornáit „eltömítő" programokat. Az ilyen programok külön típusként (e-mail-elárasztó, IM-elárasztó és SMS-elárasztó) szerepelnek ebben a táblázatban.
HackTool	Hackelő eszközök	Az ilyenek teszik lehetővé azon számítógép feletti uralom átvételét, amelyre feltelepültek, vagy más számítógépek megtámadását (például új rendszerfiók felvételét a felhasználó engedélye nélkül, a rendszernapló törlését, hogy elrejthető legyen a jelenlétük az operációs rendszerben). Ebbe a típusba tartoznak némely szimatoló programok, amelyek jelszavakat térítenek el. A Szimatolók olyan programok, amelyek a hálózati forgalmat képesek megjeleníteni.
Hoax	Hoaxok	Az ilyenek a felhasználót vírus jellegű üzenetekkel riogatják: ezek nem fertőzött fájlban is „észlelik a vírust", vagy olyan formázásról értesítik a felhasználót, ami a valóságban nem történik meg.
Spoofer	Hamisító eszközök	Ezek a feladó hamis címéről küldenek üzeneteket és hálózati kéréseket. A behatolók hamisító jellegű eszközöket alkalmaznak, hogy például üzenetek valódi feladóinak adják ki magukat.
VirTool	Rosszindulatú alkalmazásokat módosító eszközök	Ezek lehetővé teszik más rosszindulatú programok módosítását, hogy elrejtsék azokat víruskereső alkalmazások elől.
Email-Flooder	E-mail címeket „szennyező" programok	Ezek nagy mennyiségű üzenetet küldenek számos e-mail címre, így„szennyezve" azokat. A nagy mennyiségű beérkező üzenet gátolja a felhasználót a hasznos üzenetei kezelésében.
IM-Flooder	Az azonnali üzenetküldők forgalmát SMS üzenetekkel „szennyező" programok	Az azonnali üzenetküldők felhasználóit elárasztják üzenetekkel. Az üzenetek nagy száma akadályozza a felhasználót a hasznos üzenetek kezelésében.
SMS-Flooder	A forgalmat SMS üzenetekkel „szennyező" programok	Ezek nagy mennyiségű SMS-üzenetet küldenek a mobiltelefonra.

- **Reklámprogram**

  Alkategória: hirdetési szoftver (reklámprogram)

  Veszély szintje: közepes

A reklámprogram a felhasználó számára biztosít reklámokat. A reklámprogram más program kezelőfelületén reklámcsík hirdetést jelenít meg, és a kereső kérését a hirdető weboldalára irányítja. Néhányuk marketinginformációkat gyűjt a felhasználóról, majd elküldi a fejlesztőnek: ezek az információk a felhasználó által meglátogatott weboldalak neveit, az általa használt keresési kulcsszavakat tartalmazhatják. A trójai kémprogramokkal ellentétben a reklámprogramok ezeket az adatokat a felhasználó beleegyezésével küldik el a fejlesztőnek.

- **Autotárcsázók**

  Alkategória: autotárcsázók (tárcsázó).

  Veszély szintje: közepes

  Az automata tárcsázók a modem segítségével titokban telefonkapcsolatot tudnak létrehozni.

- **Legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait**

  Alkategória: legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.

  Veszély szintje: közepes

  A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetek IRC-kliensek, tárcsázók, fájlletöltő programok, számítógépes rendszertevékenység-figyelők, jelszókezelők, internetkiszolgálók FTP, HTTP, és Telnet szolgáltatásokhoz.

  Mindazonáltal ha a betolakodók hozzáféréssel rendelkeznek az ilyen programokhoz vagy bejuttatják a felhasználó számítógépébe, akkor néhány funkciójukat a biztonság feltörésére használhatják.

  Ezeknek az alkalmazásoknak eltérőek a funkcióik; az alábbi táblázat a típusaikat tartalmazza.

Típus	Name	Leírás
Client-IRC	Internet csevegő kliensek	A felhasználó az ilyen programokat másokkal való kapcsolattartásra használja internetes csevegéseken. A betolakodók ezeken a programokon keresztül terjesztik a rosszindulatú programokat.
Downloader	Letöltéshez használható programok	Ezek rejtve töltenek le fájlokat különböző weboldalakról.
Monitor	Monitorozásra alkalmas programok	Ezek monitorozást tesznek lehetővé azon a számítógépen, amelyre feltelepültek (azt figyelve, hogy mely alkalmazások aktívak, és azok miként folytatják az adatcserét más számítógépekre telepített programokkal).
PSWTool	Jelszó visszaállítók	Ezek elfelejtett jelszavak megtekintését és helyreállítását teszik lehetővé. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal:
RemoteAdmin	Távoli rendszerfelügyeletet lehetővé tevő programok	Ezeket széles körben alkalmazzák rendszergazdák. A programok a távoli számítógép kezelőfelületét teszik elérhetővé, annak monitorozása és felügyelése céljából. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal: a távoli számítógép monitorozása és felügyelete céljából. A legális távfelügyeleti programok különböznek a hátsó kapu típusú trójai távfelügyeleti programoktól. A trójai programok jellegzetessége, hogy függetlenül bejutnak az operációs rendszerbe, és magukat feltelepítik; a jogszerű programok nem rendelkeznek ilyen funkcióval.
Server-FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Server-Proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Server-Telnet	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Server-Web	Webkiszolgálók	Ezek webkiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy HTTP-n keresztül távoli elérést nyissanak hozzá.

Típus	Name	Leírás
RiskTool	Helyi számítógépen történő munkavégzésre szolgáló eszközök	A felhasználó számára további lehetőségeket biztosítanak, amikor a számítógépén dolgozik. Az eszköz segítségével a felhasználó aktív alkalmazások ablakait, fájljait rejtheti el, és aktív folyamatokat állíthat le.
NetTool	Hálózati eszközök	A felhasználó számára további lehetőségeket biztosítanak, amikor a hálózaton más számítógépeken dolgozik. Segítségével újraindíthatja a távoli gépeket, felderítheti a nyitott portokat, és a távoli gépre telepített alkalmazásokat futtathat.
Client-P2P	P2P hálózati ügyfelek	Segítségükkel a felhasználó fájlcserélő (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.
Client-SMTP	SMTP-kliensek	E-mail üzeneteket küldenek a felhasználó tudta nélkül. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
WebToolbar	Webes eszköztárak	Ezek eszköztárakkal egészítik ki más alkalmazások kezelőfelületeit, keresőmotorok elérését megkönnyítve.
FraudTool	Pszeudoprogramok	Ezek más programoknak adják ki magukat. Lehetnek például pszeudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.

- **Csomagolt objektumok, melyek tömörítése felhasználható károkozásra képes kód védelmére**

  Alkategória: csomagolt fájlok, amelyek kárt okozhatnak.

  Veszély szintje: közepes.

  A fájl csomagolása egy speciális csomagolóprogrammal történik, amelyet rosszindulatú programok (vírusok, férgek, trójaiak) csomagolására használnak. A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található önkicsomagoló modult ellenőrzi.

  A hackerek a kártevőket speciális csomagolóprogramok segítségével csomagolják be, hogy elrejtsék azokat a vírusirtók észlelése elől. A Kaspersky szakértői azonosították a hackerek által leggyakrabban alkalmazott csomagolóprogramokat.

- **Többszörösen csomagolt objektumok**

  Alkategória: többszörösen csomagolt fájlok.

  Veszély szintje: közepes.

  A fájl háromszor vagy többször van becsomagolva egy vagy több csomagolóprogrammal.

  Ahhoz, hogy a vírusirtók ne észleljék a kártevőket, a hackerek többször is becsomagolhatnak egy fájlt. A Kaspersky Endpoint Security vizsgálja a csomagolt fájlokat.

Alapértelmezés szerint a Kaspersky Endpoint Security bármilyen típusú objektumot észlel. Javasoljuk, hogy hagyja engedélyezve az összes típusú objektum észlelését a számítógép biztonságának javítása érdekében. Ha olyan házon belüli segédprogramokat használ, amelyeket az alkalmazás rosszindulatúként észlel, adja hozzá ezeket a segédprogramokat egy kizárási listához, de ne tiltsa le az ilyen objektumok teljes típusának az észlelését.

Az észlelhető objektumok típusainak kiválasztása az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

4. A szabályzat ablakban válassza ki az **Általános beállítások** → **Jelentések és objektumtípusok** részt.
5. Az **Észlelt objektumok típusai** blokkban kattintson a **Beállítások** gombra.
6. A megnyíló ablakban jelölje be a négyzeteket azokkal az objektumtípusokkal szemben, amelyeket észlelni szeretne a Kaspersky Endpoint Security alkalmazással:
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az észlelhető objektumtípusok kiválasztása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

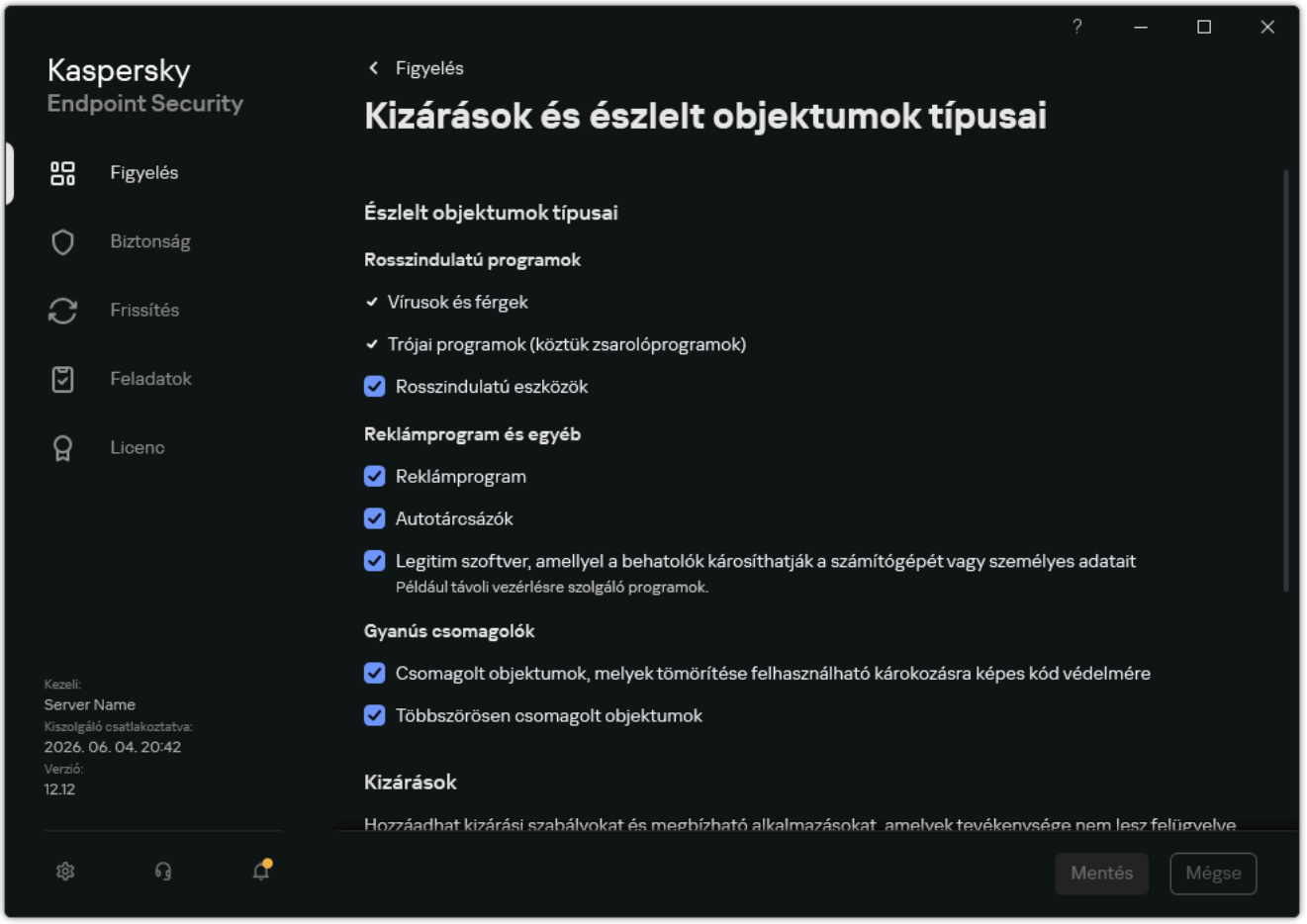
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Detection Settings** elemet.
5. A(z) **Detection of other types of objects**blokkban jelölje be a négyzeteket azokkal az objektumtípusokkal szemben, amelyeket észlelni szeretne a Kaspersky Endpoint Security alkalmazással:
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az észlelhető objektumok típusainak kiválasztása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Kizárások és észlelt objektumok típusai** lehetőséget.

3. Az **Észlelt objektumok típusai** területen jelölje be a jelölőnégyzeteket azokkal az objektumtípusokkal szemben, amelyeket észlelni szeretne a Kaspersky Endpoint Security alkalmazással.

4. Mentse el a módosításokat.



Észlelhető objektumok típusai

A megbízható alkalmazások listájának szerkesztése

A *megbízható alkalmazások listája* azon alkalmazások listája, amelyeknek fájl- és hálózati tevékenységét (ideértve a rosszindulatú tevékenységet is) és a rendszer beállításjegyzékéhez való hozzáférését a Kaspersky Endpoint Security nem kíséri figyelemmel. A Kaspersky Endpoint Security alapértelmezés szerint figyeli a megnyitott, végrehajtott vagy bármilyen alkalmazásfolyamat által mentett objektumokat, és felügyeli az összes alkalmazás tevékenységét és az általuk generált hálózati forgalmat. Miután egy alkalmazás felkerült a megbízható alkalmazások listájára, a Kaspersky Endpoint Security nem figyeli tovább az alkalmazás tevékenységét.

A különbség a vizsgálati kizárások és a megbízható alkalmazások között az, hogy a kizárások esetében a Kaspersky Endpoint Security nem vizsgálja a fájlokat, míg a megbízható alkalmazások esetében nem ellenőrzi az indított folyamatokat. Ha egy megbízható alkalmazás rosszindulatú fájlt hoz létre egy olyan mappában, amely nem szerepel a vizsgálati kizárások között, a Kaspersky Endpoint Security észleli a fájlt, és megszünteti a fenyegetést. Ha a mappa hozzá van adva a kizárásokhoz, a Kaspersky Endpoint Security kihagyja ezt a fájlt.

Ha például a Microsoft Windows Jegyzettömb szabványos alkalmazás által használt objektumokat biztonságosnak tekinti, azaz megbízik ebben az alkalmazásban, akkor felveheti a megbízható alkalmazások listájára, így az általa használt objektumok nem kerülnek megfigyelésre. Ez növeli a számítógép teljesítményét, ami különösen fontos a kiszolgálói alkalmazások használatakor.

Ezenkívül bizonyos, a Kaspersky Endpoint Security által gyanúsként osztályzott műveletek számos alkalmazás funkcióinak kontextusában biztonságos lehet. A billentyűzeten begépelt szöveg rögzítése például az automatikus billentyűzetkiosztás-átváltók esetén rutinszerű eljárás (ilyen például a Punto Switcher). Az ilyen alkalmazások jellemzőinek figyelembe vételéhez és tevékenységük figyelésből való kizárásához célszerű őket a megbízható alkalmazások listájára felvenni.

A megbízható alkalmazások segítenek elkerülni a Kaspersky Endpoint Security és más alkalmazások közötti kompatibilitási problémákat (például egy külső számítógép hálózati forgalmának a Kaspersky Endpoint Security és egy másik vírusirtó alkalmazás általi kettős vizsgálatát).

A megbízható alkalmazás végrehajtható fájljában és folyamatában ugyanakkor továbbra is sor kerül a vírusok és egyéb rosszindulatú programok jelenlétének vizsgálatára. Egy alkalmazás teljes mértékben kizárható a Kaspersky Endpoint Security vizsgálatából a vizsgálati kizárások segítségével.

A megbízható alkalmazások listájának módosítását a szülőházirend tulajdonságai blokkolhatják. A lista módosításához engedélyeznie kell a megbízható zóna beállításainak módosítását a Web Console-ban (a „lakat" nyitva kell legyen).

A megbízható zónák másként vannak csoportosítva a Felügyeleti konzolon (MMC) és a Web Console-on. Hasonlóképpen, a megbízható zóna paramétereinek módosítását is másféleképpen lehet megelőzni (különböző „lakatok" használatával). Javasoljuk, hogy az alkalmazás kezeléséhez csak a Web Console-t használja. Ha a megbízható zónát különböző konzolokon konfigurálja, az adminisztrációs bővítménnyel visszaállíthatja a „lakatot" az alapértelmezett állapotra.

Alkalmazás megbízható listához való hozzáadásának menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.
4. A **Kizárások a vizsgálatból és megbízható alkalmazások → Megbízható alkalmazások** területen kattintson a **Beállítások** gombra.

   Ez megnyitja a megbízható alkalmazások listáját tartalmazó ablakot.
5. Válassza az **Merge values when inheriting** jelölőnégyzetet, ha egy összesített listát szeretne létrehozni a vállalat összes számítógépén lévő megbízható alkalmazásról. A szülő és gyermek rendszabályokban lévő megbízható alkalmazások listája egyesítve lesz. A lista egyesítve lesz, ha öröklésekor az értékek egyesítése öröklésekor engedélyezve van. A szülő rendszabályban lévő megbízható alkalmazások a gyermek rendszabályokban csak olvasható nézetben jelennek meg. A szülő rendszabályban lévő megbízható alkalmazásokat nem tudja módosítani vagy törölni.
6. Jelölje be a **Allow use of local trusted applications** jelölőnégyzetet, ha szeretné engedélyezni a felhasználó számára a megbízható alkalmazások helyi listájának létrehozását. Így a felhasználó létrehozhatja saját megbízható alkalmazásainak listáját a házirendben létrehozott megbízható alkalmazások általános listája mellett. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.

   Ha a jelölőnégyzet nincs bejelölve, a felhasználó csak a házirendben létrehozott megbízható alkalmazások általános listájához férhet hozzá. Ezenkívül, ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security elrejti a megbízható alkalmazások összevont listáját az alkalmazás felhasználói felületén.

7. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

- **Kategória**. A megbízható alkalmazásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy megbízható alkalmazást a kategóriához.
- **Új kizárás**. A Kaspersky Endpoint Security egy új megbízható alkalmazást ad hozzá a lista gyökeréhez.
- **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált megbízható alkalmazásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált megbízható alkalmazások is hozzá lettek adva. Előre definiált megbízható alkalmazásokat kell kiválasztania a védett kiszolgáló céljától függően.
- **Új kizárás a kiválasztott kategóriában**. Ha új megbízható alkalmazást szeretne hozzáadni egy adott kategóriához, válassza ki a kategóriát.

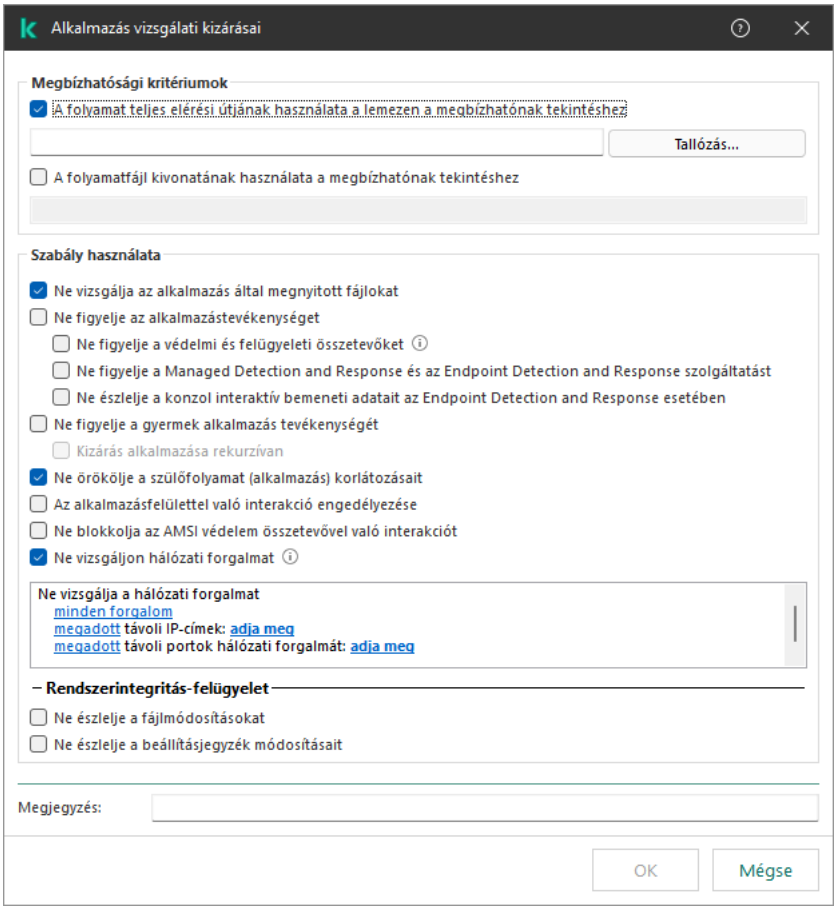
8. Válassza ki a megbízhatósági feltételeket:

- **A folyamat teljes elérési útjának használata a lemezen a megbízhatónak tekintéshez** Adja meg a megbízható alkalmazás futtatható fájljának elérési útvonalát.

  A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

  A Kaspersky Endpoint Security a megbízható alkalmazások fájlnevét a nagy- és kisbetűket megkülönböztető módon kezeli. Ha a beírt fájlnév nem a megfelelő módon van megadva, a Kaspersky Endpoint Security nem fogja felismerni a megbízható alkalmazást.
- **A folyamatfájl kivonatának használata a megbízhatónak tekintéshez**

A Kaspersky Endpoint Security nem támogatja a `%userprofile%` környezeti változót a megbízható alkalmazások listájának létrehozásakor a Kaspersky Security Center konzolon. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a * karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást.



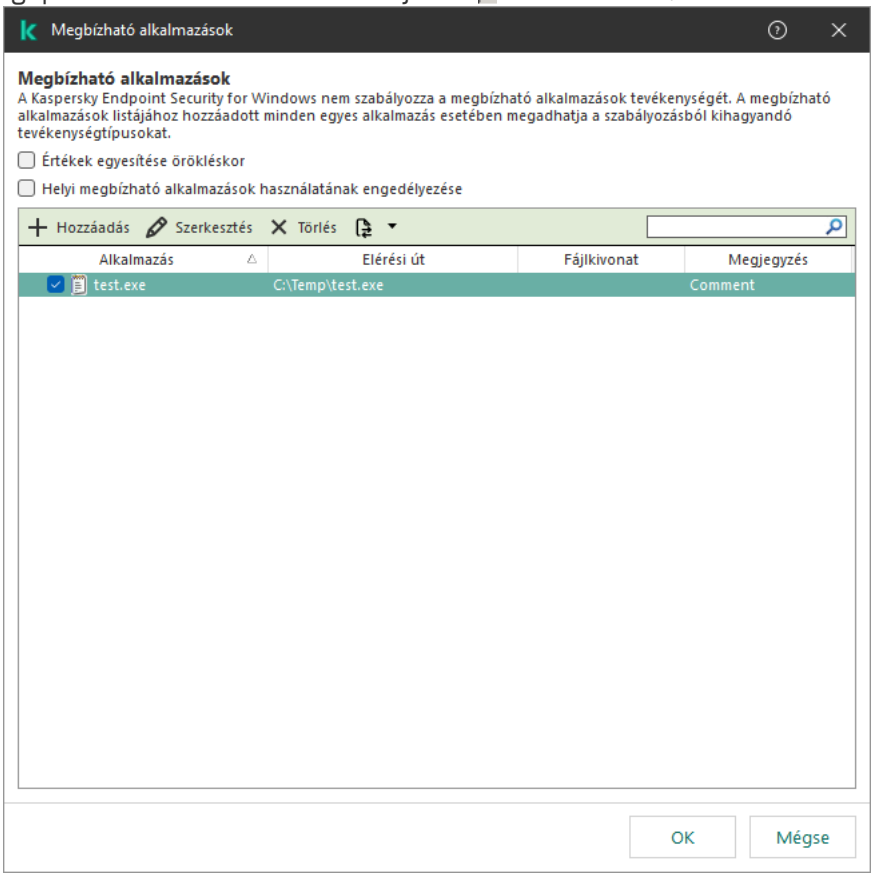
Megbízható alkalmazás beállításai

9. Konfigurálja a megbízható alkalmazás speciális beállításait (lásd az alábbi táblázatot).

10. Kattintson az **OK** gombra.

    Az új megbízható alkalmazás felkerül a listára. Az objektum melletti jelölőnégyzet segítségével bármikor kizárhat egy alkalmazást a megbízható zónából.

11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.



Megbízható alkalmazások listája

Az alkalmazás a megbízható listához való hozzáadásának menete a Web Console-ban, illetve a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Trusted Zone** szakaszt.
5. Az ablakban kattintson a **Applications** hivatkozásra.

   Ez megnyitja a megbízható alkalmazások listáját tartalmazó ablakot.
6. Jelölje be a **Merge values when inheriting** négyzetet, ha összesített listát szeretne létrehozni a vállalat összes számítógépén lévő megbízható alkalmazásokról. A szülő és gyermek rendszabályokban lévő megbízható alkalmazások listája egyesítve lesz. A lista egyesítve lesz, ha örökléskor az értékek egyesítése örökléskor engedélyezve van. A szülő rendszabályban lévő megbízható alkalmazások a gyermek rendszabályokban csak olvasható nézetben jelennek meg. A szülő rendszabályban lévő megbízható alkalmazásokat nem tudja módosítani vagy törölni.

7. Jelölje be a **Allow use of local exclusions** négyzetet, ha engedélyezni szeretné a felhasználó számára a megbízható alkalmazások helyi listájának létrehozását. Így a felhasználó létrehozhatja saját megbízható alkalmazásainak listáját a házirendben létrehozott megbízható alkalmazások általános listája mellett. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.

   Ha a jelölőnégyzet nincs bejelölve, a felhasználó csak a házirendben létrehozott megbízható alkalmazások általános listájához férhet hozzá. Ezenkívül, ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security elrejti a megbízható alkalmazások összevont listáját az alkalmazás felhasználói felületén.

8. Kattintson a **Add** gombra, és válasszon ki egy műveletet:

   - **Category**. A megbízható alkalmazásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy megbízható alkalmazást a kategóriához.
   - **New exclusion**. A Kaspersky Endpoint Security egy új megbízható alkalmazást ad hozzá a lista gyökeréhez.
   - **Select exclusion from list**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált megbízható alkalmazásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált megbízható alkalmazások is hozzá lettek adva. Előre definiált megbízható alkalmazásokat kell kiválasztania a védett kiszolgáló céljától függően.

   Ha új megbízható alkalmazást szeretne hozzáadni egy adott kategóriához, jelölje be az adott kategória melletti négyzetet, és válassza a(z) **New exclusion** lehetőséget.

9. Válassza ki a megbízhatósági feltételeket:

   - **Path to the file or folder**. Adja meg a megbízható alkalmazás futtatható fájljának elérési útvonalát.

     A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

     A Kaspersky Endpoint Security a megbízható alkalmazások fájlnevét a nagy- és kisbetűket megkülönböztető módon kezeli. Ha a beírt fájlnév nem a megfelelő módon van megadva, a Kaspersky Endpoint Security nem fogja felismerni a megbízható alkalmazást.

   - **Application hash**.

   A Kaspersky Endpoint Security nem támogatja a(z) %userprofile% környezeti változót a megbízható alkalmazások listájának létrehozásakor a Kaspersky Security Center konzolon. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a `*` karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást.

10. Konfigurálja a megbízható alkalmazás speciális beállításait (lásd az alábbi táblázatot).

11. Kattintson az **OK** gombra.

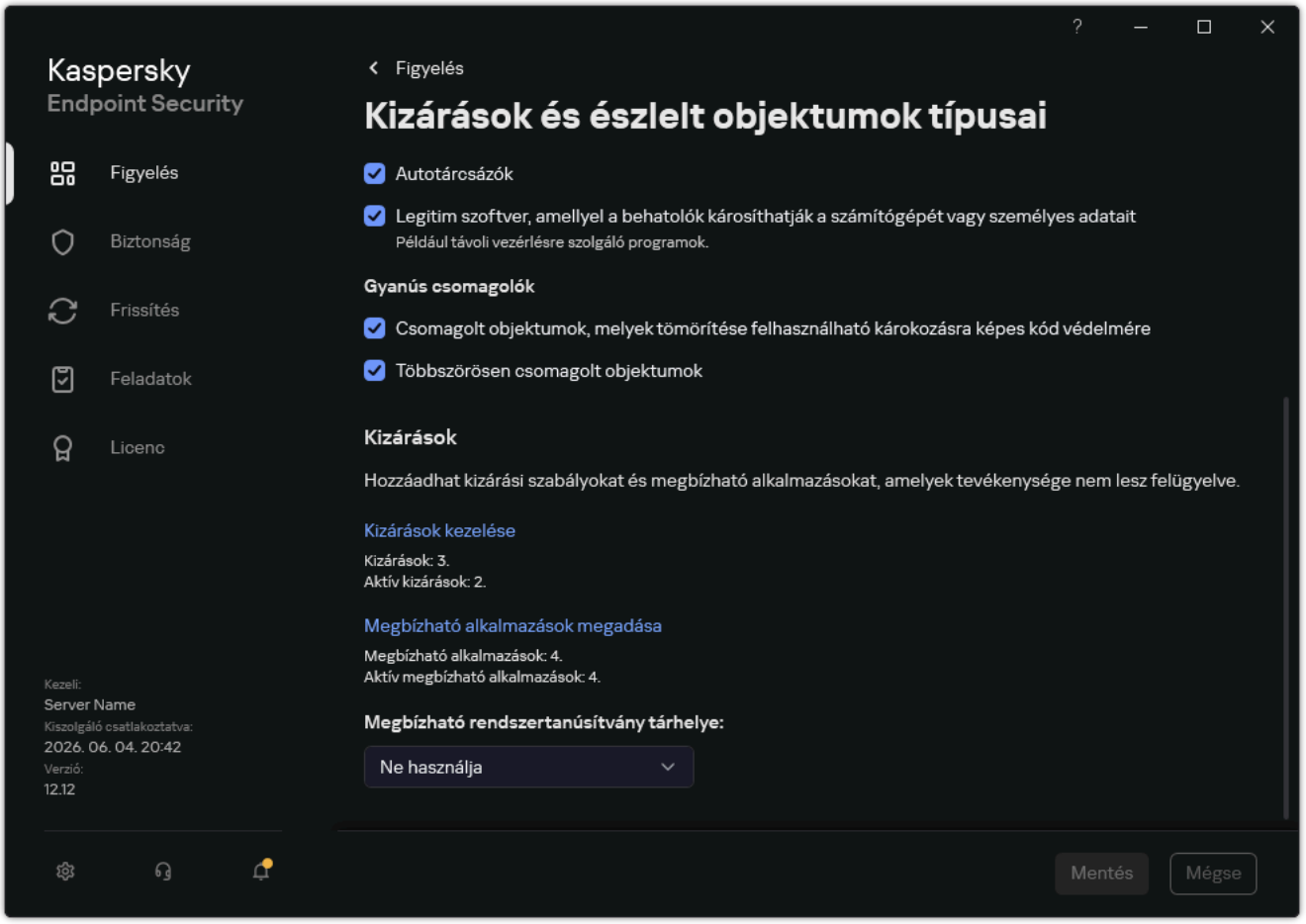
    Az új megbízható alkalmazás felkerül a listára. A(z) **Status** oszlopban található jelölőnégyzet segítségével bármikor kizárhat egy alkalmazást a megbízható zónából.

12. Mentse el a módosításokat.

Alkalmazás megbízható listához való hozzáadásának menete az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.

A Kaspersky Endpoint Security elrejti a megbízható alkalmazások összevont listáját az alkalmazás felhasználói felületén, ha a rendszergazda a konzolon letiltotta a megbízható alkalmazások konfigurálását („zárt lakat" szimbólum), és a helyi megbízható alkalmazások tiltva vannak (a **Helyi megbízható alkalmazások használatának engedélyezése** jelölőnégyzet nincs bejelölve).



Kizárások beállításai

4. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

- **Kategória**. A megbízható alkalmazásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy megbízható alkalmazást a kategóriához.
- **Új kizárás**. A Kaspersky Endpoint Security egy új megbízható alkalmazást ad hozzá a lista gyökeréhez.
- **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált megbízható alkalmazásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált megbízható alkalmazások is hozzá lettek adva. Előre definiált megbízható alkalmazásokat kell kiválasztania a védett kiszolgáló céljától függően.

Ha új megbízható alkalmazást szeretne hozzáadni egy adott kategóriához, jelölje be az adott kategória melletti jelölőnégyzetet, és válassza az **Új kizárás** lehetőséget.

5. Válassza ki a megbízhatósági feltételeket:

   - **A folyamat teljes elérési útjának használata a lemezen a megbízhatónak tekintéshez** Adja meg a megbízható alkalmazás futtatható fájljának elérési útvonalát.

     A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

     A Kaspersky Endpoint Security a megbízható alkalmazások fájlnevét a nagy- és kisbetűket megkülönböztető módon kezeli. Ha a beírt fájlnév nem a megfelelő módon van megadva, a Kaspersky Endpoint Security nem fogja felismerni a megbízható alkalmazást.

   - **A folyamatfájl kivonatának használata a megbízhatónak tekintéshez**

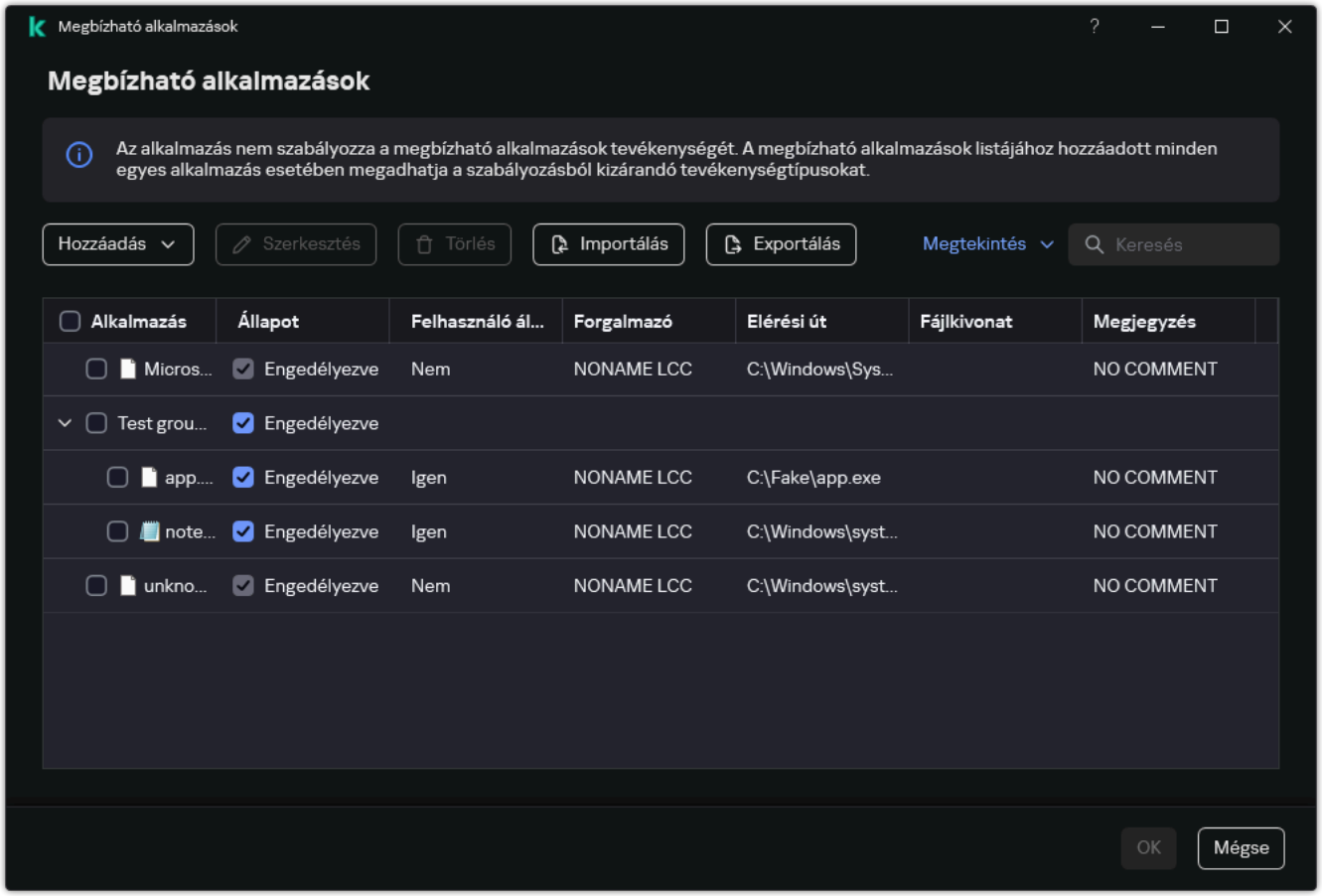
   A Kaspersky Endpoint Security támogatja a környezeti változókat, és átalakítja az elérési utat az alkalmazás helyi felületén. Más szóval, ha a `%userprofile%\Documents\File.exe` fájl elérési útvonalát adja meg, az alkalmazás helyi felületén a `C:\Users\Fred123\Documents\File.exe` rekord kerül hozzáadásra a Fred123 felhasználó esetében. Ennek megfelelően a Kaspersky Endpoint Security figyelmen kívül hagyja a `File.exe` megbízható programot más felhasználók esetében. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a `*` karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást.

6. A megbízható alkalmazás tulajdonságai ablakban konfigurálja a speciális beállításokat.

7. Kattintson az **OK** gombra.

   Az új megbízható alkalmazás felkerül a listára. Az **Állapot** oszlopban található jelölőnégyzet segítségével bármikor kizárhat egy alkalmazást a megbízható zónából.

8. Mentse el a módosításokat.



Megbízható alkalmazások listája

Megbízható alkalmazás beállításai

Paraméter	Leírás
Ne vizsgálja meg az alkalmazás által megnyitott fájlokat	Az alkalmazás által megnyitott összes fájl ki van zárva a Kaspersky Endpoint Security általi vizsgálatból. Például, ha alkalmazásokat használ fájlok biztonsági mentésére, ez a szolgáltatás segít csökkenteni a Kaspersky Endpoint Security erőforrás-felhasználását.
Ne figyelje az alkalmazástevékenységet	A Kaspersky Endpoint Security nem fogja figyelni az alkalmazás fájl- és hálózati tevékenységét az operációs rendszerben. Beállíthatja az alkalmazástevékenység-figyelést a Kaspersky Endpoint Security különböző összetevőihez: • **Ne figyelje a védelmi és felügyeleti összetevőket**. Az alkalmazástevékenységet a következő összetevők figyelik: Behavior analysis, Biztonsági rések kihasználásának megelőzése, Behatolásmegelőző rendszer, Kármentesítő motor és Tűzfal. • **Ne figyelje a Managed Detection and Response és az Endpoint Detection and Response megoldásokat**. Az alkalmazások tevékenységét figyeli a beépített MDR agent és beépített EDR (KATA) agent. • **Ne szerezze meg a konzol interaktív bemenetét az Endpoint Detection and Response esetében**. A Kaspersky Endpoint Security nem küld telemetriai adatokat az alkalmazás konzolon történő kezeléséről. A telemetriai adatokat Kaspersky Anti Targeted Attack Platform (EDR) használja.
Ne figyelje a gyermek alkalmazás tevékenységét	A Kaspersky Endpoint Security nem figyeli az ezen alkalmazás által elindított alkalmazások fájl- vagy hálózati tevékenységét. A kizárást rekurzívan is alkalmazhatja. Annak érdekében, hogy az alkalmazás ne figyelje a gyermekalkalmazások teljes láncának tevékenységét.
Ne örökölje a szülőfolyamat (alkalmazás) korlátozásait	A szülői folyamathoz konfigurált korlátozásokat a Kaspersky Endpoint Security nem alkalmazza utódfolyamatra. A szülői folyamatot egy olyan alkalmazás indítja, amelyhez konfigurálva vannak az alkalmazásjogok (Behatolásmegelőző rendszer) és az alkalmazás hálózati szabályai (Tűzfal).
Ne figyelje a gyermek alkalmazás tevékenységét	A Kaspersky Endpoint Security nem figyeli az ezen alkalmazás által elindított alkalmazások fájl- vagy hálózati tevékenységét. A kizárást rekurzívan is alkalmazhatja. Annak érdekében, hogy az alkalmazás ne figyelje a gyermekalkalmazások teljes láncának tevékenységét.
Az alkalmazásfelülettel való interakció engedélyezése	A Kaspersky Endpoint Security Önvédelem blokkolja az alkalmazásszolgáltatások távoli számítógépről történő kezelésének minden kísérletét. Ha a jelölőnégyzet be van jelölve, a távoli hozzáférési alkalmazás a Kaspersky Endpoint Security beállításait a Kaspersky Endpoint Security felületen keresztül kezelheti.
Ne blokkolja az AMSI védelmi összetevővel való interakciót	A Kaspersky Endpoint Security nem figyeli a megbízható alkalmazások kéréseit az AMSI védelmi összetevő által vizsgált objektumok esetében.

Paraméter	Leírás
Ne vizsgálja a hálózati forgalmat	Az alkalmazás által kezdeményezett hálózati forgalom ki lesz zárva a Kaspersky Endpoint Security vizsgálataiból. A vizsgálatokból kizárhatja a teljes forgalmat vagy csak a titkosított forgalmat. Kizárhatja az egyes IP-címeket és portszámokat is a vizsgálatokból. A Kaspersky Endpoint Security 14.0 vagy annál korábbi verziói nem támogatják a hálózati forgalom kizárását, ha egy megbízható alkalmazáshoz elérési út helyett kivonatot adnak meg.
Ne észlelje a fájlmódosításokat *(csak a Kaspersky Security Center konzolon érhető el)*	A Kaspersky Endpoint Security nem figyeli a fájlok módosításait a Rendszerintegritás-felügyelet felügyeleti hatókörből. Az alkalmazás a kizárást az összes Rendszerintegritás-felügyeleti módra alkalmazza: Valós idejű rendszerintegritás-felügyelet és Igény szerinti rendszerintegritás-ellenőrzés.
Ne észlelje a beállításjegyzék módosításait *(csak a Kaspersky Security Center konzolon érhető el)*	A Kaspersky Endpoint Security nem figyeli a beállításkulcsok módosításait a Rendszerintegritás-felügyelet felügyeleti hatókörből. Az alkalmazás a kizárást az összes Rendszerintegritás-felügyeleti módra alkalmazza: Valós idejű rendszerintegritás-felügyelet és Igény szerinti rendszerintegritás-ellenőrzés.
Megjegyzés	Ha szükséges, rövid megjegyzést adhat a megbízható alkalmazáshoz. A megjegyzések megkönnyítik a megbízható alkalmazások keresését és rendezését.
Státusz	A megbízható alkalmazás állapota: • Az **Aktív** állapot azt jelenti, hogy az alkalmazás a megbízható zónában van. • Az **Inaktív** állapot azt jelenti, hogy az alkalmazás ki van zárva a megbízható zónából.

Helyi megbízható zóna létrehozása

A felhasználó mostantól létrehozhatja saját helyi megbízható zónáját egy adott számítógéphez. Így a felhasználó a házirendben található általános megbízható zóna mellett létrehozhatja a vizsgálati kizárásokra és megbízható alkalmazásokra vonatkozó saját listáját is. A rendszergazda engedélyezheti vagy blokkolhatja a helyi kizárások vagy helyi megbízható alkalmazások használatát a szabályzati beállításokban. Ehhez jelölje be a **Helyi kizárások használatának engedélyezése** és a **Helyi megbízható alkalmazások használatának engedélyezése** jelölőnégyzeteket a szabályzat **Kizárások** szakaszában.

Ha a rendszergazda engedélyezi a helyi megbízható zóna létrehozását, a felhasználó hozzáadhatja a saját vizsgálati kizárásait és megbízható alkalmazásait az alkalmazás felhasználói felületén. Ugyanakkor a felhasználónak nincs engedélye objektumok módosítására vagy törlésére a szabályzatban konfigurált megbízható zónából. A rendszergazda a Kaspersky Security Center konzolon is megtekintheti, hozzáadhatja, módosíthatja vagy törölheti a listaelemeket, ha kizárásokat kell hozzáadni egy adott számítógéphez.

A Kaspersky Endpoint Security elrejti a vizsgálati kizárások és a megbízható alkalmazások listáját az alkalmazás felhasználói felületén, ha a rendszergazda a konzolon blokkolja a megbízható zóna konfigurálását („zárt lakat” szimbólum), és a helyi vizsgálati kizárások és a megbízható alkalmazások tiltva vannak.

Objektum helyi megbízható zónához való hozzáadásának menete az Adminisztrációs Konzolon (MMC)

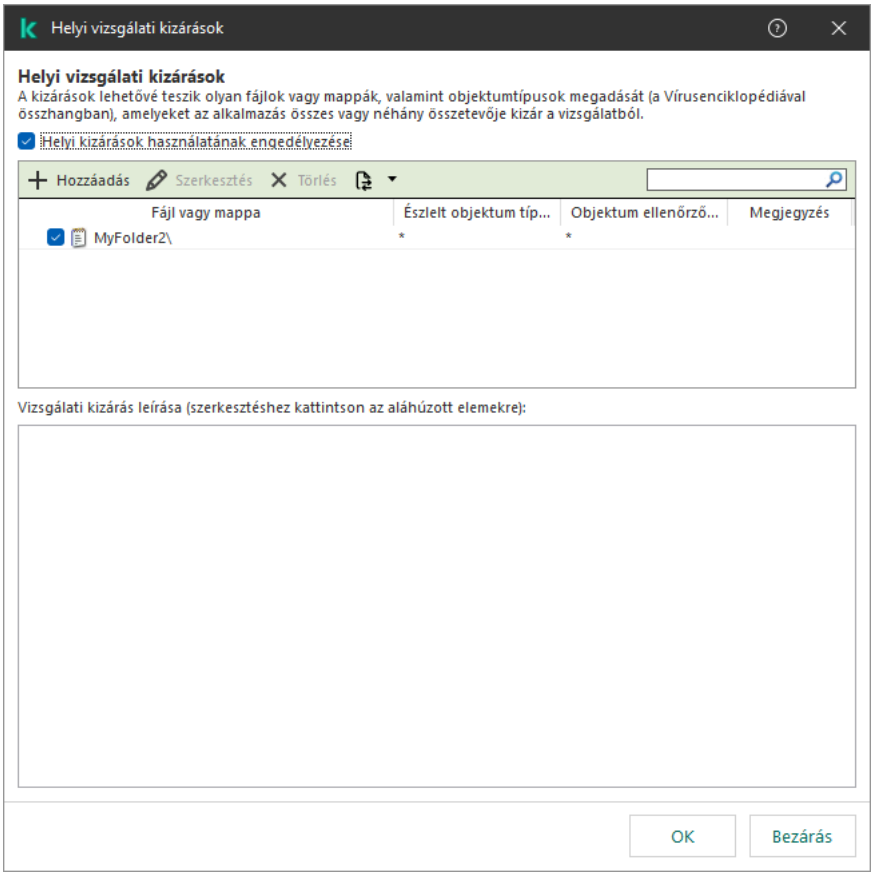
1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Devices** lapot.
4. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.
5. Válassza ki a számítógép tulajdonságainak ablakában a **Applications** részt.

6. A számítógépre telepített Kaspersky alkalmazások listájában válassza a **Kaspersky Endpoint Security for Windows (14.1)** lehetőséget, és kattintson rá duplán az alkalmazás tulajdonságainak megnyitásához.

7. Az alkalmazásbeállítások ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.

8. A **Kizárások a vizsgálatból és megbízható alkalmazások → Helyi vizsgálati kizárások** részen kattintson a **Beállítások** gombra.

   Ez megnyitja a helyi kizárások listáját tartalmazó ablakot.



Megbízható zóna beállításai

9. Készítsen listát a helyi vizsgálati kizárásokról.

   A helyi vizsgálati kizárások létrehozásának szabályai ugyanazok, mint az általános kizárásoknál. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a * és ? karaktereket egy maszk megadásakor.

10. A **Kizárások a vizsgálatból és megbízható alkalmazások → Helyi megbízható alkalmazások** részen kattintson a **Beállítások** gombra.

    Ez megnyitja a helyi megbízható alkalmazások listáját tartalmazó ablakot.

11. Készítsen listát a helyi megbízható alkalmazásokról.

    Az alkalmazásoknak a helyi megbízható alkalmazások listájára történő felvételére ugyanazok a szabályok vonatkoznak, mint az általános listára történő felvételre. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a * és ? karaktereket egy maszk megadásakor.

12. Mentse el a módosításokat.

Objektum hozzáadása a helyi megbízható zónához a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Kattintson annak a számítógépnek a nevére, amelyen a felhasználónak engedélyezni kívánja a tiltott művelet végrehajtását.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.

   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Az alkalmazáskonfigurációs ablakban válassza ki a **General settings** → **Exclusions and types of detected objects** lehetőséget.
7. A **Scan exclusions and trusted applications** részen kattintson a **Local scan exclusions** hivatkozásra.
8. Készítsen listát a helyi vizsgálati kizárásokról.

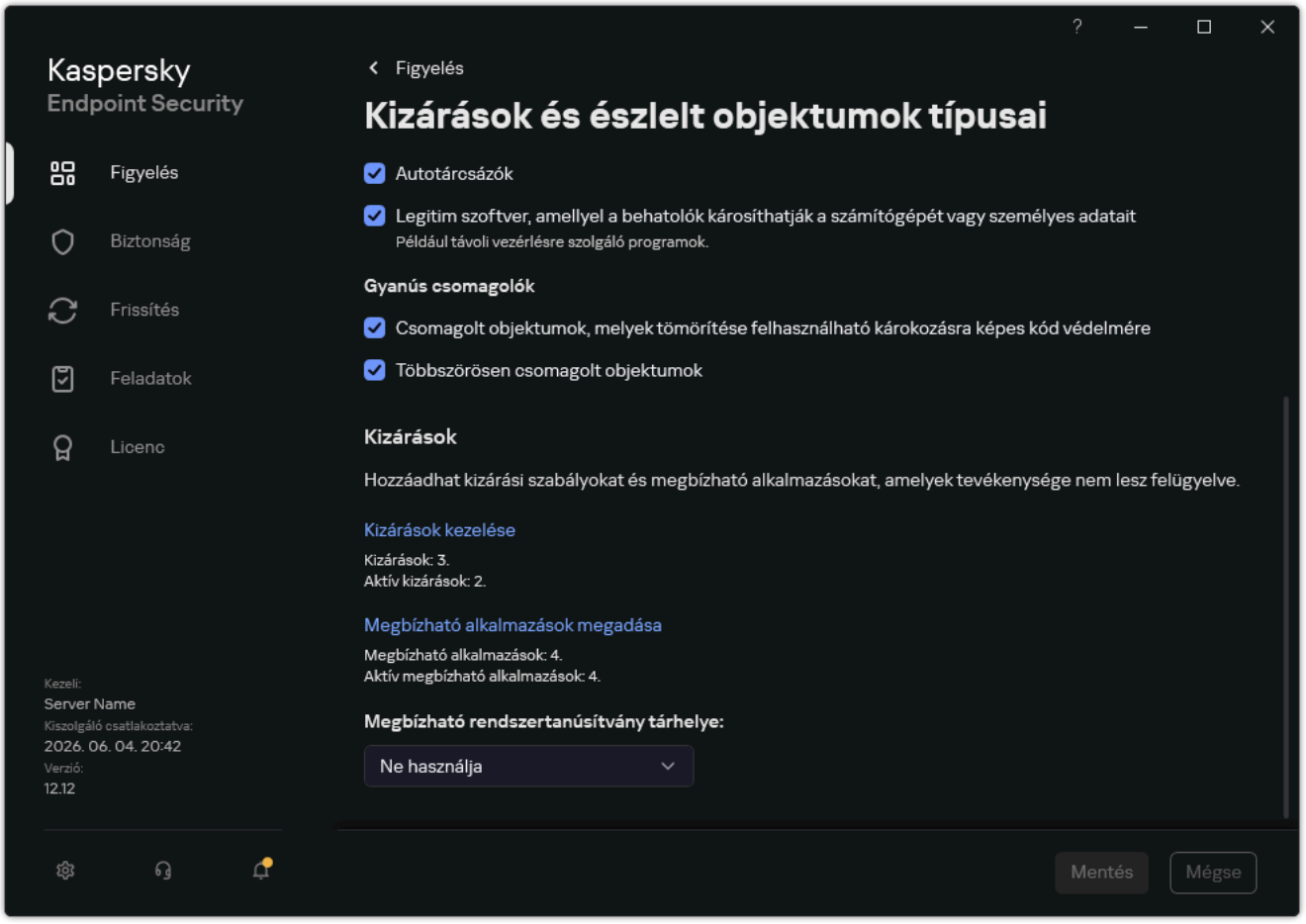
   A helyi kizárások létrehozására vonatkozó szabályok megegyeznek az általános kizárások létrehozására vonatkozó szabályokkal. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a * és ? karaktereket egy maszk megadásakor.
9. A **Scan exclusions and trusted applications** részen kattintson a **Local trusted applications** hivatkozásra.
10. Készítsen listát a helyi megbízható alkalmazásokról.

    Az alkalmazásoknak a helyi megbízható alkalmazások listájára történő felvételére ugyanazok a szabályok vonatkoznak, mint az általános listára történő felvételre. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a * és ? karaktereket egy maszk megadásakor.
11. Mentse el a módosításokat.

Helyi vizsgálati kizárás létrehozásának menete az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Kizárások és észlelt objektumok típusai** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

A Kaspersky Endpoint Security elrejti a vizsgálati kizárások listáját az alkalmazás felhasználói felületén, ha a konzolon a rendszergazda letiltotta a vizsgálati kizárások konfigurálását („zárt lakat" szimbólum), és a helyi vizsgálati kizárások tiltva vannak (a **Helyi kizárások használatának engedélyezése** jelölőnégyzet nincs bejelölve).



Kizárások beállításai

4. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

   - **Kategória**. A vizsgálati kizárásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy vizsgálati kizárást a kategóriához.
   - **Új kizárás**. A Kaspersky Endpoint Security egy új vizsgálati kizárást ad hozzá a lista gyökeréhez.
   - **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált vizsgálati kizárásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált vizsgálati kizárások is hozzá lettek adva. Előre definiált vizsgálati kizárásokat kell kiválasztania a védett kiszolgáló céljától függően.

   Ha új vizsgálati kizárást szeretne hozzáadni egy adott kategóriához, jelölje be a kategória melletti jelölőnégyzetet, és válassza az **Új kizárás** lehetőséget.

5. Ha ki szeretne zárni egy fájlt vagy mappát a vizsgálatokból, válassza ki a fájlt vagy mappát a **Tallózás** gombra kattintással.

Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

  Maszkokat az elérési út elején, közepén vagy végén is használhat. Ha például meg szeretne adni egy kizárási mappát az összes felhasználóhoz, írja be a `?:\Users\*\Folder\` maszkot.

  Kizárhatja a hálózati mappákat. Ehhez manuálisan adja meg a hálózati mappa elérési útját (például `\\Network Share\*`).

6. Ha egy adott típusú objektumot szeretne kizárni a vizsgálatokból, az **Észlelt objektum típusa** mezőben adja meg az objektumtípus nevét a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például: `Email-Worm`, `Rootkit` vagy `RemoteAdmin`).

   Használhat maszkokat a `?` karakterrel (bármely karaktert helyettesíti) és a `*` karakterrel (tetszőleges számú karaktert helyettesít). Például, ha a `Client*` maszk van megadva, a Kaspersky Endpoint Security kizárja a `Client-IRC`, `Client-P2P` és a `Client-SMTP` objektumokat is a vizsgálatokból.

7. Ha ki szeretne zárni egy fájlt a vizsgálatokból, adja meg a fájl ellenőrzőösszeget az **Objektumkivonat** mezőben.

   Ha a fájl megváltozik, a fájl ellenőrzőösszege is megváltozik. Ebben az esetben a módosított fájl nem lesz hozzáadva a kizárásokhoz.

8. A **Védelmi összetevők** blokkban válassza ki az összetevőket, amelyekre alkalmazni szeretné a kizárást a vizsgálatból.

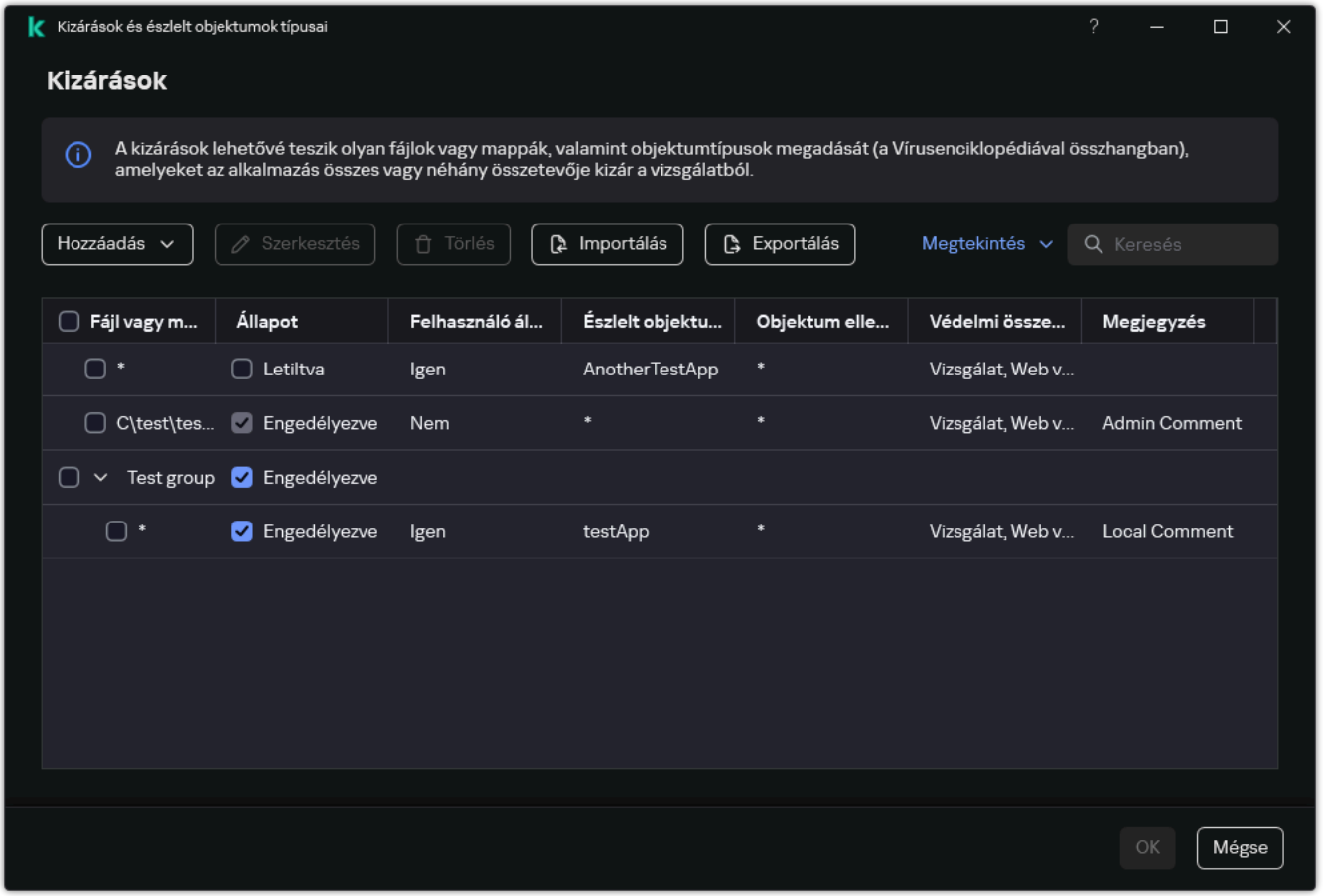
9. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

10. Válassza ki az **Aktív** állapotot a kizáráshoz.

11. Kattintson **Hozzáadás** gombra.

    Az új kizárás bekerül a listába. A kizárást bármikor letilthatja az **Állapot** oszlopban található jelölőnégyzet segítségével.

12. Mentse el a módosításokat.



Kizárások listája

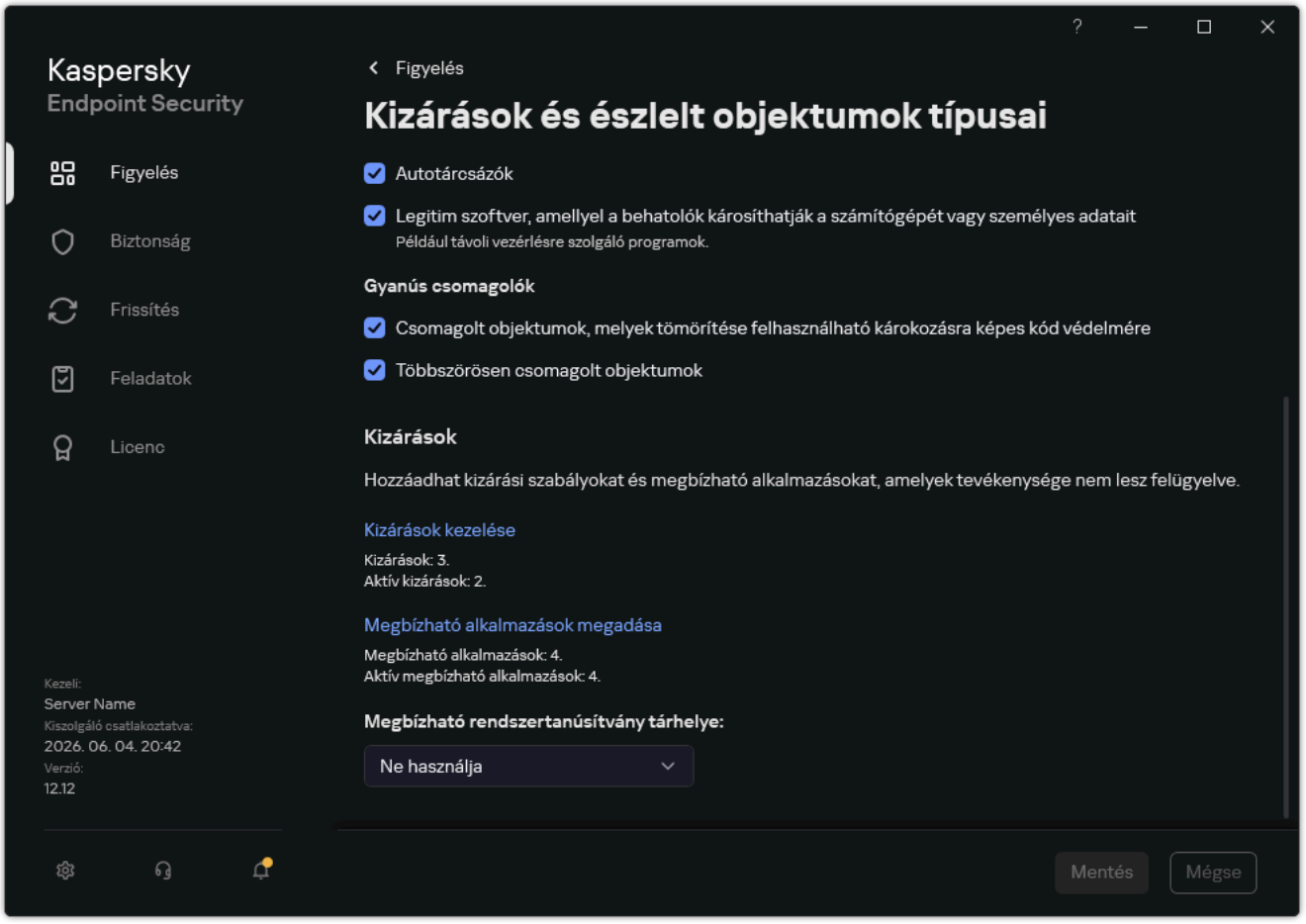
Alkalmazás hozzáadása a helyi megbízható alkalmazások listájához az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.

3. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.

A Kaspersky Endpoint Security elrejti a megbízható alkalmazások összevont listáját az alkalmazás felhasználói felületén, ha a rendszergazda a konzolon letiltotta a megbízható alkalmazások konfigurálását („zárt lakat" szimbólum), és a helyi megbízható alkalmazások tiltva vannak (a **Helyi megbízható alkalmazások használatának engedélyezése** jelölőnégyzet nincs bejelölve).



Kizárások beállításai

4. Kattintson a **Hozzáadás** gombra, és válasszon ki egy műveletet:

   - **Kategória**. A megbízható alkalmazásokat külön kategóriákba csoportosíthatja. Új kategória létrehozásához adja meg a kategória nevét, és adjon hozzá legalább egy megbízható alkalmazást a kategóriához.
   - **Új kizárás**. A Kaspersky Endpoint Security egy új megbízható alkalmazást ad hozzá a lista gyökeréhez.
   - **Válassza ki a kizárást a listáról**. A Kaspersky Endpoint Security gyors konfigurálásához SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben az alkalmazás *előre definiált megbízható alkalmazásokat* tartalmaz. A Citrix és VMware virtuális környezetekben történő alkalmazásbeállítás támogatásához előre definiált megbízható alkalmazások is hozzá lettek adva. Előre definiált megbízható alkalmazásokat kell kiválasztania a védett kiszolgáló céljától függően.

   Ha új megbízható alkalmazást szeretne hozzáadni egy adott kategóriához, jelölje be az adott kategória melletti jelölőnégyzetet, és válassza az **Új kizárás** lehetőséget.

5. Válassza ki a megbízhatósági feltételeket:

   - **A folyamat teljes elérési útjának használata a lemezen a megbízhatónak tekintéshez** Adja meg a megbízható alkalmazás futtatható fájljának elérési útvonalát.

     A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.

A Kaspersky Endpoint Security a megbízható alkalmazások fájlnevét a nagy- és kisbetűket megkülönböztető módon kezeli. Ha a beírt fájlnév nem a megfelelő módon van megadva, a Kaspersky Endpoint Security nem fogja felismerni a megbízható alkalmazást.

- **A folyamatfájl kivonatának használata a megbízhatónak tekintéshez**

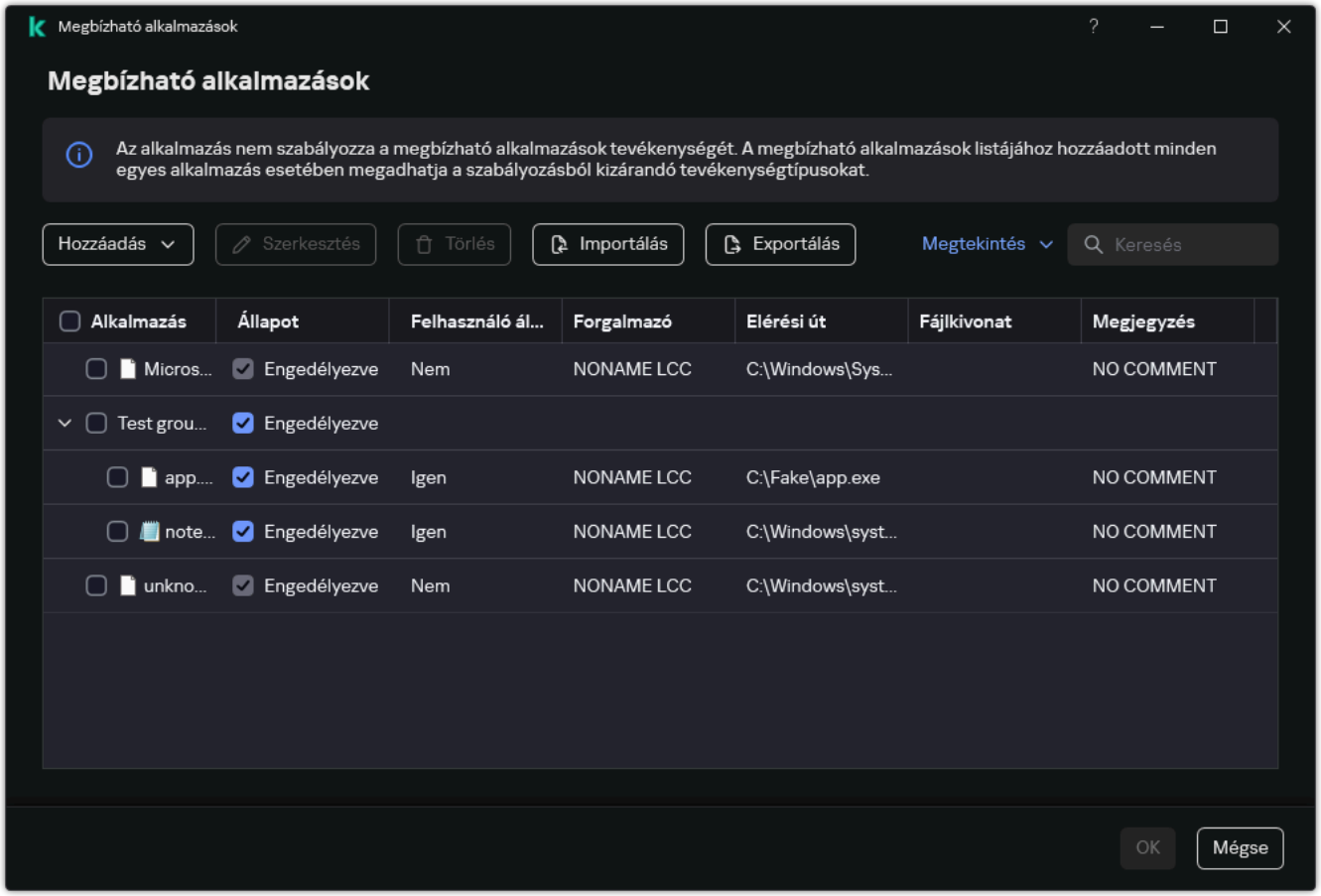
A Kaspersky Endpoint Security támogatja a környezeti változókat, és átalakítja az elérési utat az alkalmazás helyi felületén. Más szóval, ha a `%userprofile%\Documents\File.exe` fájl elérési útvonalát adja meg, az alkalmazás helyi felületén a `C:\Users\Fred123\Documents\File.exe` rekord kerül hozzáadásra a Fred123 felhasználó esetében. Ennek megfelelően a Kaspersky Endpoint Security figyelmen kívül hagyja a `File.exe` megbízható programot más felhasználók esetében. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a `*` karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást.

6. A megbízható alkalmazás tulajdonságai ablakban konfigurálja a speciális beállításokat.

7. Kattintson az **OK** gombra.

   Az új megbízható alkalmazás felkerül a listára. Az **Állapot** oszlopban található jelölőnégyzet segítségével bármikor kizárhat egy alkalmazást a megbízható zónából.

8. Mentse el a módosításokat.



Megbízható alkalmazások listája

A megbízható zóna exportálása és importálása

A *megbízható zóna* olyan, a rendszergazda által beállított objektumok és alkalmazások listája, melyeket a Kaspersky Endpoint Security aktív módban nem figyel. A megbízható zóna a következő listákból áll: *kizárások a vizsgálatból* és *megbízható alkalmazások*. Exportálhatja ezeket a listákat XML-fájlokba és más formátumokba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú kizárás hozzáadásával. Használhatja az exportálás/importálás funkciót a kizárások és a megbízható alkalmazások lista biztonsági mentésének létrehozásához, vagy a listák egy másik kiszolgálóra való áttelepítéséhez.

Az alkalmazás a következő formátumokat használja a *kizárások listájának* exportálásához és importálásához:

- Az XML az adminisztrációs konzolban (MMC), a Web Console-ban és a Cloud Console-ban érhető el.
- A DAT csak az adminisztrációs konzolban (MMC) importálható. Ennek a formátumnak az a célja, hogy fenntartsa a kompatibilitást az alkalmazás régebbi verzióival. A DAT-fájlt XML-re konvertálhatja az Adminisztrációs konzolban (MMC), hogy a kizárási listákat áttelepítse a Web Console-ba.
- A CSV csak az alkalmazás helyi felületén érhető el.

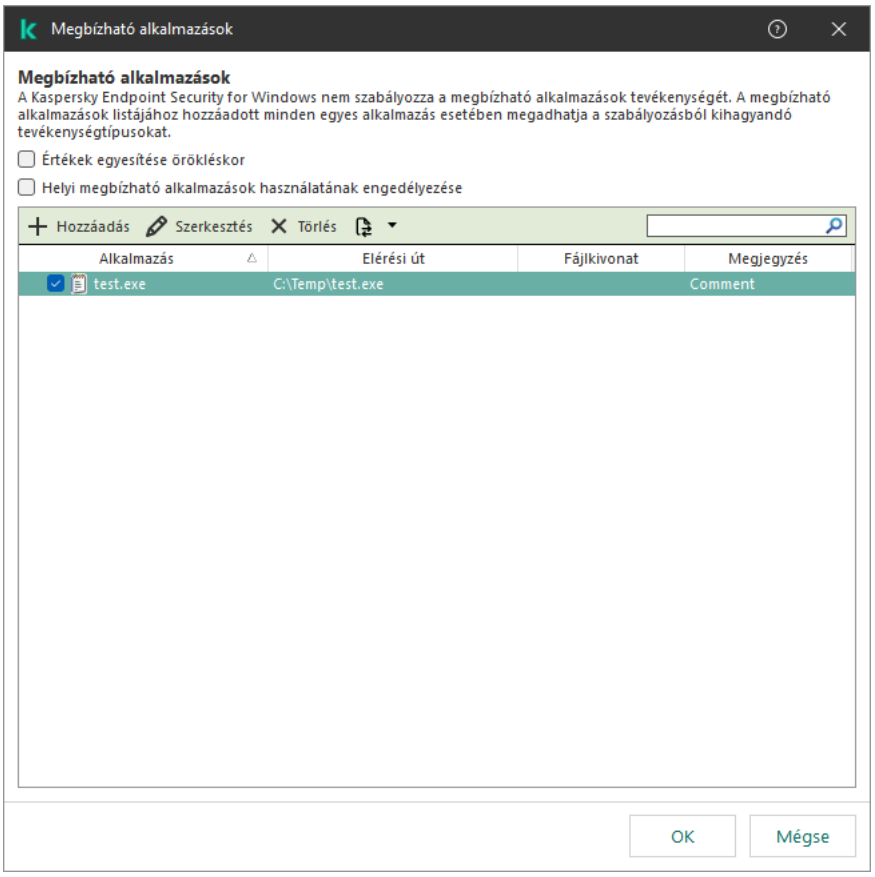
A Kaspersky Endpoint Security az XML formátumot használja a *megbízható alkalmazások listájának* exportálásához és importálásához.

A megbízható zóna exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakban válassza ki az **Általános beállítások** → **Jelentések és objektumtípusok** részt.
4. A **Kizárások és megbízható alkalmazások vizsgálata** területen válassza ki a megbízható zóna exportálni vagy importálni kívánt összetevőjét: **Kizárás a vizsgálatból** vagy **Megbízható alkalmazások**.
5. Kattintson a **Beállítások** gombra.
6. A szabályok listájának exportálása:
   a. Jelölje ki az exportálni kívánt kizárásokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
      Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.
   b. Kattintson a → **Hozzáadás** gombra.
   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.

d. Mentse a fájlt.

A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba. A Kaspersky Endpoint Security támogatja a kizárások listájának exportálását is DAT-fájlba.



Megbízható alkalmazások listája

7. A kizárások listájának importálása:

a. Kattintson a → **Hozzáadás** gombra.

b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kizárások listáját.

c. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból. A Kaspersky Endpoint Security támogatja a kizárások listájának DAT-fájlból történő importálását is.

8. Mentse el a módosításokat.

A megbízható zóna exportálása vagy importálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Trusted Zone** szakaszt.

5. A szabályok listájának exportálása:

   a. Kattintson a **Malware Scan exclusions** hivatkozásra.

   b. Jelölje ki az exportálni kívánt kizárásokat.

   c. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a kizárások listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

6. Megbízható alkalmazások listájának exportálása:

   a. Jelölje ki az exportálni kívánt megbízható alkalmazásokat.

   b. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security az alkalmazások listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.

7. A kizárások listájának importálása:

   a. Kattintson a **Malware Scan exclusions** hivatkozásra.

   b. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a kizárások listáját.

   c. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.

8. Megbízható alkalmazások listájának importálása:

   a. Kattintson a **Applications** hivatkozásra.

   b. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a megbízható alkalmazások listáját.

   c. Nyissa meg a fájlt.

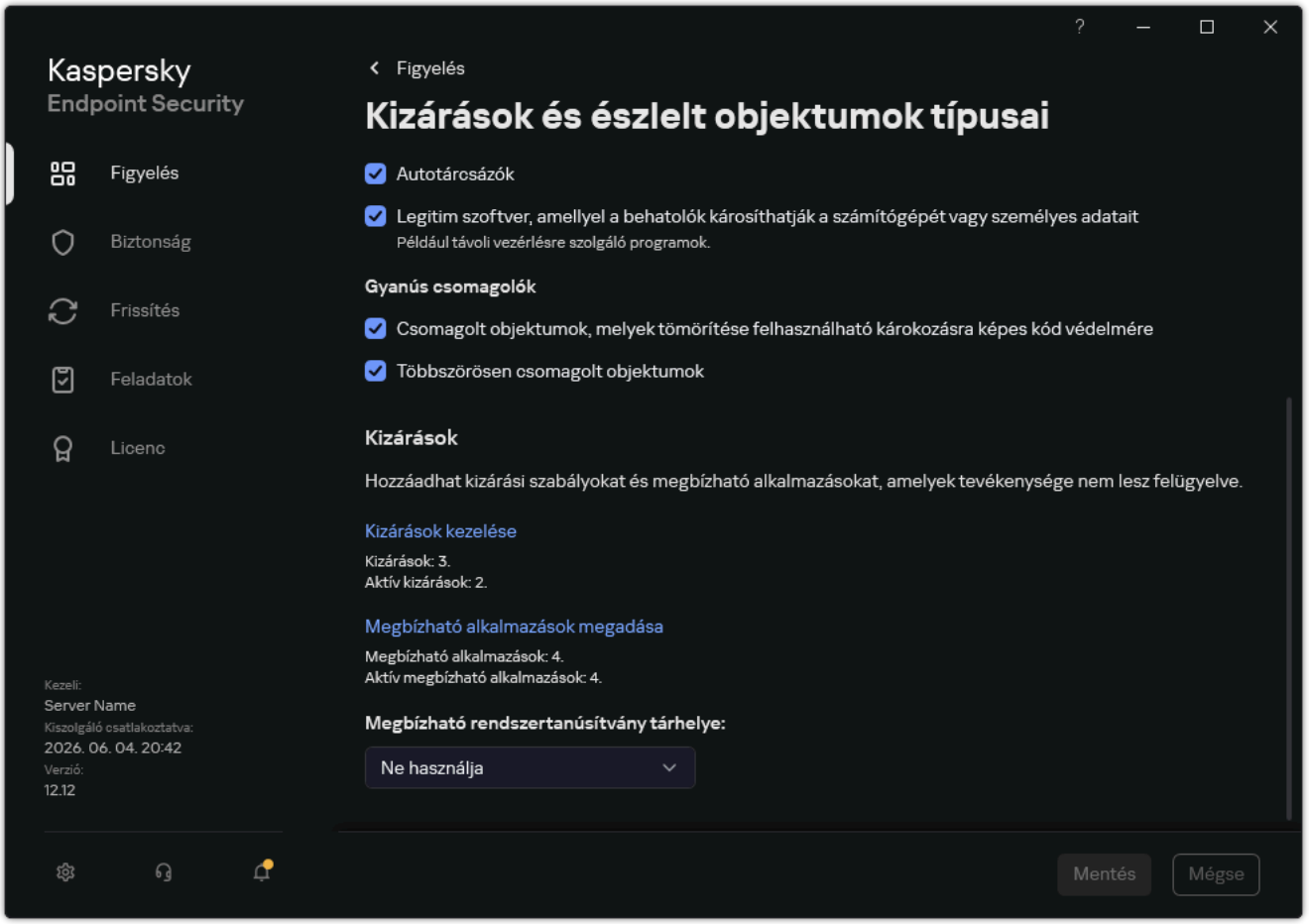
   Ha a számítógépen már létezik egy lista a megbízható alkalmazásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba az JSON-fájlból.

9. Mentse el a módosításokat.

A megbízható zóna exportálása vagy importálása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.



Kizárások beállításai

3. A szabályok listájának exportálása:

   a. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

   b. Jelölje ki az exportálni kívánt kizárásokat.

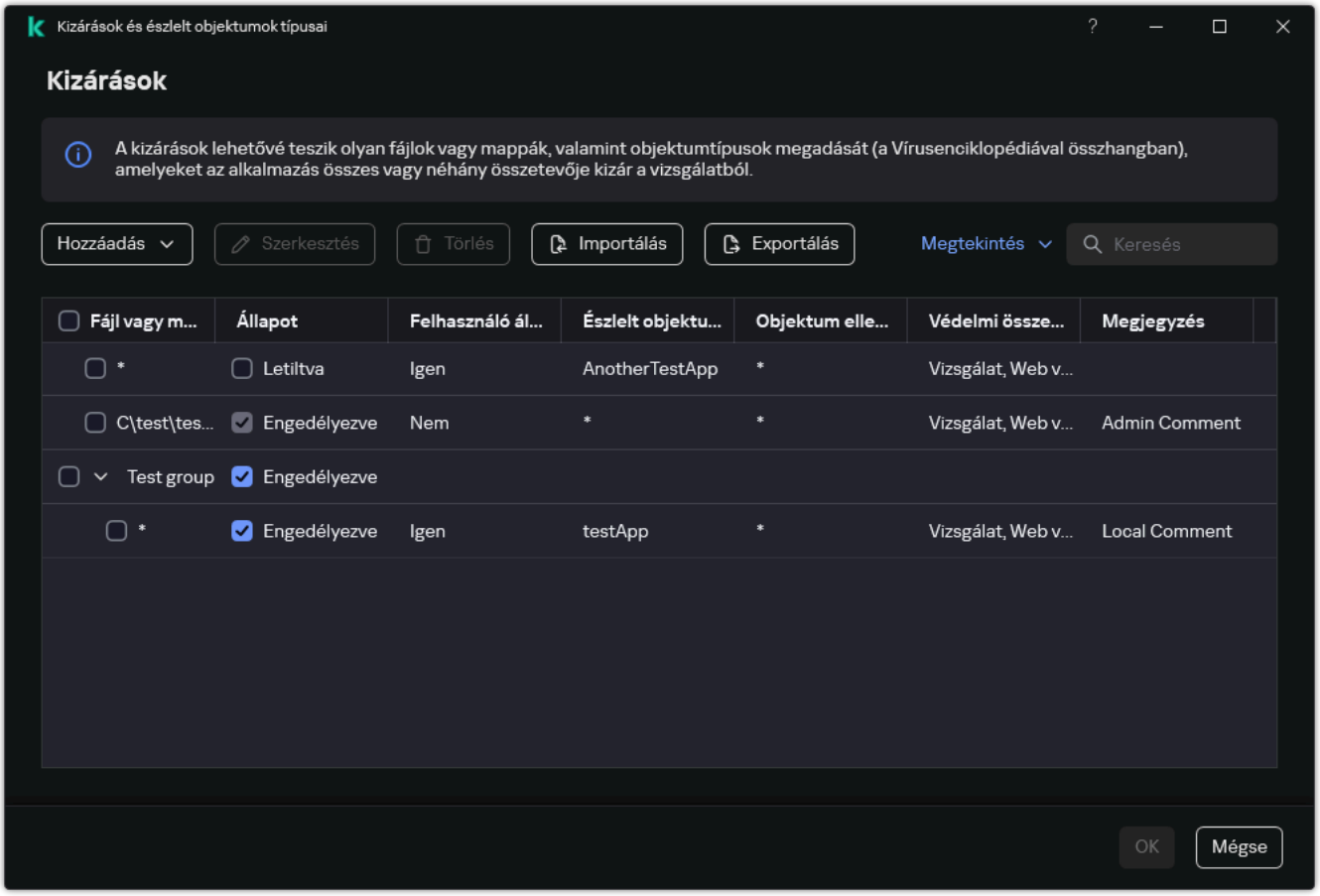
   c. Kattintson az **Export** gombra.

   d. Erősítse meg, hogy csak a kijelölt kizárásokat, vagy a kizárások teljes listáját szeretné exportálni.

   e. A megnyíló ablakban adja meg az CSV-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.

f. Mentse a fájlt.

A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az CSV-fájlba.



Kizárások listája

4. Megbízható alkalmazások listájának exportálása:

a. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.

b. Jelölje ki az exportálni kívánt megbízható alkalmazásokat.

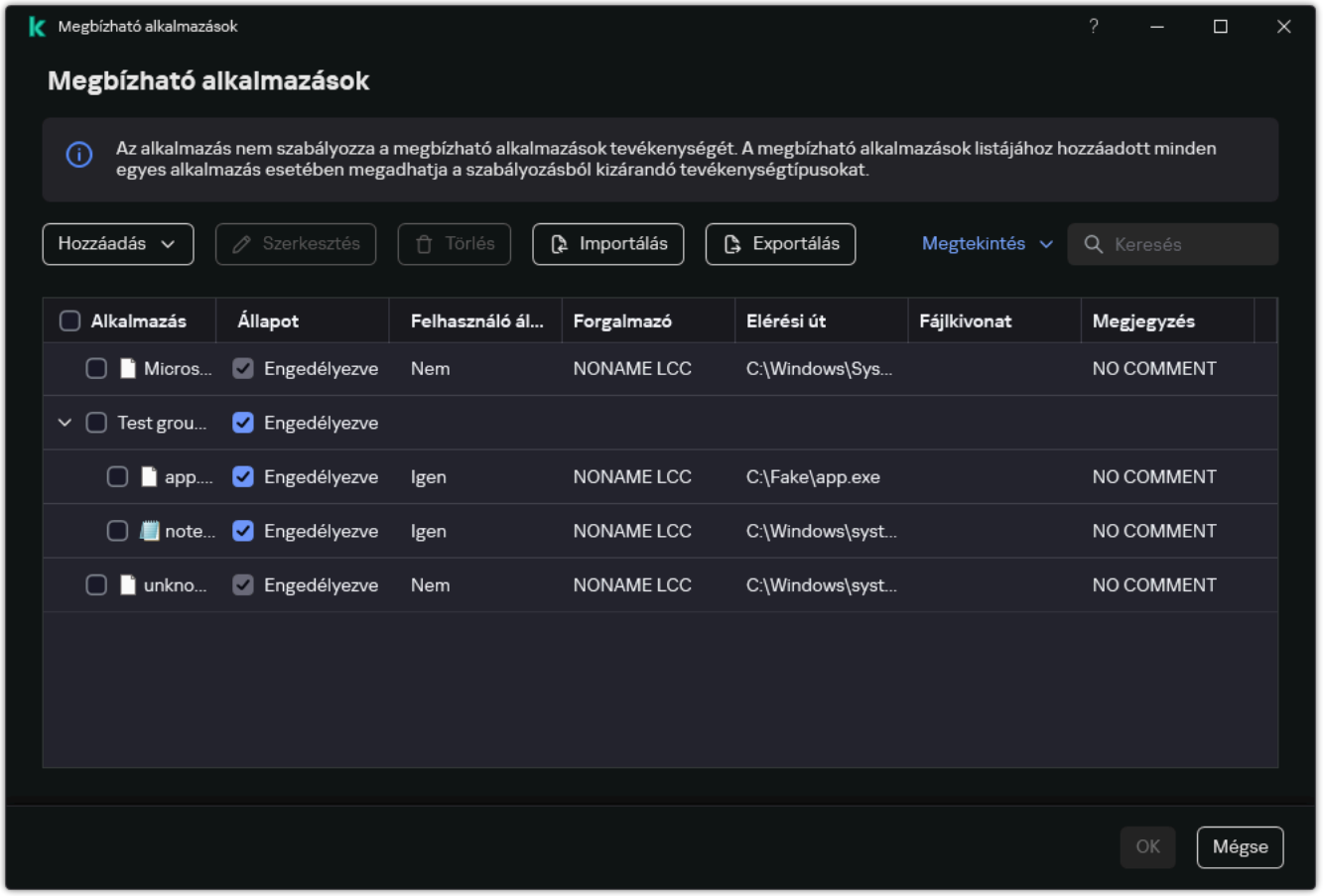
c. Kattintson az **Export** gombra.

d. Erősítse meg, hogy csak a kijelölt megbízható alkalmazásokat vagy a teljes listát szeretné exportálni.

e. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a megbízható alkalmazások listáját, és válassza a fájl mentésére kiszemelt mappát.

f. Mentse a fájlt.

A Kaspersky Endpoint Security a megbízható alkalmazások teljes listáját exportálja az XML-fájlba.



Megbízható alkalmazások listája

5. A kizárások listájának importálása:

a. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

b. Kattintson az **Import** gombra.

c. A megnyíló ablakban válassza ki azt az CSV-fájlt, amelyből importálni szeretné a kizárások listáját.

d. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a CSV-fájlból.

6. Megbízható alkalmazások listájának importálása:

a. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.

b. Kattintson az **Import** gombra.

c. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a megbízható alkalmazások listáját.

d. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a megbízható alkalmazásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba az XML-fájlból.

7. Mentse el a módosításokat.

Megbízható digitális aláírással rendelkező alkalmazások kezelése

A rendszertanúsítvány tárhelyének alkalmazásával kizárhatja a megbízható digitális aláírást tartalmazó alkalmazásokat a vírusvizsgálatból. A Kaspersky Endpoint Security automatikusan hozzárendeli ezeket az alkalmazásokat a *Megbízható* csoporthoz.

A megbízható rendszertanúsítvány-tároló használatának megkezdése az Adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.
4. A **Megbízható rendszertanúsítvány-tárhely** területen jelölje be a **Megbízható rendszertanúsítvány-tárhely használata** négyzet.
5. A legördülő listából válassza ki, hogy a Kaspersky Endpoint Security melyik rendszertárhelyet tekintse megbízhatónak.
6. Mentse el a módosításokat.

A megbízható rendszertanúsítvány-tárhely használatának megkezdése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Trusted Zone** szakaszt.
5. Az ablakban kattintson a **Root certificates** hivatkozásra.
6. A megnyíló ablakban jelölje be a **Use trusted system certificate store** négyzetet.
7. Válassza ki, hogy a Kaspersky Endpoint Security melyik rendszertárhelyet tekintse megbízhatónak.
8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A megbízható rendszertanúsítvány-tároló használatának megkezdése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.
3. Válassza ki a **Megbízható rendszertanúsítvány tárhelye** legördülő listán, hogy a Kaspersky Endpoint Security melyik rendszertárhelye tekintendő megbízhatónak.
4. Mentse el a módosításokat.

Melléklet. Előre definiált vizsgálati kizárások és megbízható alkalmazások

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazást Light Agent üzemmódban is telepítheti a virtuális környezetek védelme céljából. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben.

Az előre definiált kizárásokat és megbízható alkalmazásokat a következő módokon választhatja ki:

- Az alkalmazás telepítése.
  - Az alkalmazás telepítése helyben, a Varázsló segítségével
  - Telepítőcsomag tulajdonságai
- A házirend beállítása.
  - Új szabályzat varázsló
  - Szabályzat tulajdonságai: vizsgálati kizárások és megbízható alkalmazások

SQL kiszolgáló

Amikor a Kaspersky Endpoint Security terméket SQL-kiszolgálóra telepíti, létre kell hoznia egy megbízható zónát az előre definiált kizárásokból és megbízható alkalmazásokból, hogy a kiszolgáló működését ne zavarja.

Előre definiált vizsgálati kizárások

Elérési út	SQL verzió
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 R2 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012 R2
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012 R2
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 R2 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012 R2
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012 R2
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 R2 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 R2 2014 2016 2017 2019 2022

Microsoft Exchange-kiszolgáló

Amikor a Kaspersky Endpoint Security terméket Microsoft Exchange-kiszolgálóra telepíti, létre kell hoznia egy megbízható zónát az előre definiált kizárásokból és megbízható alkalmazásokból, hogy a kiszolgáló működését ne zavarja.

Előre definiált vizsgálati kizárások

Elérési út	Microsoft Exchange-verzió
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Elérési út	Microsoft Exchange-verzió
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Előre definiált megbízható alkalmazások

Elérési út	Microsoft Exchange-verzió
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

Előre definiált vizsgálati kizárások

Elérési út	A System Center Configuration Manager verziója
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 R2 2012 R2

Citrix

Amikor a Kaspersky Endpoint Security terméket egy Citrix virtuális környezetbe telepíti, létre kell hoznia egy megbízható zónát az előre definiált kizárásokból és megbízható alkalmazásokból, hogy a kiszolgáló működését ne zavarja.

Előre definiált vizsgálati kizárások

Elérési út
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf

Elérési út
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache

Elérési út	
vdiskdif.vhdx	
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb	

Előre definiált megbízható alkalmazások

Elérési út	Citrix megoldás
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtuális alkalmazásc és asztali számítógépe
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtuális alkalmazásc és asztali számítógépe

Elérési út	Citrix megoldás
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtuális alkalmazásc és asztali számítógépe
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Munkaterüle alkalmazás
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Munkaterüle alkalmazás
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Kiépítés

Elérési út	Citrix megoldás
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Kiépítés
%SystemRoot%\System32\drivers\bnistack6.sys	Kiépítés
%SystemRoot%\System32\drivers\CfsDep2.sys	Kiépítés
%SystemRoot%\System32\drivers\cnicteam.sys	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Kiépítés
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Kiépítés
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Amikor a Kaspersky Endpoint Security terméket egy VMware virtuális környezetbe telepíti, létre kell hoznia egy megbízható zónát az előre definiált megbízható alkalmazásokból, hogy a kiszolgáló működését ne zavarja.

Előre definiált megbízható alkalmazások

Elérési út	VMware megoldás
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon

Elérési út	VMware megoldás
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

A Biztonsági mentés kezelése

A *Biztonsági mentés* tárolja az olyan fájlok másolatait, amelyek törölve vagy módosítva lettek a vírusmentesítés során. A *biztonsági másolat* egy másolt fájl, mely a fájl vírusmentesítése vagy törlése előtt lett létrehozva. A fájlok biztonsági másolatai különleges formátumban vannak tárolva, és nem jelentenek fenyegetést.

A fájlok biztonsági másolatai a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappában vannak tárolva.

A Rendszergazda csoportban lévő felhasználók számára elérhető ez a mappa. A felhasználó, akinek a fiókjáról telepítve lett a Kaspersky Endpoint Security, korlátozott hozzáféréssel rendelkezik ehhez a mappához.

A Kaspersky Endpoint Security nem biztosít lehetőséget a fájlok biztonsági másolatához való felhasználói hozzáférések beállítására.

A vírusmentesítés során néha nem lehet megőrizni az integritást. Ha a vírusmentesítést követően egy vírusmentesített fájlban lévő fontos információkhoz való hozzáférés részben vagy egészben elvész, megpróbálhatja visszaállítani a biztonsági fájlmásolatot az eredeti mappába.

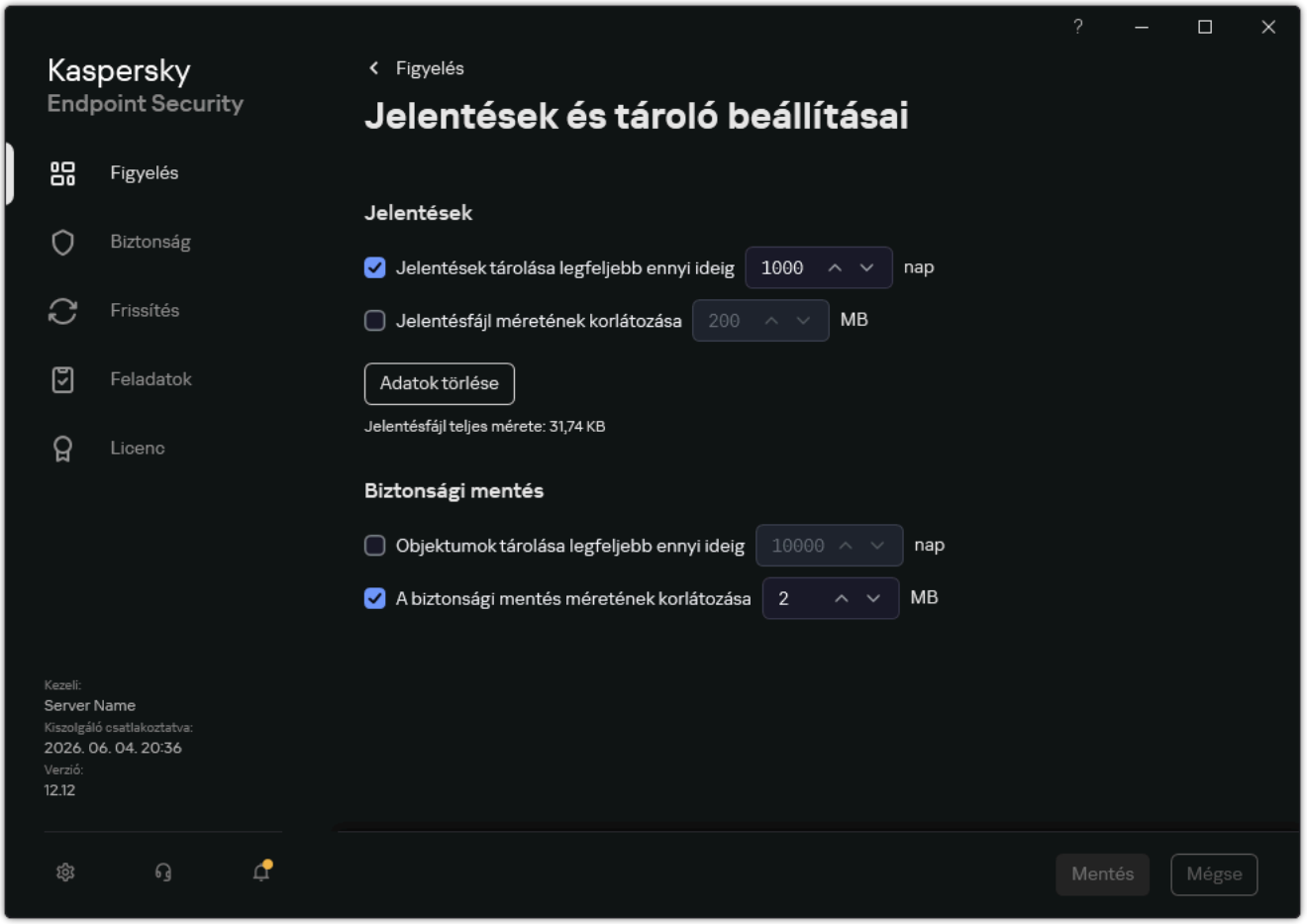
Ha a Kaspersky Endpoint Security a Kaspersky Security Center irányítása alatt fut, előfordulhat, hogy a fájlok biztonsági másolatait megkapja a Kaspersky Security Center felügyeleti kiszolgáló. A Kaspersky Security Center fájlok biztonsági másolatainak kezeléséről szóló további részletekért lásd a Kaspersky Security Center súgórendszerét.

A biztonsági mentésben lévő fájlok maximális tárolási idejének beállítása.

A fájlok másolatainak a biztonsági mentésben való maximális tárolási időtartama alapértelmezett esetben 30 nap. A maximális tárolási időtartam lejárata után a Kaspersky Endpoint Security törli a legrégebbi fájlokat a Biztonsági mentésből.

A biztonsági mentésben lévő fájlok maximális tárolási idejének beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban az **Általános beállítások** alatt válassza a **Jelentések és tároló** részt.



Biztonsági mentés beállításai

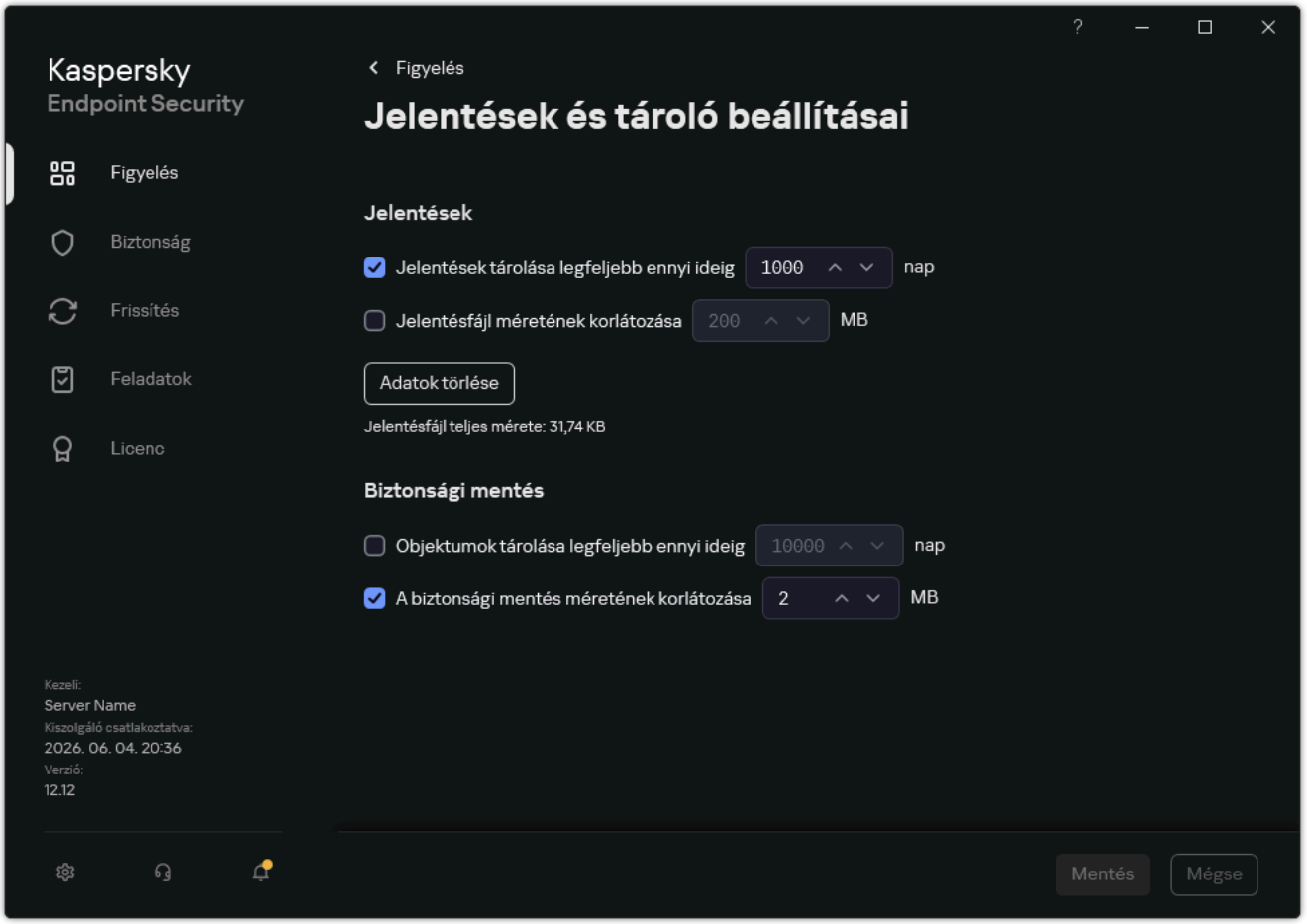
3. Ha a biztonsági mentésben lévő fájlok másolatainak tárolási idejét korlátozni szeretné, jelölje be az **Objektumok tárolása legfeljebb ennyi ideig N nap** jelölőnégyzetet a **Biztonsági mentés** részen. Adja meg a biztonsági mentésben lévő fájlok másolatainak maximális tárolási idejét.
4. Mentse el a módosításokat.

A biztonsági mentés maximális méretének megadása

Meghatározhatja a Biztonsági mentés maximális méretét. A biztonsági mentés mérete alapértelmezés szerint korlátlan. A Kaspersky Endpoint Security automatikusan törli a legrégebbi fájlokat a biztonsági mentésből, ha a tároló eléri a maximális méretét.

A biztonsági mentés maximális méretének megadása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban az **Általános beállítások** alatt válassza a **Jelentések és tároló** részt.



Biztonsági mentés beállításai

3. A **Biztonsági mentés** részen válassza ki **A biztonsági mentés méretének korlátozása N MB-ra** jelölőnégyzetet. Ha a jelölőnégyzet be van jelölve, a maximális tárhelyet a meghatározott érték korlátozza. Alapértelmezés szerint a maximális méret 1024 MB. A tárhely maximális méretének túllépését elkerülve a Kaspersky Endpoint Security automatikusan törli a tárhely legrégebbi fájljait a maximális méret elérésekor.
4. Mentse el a módosításokat.

Fájlok visszaállítása a Biztonsági mentésből

Ha egy fájlban rosszindulatú kód észlelhető, a Kaspersky Endpoint Security blokkolja a fájlt, hozzárendeli a *Nincs vírusmentesítve* állapotot, majd elhelyezi másolatát a Biztonsági mentésbe, és megkísérli a vírusmentesítést. Ha a fájl vírusmentesítése sikerül, akkor biztonsági másolatának állapota *Vírusmentesített* értékűre változik. A fájl az eredeti mappában elérhetővé válik. Ha egy fájlt nem lehet vírusmentesíteni, a Kaspersky Endpoint Security törli eredeti mappájából. A fájl a biztonsági másolatból visszaállítható az eredeti mappába.

A számítógép újraindításakor törlésre kerül állapottal rendelkező fájlok nem állíthatóak vissza. Indítsa újra a számítógépet, és a fájlállapot *Vírusmentesítve* vagy *Törölve* állapotra módosul. A fájl a biztonsági másolatból is visszaállítható az eredeti mappába.

Ha Windows Store alkalmazás részét alkotó fájlban észlelhető rosszindulatú kód, a Kaspersky Endpoint Security azonnal törli a fájlt, anélkül, hogy a Biztonsági mentésbe helyezné. A Windows Store alkalmazás integritása az operációs rendszer megfelelő eszközeivel állítható vissza (a Windows Store alkalmazások visszaállításával kapcsolatos részleteket lásd a Microsoft Windows súgófájljaiban).

A fájlok biztonsági másolatai táblázatos formában jelennek meg. A biztonsági másolatánál megjelenik az útvonal az fájl eredeti mappájához. A fájl eredeti mappájának útvonala személyes adatokat is tartalmazhat.

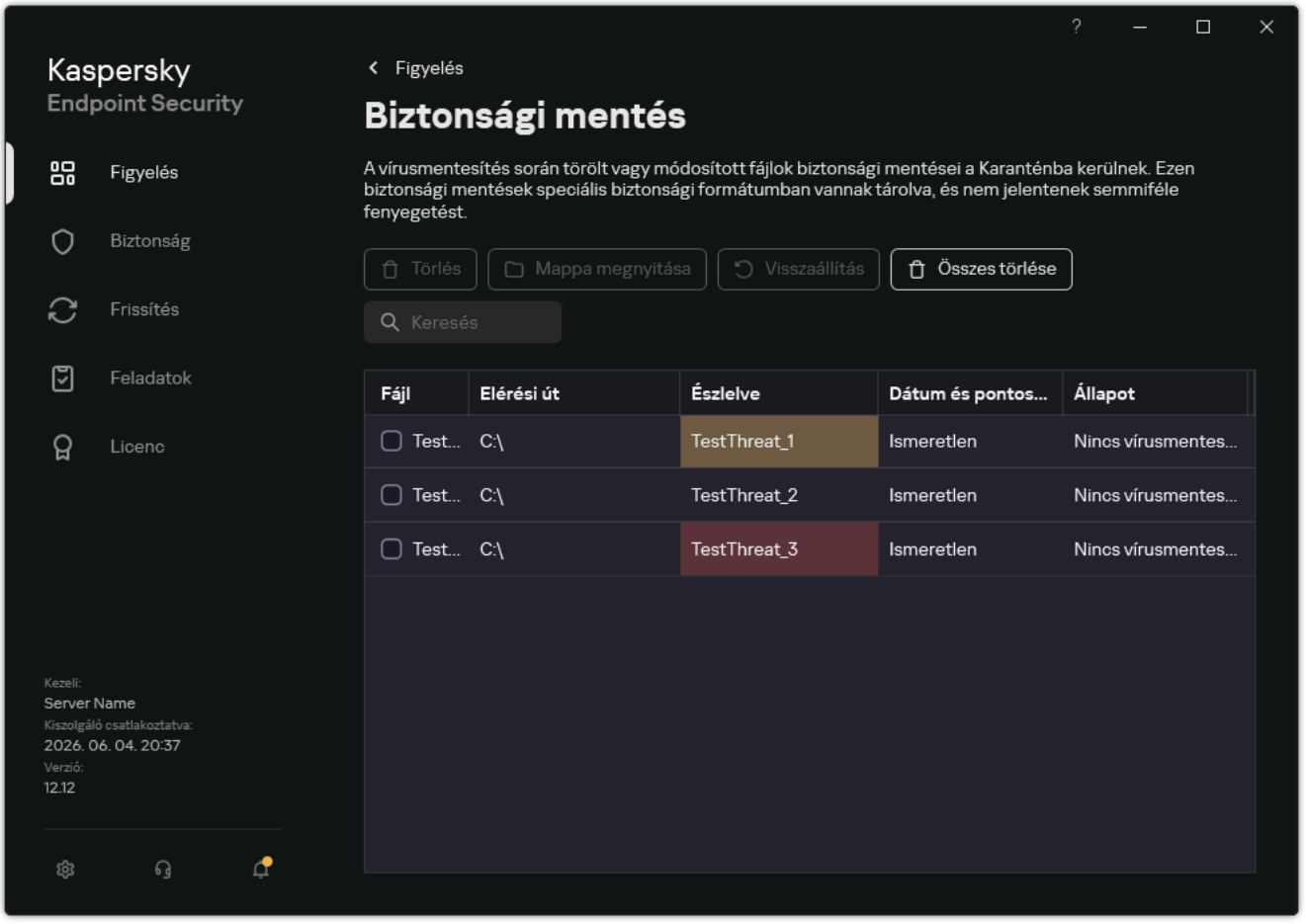
Ha a Biztonsági mentésbe több, ugyanazon nevű, de más tartalmú fájl kerül, akkor csak az utolsóként elhelyezett fájl állítható vissza.

Fájlok visszaállítása a Biztonsági mentésből:

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Biztonsági mentés** csempére.

2. Ez megnyitja a biztonsági mentésben található fájlok listáját; a listában válassza ki a visszaállítani kívánt fájlokat, majd kattintson a **Visszaállítás** gombra.

A Kaspersky Endpoint Security a kiválasztott fájlokat visszaállítja a biztonsági mentésből eredeti mappájukba.



Biztonsági mentés

Fájlok biztonsági másolatainak törlése a Biztonsági mentésből

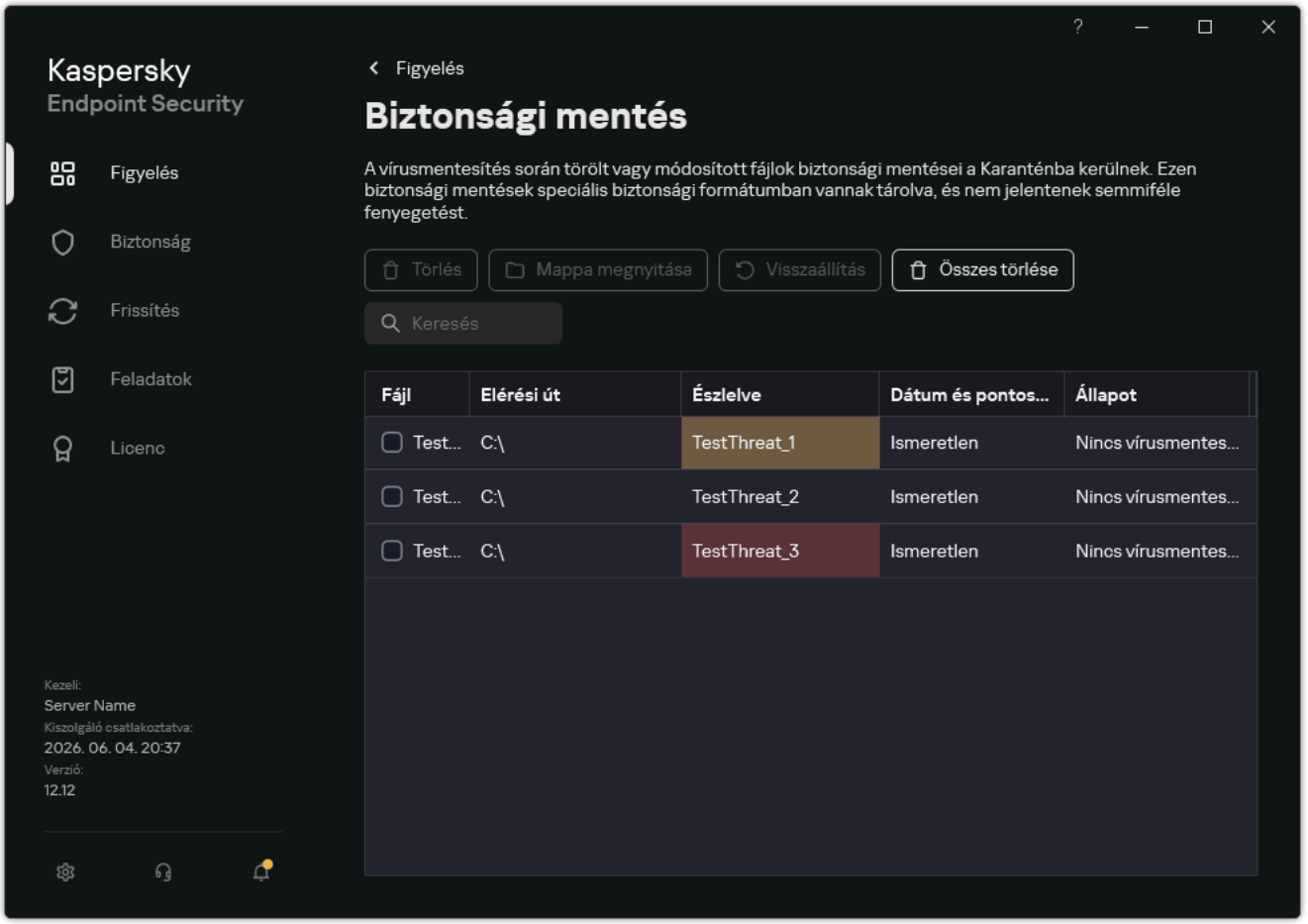
A Kaspersky Endpoint Security minden állapotú fájl biztonsági másolatait automatikusan törli a Biztonsági mentésből az alkalmazás beállításokban megadott tárolási időtartam elteltével. A fájlok biztonsági másolata kézileg is törölhető a Biztonsági mentésből.

Fájlok biztonsági másolatainak törlése a Biztonsági mentésből:

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Biztonsági mentés** csempére.

2. Ez megnyitja a biztonsági mentésben található fájlok listáját; ebben a listában válassza ki a biztonsági mentésből törlendő fájlokat, majd kattintson a **Törlés** gombra.

A Kaspersky Endpoint Security a kiválasztott fájlok biztonsági másolatait törli a Biztonsági mentésből.



Biztonsági mentés

Értesítési szolgáltatás

A Kaspersky Endpoint Security működése során különböző események léphetnek fel. Az ilyen eseményekről szóló értesítések lehetnek tisztán tájékoztató jellegűek, vagy tartalmazhatnak létfontosságú információkat. Az értesítések tájékoztatást nyújthatnak például adatbázisok és alkalmazásmodulok sikeres frissítéséről, vagy a javítást igénylő összetevőhibákról.

A Kaspersky Endpoint Security támogatja az információk naplózását az eseményekről a Microsoft Windows eseménynaplóban és / vagy a Kaspersky Endpoint Security eseménynaplójában.

A Kaspersky Endpoint Security az alábbi módokon adja át az értesítéseket:

- a Microsoft Windows tálca értesítési területén előbukkanó értesítések formájában;
- e-mailben.

Az események értesítéseinek kézbesítése beállítható. Az események értesítéseinek módját eseménytípusonként lehet beállítani.

Ha az események táblázata segítségével állítja be az értesítési szolgáltatást, az alábbi műveleteket végezheti el:

- Az értesítési szolgáltatás eseményeinek szűrése oszlopértékek vagy egyéni szűrési feltételek szerint.
- Keresési funkció használata az értesítési szolgáltatás eseményeinél.
- Értesítési szolgáltatás eseményeinek sorba rendezése.
- Az értesítési szolgáltatás eseményeinek listáján látható oszlopok sorrendjének és készletének módosítása.

Az eseménynapló beállításainak megadása

Az eseménynapló beállításainak megadása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
3. Az **Értesítések** részen kattintson az **Értesítések konfigurálása** gombra.

   A Kaspersky Endpoint Security összetevők és feladatok az ablak bal oldalán jelennek meg. Az ablak jobb oldalán a kiválasztott összetevőnél vagy feladatnál előállított események listája látható.

   Az események a következő felhasználói adatokat tartalmazhatják:

   - Útvonalak a Kaspersky Endpoint Security által vizsgált fájlokhoz.
   - Útvonalak a Kaspersky Endpoint Security futása közben módosított beállításkulcsokhoz.
   - Microsoft Windows felhasználónév.
   - A felhasználó által megnyitott weboldalak címei.

4. Az ablak bal oldalán válassza ki azt az összetevőt vagy feladatot, amelynek az eseménynaplózási beállításait be szeretné állítani.

5. Tegyen jelölést a releváns eseményekkel szembeni jelölőnégyzetekbe a **Mentés a helyi jelentésbe** és a **Mentés a Windows eseménynaplóba** oszlopban.

   Azok az események, amelyek jelölőnégyzeteit bejelölte a **Mentés a helyi jelentésbe** oszlopban, megjelennek az alkalmazásnaplók alatt. Azok az események, amelyek jelölőnégyzeteit bejelölte a **Mentés a Windows eseménynaplóba** oszlopban, megjelennek az `Application` részben, a Windows-naplók alatt.

6. Mentse el a módosításokat.

Az értesítések megjelenítésének és kézbesítésének beállítása

Az értesítések megjelenítésének és kézbesítésének beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.

3. Az **Értesítések** részen kattintson az **Értesítések konfigurálása** gombra.

   A Kaspersky Endpoint Security összetevők és feladatok az ablak bal oldalán jelennek meg. Az ablak jobb oldalán a kiválasztott összetevőnél vagy feladatnál előállított események listája látható.

   Az események a következő felhasználói adatokat tartalmazhatják:

   - Útvonalak a Kaspersky Endpoint Security által vizsgált fájlokhoz.
   - Útvonalak a Kaspersky Endpoint Security futása közben módosított beállításkulcsokhoz.
   - Microsoft Windows felhasználónév.
   - A felhasználó által megnyitott weboldalak címei.

4. Az ablak bal oldalán válassza ki azt az összetevőt vagy feladatot, amelynek az értesítéskézbesítési beállításait be szeretné állítani.

5. Az **Értesítés a képernyőn** oszlopban jelölje be a vonatkozó események melletti jelölőnégyzeteket.

   A kiválasztott eseményekre vonatkozó információk a Microsoft Windows tálca értesítési területén előbukkanó értesítések formájában jelennek meg a képernyőn.

6. Az **Értesítés e-mailben** oszlopban jelölje be a vonatkozó események melletti jelölőnégyzeteket.

   A kiválasztott eseményekre vonatkozó információk e-mailben érkeznek meg, ha meg vannak adva az e-mail értesítés kézbesítési beállításai.

7. Kattintson az **OK** gombra.

8. Ha engedélyezte az e-mail értesítéseket, konfigurálja az e-mailek kézbesítésének beállításait:

   a. Kattintson az **E-mail alapú értesítések konfigurálása** gombra.

   b. Jelölje be az **Értesítés az eseményekről** jelölőnégyzetet a Kaspersky Endpoint Security **Értesítés e-mailben** oszlopban kiválasztott eseményeire vonatkozó információk kézbesítésének engedélyezéséhez.

   c. Adja meg az e-mail értesítések kézbesítési beállításait.

   d. Kattintson az **OK** gombra.

9. Mentse el a módosításokat.

Az alkalmazás állapotával kapcsolatos figyelmeztetések értesítési területen történő megjelenítésének beállítása

Az alkalmazás állapotával kapcsolatos figyelmeztetések értesítési területen történő megjelenítésének beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
3. **Az alkalmazás állapotának megjelenítése az értesítési területen** részben jelölje be a jelölőnégyzeteket azokkal az eseménykategóriákkal szemben, amelyekről értesítést szeretne látni a Microsoft Windows értesítési területén.
4. Mentse el a módosításokat.

Ha a kiválasztott kategóriába tartozó események történnek, az értesítési területen lévő alkalmazásikon a figyelmeztetés súlyosságától függően vagy ikonra változik.

Üzenetek a felhasználók és a rendszergazda között

Az Alkalmazásfelügyelő, az Eszközfelügyelő a Webfelügyelő és az Adaptív Anomáliafelügyelő összetevők lehetővé teszik, hogy azon számítógépek felhasználói, amelyeken telepítve van a Kaspersky Endpoint Security, üzeneteket küldjenek a rendszergazdának.

Az alábbi esetekben válhat szükségessé, hogy a felhasználók üzenetet küldjenek a helyi hálózati rendszergazda részére:

- Az Eszközfelügyelő blokkolta a hozzáférést az eszközhöz.

  A blokkolt eszközhöz való hozzáférést kérő üzenet sablonja a Kaspersky Endpoint Security felületén az Eszközfelügyelő részben található.

- Az Alkalmazásfelügyelő blokkolta egy alkalmazás indítását.

  A blokkolt alkalmazás indításának engedélyezését kérő üzenet sablonja a Kaspersky Endpoint Security felületén az Alkalmazásfelügyelő részben található.

- A Webfelügyelő blokkolta a hozzáférést egy webes erőforráshoz.

  A blokkolt webes erőforráshoz való hozzáférést kérő üzenet sablonja a Kaspersky Endpoint Security felületén a Webfelügyelő részben található.

Az üzenetküldés módszere és a sablonválasztás attól függ, hogy fut-e aktív Kaspersky Security Center irányelv azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, és hogy van-e kapcsolat a Kaspersky Security Center felügyeleti kiszolgálóval. Az alábbi forgatókönyvek lehetségesek:

- Ha nem fut Kaspersky Security Center irányelv azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, akkor a felhasználó üzenetét a helyi hálózati rendszergazda kapja meg e-mailben.

  Az üzenet mezőibe a Kaspersky Endpoint Security helyi felületén megadott sablonból származó mezőértékek kerülnek.

- Ha fut Kaspersky Security Center irányelv azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, akkor szokásos üzenet kerül a Kaspersky Security Center felügyeleti kiszolgálóra.

  Ebben az esetben a felhasználói üzeneteket a Kaspersky Security Center eseménytárhelyen lehet megtekinteni (lásd az alábbi ábrát). Az üzenet mezőibe a Kaspersky Security Center irányelvben megadott sablonból származó mezőértékek kerülnek.

- Ha a Kaspersky Security Center vakáció-irányelve fut azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, akkor az üzenetküldés módszere attól függ, hogy van-e kapcsolat a Kaspersky Security Centerrel.

  - Ha kapcsolat létesül a Kaspersky Security Centerrel, akkor a Kaspersky Endpoint Security a szokásos üzenetet elküldi a Kaspersky Security Center felügyeleti kiszolgálóra.

  - Ha nincs kapcsolat a Kaspersky Security Centerrel, akkor a felhasználó üzenetét a helyi hálózati rendszergazda kapja meg e-mailben.

  Az üzenet mezőibe mindkét esetben a Kaspersky Security Center irányelvben megadott sablonból származó mezőértékek kerülnek.

A Kaspersky Security Center eseménytárában lévő felhasználói üzenet megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Events** lapot.

   A Kaspersky Security Center munkaterületen megjelenik a Kaspersky Endpoint Security működése során előforduló összes esemény, köztük a rendszergazdának szóló, a helyi hálózat felhasználóitól érkezett üzenetek.

3. Az eseményszűrő beállításához válassza ki az **Event selections** legördülő listán a **User requests** lehetőséget.

4. Válassza ki a rendszergazdának elküldött üzenetet.

5. Kattintson az **Open event properties window** gombra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

A jelentések kezelése

Az egyes Kaspersky Endpoint Security összetevők működésére, az egyes vizsgálati feladatok, frissítési feladatok, integritási ellenőrzési feladatok teljesítményére, valamint az alkalmazás általános működésére vonatkozó információk jelentésekbe kerülnek.

A jelentések a `C:\ProgramData\Kaspersky Lab\KES.14.1\Report` mappában vannak tárolva.

A jelentések a következő felhasználói adatokat tartalmazhatják:

- Útvonalak a Kaspersky Endpoint Security által vizsgált fájlokhoz.
- Útvonalak a Kaspersky Endpoint Security futása közben módosított beállításkulcsokhoz.
- Microsoft Windows felhasználónév.
- A felhasználó által megnyitott weboldalak címei.

A jelentésben szereplő adatok táblázatos formában érhetők el. A táblázatban minden sor egy-egy különálló esemény adatait tartalmazza. Az események attribútumai a táblázatoszlopokban helyezkednek el. Egyes oszlopok összetettek, melyekben további attribútumokat tartalmazó beágyazott oszlopok találhatók. A további attribútumok megtekintéséhez kattintson az oszlop neve melletti ⊞ gombra. A különféle összetevők működése, illetve a különféle feladatok végrehajtása közben naplózott eseményekhez más-más attribútumkészlet tartozik.

A következő jelentések állnak rendelkezésre:

- **Rendszer-felülvizsgálati** jelentés. Információkat tartalmaz a felhasználó és az alkalmazás közti interakció során és általában az alkalmazás működése közben előforduló olyan eseményekről, amelyek nem kapcsolódnak a Kaspersky Endpoint Security valamelyik konkrét összetevőjéhez vagy feladatához.
- A Kaspersky Endpoint Security összetevőinek működésére vonatkozó jelentések.
- Kaspersky Endpoint Security feladatjelentések.
- **Adattitkosítási** jelentés. Információkat tartalmaz az adattitkosítás és -visszafejtés során előforduló eseményekről.

A jelentések az alábbi fontossági szinteket alkalmazzák:

ⓘ **Informational messages**. Az általában fontos információkat nem tartalmazó referenciaesemények.

⚠ **Figyelmeztetések**. Olyan fontos eseményekről szóló értesítések, amelyekre figyelni kell, mert fontos helyzeteket jeleznek a Kaspersky Endpoint Security program működésében.

⊘ **Kritikus események**. Kritikus jelentőségű események, amelyek a Kaspersky Endpoint Security működésével kapcsolatos problémákra vagy a felhasználó számítógépe védelmének sebezhetőségére utalnak.

A jelentések kényelmes feldolgozása érdekében az adatok képernyőn való megjelenése az alábbi módokon módosítható:

- Az események listájának szűrése különböző feltételek szerint.
- Adott esemény megtalálása a keresési funkcióval.
- A kiválasztott esemény megtekintése egy külön részben.
- Az események listájának rendezése jelentésoszlopok szerint.
- Az eseményszűrő által csoportosított események megjelenítése és elrejtése a ⊞ gombbal.
- A jelentésben látható oszlopok sorrendjének és elrendezésének módosítása.

Az előállított jelentést szükség esetén szövegfájlba mentheti. A jelentésből törölhetők továbbá a csoportokba helyezett Kaspersky Endpoint Security összetevőkre és feladatokra vonatkozó információk.

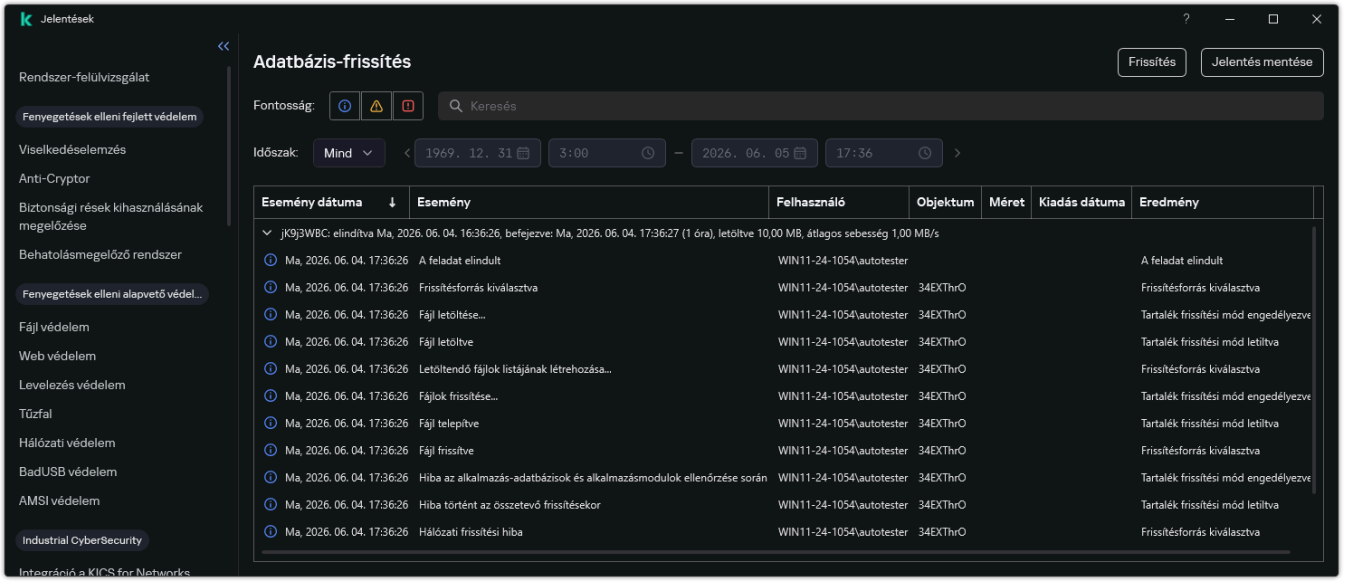
Ha a Kaspersky Endpoint Security alkalmazás a Kaspersky Security Center felügyelete alatt fut, az eseményekre vonatkozó információkat továbbíthatja az alkalmazás a Kaspersky Security Center felügyeleti kiszolgálónak (további részletekről tájékozódjon a Kaspersky Security Center súgójában).

Jelentések megtekintése

Ha a felhasználó meg tudja tekinteni a jelentéseket, láthatja a jelentésekben szereplő eseményeket is.

Jelentések megtekintése:

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Jelentések** csempére.



Jelentések

2. Válassza ki az összetevők és feladatok listájában az adott összetevőt vagy feladatot.

   A képernyő kijelzőjének jobb oldalán megjelenik egy jelentés, mely a Kaspersky Endpoint Security kiválasztott összetevőjének vagy feladatának működése által okozott események listáját tartalmazza. A jelentésben szereplő eseményeket az egyik oszlop celláinak értékei alapján rendezheti.

3. Részletes információkat tekinthet meg az eseményről, kiválaszthat eseményt a jelentésben.

Az ablak alsó részén megjelenik egy terület az esemény összegzésével.

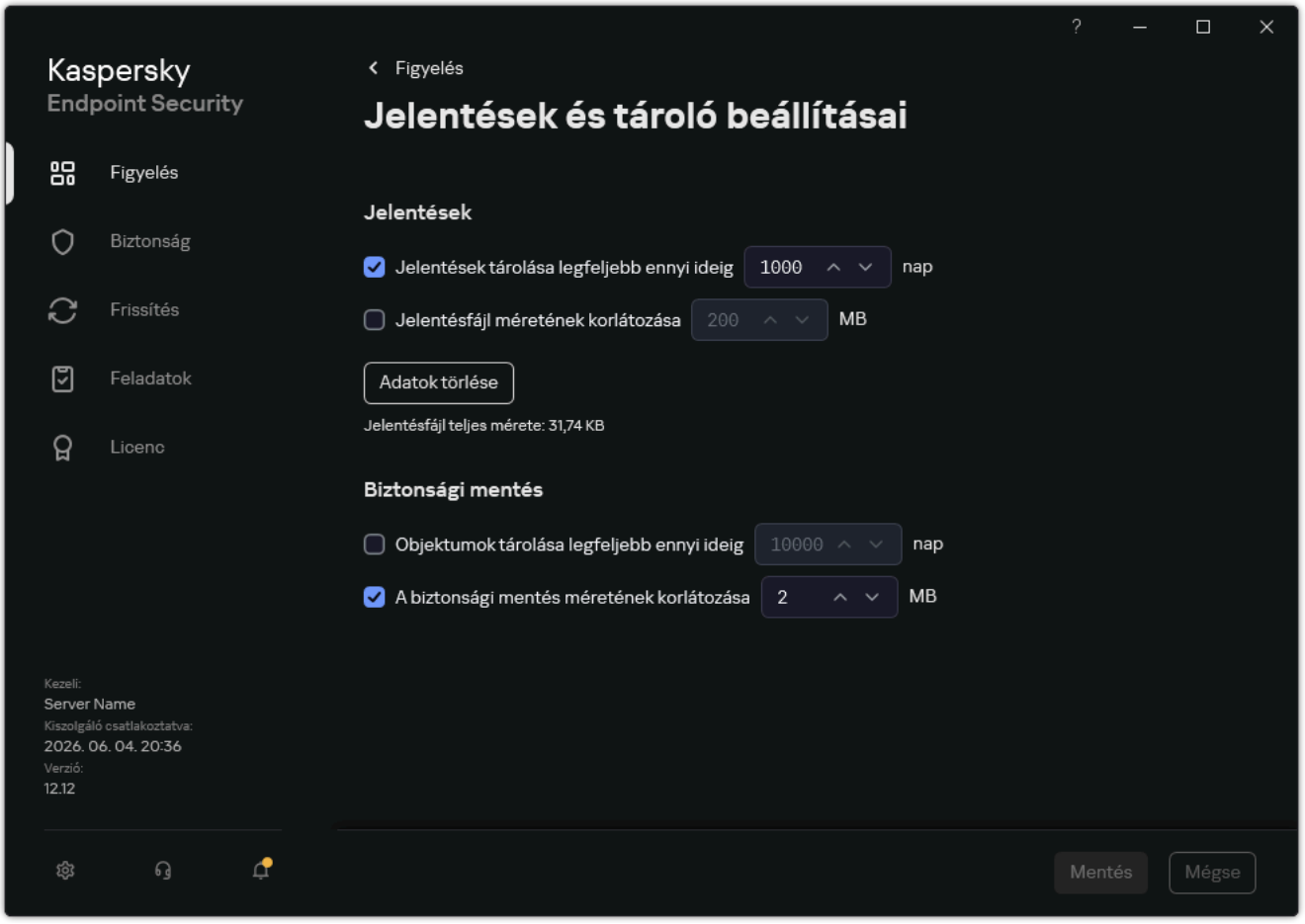
A jelentés maximális tárolási időtartamának beállítása

A Kaspersky Endpoint Security által naplózott eseményekről szóló jelentések maximális tárolási időtartama alapértelmezett esetben 30 nap. Ezt követően a Kaspersky Endpoint Security automatikusan törli a jelentésfájlban lévő legrégebbi bejegyzéseket.

A jelentések maximális tárolási időtartamának módosítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakban az **Általános beállítások** alatt válassza a **Jelentések és tároló** részt.



Jelentésbeállítások

3. Ha korlátozni szeretné a jelentés tárolási idejét, jelölje be a **Jelentések tárolása legfeljebb ennyi ideig N napig** jelölőnégyzetet a **Jelentések** részen. Határozza meg a jelentés maximális tárolási időtartamát.

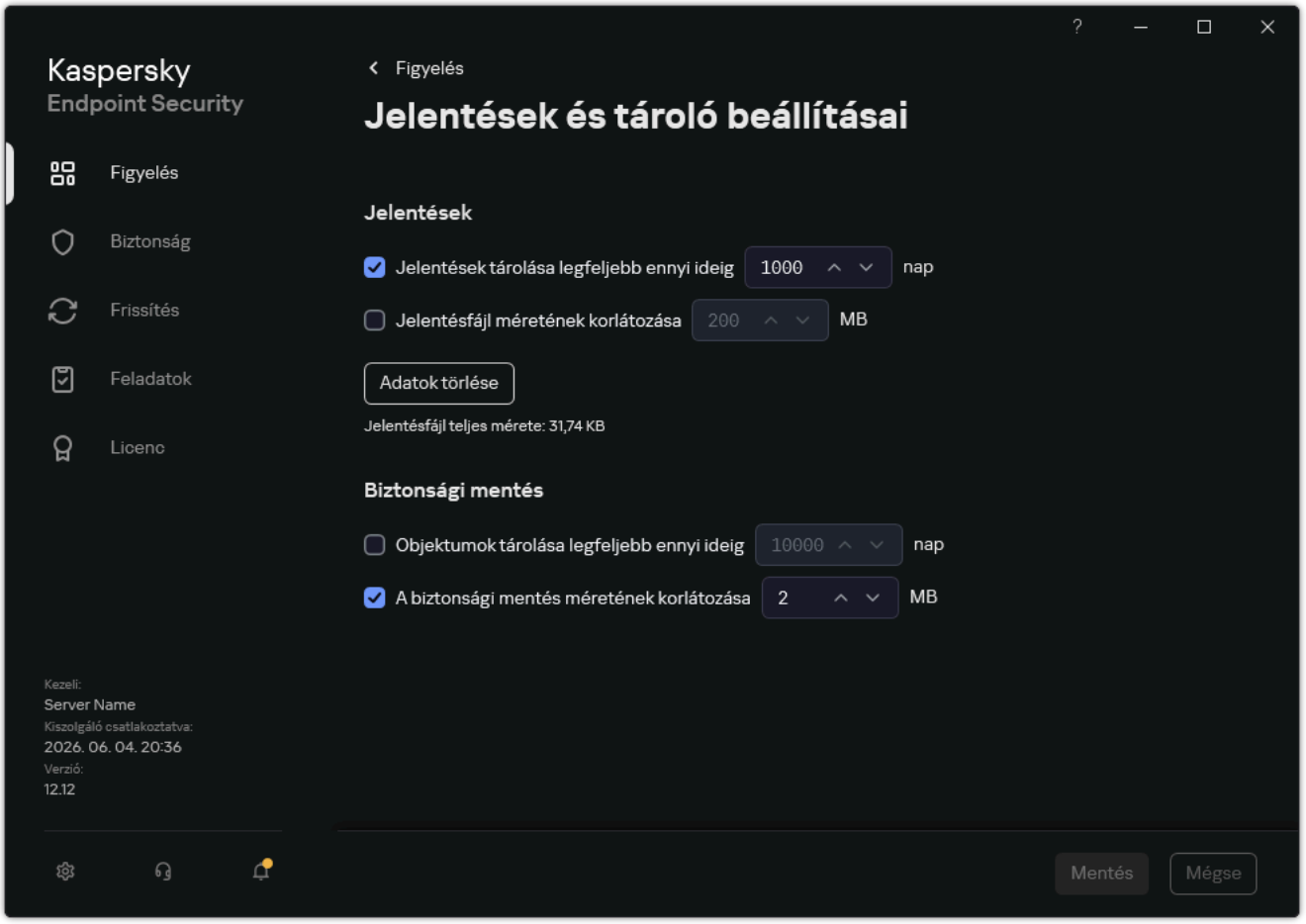
4. Mentse el a módosításokat.

A jelentésfájlok maximális méretének beállítása

Korlátozhatja a jelentést tartalmazó fájl maximális méretét. Alapértelmezés szerint a jelentésfájl maximális mérete 1024 MB. A jelentésfájlok maximális méretének túllépését elkerülendő a Kaspersky Endpoint Security automatikusan törli a jelentésfájlok legrégebbi bejegyzéseit a maximális méret elérésekor.

A jelentés maximális fájlméretének beállítása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban az **Általános beállítások** alatt válassza a **Jelentések és tároló** részt.



Jelentésbeállítások

3. A **Jelentések** részen jelölje be a **Jelentésfájl méretének korlátozása N MB-ra** jelölőnégyzetet, ha korlátozni szeretné egy jelentésfájl méretét. Határozza meg a jelentésfájl maximális méretét.
4. Mentse el a módosításokat.

Jelentés mentése fájlba

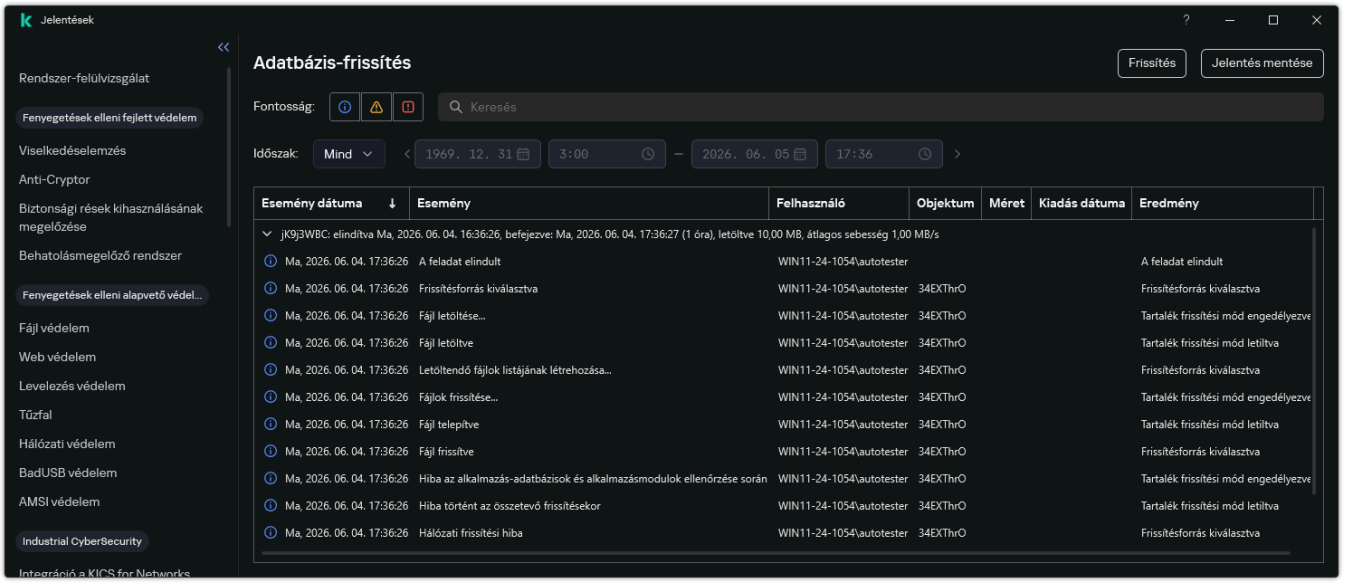
A felhasználó személyes felelőssége, hogy gondoskodjon a fájlba mentett jelentés információinak biztonságáról, főleg az ehhez való hozzáférés felügyeletéről és korlátozásáról.

Az előállított jelentések szöveg formátumú fájlba (TXT), illetve CSV-fájlba menthetők.

A Kaspersky Endpoint Security a jelentésekben lévő eseményeket ugyanúgy naplózza, ahogy azok a képernyőn megjelennek, azaz ugyanazzal az eseményattribútum-készlettel és -sorrendben.

Jelentés mentése fájlba:

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Jelentések** csempére.



Jelentések

2. Ez megnyit egy ablakot; ebben az ablakban válassza ki az összetevőt vagy a feladatot.

   A jelentés az ablak jobb oldali részén jelenik meg, amely a Kaspersky Endpoint Security kiválasztott védelmi összetevőjének működése során történő események listáját tartalmazza.

3. Szükség esetén az adatok jelentésekben való megjelenését az alábbiakkal módosíthatja:

   - Események szűrése
   - Események közötti keresés
   - Oszlopok átrendezése
   - Események rendezése

4. Kattintson a **Jelentés mentése** gombra az ablak jobb felső részén.

5. A megnyíló ablakban adja meg a jelentésfájl célmappáját.

6. Adja meg a jelentésfájl nevét.

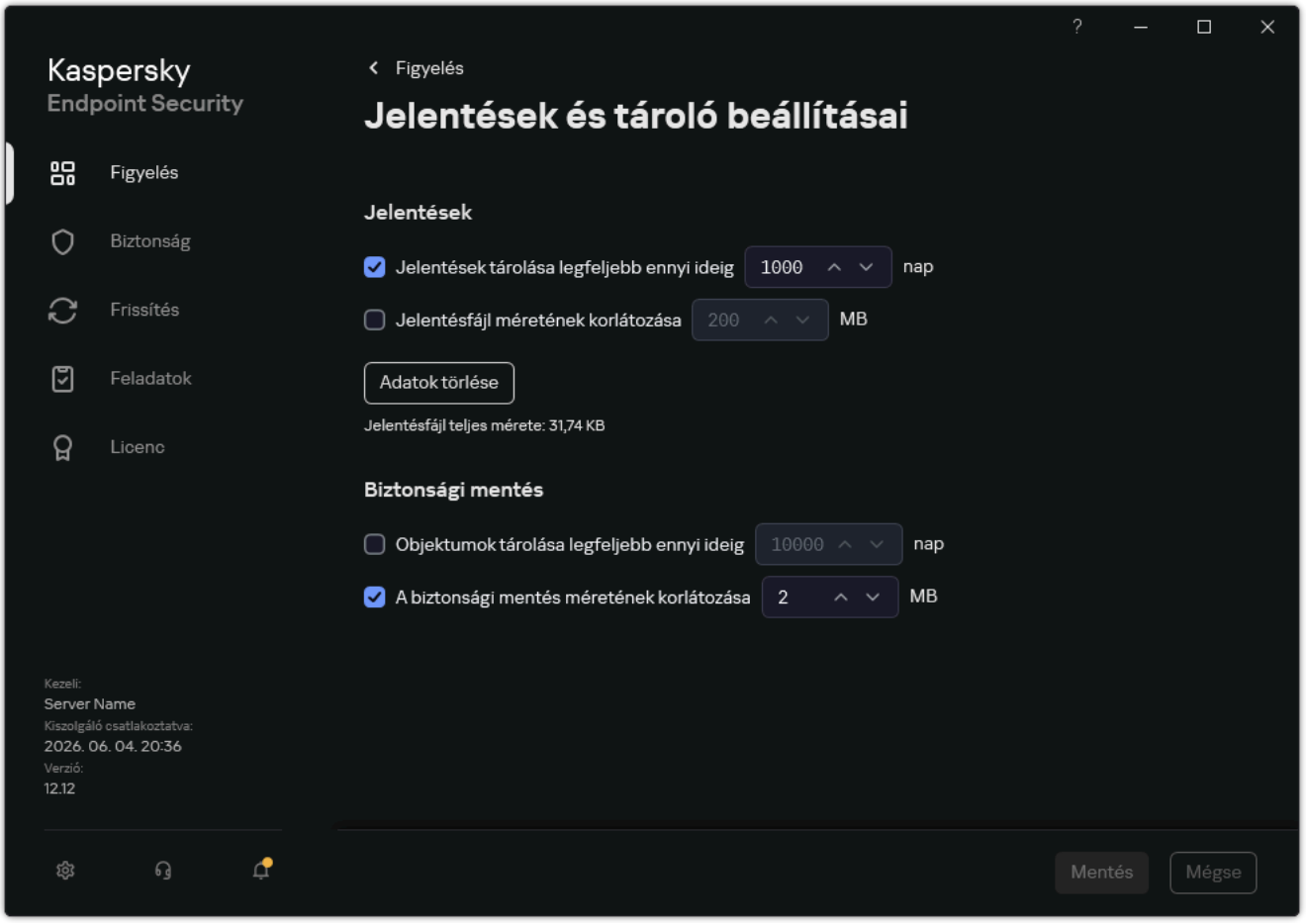
7. Válassza ki a jelentésfájl szükséges formátumát: TXT vagy CSV.

8. Mentse el a módosításokat.

Jelentések törlése

Információk törlése jelentésekből:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakban az **Általános beállítások** alatt válassza a **Jelentések és tároló** részt.



Jelentésbeállítások

3. A **Jelentések** részen kattintson a **Törlés** gombra.
4. Ha a Jelszóvédelem engedélyezve van, a Kaspersky Endpoint Security kérheti a felhasználói fiók bejelentkezési adatait. Az alkalmazás kéri a felhasználói fiók bejelentkezési adatait, ha a felhasználó nem rendelkezik a szükséges jogosultsággal.

A Kaspersky Endpoint Security törli az alkalmazás összetevőire és a feladatokra vonatkozó összes jelentést.

A Kaspersky Endpoint Security önvédelme

Az Önvédelem megakadályozza, hogy más alkalmazások olyan műveleteket hajtsanak végre, amelyek zavarhatják a Kaspersky Endpoint Security működését, például eltávolíthatják a Kaspersky Endpoint Security alkalmazást a számítógépről. A Kaspersky Endpoint Security számára rendelkezésre álló önvédelmi technológiák készlete attól függ, hogy az operációs rendszer 32 bites vagy 64 bites verziójú-e (lásd az alábbi táblázatot). Az Önvédelem magában foglalja a Jelszóvédelem és a Felügyeleti kiszolgáló kapcsolatvédelmét is.

A *Jelszóvédelemmel* korlátozhatja a felhasználók Kaspersky Endpoint Security-hez történő hozzáférését, a megadott jogosultságok alapján (például, jogosultság az alkalmazásból való kilépéshez).

A *Felügyeleti kiszolgálói kapcsolatvédelem* megakadályozza a számítógép illetéktelen újracsatlakozását egy nem megbízható kiszolgálóhoz.

A Kaspersky Endpoint Security önvédelmi technológiái

Technológia	Leírás	x86 rendszerű számítógép	x64 rendszerű számítógép
Önvédelmi mechanizmus	A technológia blokkolja a hozzáférést a következő alkalmazásösszetevőkhöz: • a Kaspersky Endpoint Security telepítési mappájában található fájlok és az alkalmazás egyéb fájljai; • beállításkulcsok az alkalmazáshoz tartozó rekordokkal; • az alkalmazás által futtatott folyamatok.	✓	✓
AM-PPL (Antimalware Protected Process Light)	A technológia védi a Kaspersky Endpoint Security-folyamatokat a rosszindulatú tevékenységek ellen. Az AM-PPL technológia részleteiért lásd a Microsoft weboldalt. Az AM-PPL technológia a Windows 10 1703-as (RS2) vagy újabb verziói, valamint a Windows Server 2019 operációs rendszerek számára érhető el.	✓	✓
Külső kezelés elleni védelmi mechanizmus	Ez a technológia megakadályozza, hogy a más alkalmazások (például a TeamViewer vagy a RemotelyAnywhere) hozzáférjenek a Kaspersky Endpoint Security szolgáltatáshoz.	✓	– (kivéve Windows 7 esetén)

Az Önvédelem be- és kikapcsolása

A Kaspersky Endpoint Security megakadályozza a merevlemezen lévő alkalmazásfájlok, a memóriafolyamatok és a beállításjegyzék bejegyzései módosítását és törlését.

A technológia blokkolja a hozzáférést a következő alkalmazásösszetevőkhöz:

- a Kaspersky Endpoint Security telepítési mappájában található fájlok és az alkalmazás egyéb fájljai;
- beállításkulcsok az alkalmazáshoz tartozó rekordokkal;
- az alkalmazás által futtatott folyamatok.

A Kaspersky Endpoint Security önvédelmi mechanizmusa alapértelmezés szerint be van kapcsolva.

Az Önvédelem engedélyezése vagy letiltása a felügyeleti konzolon (MMC)

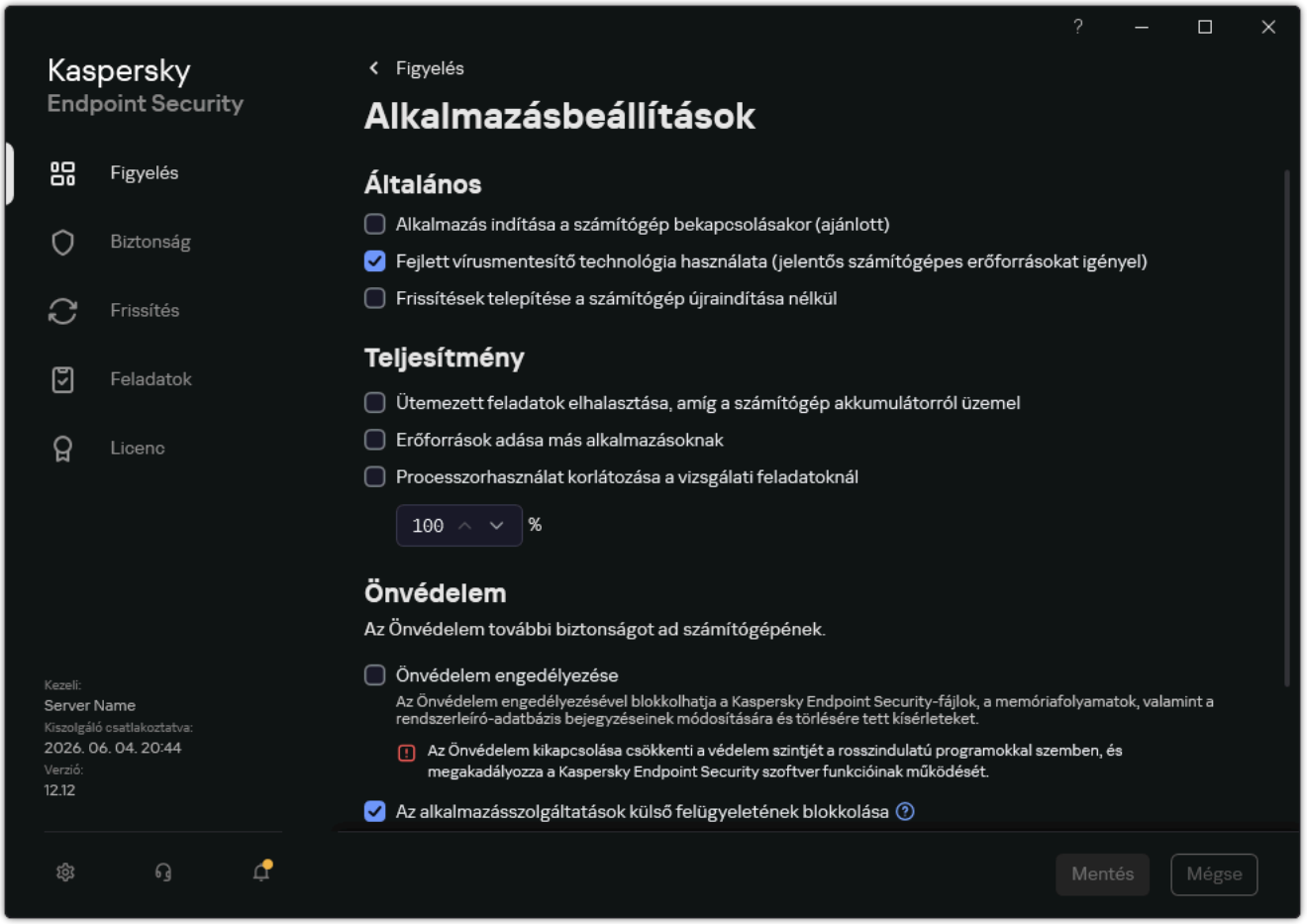
1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. Az **Önvédelem engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le az Önvédelem mechanizmusát.
5. Mentse el a módosításokat.

Az Önvédelem engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Self-Defense** elemet.
5. Használja a(z) **Self-Defense ENABLED** kapcsolót az Önvédelmi mechanizmus engedélyezésére vagy letiltására.
6. Mentse el a módosításokat.

Az Önvédelem engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. Az **Önvédelem engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le az Önvédelem mechanizmusát.
4. Mentse el a módosításokat.

Az AM-PPL támogatás engedélyezése és kikapcsolása

A Kaspersky Endpoint Security támogatja a Microsoft Antimalware Protected Process Light technológiáját (a továbbiakban „AM-PPL”). Az AM-PPL védi a Kaspersky Endpoint Security folyamatokat a rosszindulatú műveletektől (például az alkalmazás leállításától). Az AM-PPL csak megbízható folyamatok futását engedélyezi. A Kaspersky Endpoint Security folyamatok a Windows biztonsági követelmények alapján vannak aláírva, így megbízhatóak. Az AM-PPL technológia részleteiért lásd a Microsoft weboldalt. Az AM-PPL technológia alapértelmezetten engedélyezve van.

A Kaspersky Endpoint Security beépített mechanizmusokkal rendelkezik, amik védik az alkalmazásfolyamatokat. Az AM-PPL támogatás segítségével delegálhatja a folyamatbiztonsági funkciókat az operációs rendszer számára. Így növelheti az alkalmazás sebességét, és csökkentheti a számítógépes erőforrások fogyasztását.

Folyamatosan használja az AM-PPL technológiát. Az AM-PPL az operációs rendszer védelmének fontos összetevője. Az AM-PPL támogatásának letiltása a Kaspersky Endpoint Security egyes funkcióinak meghibásodását okozhatja (például az alkalmazás integrációja a Windows Security Center szolgáltatással). Az AM-PPL támogatás letiltása hibaelhárítási célból csak külön tesztkörnyezetben engedélyezett.

Az AM-PPL technológia a Windows 10 1703-as (RS2) vagy újabb verziói, valamint a Windows Server 2019 operációs rendszerek számára érhető el.

Az AM-PPL technológia engedélyezéséhez vagy kikapcsolásához:

1. Kapcsolja ki az alkalmazás Önvédelmi mechanizmusát.

   Az Önvédelmi mechanizmus megakadályozza a számítógépes memória alkalmazásfolyamatainak módosítását vagy törlését, köztük az AM-PPL állapotét is.

2. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.

3. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

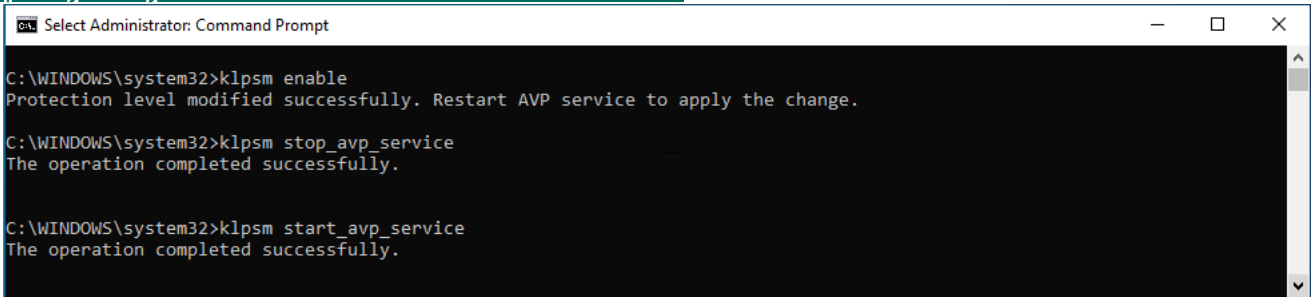
   Az alkalmazás telepítése során a futtatható fájl elérési útját hozzáadhatja a %PATH% rendszerváltozóhoz.

4. Gépelje be a következőt a parancssorba:

   - `klpsm.exe enable` – az AM-PPL technológia támogatásának engedélyezése (lásd az alábbi ábrát).
   - `klpsm.exe disable` – az AM-PPL technológia támogatásának kikapcsolása.

5. Indítsa újra a Kaspersky Endpoint Security alkalmazást.

6. Kapcsolja be újra az alkalmazás Önvédelmi mechanizmusát.



Az AM-PPL technológia támogatásának engedélyezése

Az alkalmazásszolgáltatások külső felügyelettel szembeni védelme

Az alkalmazásszolgáltatások külső felügyelettel szembeni védelme blokkolja a felhasználók és más alkalmazások azon kísérleteit, hogy leállítsák a Kaspersky Endpoint Security szolgáltatásait. A védelem az alábbi szolgáltatások működését biztosítja:

- Kaspersky Endpoint Security Service (AVP.KES.14.1)
- Kaspersky Seamless Update Service szolgáltatás (AVPSUS.KES.14.1)

Ha az alkalmazást kis szeretné léptetni a parancssorból, tiltsa le a Kaspersky Endpoint Security szolgáltatásainak külső felügyelettel szembeni védelmét.

Az alkalmazásszolgáltatások külső kezelését csak olyan számítógépeken engedélyezheti, amelyek nem támogatják az AM-PPL technológiát, illetve olyan számítógépeken, amelyeken a technológia le van tiltva.

Az alkalmazásszolgáltatások külső felügyelettel szembeni védelmének engedélyezése vagy letiltása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. **Az alkalmazásszolgáltatások külső kezelésének blokkolása** jelölőnégyzettel engedélyezheti vagy letilthatja a Kaspersky Endpoint Security szolgáltatásainak külső felügyelettel szembeni védelmét.
5. Mentse el a módosításokat.

Az alkalmazásszolgáltatások külső felügyelettel szembeni védelmének engedélyezése vagy letiltása a Web Console-on és a Cloud Console-on

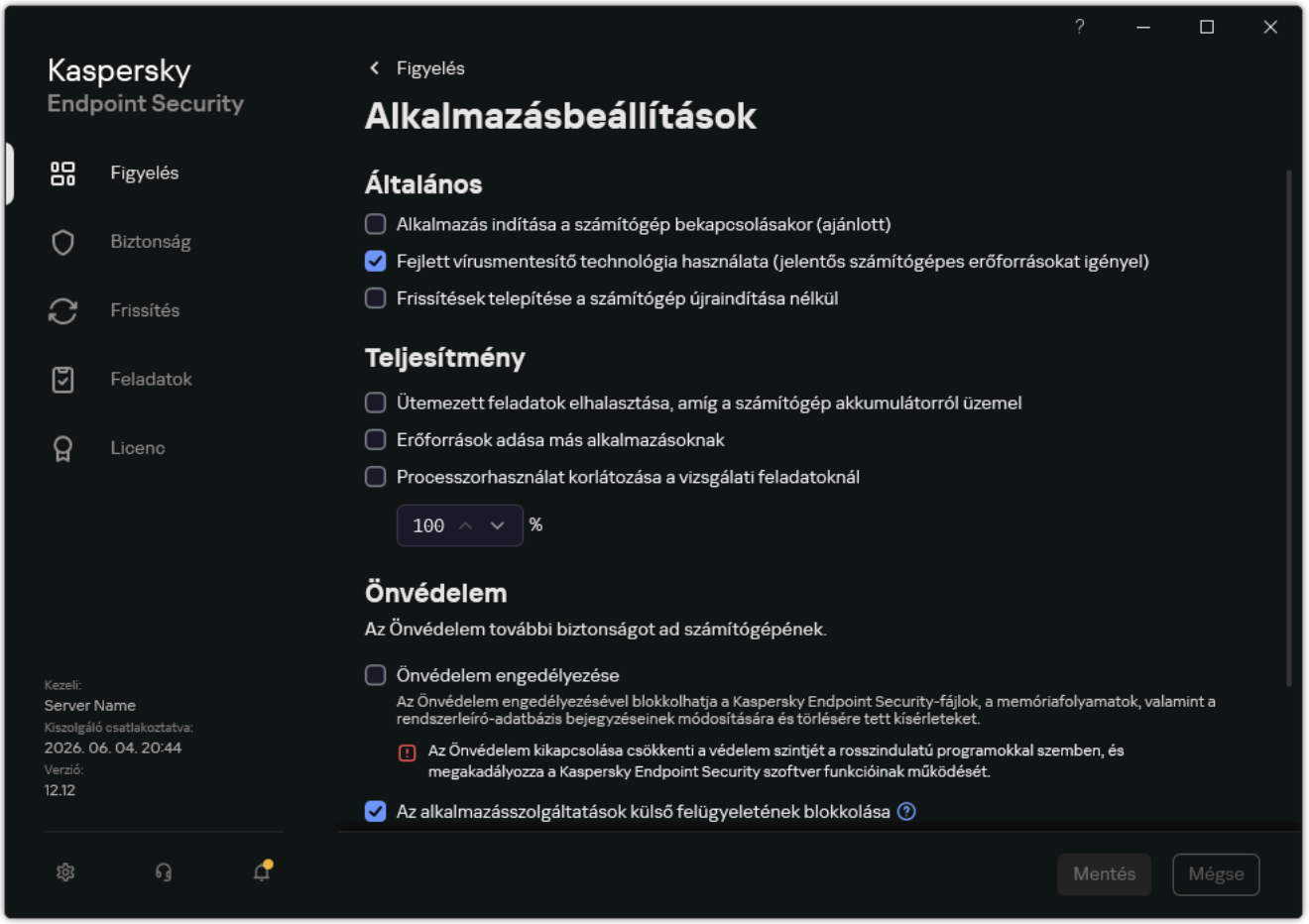
1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Self-Defense** elemet.
5. **Block external management of application services** jelölőnégyzettel engedélyezheti vagy letilthatja a Kaspersky Endpoint Security szolgáltatásainak külső felügyelettel szembeni védelmét.
6. Mentse el a módosításokat.

Az alkalmazásszolgáltatások külső felügyelettel szembeni védelmének engedélyezése vagy letiltása az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.

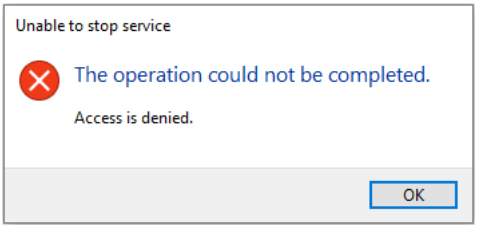


A Kaspersky Endpoint Security for Windows beállításai

3. **Az alkalmazásszolgáltatások külső kezelésének blokkolása** jelölőnégyzettel engedélyezheti vagy letilthatja a Kaspersky Endpoint Security szolgáltatásainak külső felügyelettel szembeni védelmét.

4. Mentse el a módosításokat.

Ennek eredményeként, amikor a felhasználó megpróbálja leállítani az alkalmazásszolgáltatásokat, megjelenik egy hibaüzenetet tartalmazó rendszerablak. A felhasználó csak a Kaspersky Endpoint Security felületéről kezelheti az alkalmazásszolgáltatásokat.



Alkalmazásszolgáltatás hozzáférési hibája

A távoli adminisztrációs alkalmazások támogatása

Időnként szükség lehet távoli adminisztrációs alkalmazás használatára, miközben be van kapcsolva a külső kezelés elleni védelem.

A távoli adminisztrációs alkalmazások működésének bekapcsolása:

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások → Kizárások és észlelt objektumok típusai** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.
4. Az ablakban kattintson a **Hozzáadás** gombra.
5. Válassza ki a távoli adminisztrációs alkalmazás futtatható fájlját.

   Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.
6. Jelölje be az **Interakció engedélyezése a Kaspersky Endpoint Security felületével** jelölőnégyzetet.
7. Mentse el a módosításokat.

Jelszóvédelem

Egy-egy számítógépet több, a számítógéphez különböző méretekben értő felhasználó is használhat. Ha a felhasználók korlátlanul hozzáférhetnek a Kaspersky Endpoint Security alkalmazáshoz és beállításaihoz, csökkenhet a számítógép védelmének általános szintje. A Jelszóvédelemmel korlátozhatja a felhasználók Kaspersky Endpoint Security-hez történő hozzáférését, a megadott jogosultságok alapján (például, jogosultság az alkalmazásból való kilépéshez).

Ha a felhasználónak, aki elindította a Windows munkamenetet, (*munkamenet felhasználó*) jogosultsága van a művelet végrehajtására, akkor a Kaspersky Endpoint Security nem kér felhasználónevet és jelszót vagy ideiglenes jelszót. A felhasználó hozzáférést kap a Kaspersky Endpoint Security alkalmazáshoz, a kapott jogosultságok alapján.

Ha a munkamenet-felhasználónak nincs jogosultsága a művelet végrehajtására, akkor a következő módokon kaphat elérést az alkalmazáshoz:

- Felhasználónév és jelszó megadása.

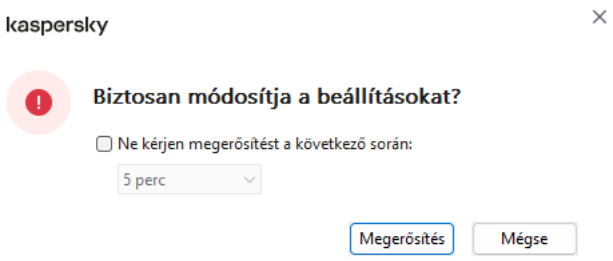
  Ez a módszer alkalmas a napi műveletekhez. A jelszóval védett művelet végrehajtásához meg kell adnia a kért jogosultsággal rendelkező felhasználó tartományfiókjának bejelentkezési adatait. Ebben az esetben a számítógépnek a tartományban kell lennie. Ha a számítógép nincs a tartományban, akkor használhatja a KLAdmin fiókot vagy egy manuálisan hozzáadott fiókot.

- Átmeneti jelszó megadása.

  Ez a módszer alkalmas átmeneti jogosultságok megadásához, hogy a vállalati hálózaton lévő felhasználó számára tiltott műveleteket végezzen el (például az alkalmazásból való kilépés). Ha az átmeneti jelszó lejár, vagy a munkamenet véget ér, a Kaspersky Endpoint Security visszaállítja a beállításokat a korábbi állapotra.

Ha a felhasználó jelszóval védett tevékenységet végez el, a Kaspersky Endpoint Security kéri a felhasználótól a felhasználónevet, jelszót vagy az átmeneti jelszót (lásd a korábbi ábrát).

A jelszóbeviteli ablakban csak az **ALT+SHIFT** billentyűkombináció használatával válthat nyelvet. Más gyorsgombok használata nem működik a nyelvváltásnál – még akkor sem, ha azok az operációs rendszerben vannak konfigurálva.



Kaspersky Endpoint Security elérési jelszó kérése

Felhasználónév és jelszó

A Kaspersky Endpoint Security eléréséhez meg kell adnia a fiók bejelentkezési adatait. A jelszóvédelem a következő fiókokat támogatja:

- **KLAdmin**. Egy Rendszergazda fiók, ami korlátozott hozzáféréssel rendelkezik a Kaspersky Endpoint Security-ben. A KLAdmin felhasználói fióknak joga van végrehajtani bármilyen olyan tevékenységet, ami jelszóvédett. A KLAdmin fiók jogosultságait nem lehet megvonni. Ha engedélyezi a jelszóvédelmet, a Kaspersky Endpoint Security kérni fogja, hogy állítson be egy új jelszót a KLAdmin fiókhoz.

- **Manuálisan hozzáadott fiók**. Az Active Directory tartományon kívüli fiók. Ezt a szolgáltatásfiókot használhatja a KLAdmin helyett, ha nem szeretné megosztani a rendszergazdai jelszót. Bármilyen felhasználónevet és jelszót beállíthat, és egyéni jogosultságokat konfigurálhat.

- **A Mindenki csoport**. Egy beépített Windows-csoport, amelybe a vállalati hálózaton lévő összes felhasználó beletartozik. A Mindenki csoportban lévő felhasználók a jogosultságaik alapján hozzáférnek az alkalmazáshoz.

- **Egyéni felhasználók vagy csoportok**. Felhasználói fiókok, amikhez egyéni jogosultságokat adhat meg. Például, ha egy tevékenységet tilt a Mindenki csoport, akkor engedélyezheti ezt a tevékenységet egy egyéni felhasználó vagy csoport számára.

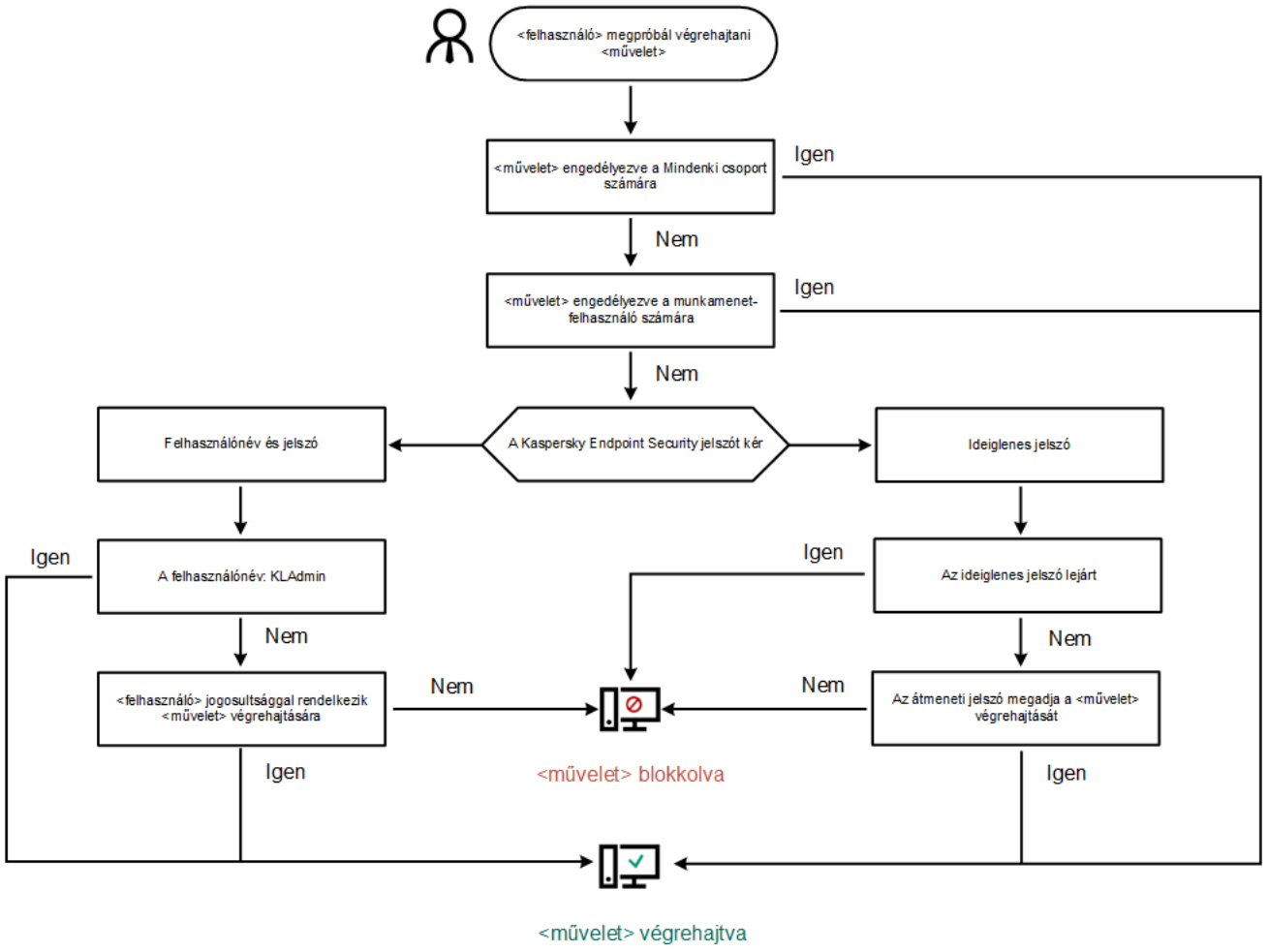
- **Munkamenet felhasználó**. A felhasználó fiókja, aki elindította a Windows munkamenetet. Válthat más munkamenet-felhasználóra, ha jelszót kell megadnia (a **Jelszó mentése az aktuális munkamenethez** jelölőnégyzet). Ebben az esetben a Kaspersky Endpoint Security azt a Windows munkamenetet elindító felhasználó helyett azt a felhasználót üdvözli, akinek a bejelentkezési adatai meg lettek adva a munkamenethez.

Ideiglenes jelszó

Az ideiglenes jelszó használható arra, hogy átmeneti elérést adjon a Kaspersky Endpoint Security-hez egy olyan egyéni számítógépnek, ami a vállalati hálózaton kívül található. A Rendszergazda létrehoz egy ideiglenes jelszót az egyéni számítógép számára a Kaspersky Security Center számítógépes tulajdonságaiban. A Rendszergazda kiválasztja a tevékenységeket, amiket védeni fog az ideiglenes jelszó, majd megadja az ideiglenes jelszó érvényességi idejét.

Jelszóvédelem működési algoritmus

A Kaspersky Endpoint Security a következő algoritmus alapján dönti el, hogy engedélyezze vagy letiltsa a jelszóval védett tevékenységet (lásd az alábbi ábrán).



Jelszóvédelem működési algoritmus

Jelszóvédelem engedélyezése

A Jelszóvédelemmel korlátozhatja a felhasználók Kaspersky Endpoint Security-hez történő hozzáférését, a megadott jogosultságok alapján (például, jogosultság az alkalmazásból való kilépéshez).

Jelszóvédelem engedélyezése az Administration Console-ban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.
4. A **Jelszóvédelem** részen kattintson a **Beállítások** gombra.

   Ezzel megnyílik egy ablak a jelszóvédelmi beállításokkal.
5. A **Jelszóvédelem engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
6. Az **Engedélyek** részen válassza ki a KLAdmin fiókot.
7. Ezzel megnyílik egy ablak; ebben az ablakban kattintson a **Jelszó** elemre, és állítson be egy jelszót a KLAdmin fiókhoz.

   A KLAdmin felhasználói fióknak joga van végrehajtani bármilyen olyan tevékenységet, ami jelszóvédett.

   > Ha elfelejtette a KLAdmin fiók jelszavát, a házirend tulajdonságaiban visszaállíthatja a jelszót.
8. Térjen vissza a fiókok listájához.
9. Állítsa be az összes felhasználó jogosultságát a vállalati hálózaton:

   a. Az **Engedélyek** részen válassza ki a „Mindenki" csoportot.

   A Mindenki csoport egy beépített Windows-csoport, amelybe a vállalati hálózaton lévő összes felhasználó beletartozik.

   b. A megnyílt ablakban válassza ki azon tevékenységek melletti jelölőnégyzeteket, amiket a felhasználók jelszó megadása nélkül is végrehajthatnak.

   Ha a jelölőnégyzet törölve van, a felhasználók számára tiltva lesz a tevékenység végrehajtása. Például, ha a **Kilépés az alkalmazásból** jogosultság mellett lévő jelölőnégyzet törölve van, akkor csak akkor léphet ki az alkalmazásból, ha KLAdmin-ként van bejelentkezve, vagy egy olyan egyéni felhasználóként, aki rendelkezik a szükséges jogosultságokkal, vagy akkor, ha megad egy ideiglenes jelszót.

   > A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai, amiket figyelembe kell venni. Győződjön meg róla, hogy a Kaspersky Endpoint Security elérésének minden feltétele teljesül.
10. Mentse el a módosításokat.

Jelszóvédelem engedélyezése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Self-Defense** elemet.

5. A **Password Protection** területen a **Password Protection ENABLED** kapcsolóval engedélyezheti vagy tilthatja le az összetevőt.

6. Adja meg a KLAdmin felhasználói fiók jelszavát, majd erősítse meg.

   A KLAdmin felhasználói fióknak joga van végrehajtani bármilyen olyan tevékenységet, ami jelszóvédett.

   Ha elfelejtette a KLAdmin fiók jelszavát, a házirend tulajdonságaiban visszaállíthatja a jelszót.

7. Térjen vissza a fiókok listájához.

8. Állítsa be az összes felhasználó jogosultságát a vállalati hálózaton:

   a. A fiókok táblázatában válassza ki a „Mindenki" csoportot.

      A Mindenki csoport egy beépített Windows-csoport, amelybe a vállalati hálózaton lévő összes felhasználó beletartozik.

   b. A megnyílt ablakban válassza ki azon tevékenységek melletti jelölőnégyzeteket, amiket a felhasználók jelszó megadása nélkül is végrehajthatnak.

      Ha a jelölőnégyzet törölve van, a felhasználók számára tiltva lesz a tevékenység végrehajtása. Például, ha a **Exit the application** jogosultság mellett lévő jelölőnégyzet törölve van, akkor csak akkor léphet ki az alkalmazásból, ha KLAdmin-ként van bejelentkezve, vagy egy olyan egyéni felhasználóként, aki rendelkezik a szükséges jogosultságokkal, vagy akkor, ha megad egy ideiglenes jelszót.

      A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai, amiket figyelembe kell venni. Győződjön meg róla, hogy a Kaspersky Endpoint Security elérésének minden feltétele teljesül.

9. Mentse el a módosításokat.

A Jelszóvédelem engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.

3. A **Jelszóvédelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Adja meg a KLAdmin felhasználói fiók jelszavát, majd erősítse meg.

   A KLAdmin felhasználói fióknak joga van végrehajtani bármilyen olyan tevékenységet, ami jelszóvédett.

   Ha a számítógép egy rendszabály alapján fut, a Rendszergazda visszaállíthatja a KLAdmin felhasználói fiók jelszavát a rendszabály tulajdonságaiban. Ha a számítógép nincs csatlakoztatva a Kaspersky Security Centerhez, és elfelejtette a KLAdmin felhasználói fiók jelszavát, akkor nem lehet visszaállítani a jelszót.

5. Állítsa be az összes felhasználó jogosultságát a vállalati hálózaton:

   a. A fióktáblában kattintson a **Szerkesztés** gombra, hogy megnyissa a Mindenki csoport jogosultságainak listáját.

      A Mindenki csoport egy beépített Windows-csoport, amelybe a vállalati hálózaton lévő összes felhasználó beletartozik.

b. Jelölje be azon tevékenységek melletti jelölőnégyzeteket, amiket a felhasználók jelszó megadása nélkül is végrehajthatnak.

Ha a jelölőnégyzet törölve van, a felhasználók számára tiltva lesz a tevékenység végrehajtása. Például, ha a **Kilépés az alkalmazásból** jogosultság mellett lévő jelölőnégyzet törölve van, akkor csak akkor léphet ki az alkalmazásból, ha KLAdmin-ként van bejelentkezve, vagy egy olyan egyéni felhasználóként, aki rendelkezik a szükséges jogosultságokkal, vagy akkor, ha megad egy ideiglenes jelszót.

A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai, amiket figyelembe kell venni. Győződjön meg róla, hogy a Kaspersky Endpoint Security elérésének minden feltétele teljesül.

6. Mentse el a módosításokat.

Ha a jelszóvédelem engedélyezve van, az alkalmazás korlátozni fogja a felhasználók hozzáférését a Kaspersky Endpoint Security-hez, a Mindenki csoportban megadott jogosultságok alapján. Csak akkor végezheti el a Mindenki csoportban tiltott tevékenységeket, ha KLAdmin fiókot vagy egy jogosultságokkal rendelkező, másik fiókot használ, vagy akkor, ha megad egy átmeneti jelszót.

A jelszóvédelmet csak akkor kapcsolhatja ki, ha KLAdminként van bejelentkezve. A jelszóvédelmet nem lehetséges kikapcsolni, ha más felhasználói fiókot vagy ideiglenes jelszót használ.

A jelszóellenőrzés alatt bejelölheti a **Jelszó mentése az aktuális munkamenethez** jelölőnégyzetet. Ebben az esetben a Kaspersky Endpoint Security nem kér jelszót, ha egy felhasználó más jelszóval védett tevékenységet próbál végrehajtani a munkamenet alatt.

Jogosultságok megadása egyéni felhasználóknak vagy csoportoknak

A jelszóvédelem lehetővé teszi a Kaspersky Endpoint Security hozzáférését az egyes Active Directory felhasználói fiókokhoz és a manuálisan hozzáadott felhasználói fiókokhoz.

Active Directory felhasználói fiókok

A Kaspersky Endpoint Security hozzáférést biztosíthat az Active Directory tartományon belüli egyes felhasználóknak vagy csoportoknak. Például, ha az alkalmazásból való kilépés tiltva van a Mindenki csoportnak, akkor megadhatja a **Kilépés az alkalmazásból** jogosultságot egy egyéni felhasználónak. Ennek eredményeképpen csak akkor léphet ki az alkalmazásból, ha azon felhasználóval vagy a KLAdmin fiókkal van bejelentkezve.

A hitelesítő adatokkal csak akkor tud hozzáférni az alkalmazáshoz, ha a számítógép a tartományban van. Ha a számítógép nincs a tartományban, akkor használhatja a KLAdmin fiókot vagy egy ideiglenes jelszót.

Manuálisan hozzáadott felhasználói fiókok

Létrehozhat olyan felhasználói fiókot, amely nincs jelen az Active Directoryban, és egyéni jogosultságokat rendelhet hozzá. Ez azt jelenti, hogy létrehozhat egy *szolgáltatási felhasználói fiókot*, és azt használhatja a KLAdmin helyett. Így nem kell megosztania a KLAdmin jelszavát más felhasználókkal, és nem kell új Active Directory felhasználói fiókokat létrehoznia. Bármilyen felhasználónevet és jelszót megadhat. Például megadhatja a **Jelentések megtekintése** engedélyt a szolgáltatási felhasználói fióknak. Ennek eredményeképpen, ha a jelentések megtekintése a „Mindenki" csoport számára tilos, a jelentéseket a szolgáltatási felhasználói fiókkal vagy a KLAdmin felhasználói fiókkal nyithatja meg.

Jogosultságok megadása egyéni felhasználóknak vagy csoportoknak

Engedélyek megadása egyéni felhasználóknak vagy csoportoknak az Administration Console-on (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.
4. A **Jelszóvédelem** részen kattintson a **Beállítások** gombra.

   Ezzel megnyílik egy ablak a jelszóvédelmi beállításokkal.
5. A fióktáblában kattintson a **Hozzáadás** gombra.
6. Válassza ki a hozzáadni kívánt felhasználói fiók típusát:

   - **Válasszon ki egy felhasználót/csoportot az Active Directoryból** – Active Directory felhasználói fiókok.

     Egy felhasználói fiók kiválasztásához kattintson a **Kijelölés** gombra. Válasszon ki egy felhasználót vagy csoportot az Active Directory helyről, és erősítse meg a választását.

   - **Felhasználó/felhasználócsoport hozzáadása manuálisan** egy manuálisan hozzáadott szolgáltatási felhasználói fiókhoz.

     Egy szolgáltatási felhasználói fiók hozzáadásához adjon meg egy felhasználónevet és egy jelszót (például SecureAdmin).

     > A szolgáltatási felhasználói fiók jelszavát a házirend beállításaiban állíthatja vissza. A szolgáltatási felhasználói fiók jelszavát ugyanúgy kell visszaállítani, mint a KLAdmin jelszavát. Ha a jelszóvédelmi beállítások szerkesztése engedélyezett (a „zár" nyitva van), vagy a számítógépen nincs házirend alkalmazva, akkor az alkalmazás felületén visszaállíthatja a szolgáltatási felhasználói fiók jelszavát. Ehhez erősítse meg a szolgáltatási felhasználói fiók adatainak módosítását a KLAdmin jelszóval.
7. A **Engedélyek** listában jelölje be a jelölőnégyzeteket azon tevékenységek mellett, amiket a felhasználó vagy csoport jelszó nélkül is elvégezhet.

   Ha a jelölőnégyzet törölve van, a felhasználók számára tiltva lesz a tevékenység végrehajtása. Például, ha a **Kilépés az alkalmazásból** jogosultság mellett lévő jelölőnégyzet törölve van, akkor csak akkor léphet ki az alkalmazásból, ha KLAdmin-ként van bejelentkezve, vagy egy olyan egyéni felhasználóként, aki rendelkezik a szükséges jogosultságokkal, vagy akkor, ha megad egy ideiglenes jelszót.

A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai, amiket figyelembe kell venni. Győződjön meg róla, hogy a Kaspersky Endpoint Security elérésének minden feltétele teljesül.

8. Mentse el a módosításokat.

Engedélyek megadása egyéni felhasználóknak vagy csoportoknak a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Self-Defense** elemet.
5. A **Password Protection** részen kattintson a **User permissions** hivatkozásra.

   Megnyílik a jelszó engedélyezéséhez szükséges űrlap.
6. Kattintson az **Add** gombra.
7. Válassza ki a hozzáadni kívánt felhasználói fiók típusát:

   - **Select from Active Directory** – Active Directory felhasználói fiókok.

     A felhasználói fiók kiválasztásához kattintson a(z)**Edit** elemre. Válasszon ki egy felhasználót vagy csoportot az Active Directory helyről, és erősítse meg a választását.

   - **Add manually** egy manuálisan hozzáadott szolgáltatási felhasználói fiókhoz.

     Egy szolgáltatási felhasználói fiók hozzáadásához adjon meg egy felhasználónevet és egy jelszót (például SecureAdmin).

     A szolgáltatási felhasználói fiók jelszavát a házirend beállításaiban állíthatja vissza. A szolgáltatási felhasználói fiók jelszavát ugyanúgy kell visszaállítani, mint a KLAdmin jelszavát. Ha a jelszóvédelmi beállítások szerkesztése engedélyezett (a „zár” nyitva van), vagy a számítógépen nincs házirend alkalmazva, akkor az alkalmazás felületén visszaállíthatja a szolgáltatási felhasználói fiók jelszavát. Ehhez erősítse meg a szolgáltatási felhasználói fiók adatainak módosítását a KLAdmin jelszóval.
8. A(z) **Permissions** listában jelölje be a négyzeteket azon tevékenységek mellett, amelyeket a felhasználó vagy csoport jelszó nélkül is elvégezhet.

   Ha a jelölőnégyzet törölve van, a felhasználók számára tiltva lesz a tevékenység végrehajtása. Például, ha a **Exit the application** jogosultság mellett lévő jelölőnégyzet törölve van, akkor csak akkor léphet ki az alkalmazásból, ha KLAdmin-ként van bejelentkezve, vagy egy olyan egyéni felhasználóként, aki rendelkezik a szükséges jogosultságokkal, vagy akkor, ha megad egy ideiglenes jelszót.

   A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai, amiket figyelembe kell venni. Győződjön meg róla, hogy a Kaspersky Endpoint Security elérésének minden feltétele teljesül.
9. Kattintson az **Add** gombra.
10. Mentse el a módosításokat.

Engedélyek megadása egyéni felhasználóknak vagy csoportoknak az alkalmazás felhasználói felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
3. A fióktáblában kattintson a **Hozzáadás** gombra.
4. Válassza ki a hozzáadni kívánt felhasználói fiók típusát:
   - **Válasszon ki egy felhasználót/csoportot az Active Directoryból** – Active Directory felhasználói fiókok.

     Egy felhasználói fiók kiválasztásához kattintson a **Felhasználó vagy csoport kijelölése** gombra. Válasszon ki egy felhasználót vagy csoportot az Active Directory helyről, és erősítse meg a választását.
   - **Felhasználó hozzáadása manuálisan** egy manuálisan hozzáadott szolgáltatási felhasználói fiókhoz.

     Egy szolgáltatási felhasználói fiók hozzáadásához adjon meg egy felhasználónevet és egy jelszót (például SecureAdmin).

     A szolgáltatási felhasználói fiók jelszavát a házirend beállításaiban állíthatja vissza. A szolgáltatási felhasználói fiók jelszavát ugyanúgy kell visszaállítani, mint a KLAdmin jelszavát. Ha a jelszóvédelmi beállítások szerkesztése engedélyezett (a „zár" nyitva van), vagy a számítógépen nincs házirend alkalmazva, akkor az alkalmazás felületén visszaállíthatja a szolgáltatási felhasználói fiók jelszavát. Ehhez erősítse meg a szolgáltatási felhasználói fiók adatainak módosítását a KLAdmin jelszóval.
5. A **Engedélyek** listában jelölje be a jelölőnégyzeteket azon tevékenységek mellett, amiket a felhasználó vagy csoport jelszó nélkül is elvégezhet.

   Ha a jelölőnégyzet törölve van, a felhasználók számára tiltva lesz a tevékenység végrehajtása. Például, ha a **Kilépés az alkalmazásból** jogosultság mellett lévő jelölőnégyzet törölve van, akkor csak akkor léphet ki az alkalmazásból, ha KLAdmin-ként van bejelentkezve, vagy egy olyan egyéni felhasználóként, aki rendelkezik a szükséges jogosultságokkal, vagy akkor, ha megad egy ideiglenes jelszót.

   A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai, amiket figyelembe kell venni. Győződjön meg róla, hogy a Kaspersky Endpoint Security elérésének minden feltétele teljesül.
6. Mentse el a módosításokat.

Ennek eredményeképpen, ha az alkalmazás elérése korlátozva van a Mindenki csoport számára, a felhasználók jogosultságot kapnak a Kaspersky Endpoint Security eléréséhez, a felhasználók egyéni jogosultságai alapján.

Ideiglenes jelszó használata a jogosultságok megadásához

Az ideiglenes jelszó használható arra, hogy átmeneti elérést adjon a Kaspersky Endpoint Security-hez egy olyan egyéni számítógépnek, ami a vállalati hálózaton kívül található. Szükséges engedélyezni a felhasználónak, hogy tiltott tevékenységeket végezhessen el a KLAdmin fiók bejelentkezési adatai nélkül. Az ideiglenes jelszó használatához a számítógépet hozzá kell adni a Kaspersky Security Center-hez.

Hogyan engedélyezheti a felhasználónak, hogy ideiglenes jelszóval végezzen el egy tiltott műveletet az adminisztrációs konzolon (MMC) keresztül?

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Devices** lapot.
4. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.
5. Válassza ki a számítógép tulajdonságainak ablakában a **Applications** részt.
6. A számítógépre telepített Kaspersky alkalmazások listájában válassza a **Kaspersky Endpoint Security for Windows (14.1)** lehetőséget, és kattintson rá duplán az alkalmazás tulajdonságainak megnyitásához.
7. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
8. A **Jelszóvédelem** részen kattintson a **Beállítások** gombra.
9. A megnyíló ablakban az **Ideiglenes jelszó** részben kattintson az **Ideiglenes jelszavak listája** gombra.

   Megnyílik az Ideiglenes jelszavak kezelése ablak.
10. Kattintson **Hozzáadás** gombra.
11. A **Expiration date** mezőben adja meg a dátumot, amikor az ideiglenes jelszó le fog járni.
12. Jelölje be az **Temporary password scope** táblázatban a jelölőnégyzeteket azon műveletek mellett, amelyeknek a felhasználó rendelkezésére kell állniuk, miután megadja az ideiglenes jelszót.
13. Kattintson a **Létrehozás** gombra.

    Megnyílik az ideiglenes jelszót tartalmazó ablak (lásd az alábbi ábrát).
14. Másolja le a jelszót, és adja meg a felhasználónak.

Hogyan engedélyezheti a felhasználónak, hogy ideiglenes jelszóval végezzen el egy tiltott műveletet a webkonzolon és a felhőkonzolon keresztül?

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Kattintson annak a számítógépnek a nevére, amelyen a felhasználónak engedélyezni kívánja a tiltott művelet végrehajtását.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.

   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Az alkalmazáskonfigurációs ablakban válassza ki a **General settings** → **Interface** lehetőséget.
7. A **Temporary passwords** részen kattintson a **Add** gombra.

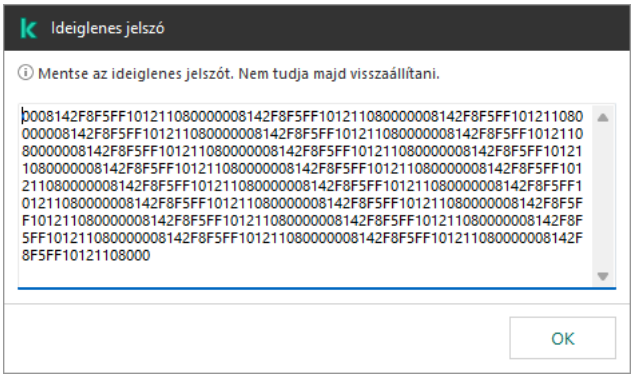
8. A **Expiration date** mezőben adja meg a dátumot, amikor az ideiglenes jelszó le fog járni.

9. Jelölje be az **Temporary password scope** táblázatban a jelölőnégyzeteket azon műveletek mellett, amelyeknek a felhasználó rendelkezésére kell állniuk, miután megadja az ideiglenes jelszót.

10. Kattintson a **Létrehozás** gombra.

    Megnyílik az ideiglenes jelszót tartalmazó ablak.

11. Másolja le a jelszót, és adja meg a felhasználónak.



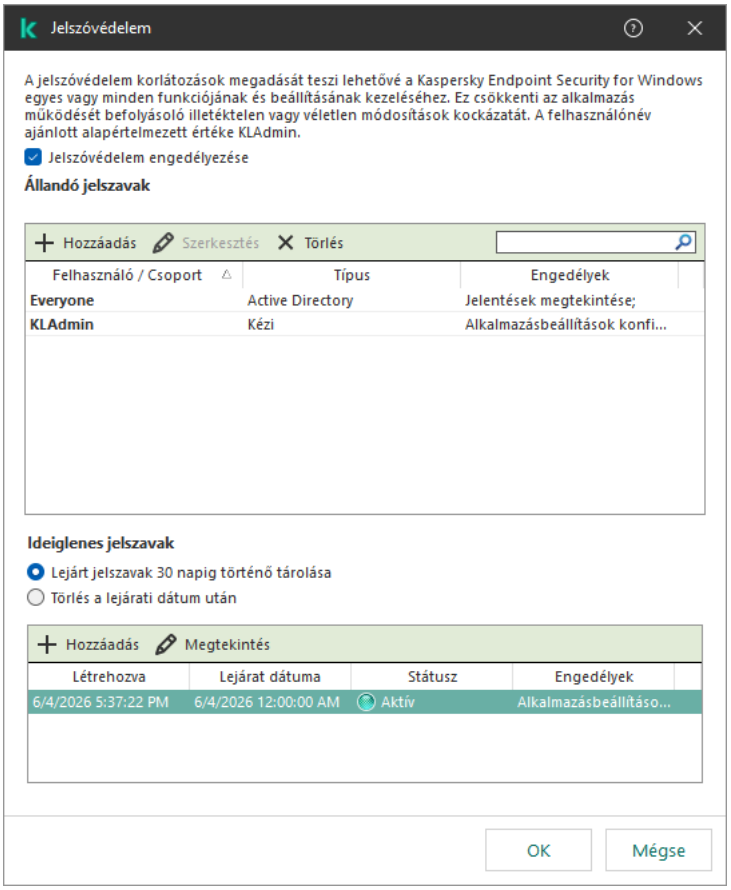
Ideiglenes jelszó

Ideiglenes jelszó visszavonása

A 12.9-es verziótól kezdve a Kaspersky Endpoint Security for Windows tartalmazza az *Ideiglenes jelszavak kezelése* funkciót. Az ideiglenes jelszavak kezelése a következő műveletek elvégzését teszi lehetővé:

- Jelszóelőzmények mentése (legfeljebb 30 nap).
- Ideiglenes jelszóállapot figyelése: *Aktív*, *Lejárt*, *Visszavonva*.

- Ideiglenes jelszavak visszavonása.



Ideiglenes jelszavak kezelése

Az ideiglenes jelszavak kezelése csak a számítógép Kaspersky Security Centerrel való szinkronizálása után frissíti a jelszó állapotát, és vonja vissza a jelszót.

Ideiglenes jelszó visszavonása a felügyeleti konzol (MMC) használatával

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Devices** lapot.
4. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.
5. Válassza ki a számítógép tulajdonságainak ablakában a **Applications** részt.
6. A számítógépre telepített Kaspersky alkalmazások listájában válassza a **Kaspersky Endpoint Security for Windows (14.1)** lehetőséget, és kattintson rá duplán az alkalmazás tulajdonságainak megnyitásához.
7. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
8. A **Jelszóvédelem** részen kattintson a **Beállítások** gombra.
9. Ez megnyit egy ablakot, ahol az **Ideiglenes jelszó** részen konfigurálja a tárolási beállításokat a lejárt jelszavakhoz.
10. Kattintson az **Ideiglenes jelszavak listája** elemre.

    Megnyílik az Ideiglenes jelszavak kezelése ablak. Az ideiglenes jelszavak kezelése megjeleníti a jelszó lejárati dátumát, a jelszó állapotát és az engedélyek listáját.

11. Válassza ki a visszavonni kívánt aktív ideiglenes jelszót, és kattintson duplán a jelszóra a tulajdonságok megnyitásához.

12. A megnyíló ablakban kattintson a **Visszavonás** gombra.

13. Mentse el a módosításokat. A házirend számítógépeken való alkalmazásához zárolja a lakatokat .

Ideiglenes jelszó visszavonása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.

2. Kattintson annak a számítógépnek a nevére, amelyen a felhasználónak engedélyezni kívánja a tiltott művelet végrehajtását.

3. Válassza ki az **Applications** lapot.

4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.

   Ez megnyitja a helyi alkalmazásbeállításokat.

5. Válassza ki az **Application settings** lapot.

6. Az alkalmazáskonfigurációs ablakban válassza ki a **General settings** → **Interface** lehetőséget.

7. Az **Temporary passwords** részen konfigurálja a lejárt jelszavak tárolását.

8. Kattintson a **Temporary password** hivatkozásra.

   Megnyílik az Ideiglenes jelszavak kezelése ablak. Az ideiglenes jelszavak kezelése megjeleníti a jelszó lejárati dátumát, a jelszó állapotát és az engedélyek listáját.

9. Válassza ki a visszavonni kívánt aktív ideiglenes jelszót.

10. Az ablakban kattintson a **Revoke password** gombra.

11. Mentse el a módosításokat. A házirend számítógépeken való alkalmazásához zárolja a lakatokat .

Ennek eredményeként az Ideiglenes jelszavak kezelése a jelszó állapotát *Visszavonás (szinkronizálás gazdagéppel)* értékre állítja. Miután szinkronizálta a számítógépet a Kaspersky Security Centerrel, az alkalmazás azonnal visszavonja az ideiglenes jelszót, és blokkolja a megadott engedélyeket.

A Jelszóvédelem jogosultságok speciális szempontjai

A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai és korlátozásai, amiket figyelembe kell venni.

Alkalmazásbeállítások konfigurálása

Ha egy felhasználói számítógép egy rendszabály alatt fut, akkor győződjön meg róla, hogy a rendszabály összes szükséges beállítása szerkeszthető (a tulajdonságok nyitottak).

Kilépés az alkalmazásból

Nincsenek külön szempontok vagy korlátozások.

Védelmi összetevők letiltása

- Nem lehet a védelmi összetevők kikapcsolására vonatkozó jogosultságot adni a „Mindenki” csoport számára. Ahhoz, hogy a KLAdmin fiókon kívül más felhasználó is ki tudjon kapcsolni felügyeleti összetevőt, adjon hozzá egy felhasználót vagy csoportot, amely rendelkezik a **Védelmi összetevők letiltása** jogosultsággal a Jelszóvédelem beállításaiban.
- Ha egy felhasználói számítógép egy rendszabály alatt fut, akkor győződjön meg róla, hogy a rendszabály összes szükséges beállítása szerkeszthető (a tulajdonságok nyitottak).
- Ahhoz, hogy letiltsa a védelmi összetevőket az alkalmazásbeállításokban, a felhasználónak rendelkeznie kell az **Alkalmazásbeállítások konfigurálása** jogosultsággal.
- Ahhoz, hogy letiltsa a védelmi összetevőket a helyi menüből (a **Védelem felfüggesztése** menüelemmel), a felhasználónak rendelkeznie kell a **Védelmi összetevők letiltása** jogosultsággal a **Felügyeleti összetevők letiltása** jogosultság mellett.

Felügyeleti összetevők letiltása

- Nem lehet a felügyeleti összetevők kikapcsolására vonatkozó jogosultságot adni a „Mindenki” csoport számára. Ahhoz, hogy a KLAdmin fiókon kívül más felhasználó is ki tudjon kapcsolni felügyeleti összetevőt, adjon hozzá egy felhasználót vagy csoportot, amely rendelkezik a **Felügyeleti összetevők letiltása** jogosultsággal a Jelszóvédelem beállításaiban.
- Ha egy felhasználói számítógép egy rendszabály alatt fut, akkor győződjön meg róla, hogy a rendszabály összes szükséges beállítása szerkeszthető (a tulajdonságok nyitottak).
- Ahhoz, hogy kikapcsolja a felügyeleti összetevőket az alkalmazásbeállításokban, a felhasználónak rendelkeznie kell az **Alkalmazásbeállítások konfigurálása** jogosultsággal.
- Ahhoz, hogy letiltsa a felügyeleti összetevőket a helyi menüből (a **Védelem felfüggesztése** menüelemmel), a felhasználónak rendelkeznie kell a **Felügyeleti összetevők letiltása** jogosultsággal a **Védelmi összetevők letiltása** jogosultság mellett.

A Kaspersky Security Center rendszabályának letiltása.

A „Mindenki” csoport számára megadhatja a Kaspersky Security Center rendszabály letiltását. Ahhoz, hogy a KLAdmin fiókon kívül más felhasználó is le tudjon tiltani rendszabályt, adjon hozzá egy felhasználót vagy csoportot, ami rendelkezik az **A Kaspersky Security Center házirendjének letiltása** jogosultsággal a Jelszóvédelem beállításaiban.

Kulcs eltávolítása

Nincsenek külön szempontok vagy korlátozások.

Alkalmazás eltávolítása/módosítása/visszaállítása

Ha engedélyezte az „Összes" csoport alkalmazásának eltávolítását, módosítását és visszaállítását, a Kaspersky Endpoint Security nem kér jelszót, amikor a felhasználó megpróbálja végrehajtani ezeket a műveleteket. Ezért minden felhasználó – beleértve a tartományon kívüli felhasználókat is – telepítheti, módosíthatja vagy visszaállíthatja az alkalmazást.

Hozzáférés visszaállítása a titkosított meghajtón tárolt adatokhoz

Csak a KLAdmin állíthatja vissza a titkosított meghajtókon tárolt adatok elérését. Ilyen tevékenység végrehajtásának jogosultságát nem adhatja meg más felhasználó.

Jelentések megtekintése

Nincsenek külön szempontok vagy korlátozások.

Visszaállítás a Biztonsági mentésből

Nincsenek külön szempontok vagy korlátozások.

Beállítások exportálása

Alapértelmezés szerint az alkalmazásbeállítások exportálása az „Összes" csoport számára tiltott. Az alkalmazás beállításait a KLAdmin felhasználói fiók segítségével exportálhatja. Az alkalmazásbeállítások exportálása csak egy konfigurációs fájl létrehozását jelenti, amely tartalmazza a Kaspersky Endpoint Security beállításait az alkalmazás felületén. Az engedély nem korlátozza a vizsgálati kizárásokat tartalmazó listák, megbízható webcímek, megbízható eszközök és az alkalmazás összetevői által felügyelt egyéb listák exportálását.

A KLAdmin jelszó visszaállítása

Ha elfelejtette a KLAdmin fiók jelszavát, a házirend tulajdonságaiban visszaállíthatja a jelszót. Az alkalmazás felületén nem állíthatja vissza a jelszót.

Jelszóval védett műveleteket ideiglenes jelszóval hajthat végre. Ebben az esetben nem kell megadnia a KLAdmin hitelesítő adatait.

Ha a számítógép nincs csatlakoztatva a Kaspersky Security Centerhez, és elfelejtette a KLAdmin felhasználói fiók jelszavát, akkor nem lehet visszaállítani a jelszót.

A KLAdmin fiók jelszavának visszaállítása az Adminisztrációs konzol (MMC) segítségével

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.
4. A **Jelszóvédelem** részen kattintson a **Beállítások** gombra.
5. A megnyíló ablakban törölje a **Jelszóvédelem engedélyezése** jelölőnégyzet bejelölését.
6. Mentse el a módosításokat.
7. Jelölje be ismét a **Jelszóvédelem engedélyezése** jelölőnégyzetet.
8. Kattintson az **OK** gombra.
   Ezzel megnyílik a rendszergazdai jelszó ablaka.
9. Adja meg a KLAdmin fiók új jelszavát, majd erősítse meg.
10. Mentse el a módosításokat.

A KLAdmin fiók jelszavának visszaállítása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.
   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.
   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Nyissa meg a **General Settings** → **Self-Defense** elemet.
7. A **Jelszóvédelem** alatt kapcsolja ki a **Jelszóvédelem** kapcsolót.
8. Mentse el a módosításokat.
9. Kapcsolja be újra a **Jelszóvédelem** kapcsolót.

10. Adja meg a KLAdmin fiók új jelszavát, majd erősítse meg.

11. Mentse el a módosításokat.

Ennek eredményeként a házirend alkalmazása után a KLAdmin fiók jelszava frissül.

Felügyeleti kiszolgálói kapcsolat védelme

A számítógép és a felügyeleti kiszolgáló összekapcsolása a Kaspersky Security Center *Hálózati ügynök* összetevőjével történik. Ha egy behatoló elegendő joggal rendelkezik a kiszolgálókapcsolati beállítások módosításához, fennáll a veszélye annak, hogy a számítógépet egy nem megbízható kiszolgálóhoz csatlakoztatja. Ez lehetővé tenné a behatoló számára, hogy saját csoportházirendeket alkalmazzon, és például letiltsa az alkalmazás önvédelmét. A Kaspersky Endpoint Security képes megakadályozni a számítógép jogosulatlan újracsatlakozását egy másik kiszolgálóhoz. A kiszolgálói kapcsolat védelme céljából az alkalmazás jelszó megadására és Password-Based key Derivation Function (PBKDF2) használatára tesz javaslatot. Ennek eredményeképpen az alkalmazáshoz való hozzáférés jelszó nélkül lehetetlen.

A Kaspersky Endpoint Security és a Hálózati ügynök jogosulatlan hozzáféréssel szembeni átfogó védelmének biztosítása céljából ajánlott a további védelem engedélyezése. A Kaspersky Endpoint Security esetében javasoljuk a Jelszóvédelem engedélyezését. A Hálózati ügynök védelme céljából ajánlott egy eltávolítási jelszó beállítása. A Hálózati ügynök eltávolítás elleni védelmével kapcsolatos részletekről a Kaspersky Security Center súgójából tájékozódhat.

A számítógép és a felügyeleti kiszolgáló kapcsolatának kezelése a *Felügyeleti kiszolgáló kapcsolatvédelme* feladat segítségével valósul meg. A feladat a következő műveletek elvégzését teszi lehetővé:

- Beállíthat egy jelszót a kiszolgálókapcsolat védelmére.
- Módosíthatja a jelszót.
- Újból csatlakoztathatja a számítógépet egy másik kiszolgálóhoz.
- Letilthatja a kiszolgálói kapcsolat védelmét.

A számítógép hitelesítése a felügyeleti kiszolgálóhoz való csatlakozáskor

A jelszóbeállítás után az alkalmazás a jelszó PBKDF2 transzformációjával létrehoz egy adattömböt. Az alkalmazás ezt követően a hálózati ügynök kulcsával titkosítja ezt az adattömböt. Az alkalmazás a titkosított adattömböt használja a felügyeleti kiszolgáló jogainak és jogosultságainak ellenőrzésére a későbbi csatlakozások esetében.

Ezt követően, amikor a számítógépet újra megpróbálják csatlakoztatni a felügyeleti kiszolgálóhoz, az alkalmazás a hálózati ügynök kulcsával visszafejti az adattömböt, és összehasonlítja azt a helyi másolattal. Ha nem egyeznek, az alkalmazáshoz való hozzáférés korlátozott.

Felügyeleti kiszolgálói kapcsolat védelme

Jelszó beállítása a kiszolgálói kapcsolat védelme céljából a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Adminisztrációs kiszolgáló kapcsolódási védelme** elemet.

2. lépés. A felügyeleti kiszolgáló kapcsolatvédelme

Beállíthat egy jelszót a felügyeleti kiszolgáló kapcsolatvédelmére:

1. A **Felügyeleti kiszolgáló kapcsolatvédelme** részen válassza a **Jelszóval való védelem** lehetőséget.

2. A **Felügyeleti kiszolgáló** legördülő listában válassza az **Új kiszolgáló** lehetőséget.

3. A **Jelszó a felügyeleti kiszolgálóhoz való csatlakozáshoz** mezőben állítson be egy jelszót a felügyeleti kiszolgálóhoz való csatlakozáshoz, és erősítse meg azt.

   Ha elfelejti a jelszót, a megfelelő feladat segítségével megváltoztathatja azt.

4. Ha a Kaspersky Endpoint Security 12.7 vagy az alkalmazás korábbi verziója van telepítve, jelölje be az **Engedélyezze a jelszótitkosítási kompatibilitást a korábbi alkalmazásverziókhoz (12.7 és korábbi)** jelölőnégyzetet.

   A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazás erősebb jelszótitkosítást használ. Ha a Kaspersky Endpoint Security 12.8 vagy újabb verziója van telepítve, javasoljuk, hogy törölje a jelölőnégyzetet, és használja az erősebb jelszótitkosítást. Az alkalmazás korábbi verziói nem támogatják az erős jelszavas titkosítást. A feladat futtatásához be kell jelölnie a jelölőnégyzetet.

3. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válassza a **Default account** lehetőséget. Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

4. lépés Feladatindítási ütemezés konfigurálása

A **Scheduled start** részen válassza a **Manually** elemet.

5. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *Elsődleges kiszolgálói kapcsolat jelszava*.

6. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Jelölje be a **Run the task after the wizard finishes** jelölőnégyzetet, vagy futtassa a feladatot manuálisan. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Jelszó beállítása a kiszolgálói kapcsolat védelme céljából a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Administration Server connection protection** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *Elsődleges kiszolgálói kapcsolat jelszava*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon ki egy alapértelmezett felhasználói fiókot. Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson a Kaspersky Endpoint Security **Administration Server connection protection** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. A **Administration Server connection protection** részen válassza a **Protect with a password** elemet.
10. A **Connection to the Administration Server** legördülő listából válassza ki az **New password** lehetőséget.
11. A **Password** mezőben állítson be egy jelszót a felügyeleti kiszolgálóhoz való csatlakozáshoz, és erősítse meg azt.

    Ha elfelejti a jelszót, a megfelelő feladat segítségével megváltoztathatja azt.
12. Ha a Kaspersky Endpoint Security 12.7-es vagy az alkalmazás korábbi verziója van telepítve, jelölje be a **Enable password encryption compatibility for previous application versions (12.7 and lower)** jelölőnégyzetet.

    A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazás erősebb jelszótitkosítást használ. Ha a Kaspersky Endpoint Security 12.8 vagy újabb verziója van telepítve, javasoljuk, hogy törölje a jelölőnégyzetet, és használja az erősebb jelszótitkosítást. Az alkalmazás korábbi verziói nem támogatják az erős jelszavas titkosítást. A feladat futtatásához be kell jelölnie a jelölőnégyzetet.
13. Mentse el a módosításokat.
14. Válassza ki a feladat melletti jelölőnégyzetet.
15. Kattintson az **Start** gombra.

Megfigyelheti a feladat állapotát, valamint az eszközök számát, ahol a feladat sikeresen vagy hibásan lett végrehajtva.

A számítógép újbóli csatlakoztatása egy másik felügyeleti kiszolgálóhoz

A számítógép újbóli csatlakoztatása egy másik felügyeleti kiszolgálóhoz a következő lépésekkel jár:

1. Az aktuális `[KSC1]` kiszolgáló konzolján futtassa a *Change Administration Server* feladatot a hálózati ügynöknél.

   A feladat futtatása után a számítógép ismét csatlakozik az új `[KSC2]` kiszolgálóhoz.

   A számítógép a `[KSC1]` kiszolgáló konzolján a *Critical* állapottal jelenik meg. Nem lehet konfigurálni az alkalmazást házirendekkel vagy feladatok távoli futtatásával a számítógépen.
2. Az új `[KSC2]` kiszolgálói konzolon hozzon létre egy új *Felügyeleti kiszolgálói kapcsolatvédelem* feladatot a Kaspersky Endpoint Security számára. A feladat tulajdonságaiban adja meg az előző kiszolgáló jelszavát, és állítsa be az új kiszolgáló jelszavát.

   Új jelszó beállítása az új kiszolgálóhoz való újbóli csatlakozáshoz a felügyeleti konzolon (MMC)

   1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

      Megnyílik a feladatok listája.
   2. Kattintson az **New task** gombra.

   Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Adminisztrációs kiszolgáló kapcsolódási védelme** elemet.

2. lépés. A felügyeleti kiszolgáló kapcsolatvédelme

Állítson be jelszót az új felügyeleti kiszolgálói kapcsolat védelméhez:

1. A **Felügyeleti kiszolgáló kapcsolatvédelme** részen válassza a **Jelszóval való védelem** lehetőséget.
2. A **Felügyeleti kiszolgáló** legördülő listában válassza az **Újracsatlakozás egy másik kiszolgálóról** lehetőséget.
3. Az **Aktuális jelszó** mezőbe írja be a korábban használt megbízható kiszolgálói csatlakozáshoz beállított jelszót.
4. Az **Új jelszó** mezőben állítson be egy jelszót az új felügyeleti kiszolgálóhoz való csatlakozáshoz, és erősítse meg a jelszót.

   Ha elfelejti a jelszót, a megfelelő feladat segítségével megváltoztathatja azt.
5. Ha a Kaspersky Endpoint Security 12.7 vagy az alkalmazás korábbi verziója van telepítve, jelölje be az **Engedélyezze a jelszótitkosítási kompatibilitást a korábbi alkalmazásverziókhoz (12.7 és korábbi)** jelölőnégyzetet.

   A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazás erősebb jelszótitkosítást használ. Ha a Kaspersky Endpoint Security 12.8 vagy újabb verziója van telepítve, javasoljuk, hogy törölje a jelölőnégyzetet, és használja az erősebb jelszótitkosítást. Az alkalmazás korábbi verziói nem támogatják az erős jelszavas titkosítást. A feladat futtatásához be kell jelölnie a jelölőnégyzetet.

3. lépés A feladat futtatására kiszemelt fiók kiválasztása

Válassza a **Default account** lehetőséget. Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

4. lépés Feladatindítási ütemezés konfigurálása

A **Scheduled start** részen válassza a **Manually** elemet.

5. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például *Elsődleges kiszolgálói kapcsolat jelszava*.

6. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Jelölje be a **Run the task after the wizard finishes** jelölőnégyzetet, vagy futtassa a feladatot manuálisan. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Új jelszó beállítása az új kiszolgálóhoz való újbóli csatlakozáshoz a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Administration Server connection protection** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást, például azt, hogy *Elsődleges kiszolgálói kapcsolat jelszava*.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Válasszon ki egy alapértelmezett felhasználói fiókot. Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Lépjen ki a varázslóból.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson a Kaspersky Endpoint Security **Administration Server connection protection** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. A **Administration Server connection protection** részen válassza a **Protect with a password** elemet.

10. A **Connection to the Administration Server** legördülő listából válassza ki az **Reconnect from another server** lehetőséget.

11. Az **Current password** mezőbe írja be a korábban használt megbízható kiszolgálói csatlakozáshoz beállított jelszót.

12. Az **New password** mezőben állítson be egy jelszót az új felügyeleti kiszolgálóhoz való csatlakozáshoz, és erősítse meg a jelszót.

    Ha elfelejti a jelszót, a megfelelő feladat segítségével megváltoztathatja azt.

13. Ha a Kaspersky Endpoint Security 12.7 vagy az alkalmazás korábbi verziója van telepítve, jelölje be az **Engedélyezze a jelszótitkosítási kompatibilitást a korábbi alkalmazásverziókhoz (12.7 és korábbi)** jelölőnégyzetet.

    A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazás erősebb jelszótitkosítást használ. Ha a Kaspersky Endpoint Security 12.8 vagy újabb verziója van telepítve, javasoljuk, hogy törölje a jelölőnégyzetet, és használja az erősebb jelszótitkosítást. Az alkalmazás korábbi verziói nem támogatják az erős jelszavas titkosítást. A feladat futtatásához be kell jelölnie a jelölőnégyzetet.

14. Mentse el a módosításokat.

15. Válassza ki a feladat melletti jelölőnégyzetet.

16. Kattintson az **Start** gombra.

    Megfigyelheti a feladat állapotát, valamint az eszközök számát, ahol a feladat sikeresen vagy hibásan lett végrehajtva.

A feladat elvégzése után győződjön meg arról, hogy az új `[KSC2]` kiszolgáló konzolján a számítógép *OK* állapotú. Tesztelje, hogy távolról futtathatja-e a feladatokat, és konfigurálhatja-e az alkalmazást házirendek segítségével.

A felügyeleti kiszolgálói kapcsolat jelszavának visszaállítása

Ha elfelejtette a felügyeleti kiszolgálói kapcsolat jelszavát, vagy a jelszót feltörték, a jelszót a feladat tulajdonságaiban állíthatja vissza. A jelszó visszaállítása és új jelszó beállítása a különböző felügyeleti kiszolgálói kapcsolatvédelmi státuszú számítógépek csoportja számára is lehetséges. Ez azt jelenti, hogy ha néhány számítógépen engedélyezve van a védelem, néhány számítógépen pedig le van tiltva, a feladat minden számítógépen jelszót állít be.

A felügyeleti kiszolgálói kapcsolat jelszavát csak annak a megbízható kiszolgálónak a konzolján állíthatja vissza, amelyhez a számítógép csatlakozik.

A felügyeleti kiszolgálói kapcsolat jelszavának visszaállítása az Adminisztrációs konzol (MMC) segítségével

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Tasks** lehetőséget.

3. Válassza ki a **Felügyeleti kiszolgáló kapcsolatvédelme** feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.

4. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.

5. A **Felügyeleti kiszolgáló kapcsolatvédelme** részen válassza a **Védelem és jelszó módosítása** lehetőséget.

6. A **Jelszó a felügyeleti kiszolgálóhoz való csatlakozáshoz** mezőben állítson be egy új jelszót az aktuális megbízható kiszolgálóhoz való csatlakozáshoz, és erősítse meg a jelszót.

7. Mentse el a módosításokat.

8. Futtassa a feladatot.

A felügyeleti kiszolgálói kapcsolat jelszavának visszaállítása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Administration Server connection protection** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. A **Administration Server connection protection** részen válassza a **Protect and change password** elemet.

5. A **Password** mezőben állítson be egy új jelszót az aktuális megbízható kiszolgálóhoz való csatlakozáshoz, és erősítse meg a jelszót.

6. Mentse el a módosításokat.

7. Válassza ki a feladat melletti jelölőnégyzetet.

8. Kattintson az **Start** gombra.

Ennek eredményeként a feladat befejezése után a felügyeleti kiszolgáló kapcsolódási jelszava visszaállításra kerül.

Felügyeleti kiszolgálói kapcsolat védelmének letiltása

Távolról csak annak a megbízható kiszolgálónak a konzolján lehet letiltani a Felügyeleti kiszolgáló kapcsolatvédelmét, amelyhez a számítógép csatlakozik. A védelem helyileg is letiltható a parancssorban.

A kiszolgálói kapcsolatvédelem letiltása a felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Tasks** lehetőséget.

3. Válassza ki a **Felügyeleti kiszolgáló kapcsolatvédelme** feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.

4. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.

5. A **Felügyeleti kiszolgáló kapcsolatvédelme** területen válassza a **Nincs védelem** jelölőnégyzetet.

6. Mentse el a módosításokat.

7. Futtassa a feladatot.

   Megfigyelheti a feladat állapotát, valamint az eszközök számát, ahol a feladat sikeresen vagy hibásan lett végrehajtva.

A kiszolgálói kapcsolatvédelem letiltása a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Administration Server connection protection** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. A **Administration Server connection protection** részen válassza a **Do not protect** elemet.

5. Mentse el a módosításokat.

6. Válassza ki a feladat melletti jelölőnégyzetet.

7. Kattintson az **Start** gombra.

   Megfigyelheti a feladat állapotát, valamint az eszközök számát, ahol a feladat sikeresen vagy hibásan lett végrehajtva.

A kiszolgálói kapcsolatvédelem letiltása parancssorból

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.

2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

3. Futtassa a következő parancsot:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   ahol `<password>` a KLAdmin felhasználói fiók jelszava vagy a *Felügyeleti kiszolgálói kapcsolatvédelem* feladat jelszava. Ha a paraméter nincs megadva, a Kaspersky Endpoint Security a következő sorban jelszó megadására kéri fel.

   > A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet.

Példa

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Adattitkosítás

A Kaspersky Endpoint Security lehetővé teszi a helyi és a cserélhető meghajtókon tárolt fájlok és mappák, valamint a teljes cserélhető meghajtók és merevlemezek titkosítását. Az adattitkosítás minimálisra csökkenti az információk olyan kiszivárgásainak kockázatát, amelyek hordozható számítógép, cserélhető meghajtó vagy merevlemez elvesztésekor vagy ellopásakor, illetve az adatok illetéktelen felhasználók vagy alkalmazások által történő elérésekor áll fenn. A Kaspersky Endpoint Security az Advanced Encryption Standard (AES) titkosítási algoritmust használja.

Ha a licenc lejárt, az alkalmazás nem titkosít új adatokat, a régebben titkosított adatok pedig titkosítva, használható állapotban maradnak. Ekkor az új adatok titkosításához az alkalmazást olyan új licenccel kell aktiválni, amely engedélyezi a titkosítás használatát.

Ha a Kaspersky Endpoint Security ARM-alapú számítógépen van telepítve, csak a BitLocker meghajtótitkosítás érhető el. Az alkalmazás más adattitkosítási összetevőket nem támogat.

Ha a licence lejárt, megszegte a Végfelhasználói licencszerződést, vagy valaki törölte a licenckulcsot, a Kaspersky Endpoint Security alkalmazást vagy a titkosítási összetevőket, akkor a korábban titkosított fájlok titkosított állapota nem garantálható. Ennek az oka, hogy egyes alkalmazások – például a Microsoft Office Word – szerkesztés közben a fájlokból ideiglenes másolatokat készítenek. Az eredeti fájl mentésekor az ideiglenes másolat felváltja az eredeti fájlt. Emiatt az olyan számítógépen, amelyen nincs vagy nem érhető el titkosítási funkció, a fájl titkosítás nélkül marad.

A Kaspersky Endpoint Security az alábbi fő adatvédelmi funkciókkal rendelkezik:

- **Fájlszintű titkosítás a számítógép helyi meghajtóin**. A fájlok listáit összeállíthatja kiterjesztés vagy kiterjesztések csoportja alapján, illetve a számítógép helyi meghajtóin tárolt mappák listái szerint, és létrehozhat adott alkalmazások által előállított fájlok titkosítására vonatkozó szabályokat. Rendszabály alkalmazását követően a Kaspersky Endpoint Security az alábbi fájlokat titkosítja és fejti vissza:
  - a listákra titkosítás és visszafejtés céljából egyedileg felvett fájlok;
  - a listákra titkosítás és visszafejtés céljából felvett mappákban tárolt fájlok;
  - külön alkalmazások által előállított fájlok.
- **Cserélhető meghajtók titkosítása**. Megadhat alapértelmezett titkosítási szabályt, melynek alapján az alkalmazás ugyanazt a műveletet végzi el minden cserélhető meghajtóval, illetve megadhat külön-külön titkosítási szabályokat az egyes cserélhető meghajtókhoz.

  Az alapértelmezett titkosítási szabály prioritása alacsonyabb, mint az egyes cserélhető meghajtókhoz készített titkosítási szabályoké. A megadott eszköztípusú cserélhető meghajtókhoz készített titkosítási szabályok prioritása alacsonyabb, mint a megadott eszközazonosítójú cserélhető meghajtókhoz készítetteké.

  Cserélhető meghajtón lévő fájlok titkosítási szabályának kiválasztásához a Kaspersky Endpoint Security ellenőrzi, hogy az eszköztípus vagy -azonosító ismert-e. Az alkalmazás ekkor elvégzi az alábbi műveletek közül valamelyiket:
  - Ha csak az eszköztípus ismert, az alkalmazás az adott eszköztípusú cserélhető meghajtókhoz készített titkosítási szabályt alkalmazza (ha van).
  - Ha csak az eszközazonosító ismert, az alkalmazás az adott eszközazonosítójú cserélhető meghajtókhoz készített titkosítási szabályt alkalmazza (ha van).

- Ha az eszköztípus és -azonosító egyaránt ismert, az alkalmazás az adott eszközazonosítójú cserélhető meghajtókhoz készített titkosítási szabályt alkalmazza (ha van). Ha nincs ilyen szabály, de az adott eszköztípusú cserélhető meghajtókhoz készített titkosítási szabály van, az alkalmazás ezt a szabályt alkalmazza. Ha sem az adott eszközazonosítóhoz, sem az adott eszköztípushoz nincs megadva titkosítási szabály, az alkalmazás az alapértelmezett titkosítási szabályt alkalmazza.

- Ha sem az eszköztípus, sem az eszközazonosító nem ismert, az alkalmazás az alapértelmezett titkosítási szabályt alkalmazza.

Az alkalmazás segítségével a cserélhető meghajtókat előkészítheti a rajtuk tárolt adatok hordozható módban történő használatára. A hordozható mód engedélyezését követően a titkosítási funkcióval nem rendelkező számítógépekhez csatlakoztatott cserélhető meghajtókon lévő titkosított fájlokhoz is hozzáférhet.

- **Az alkalmazások titkosított fájlokhoz való hozzáférési szabályainak kezelése** Bármelyik alkalmazáshoz készíthet a titkosított fájlokhoz való hozzáférési szabályt, amely blokkolja a hozzáférést, illetve csak titkosított szöveg formájában engedélyezi a hozzáférést. A titkosított szöveg a titkosítás alkalmazása után kapott karaktersorozat.

- **Titkosított csomagok létrehozása**. Létrehozhat titkosított archívumokat, és hozzáférésüket védheti jelszóval. A titkosított archívumok tartalmához csak azon jelszavak megadásával lehet hozzáférni, amelyekkel archívumokhoz való hozzáférést védi. Ezeket az archívumokat biztonságosan továbbíthatja hálózatokon, illetve cserélhető meghajtókon.

- **Teljes lemeztitkosítás**. Kiválaszthatja a titkosítási technológiát: Kaspersky lemeztitkosítás vagy BitLocker meghajtótitkosítás (a továbbiakban egyszerűen „BitLocker” is).

  A *BitLocker* a Windows operációs rendszer részét képező technológia. Ha egy számítógépen Trusted Platform Module (TPM) található, a BitLocker annak segítségével tárolja a titkosított merevlemezhez való hozzáférést biztosító visszaállítási kulcsokat. A számítógép indításakor a BitLocker lekéri a merevlemez visszaállítási kulcsait a Trusted Platform Module-tól, és feloldja a meghajtót. A visszaállítási kulcsokhoz való hozzáféréshez beállíthatja jelszó és / vagy PIN-kód használatát.

  Megadhatja az alapértelmezett teljes lemeztitkosítási szabályt, és listát készíthet a titkosításból kizárni kívánt merevlemezekről. A Kaspersky Endpoint Security a Kaspersky Security Center rendszabály alkalmazását követően elvégzi a teljes lemeztitkosítást. Az alkalmazás a merevlemezek összes logikai partícióját egyidejűleg titkosítja.

  A rendszermerevlemezek titkosítását követően a számítógép legközelebbi indításakor a felhasználónak a Hitelesítési ügynök segítségével hitelesítést kell végeznie, mielőtt hozzáférhetne a merevlemezekhez, és betöltődhetne az operációs rendszer. Ehhez meg kell adni a token vagy a számítógéphez csatlakoztatott okoskártya jelszavát, vagy a helyi hálózati rendszergazda által a *Hitelesítési ügynök fiókok kezelése* feladat segítségével létrehozott Hitelesítési ügynök-fiók felhasználónevét és jelszavát. Ezek a fiókok azon Microsoft Windows fiókokon alapulnak, amelyekkel a felhasználó az operációs rendszerbe bejelentkezik. Emellett használhatja az Single Sign-On (SSO) technológiát is, amely lehetővé teszi, hogy automatikusan bejelentkezzen az operációs rendszerbe a Hitelesítési ügynök-fiókja felhasználónevével és jelszavával.

  Ha egy számítógép tartalmáról biztonsági mentést készít, majd a számítógép adatait titkosítja, majd visszaállítja a biztonsági mentést és ismét titkosítja az adatokat, a Kaspersky Endpoint Security másodpéldányt hoz létre a Hitelesítési ügynök-fiókokból. A fiókok másodpéldányainak eltávolításához a klmover segédprogramot kell használni `dupfix` kulccsal. A klmover segédprogram megtalálható a Kaspersky Security Center buildben. A működéséről további információ a Kaspersky Security Center Súgóban található.

A titkosított merevlemezekhez való hozzáférés csak olyan számítógépekről lehetséges, amelyeken a Kaspersky Endpoint Security teljes lemeztitkosítási funkcióval van telepítve. Ez az óvintézkedés minimálisra csökkenti a titkosított merevlemezeken lévő adatok kiszivárgásának kockázatát, ha a vállalat helyi hálózatán kívül próbálnak hozzájuk férni.

A merevlemezeket és cserélhető meghajtókat titkosíthatja a Csak a használt lemezterület titkosítása funkció segítségével. E funkció csak új, korábban nem használt eszközök esetén javasolt. Ha már használatban lévő eszközön alkalmaz titkosítást, akkor javasolt az egész eszközt titkosítani. Ez gondoskodik az összes adat védelméről – még a korábban törölt, de esetleg visszanyerhető információt hordozó adatokéról is.

A titkosítás megkezdése előtt a Kaspersky Endpoint Security beszerzi a fájlrendszer szektorainak térképét. A titkosítás első hullámába a titkosítás indításának pillanatában fájlok által elfoglalt szektorok tartoznak. A titkosítás második hullámába azok a szektorok tartoznak, amelyekben a titkosítás megkezdését követően történt írás. A titkosítás befejeztét követően az összes, adatokat tartalmazó szektor titkosított állapotban van.

Ha a titkosítás végeztével a felhasználó töröl egy fájlt, a törölt fájlt tároló szektorok a fájlrendszer szintjén új adatok tárolására felhasználhatók lesznek, de titkosítva maradnak. Mivel a fájlok az új készülékre íródnak, az új készülék pedig rendszeresen titkosítva van a **Csak a használt lemezterület titkosítása** funkcióval, így egy idő után minden rész titkosítva lesz.

A fájlok visszafejtéséhez szükséges adatokat a számítógépet a titkosítás folyamán felügyelő Kaspersky Security Center felügyeleti kiszolgáló biztosítja. Ha egy titkosított objektummal rendelkező számítógépet valamilyen oknál fogva más Adminisztrációs kiszolgáló kezelt, akkor a következő módszerekkel kérheti le a titkosított adatokat:

- Megegyező hierarchiában lévő Adminisztrációs kiszolgáló:
  - Nem szükséges további művelet végrehajtása. A felhasználó továbbra is hozzáfér a titkosított objektumokhoz. A titkosítási kulcsok az összes Adminisztrációs kiszolgáló között oszlanak el.
- Külön Adminisztrációs kiszolgáló:
  - Titkosított objektumokhoz való hozzáférés kérése a helyi hálózati rendszergazdától.
  - Titkosított eszközökön lévő adatok visszaállítása a Helyreállító segédprogrammal.
  - A számítógépet a titkosítás folyamán felügyelő Kaspersky Security Center felügyeleti kiszolgáló beállításainak visszaállítása biztonsági másolatból, és e beállítások alkalmazása a titkosított objektumokat tartalmazó számítógépet jelenleg felügyelő Adminisztrációs kiszolgálón.

Ha nincs hozzáférése a titkosított adatokhoz, kövesse a titkosított adatokkal való munkavégzésre vonatkozó, speciális instrukciókat (Titkosított fájlok elérésének visszaállítása, Munkavégzés titkosított eszközökkel hozzáférés nélkül).

A titkosítási funkció korlátozásai

Az Adattitkosítás korlátozásai a következők:

- Az alkalmazás titkosítás közben szervizfájlokat hoz létre. A merevlemez nem töredezett szabad területének nagyjából 0.5%-a szükséges ezek tárolásához. Ha a merevlemez nem töredezett szabad területe nem elegendő, akkor a titkosítás addig nem kezdődik el, amíg fel nem szabadul a kellő terület.
- Az összes adattitkosítási összetevőt kezelheti a Kaspersky Security Center adminisztrációs konzoljában és a Kaspersky Security Center Web Console-ban. A Kaspersky Security Center Cloud Console-ban csak a Bitlockert felügyelheti.

- Az adattitkosítás csak akkor érhető el, ha a Kaspersky Endpoint Security alkalmazást a Kaspersky Security Center adminisztrációs rendszerrel vagy a Kaspersky Security Center Cloud Console (csak BitLocker) alkalmazással használja. Ha offline módban használja a Kaspersky Endpoint Security alkalmazást, akkor nem fog működni az Adattitkosítás, mivel a Kaspersky Endpoint Security a Kaspersky Security Center helyen tárolja a titkosítási kulcsokat.

- Ha a Kaspersky Endpoint Security alkalmazás Microsoft Windows for Servers operációs rendszert futtató számítógépre van telepítve, csak a BitLocker meghajtótitkosítási technológiával végzett, teljes lemeztitkosítás áll rendelkezésre. Ha a Kaspersky Endpoint Security alkalmazást Windows for Workstations operációs rendszert futtató számítógépre telepíti, minden adattitkosítási funkció rendelkezésre áll.

- Ha a Kaspersky Endpoint Security egy ARM-alapú számítógépen van telepítve, csak a BitLocker meghajtótitkosítási technológiát használó Teljes lemeztitkosítás érhető el, más titkosítási összetevők nem támogatottak.

A Kaspersky lemeztitkosítási technológiával történő teljes lemeztitkosítás a hardver- és szoftverkövetelményeknek meg nem felelő merevlemezeknél nem használható.

A Kaspersky Endpoint Security és a Kaspersky Anti-Virus for UEFI a teljes lemezes titkosítási funkciói közti kompatibilitás nem támogatott. Az operációs rendszer indulása előtt elindul a Kaspersky Anti-Virus for UEFI. A teljes lemeztitkosítás használatakor az alkalmazás észleli a számítógépen telepített operációs rendszer hiányát. Ennek eredményeként a Kaspersky Anti-Virus for UEFI működése hibával befejeződik. A fájlszintű titkosítás (FLE) nem érinti a Kaspersky Anti-Virus for UEFI működését.

A Kaspersky Endpoint Security az alábbi konfigurációkat támogatja:

- HDD-, SSD- és USB-meghajtók.

  A Kaspersky lemeztitkosítás (FDE) technológia támogatja az SSD-vel való munkát, miközben megőrzi az SSD-meghajtók teljesítményét és élettartamát.

- Buszon keresztül csatlakoztatott meghajtók: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- A SD- vagy MMC-buszon keresztül csatlakoztatott nem cserélhető meghajtók.

- 512 bájtos szektorokkal rendelkező meghajtók.

- 4096 bájtos szektorokkal rendelkező meghajtók, amelyek 512 bájtot emulálnak.

- A következő típusú partíciókkal rendelkező meghajtók: GPT, MBR és VBR (cserélhető meghajtók).

- Az UEFI 64 és a Legacy BIOS szabvány beágyazott szoftverei.

- Az UEFI szabvány beépített szoftvere a biztonságos rendszerindítás támogatásával.

  A *biztonságos rendszerindítás* egy olyan technológia, amely az UEFI betöltő alkalmazásokhoz és illesztőprogramokhoz tartozó digitális aláírások ellenőrzésére szolgál. A biztonságos rendszerindítás blokkolja az aláíratlan vagy ismeretlen kiadók által aláírt UEFI-alkalmazások és illesztőprogramok indítását. A Kaspersky lemeztitkosítás (FDE) teljes mértékben támogatja a biztonságos rendszerindítást. A Hitelesítési ügynököt a Microsoft Windows UEFI illesztőprogram-közzétevői tanúsítványa írja alá.

  Egyes eszközökön (például a Microsoft Surface Pro és a Microsoft Surface Pro 2) alapértelmezés szerint a digitális aláírás-ellenőrzési tanúsítványok elavult listája lehet telepítve. A meghajtó titkosítása előtt frissíteni kell a tanúsítványok listáját.

- Az UEFI szabvány beépített szoftvere gyors rendszerindítás támogatással.

A *gyors rendszerindítás* egy olyan technológia, amely a számítógép gyorsabb beindulását segíti. Ha a gyors rendszerindítás technológia engedélyezve van, a számítógép általában csak az operációs rendszer indításához szükséges UEFI-illesztőprogramok minimális készletét tölti be. Ha a gyors rendszerindítás technológia engedélyezve van, előfordulhat, hogy az USB-billentyűzetek, egerek, USB-tokenek, érintőpadok és érintőképernyők nem működnek a Hitelesítési ügynök futása közben.

> A Kaspersky lemeztitkosítás (FDE) használatához ajánlott a gyors rendszerindítási technológia letiltása. Az FDE tesztelő segédprogrammal tesztelheti a Kaspersky lemeztitkosítás (FDE) működését.

A Kaspersky Endpoint Security nem támogatja az alábbi konfigurációkat:

- A rendszerbetöltő az egyik meghajtón van, az operációs rendszer pedig egy másikon.
- A rendszer UEFI 32 szabványú beágyazott szoftvert tartalmaz.
- A rendszer rendelkezik Intel® Rapid Start technológiával és a hibernálási partíciót még az Intel® Rapid Start technológia kikapcsolásakor is tartalmazó meghajtókkal.
- Tíznél több kiterjesztett partíciót tartalmazó MBR formátumú meghajtók.
- A rendszer nem rendszermeghajtón található lapozófájllal rendelkezik.
- Több rendszerrel indítható, egyszerre több telepített operációs rendszert tartalmazó rendszer.
- Dinamikus partíciók (csak az elsődleges partíciók támogatottak).
- 0.5%-nál kevesebb szabad, nem töredezett lemezterülettel rendelkező meghajtók.
- 512 vagy 4096 bájttól eltérő, 512 bájtot emuláló szektorméretű meghajtók.
- Hibrid meghajtók.
- A rendszer harmadik féltől származó betöltővel rendelkezik.
- Tömörített NTFS-könyvtárakkal rendelkező meghajtók.
- A Kaspersky lemeztitkosítás (FDE) technológia nem kompatibilis más teljes lemeztitkosítási technológiákkal (például a BitLocker, a McAfee Drive Encryption vagy a WinMagic SecureDoc).
- A Kaspersky lemeztitkosítás (FDE) technológia nem kompatibilis az ExpressCache technológiával.
- A partíciók létrehozása, törlése és módosítása titkosított meghajtón nem támogatott. Elveszítheti az adatokat.
- A fájlrendszer formázása nem támogatott. Elveszítheti az adatokat.

  Ha a Kaspersky lemeztitkosítás (FDE) technológiával titkosított meghajtót kell formáznia, formázza a meghajtót olyan számítógépen, amelyen nincs Kaspersky Endpoint Security for Windows, és csak teljes lemeztitkosítást használjon.

  A gyorsformázási beállítással formázott titkosított meghajtó tévesen titkosítottként lehet azonosítva, amikor legközelebb a Kaspersky Endpoint Security for Windowst futtató számítógéphez van csatlakoztatva. A felhasználói adatok nem lesznek elérhetők.
- A Hitelesítési ügynök legfeljebb 100 fiókot támogat.
- Az egyszeri bejelentkezési technológia nem kompatibilis a külső fejlesztők más technológiáival.

- A Kaspersky lemeztitkosítás (FDE) technológia a következő eszközmodelleken nem támogatott:
  - Dell Latitude E6410 (UEFI mód)
  - HP Compaq nc8430 (Legacy BIOS mód)
  - Lenovo ThinkCentre 8811 (Legacy BIOS mód)
- A hitelesítési ügynök nem támogatja az USB-tokenekkel való munkát, ha a Legacy USB támogatása engedélyezve van. A számítógépen csak jelszóalapú hitelesítés lehetséges.
- Ha Legacy BIOS módban titkosít egy meghajtót, javasoljuk, hogy engedélyezze a Legacy USB Support funkciót a következő eszköztípusokon:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550
  - Lenovo ThinkPad L530

- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (alaplap)

A titkosítási kulcs hosszának módosítása (AES56 / AES256)

A Kaspersky Endpoint Security az Advanced Encryption Standard (AES) titkosítási algoritmust használja. A Kaspersky Endpoint Security a 256 vagy 56 bites kulcshosszú AES-titkosítási algoritmusokat támogatja. Az adattitkosítási algoritmus az AES-titkosítási könyvtártól függ, amely a terjesztőcsomagba tartozik: *Erős titkosítás (AES256)* vagy *Könnyű titkosítás (AES56)*. Az AES-titkosítási könyvtár az alkalmazással együtt van telepítve.

A titkosítási kulcs hosszának módosítása a Kaspersky Endpoint Security 11.2.0 vagy újabb verzióiban érhető el.

A titkosítási kulcs hosszának módosítása a következő lépésekből áll:

1. A titkosítási kulcs hosszának módosítása előtt fejtse vissza a Kaspersky Endpoint Security által titkosított objektumokat.
   a. A merevlemezek visszafejtése.
   b. Fájlok visszafejtése helyi meghajtókon.
   c. Cserélhető meghajtók visszafejtése.

   A titkosítási kulcs hosszának módosítását követően a korábban titkosított objektumok elérhetetlenné válnak.
2. Távolítsa el a Kaspersky Endpoint Security alkalmazást.
3. Telepítse a Kaspersky Endpoint Security alkalmazást a különböző titkosítási könyvtárat tartalmazó Kaspersky Endpoint Security terjesztőcsomagból.

Az alkalmazás frissítésével is módosíthatja a titkosítási kulcs hosszát. A kulcshossz akkor módosítható alkalmazásfrissítésen keresztül, ha teljesülnek a következő feltételek:

- A Kaspersky Endpoint Security 10 Service Pack 2 vagy újabb verziója van telepítve a számítógépen.
- Az adattitkosító összetevők (Fájl-szintű titkosítás, Teljes lemeztitkosítás) nincsenek telepítve a számítógépen.

  Alapértelmezetten az adattitkosító összetevők nem tartoznak a Kaspersky Endpoint Security alkalmazáshoz. A BitLocker kezelés összetevő nincs hatással a titkosítási kulcs hosszának módosítására.

A titkosítási kulcs hosszának módosításához futtassa a kes_win.msi vagy a setup_kes.exe fájlt a szükséges titkosítási könyvtárat tartalmazó terjesztőcsomagból. A telepítőcsomaggal távolról is frissítheti az alkalmazást.

Nem lehet módosítani a titkosítási kulcs hosszát, ha a használt terjesztőcsomag verziója megegyezik a számítógépén telepített alkalmazás verziójával. Ilyenkor először el kell távolítani az alkalmazást.

Kaspersky lemeztitkosítás

A Kaspersky lemeztitkosítás az ARM-alapú számítógépeken nem támogatott.

A Kaspersky Lemeztitkosítás csak olyan számítógépeken érhető el, melyek a munkaállomásokhoz Windows operációs rendszert futtatnak. A szerverekhez Windows operációs rendszert futtató számítógépeken használjon BitLocker meghajtótitkosítás technológiát.

A Kaspersky Endpoint Security a FAT32, NTFS és az exFat fájlrendszerek teljes lemeztitkosítását támogatja.

A teljes lemeztitkosítás megkezdése előtt az alkalmazás különböző ellenőrzések elvégzésével megállapítja, hogy az eszköz titkosítható-e, így többek között megnézi, hogy a rendszermerevlemez kompatibilis-e a Hitelesítési ügynök vagy a BitLocker titkosítási összetevőkkel. A kompatibilitás ellenőrzéséhez a számítógépet újra kell indítani. A számítógép újraindítását követően az alkalmazás automatikusan elvégzi az összes szükséges ellenőrzést. Ha a kompatibilitási ellenőrzés sikeres, a teljes lemeztitkosítás az operációs rendszer betöltését és az alkalmazás elindulását követően elindul. Ha kiderül, hogy a rendszermerevlemez nem kompatibilis a Hitelesítési ügynök vagy a BitLocker titkosítási összetevőkkel, a számítógépet a hardveres Reset gombbal kell újraindítani. A Kaspersky Endpoint Security naplózza az inkompatibilitási adatokat. Ezek alapján az alkalmazás az operációs rendszer indításakor nem kezdi meg a teljes lemeztitkosítást. Az esemény adatai a Kaspersky Security Center jelentéseiben kerülnek naplózásra.

Ha a számítógép hardverkonfigurációja megváltozott, akkor törölni kell az alkalmazás által a korábbi ellenőrzés során naplózott inkompatibilitási adatokat, hogy ismét sor kerüljön a rendszermerevlemez Hitelesítési ügynök és BitLocker titkosítási összetevőkkel való kompatibilitásának ellenőrzésére. Ehhez a teljes lemeztitkosítás előtt gépelje be a parancssorba az `avp pbatestreset` szöveget. Ha a rendszermerevlemez Hitelesítési ügynökkel való kompatibilitásának ellenőrzését követően az operációs rendszer nem töltődik be, el kell távolítani a Hitelesítési ügynök tesztműködése után visszamaradt objektumokat és adatokat a Visszaállító segédprogram segítségével, majd el kell indítani a Kaspersky Endpoint Security alkalmazást, és ismét végre kell hajtani az `avp pbatestreset` parancsot.

A teljes lemeztitkosítás megkezdését követően a Kaspersky Endpoint Security a merevlemezekre írt összes adatot titkosítja.

Ha a teljes lemeztitkosítás közben a felhasználó leállítja vagy újraindítja a számítógépet, a Hitelesítési ügynök betöltődik az operációs rendszer legközelebbi indulása előtt. A Kaspersky Endpoint Security a Hitelesítési ügynökben történő sikeres hitelesítést és az operációs rendszer elindulását követően folytatja a teljes lemeztitkosítást.

Ha az operációs rendszer a teljes lemeztitkosítás közben hibernált módba vált, a Hitelesítési ügynök betöltődik, amikor az operációs rendszer kilép a hibernált módból. A Kaspersky Endpoint Security a Hitelesítési ügynökben történő sikeres hitelesítést és az operációs rendszer elindulását követően folytatja a teljes lemeztitkosítást.

Ha az operációs rendszer a teljes lemeztitkosítás közben alvó módba lép, a Kaspersky Endpoint Security a Hitelesítési ügynök betöltése nélkül folytatja a teljes lemeztitkosítást, amikor az operációs rendszer kilép alvó módból.

A Hitelesítési ügynök segítségével kétféleképpen lehet a felhasználói hitelesítést elvégezni:

- Adja meg a hálózati rendszergazda által a Kaspersky Security Center eszközeivel létrehozott Hitelesítési ügynök-fiók felhasználónevét és jelszavát.
- Adja meg a token vagy a számítógéphez csatlakoztatott okoskártya jelszavát.

  Akkor lehet tokent vagy okoskártyát használni, ha a számítógép merevlemezeit az AES256 titkosítási algoritmus titkosította. Ha a számítógép merevlemezei az AES56 algoritmussal vannak titkosítva, a rendszer elutasítja az elektronikus tanúsítványfájl parancshoz való hozzáadását.

A Hitelesítési ügynök alábbi nyelvek billentyűzetkiosztásait támogatja:

- Angol (Egyesült Királyság)
- Angol (Egyesült Államok)
- Arab (Algéria, Marokkó, Tunézia; AZERTY kiosztás)
- Spanyol (Latin-Amerika)
- olasz
- Német (Németország és Ausztria)
- Német (Svájc)
- Portugál (Brazília, ABNT2 kiosztás)
- Orosz (105 gombos IBM/Windows billentyűzetek QWERTY kiosztással)
- Török (QWERTY kiosztás)
- Francia (Franciaország)
- Francia (Svájc)

- Francia (Belgium, AZERTY kiosztás)
- Japán (106 gombos billentyűzetek QWERTY kiosztással)

A Hitelesítési ügynökben akkor használható egy adott billentyűzetkiosztás, ha az meg van adva az operációs rendszer nyelvi és regionális beállításaiban, és a Microsoft Windows üdvözlő képernyőjén is használható.

Ha a Hitelesítési ügynök-fiók nevében olyan szimbólum szerepel, amelyet a Hitelesítési ügynökben elérhető billentyűzetkiosztások segítségével nem lehet beírni, a titkosított merevlemezekhez csak a visszaállító segédprogrammal történő visszaállításukat követően, vagy a Hitelesítési ügynök-fiók felhasználónevének és jelszavának visszaállítását követően lehet hozzáférni.

Az SSD-meghajtó titkosításának speciális jellemzői

Az alkalmazás támogatja az SSD-meghajtók, a hibrid SSHD-meghajtók és az Intel Smart Response funkcióval rendelkező meghajtók titkosítását. Az alkalmazás nem támogatja az Intel Rapid Start funkcióval rendelkező meghajtók titkosítását. Az ilyen meghajtó titkosítása előtt tiltsa le az Intel Rapid Start funkciót.

Az SSD-meghajtók titkosítása a következő speciális jellemzőkkel bír:

- Ha egy SSD-meghajtó új és nem tartalmaz bizalmas adatokat, engedélyezze csak a foglalt tárhely titkosítását. Ez lehetővé teszi az érintett meghajtószektorok felülírását.
- Ha az SSD-meghajtó használatban van és azon bizalmas adatok találhatók, akkor válassza a következő lehetőségek egyikét:
  - Teljesen törölje le az SSD-meghajtót (Secure Erase), telepítse az operációs rendszert, és futtassa az SSD-meghajtó titkosítását úgy, hogy csak a foglalt tárhely titkosítását engedélyezi.
  - Futtassa az SSD-meghajtó titkosítását úgy, hogy le van tiltva a csak a foglalt tárhely titkosítására szolgáló opció.

Az SSD-meghajtó titkosításához 5-10 GB szabad hely szükséges. A titkosítás adminisztrációs adatainak tárolására vonatkozó szabad tárhelyigényeket az alábbi táblázat tartalmazza.

Szabad tárhelyigény a titkosítás adminisztrációs adatainak tárolásához

SSD-meghajtó mérete (GB)	Szabad tárhely az SSD-meghajtó elsődleges partícióján (MB)	Szabad tárhely az SSD-meghajtó másodlagos partícióján (MB)
128	250	64
256	250	640
512	300	128

A Kaspersky lemeztitkosítás indítása

Teljes lemeztitkosítás megkezdése előtt célszerű meggyőződni arról, hogy a számítógép nem fertőzött. Ehhez indítsa el a Teljes vizsgálat vagy a Kritikus területek vizsgálata feladatot. Ha rootkittel fertőzött számítógépen teljes lemeztitkosítást végez, akkor a számítógép működésképtelenné válhat.

A lemeztitkosítás megkezdése előtt ellenőriznie kell a hitelesítési ügynök fiókjainak beállításait. Szükség van Hitelesítési ügynökre, ha a Kaspersky lemeztitkosítási (FDE) technológiával védett meghajtókkal kíván dolgozni. Az operációs rendszer betöltése előtt a felhasználónak el kell végeznie a hitelesítést az ügynökkel. A Kaspersky Endpoint Security lehetővé teszi, hogy Ön automatikusan létrehozzon Hitelesítési ügynök-fiókokat a meghajtó titkosítása előtt. A hitelesítési ügynöki fiókok automatikus létrehozását a teljes lemeztitkosítás rendszabályának beállításaiban engedélyezheti (lásd az alábbi utasításokat). Lehetősége van használni az egyszeri bejelentkezés (SSO) technológiát is.

A Kaspersky Endpoint Security lehetővé teszi, hogy Ön automatikusan létrehozzon hitelesítési ügynöki fiókokat a meghajtó titkosítása előtt:

- **A számítógépen lévő összes fiók**. A számítógépen lévő összes fiók, amely bármikor aktív volt.
- **A számítógépen lévő összes tartományfiók**. A számítógépen lévő összes olyan fiók, amely valamilyen tartományhoz tartozik, és amely bármikor aktív volt.
- **A számítógépen lévő összes helyi fiók**. Minden olyan helyi fiók a számítógépen, amely bármikor aktív volt.
- **Szolgáltatási fiók egyszeri jelszóval**. A szolgáltatásfiók szükséges a számítógéphez való hozzáféréshez, például ha a felhasználó elfelejti a jelszavát. A szolgáltatásfiókot tartalék fiókként is használhatja. Meg kell adnia a fiók nevét (alapértelmezés szerint `ServiceAccount`). A Kaspersky Endpoint Security automatikusan létrehoz egy jelszót. A jelszót megtalálja a Kaspersky Security Center konzolon.
- **Helyi rendszergazda**. A Kaspersky Endpoint Security létrehoz egy hitelesítési ügynöki felhasználói fiókot a számítógép helyi rendszergazdájának.
- **Számítógép kezelője** A Kaspersky Endpoint Security létrehoz egy hitelesítési ügynöki felhasználói fiókot a számítógépkezelő fiókjának. Az Active Directory számítógép-tulajdonságai között megtekintheti, hogy melyik fiók rendelkezik számítógépkezelői szerepkörrel. Alapértelmezés szerint a számítógépkezelői szerepkör nincs meghatározva, vagyis nem felel meg egyetlen fióknak sem.
- **Aktív fiók**. A Kaspersky Endpoint Security automatikusan létrehoz egy hitelesítési ügynöki fiókot a lemeztitkosításkor aktív fióknak.

A *Hitelesítési ügynök fiókok kezelése* feladat a felhasználóhitelesítési beállítások konfigurálására szolgál. Ezzel a feladattal új fiókokat adhat hozzá, módosíthatja a jelenlegi fiókok beállításait, vagy szükség esetén eltávolíthat fiókokat. Lehetősége van helyi feladatokat futtatni az egyes számítógépeken, valamint csoportfeladatokat különböző rendszergazdai csoportokból származó számítógépeken vagy kijelölt számítógépek csoportján.

A Kaspersky lemeztitkosítás futtatásának menete a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
4. A **Titkosítási technológia** legördülő listán válassza a **Kaspersky lemeztitkosítás** lehetőséget.

   A Kaspersky lemeztitkosítási technológia nem használható, ha a számítógépen BitLocker segítségével titkosított merevlemezek találhatók.

5. A **Titkosítási mód** legördülő listán válassza ki az **Összes merevlemez titkosítása** elemet.

Ha a számítógépen több operációs rendszer van telepítve, akkor az összes merevlemez titkosítása után csak az az operációs rendszer tölthető be, amelyeken az alkalmazás telepítve van.

Ha a titkosításból ki szeretne zárni néhány merevlemezt, készítsen listát ezekről a merevlemezekről.

6. Konfigurálja a Kaspersky lemeztitkosítás speciális beállításait (lásd az alábbi táblázatot).
7. Mentse el a módosításokat.

A Kaspersky lemeztitkosítás futtatásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

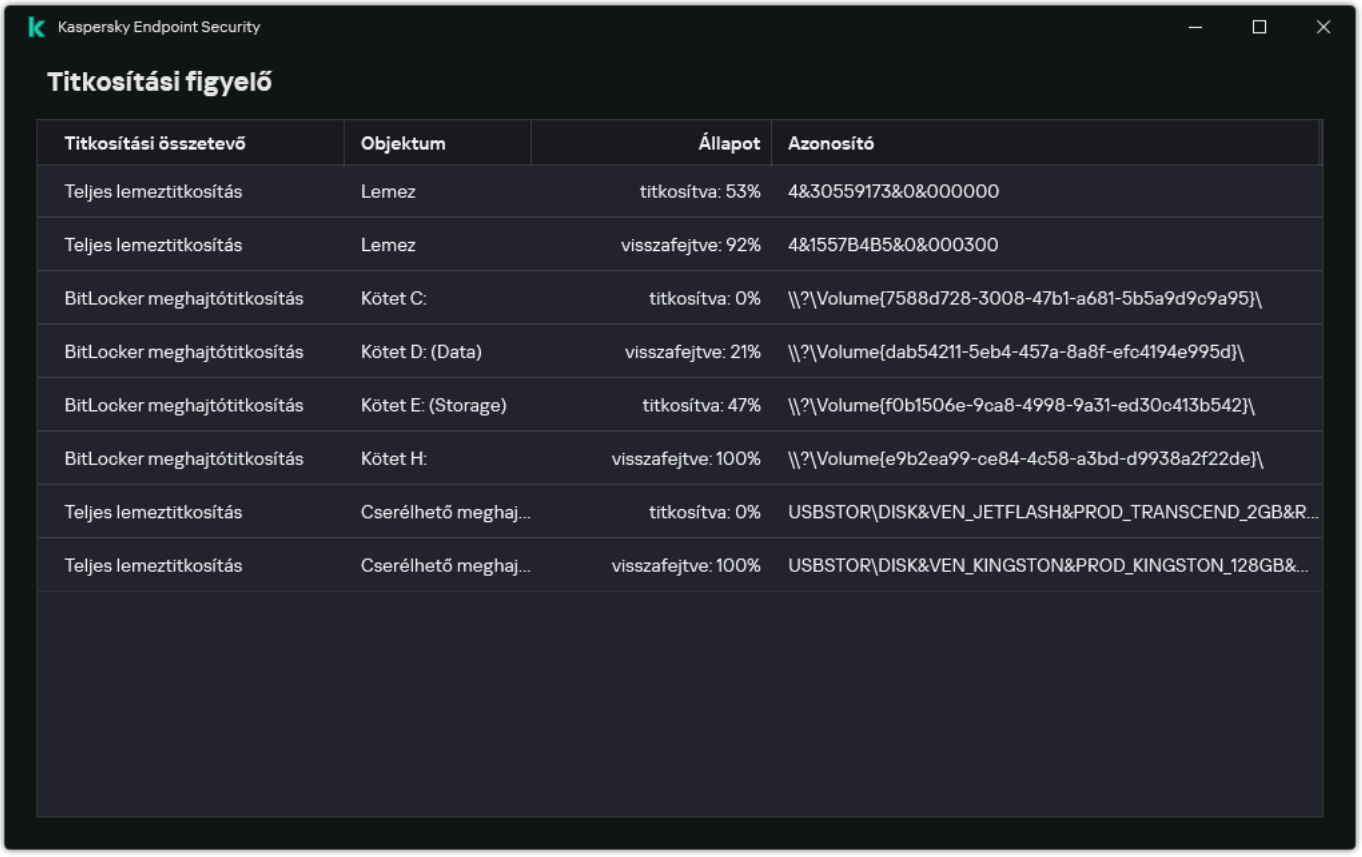
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption** → **Full Disk Encryption** elemet.
5. Válassza a **Kaspersky Disk Encryption** technológiát.

   A Kaspersky lemeztitkosítási technológia nem használható, ha a számítógépen BitLocker segítségével titkosított merevlemezek találhatók.
6. A **Action on devices** területen válassza az **Encrypt all hard drives** opciót.

   Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak azon operációs rendszer tölthető be, melyen a titkosítás el lett végezve.

   Ha a titkosításból ki szeretne zárni néhány merevlemezt, készítsen listát ezekről a merevlemezekről.
7. Konfigurálja a Kaspersky lemeztitkosítás speciális beállításait (lásd az alábbi táblázatot).
8. Mentse el a módosításokat.

A Titkosítási figyelő eszközzel vezérelheti a lemez titkosítási vagy visszafejtési folyamatát a felhasználó számítógépén. A Titkosítási figyelő eszközt a fő alkalmazásablakból futtathatja.



Titkosítási figyelő

Titkosított rendszermerevlemezek esetén a Hitelesítési ügynök az operációs rendszer elindulása előtt betöltődik. A Hitelesítési ügynök segítségével hitelesítést végezhet, így hozzáférést szerezhet a titkosított rendszermerevlemezekhez, és betöltheti az operációs rendszert. A hitelesítési eljárás sikeres befejeztével betöltődik az operációs rendszer. A hitelesítési folyamatra az operációs rendszer újraindulásakor minden alkalommal sor kerül.

A Kaspersky lemeztitkosítási összetevő beállításai

Paraméter	Leírás
Hitelesítési ügynöki fiókok automatikus létrehozása a felhasználóknak számára a titkosítás során	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás a Hitelesítési ügynöki fiókokat a számítógépen található Windows felhasználói fiókok listája alapján hozza létre. Alapértelmezés szerint a Kaspersky Endpoint Security minden helyi és tartományi fiókot felhasznál, amelynek használatával a felhasználó bejelentkezett az operációs rendszerbe az utolsó 30 nap során.
Hitelesítési ügynöki fiókok automatikusa létrehozása a számítógép összes felhasználójának bejelentkezéskor	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás a Hitelesítési ügynök elindítása előtt ellenőrzi a számítógépen található Windows felhasználói fiókok adatait. Ha a Kaspersky Endpoint Security olyan Windows felhasználói fiókot észlel, amely nem rendelkezik Hitelesítési ügynöki fiókkal, az alkalmazás új fiókot hoz létre a titkosított meghajtók eléréséhez. Az új Hitelesítési ügynöki fiók a következő alapértelmezett beállításokkal rendelkezik: csak jelszóvédett bejelentkezés és jelszó megváltoztatása az első hitelesítéskor. Ezért a már titkosított meghajtókkal rendelkező számítógépek esetében nem kell manuálisan hozzáadnia Hitelesítési ügynöki fiókokat a *Hitelesítési ügynök fiókok kezelése* feladattal.
Hitelesítési ügynökben megadott felhasználónév mentése	Ha a jelölőnégyzet ki van jelölve, az alkalmazás elmenti a Hitelesítési ügynök fiókjának nevét. Ily módon nem szükséges a fióknevet a legközelebbi alkalommal megadnia, amikor ugyanabban a fiókban a Hitelesítési ügynökben hitelesítést szeretne végezni.

Paraméter	Leírás
Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)	Ez a jelölőnégyzet engedélyezi/letiltja azt a lehetőséget, amely a titkosítási területet kizárólag a foglalt merevlemez-szektorokra korlátozza. A korlátozás révén csökkentheti a titkosítási időt. A **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemezek visszafejtése. A titkosítás megkezdése előtt kell a jelölőnégyzetet bejelölni, illetve törölni. Ha a jelölőnégyzet be van jelölve, akkor a merevlemeznek csak a fájlok által elfoglalt részei kerülnek titkosításra. A Kaspersky Endpoint Security az új adatokat hozzáadásukkor automatikusan titkosítja. Ha a jelölőnégyzet nincs bejelölve, a teljes merevlemez titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit. Ez a lehetőség új merevlemezek esetén javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha már használatban lévő merevlemezen alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről, még a törölt, esetlegesen helyreállítható adatokról is. Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.
Legacy USB Support (nem ajánlott)	Ez a jelölőnégyzet engedélyezi vagy letiltja a Legacy USB Support funkciót. A *Legacy USB Support* olyan BIOS/UEFI-funkció, amely lehetővé teszi USB-eszközök (például biztonsági token) használatát a számítógép rendszerindítási fázisában, az operációs rendszer elindítása előtt (BIOS-mód). A Legacy USB Support nem befolyásolja az USB-eszközök támogatását az operációs rendszer indulását követően. Ha a jelölőnégyzet be van jelölve, engedélyezve van az USB eszközök támogatása a számítógép indulásakor. Ha a Legacy USB Support funkció engedélyezve van, a Hitelesítési ügynök BIOS-módban nem támogatja a tokenekkel való működést USB-kapcsolaton keresztül. Ezt a lehetőséget csak akkor ajánlott alkalmazni, ha hardverkompatibilitási probléma áll fenn, és csak azokon a számítógépeken, amelyeken fennáll a probléma.

A titkosításból kizárt merevlemezek listájának létrehozása

Titkosítási kizárások listáját kizárólag Kaspersky lemeztitkosítási technológia esetén lehet létrehozni.

A titkosításból kizárt merevlemezek listájának létrehozása:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
4. A **Titkosítási technológia** legördülő listán válassza a **Kaspersky lemeztitkosítás** lehetőséget.

   A titkosításból kizárt merevlemezeknek megfelelő bejegyzések megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban. Ez a táblázat üres, ha korábban nem készített listát a titkosításból kizárt merevlemezekről.
5. Merevlemezek felvétele a titkosításból kizárt merevlemezek listájára:
   a. Kattintson **Hozzáadás** gombra.
   b. A megnyíló ablakban adja meg az **Eszköznév**, **Számítógép**, **Lemeztípus** és **Kaspersky lemeztitkosítás** értékeit.

c. Kattintson a **Frissítés**.

d. Jelölje be a **Név** oszlopban azon merevlemezeknek megfelelő táblázatsorokban a jelölőnégyzeteket, amelyeket fel szeretne venni a titkosításból kizárt merevlemezek listájára.

e. Kattintson az **OK** gombra.

A kiválasztott merevlemezek megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban.

6. Mentse el a módosításokat.

A titkosításból kizárt merevlemezek listájának exportálása és importálása:

Exportálhatja a merevlemez titkosítási kizárásainak listáját egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú azonos típusú kizárás hozzáadásával. Használhatja az exportálás/importálás funkciót a kizárások biztonsági mentésének létrehozásához, vagy a kizárások egy másik kiszolgálóra való áttelepítéséhez.

A merevlemez titkosítási szabályainak kizárásait tartalmazó lista exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.

4. A **Titkosítási technológia** legördülő listán válassza a **Kaspersky lemeztitkosítás** lehetőséget.

   A titkosításból kizárt merevlemezeknek megfelelő bejegyzések megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban.

5. A kizárások listájának exportálása:

   a. Jelölje ki az exportálni kívánt kizárásokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.

   Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.

   b. Kattintson a → **Hozzáadás** gombra.

   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.

   d. Mentse a fájlt.

   A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba.

6. A szabályok listájának importálása:

   a. Kattintson a → **Hozzáadás** gombra.

   b. A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a kizárások listáját.

c. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

7. Mentse el a módosításokat.

A merevlemez titkosítási kizárásait tartalmazó lista exportálása és importálása a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption** → **Full Disk Encryption** elemet.

   Válassza a **Kaspersky Disk Encryption** technológiát.
5. Kattintson a **Exclusions** hivatkozásra.

   Megnyílik a kizárások listája.
6. A szabályok listájának exportálása:

   a. Jelölje ki az exportálni kívánt kizárásokat.

   b. Kattintson az → **Export** gombra.

   A Kaspersky Endpoint Security a kizárások listáját egy JSON-fájlba exportálja az alapértelmezett letöltési mappában.
7. A kizárások listájának importálása:

   a. Kattintson az → **Import** gombra.

   A megnyíló ablakban válassza ki azt az JSON-fájlt, amelyből importálni szeretné a kizárások listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a kizárásokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a JSON-fájlból.
8. Mentse el a módosításokat.

A Single Sign-On (SSO) technológia engedélyezése

Az egyszeri bejelentkezést megvalósító Single Sign-On (SSO) technológia lehetővé teszi, hogy automatikusan bejelentkezzen az operációs rendszerbe a Hitelesítési ügynök belépési adataival. Ez azt jelenti, hogy a felhasználónak csak egyszer kell megadnia a jelszót a Windowsba történő bejelentkezéskor (Hitelesítési ügynök fiók jelszava). Az egyszeri bejelentkezési technológia lehetővé teszi a Hitelesítési ügynök fiók jelszavának automatikus frissítését is, amikor a Windows fiók jelszavát megváltoztatják.

A Single Sign-On technológia használata során a Hitelesítési ügynök figyelmen kívül hagyja a Kaspersky Security Centerben meghatározott jelszóerősségi követelményeket. A jelszóerősségi követelményeket az operációs rendszer beállításai között lehet megadni.

A Single Sign-On technológia engedélyezése

A Single Sign-On technológia használatának engedélyezése az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás → Általános titkosítási beállítások** lehetőséget.
4. A **Jelszóbeállítások** területen kattintson a **Beállítások** gombra.
5. A megnyíló ablak **Hitelesítési ügynök** lapján tegyen jelölést az **Egyszeri bejelentkezés (SSO) technológia használata** jelölőnégyzetbe.
6. Ha harmadik fél általi hitelesítóadat-szolgáltatót használ, válassza ki a **Külső hitelesítésszolgáltatók bevonása** jelölődobozt.
7. Mentse el a módosításokat.

Ekkor a felhasználónak mindössze egyszer kell végrehajtania a hitelesítési eljárást az ügynök segítségével. A hitelesítési eljárásra nincs szükség az operációs rendszer betöltéséhez. Az operációs rendszer betöltése automatikusan zajlik.

A Single Sign-On technológia engedélyezésének menete a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption → Full Disk Encryption** elemet.
5. Válassza a **Kaspersky Disk Encryption** technológiát.
6. A **Password settings** részen jelölje be az **Use Single Sign-On (SSO) technology** jelölőnégyzetet.
7. Ha harmadik fél általi hitelesítóadat-szolgáltatót használ, válassza ki a **Wrap third-party credential providers** jelölődobozt.
8. Mentse el a módosításokat.

Ekkor a felhasználónak mindössze egyszer kell végrehajtania a hitelesítési eljárást az ügynök segítségével. A hitelesítési eljárásra nincs szükség az operációs rendszer betöltéséhez. Az operációs rendszer betöltése automatikusan zajlik.

A Single Sign-On technológia csak akkor használható, ha a Windows-fiók jelszava és a Hitelesítési ügynök-fiók jelszava megegyezik. Ha a két jelszó nem ugyanaz, a felhasználónak kétszer kell elvégeznie a hitelesítési eljárást: a Hitelesítési ügynök kezelőfelületén, valamint az operációs rendszer betöltése előtt. A jelszavak szinkronizálása érdekében ezeket a műveleteket egyszer kell elvégezni. Ezt követően a Kaspersky Endpoint Security lecseréli a Windows-fiók jelszavát a Hitelesítési ügynök fiókjának jelszavára. Amikor a Windows fiók jelszava megváltozik, az alkalmazás automatikusan frissíti a Hitelesítési ügynök fiókjának jelszavát.

Harmadik fél hitelesítésszolgáltató

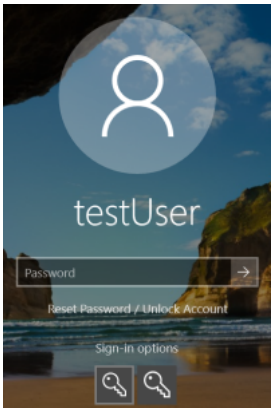
A Kaspersky Endpoint Security támogatja a külső ADSelfService Plus hitelesítési szolgáltatót.

Amikor harmadik féltől származó hitelesítésszolgáltatóval dolgozik, a Hitelesítési ügynök még az operációs rendszer betöltése előtt elfogja a jelszót. Ez azt jelenti, hogy a felhasználónak csak egyszer kell megadnia a jelszót a Windowsba történő bejelentkezéskor. Windowsba történő bejelentkezés után a felhasználó használhatja harmadik fél hitelesítőadat-szolgáltató képességeit például a vállalati szolgáltatásokban történő hitelesítéshez. A harmadik fél hitelesítésszolgáltatók szintén lehetővé teszik a felhasználóknak, hogy önállóan állítsák vissza saját jelszavukat. Ebben az esetben a Kaspersky Endpoint Security automatikusan frissíti a Hitelesítési ügynök jelszavát.

Ha az alkalmazás által nem támogatott harmadik fél általi hitelesítőadat-szolgáltatót használ, az egyszeri bejelentkezési technológia működése közben korlátozásokba ütközhet. A Windows rendszerbe történő belépéskor két profil áll majd a felhasználó rendelkezésére: egy rendszeren belüli és egy harmadik fél általi hitelesítésszolgáltató. Ezeknek a profiloknak a ikonjai azonosak lesznek (lásd az alábbi ábrát). A felhasználó a következő opciók közül választhat a folytatáshoz:

- Ha a felhasználó a *harmadik fél általi hitelesítőadat-szolgáltató* lehetőséget választja, a Hitelesítési ügynök nem tudja szinkronizálni a jelszavakat a Windows fiókkal. Ezért, ha a Felhasználó megváltoztatta a Windows fiók jelszavát, Kaspersky Endpoint Security nem tudja frissíteni a Hitelesítési ügynök fiók jelszavát. Ennek eredményeként, a felhasználónak kétszer kell elvégeznie a hitelesítési eljárást: a Hitelesítési ügynök kezelőfelületén, valamint az operációs rendszer betöltése előtt. Ebben az esetben a felhasználó használhatja a harmadik fél hitelesítőadat-szolgáltatót, például a vállalati szolgáltatásokban történő hitelesítéshez.

- Ha a felhasználó a *rendszerbe épített hitelesítőadat-szolgáltató* lehetőséget választja, a Hitelesítési ügynök szinkronizálja a jelszavakat a Windows fiókkal. Ebben az esetben a felhasználó nem használhatja harmadik fél szolgáltatót, például a vállalati szolgáltatásokban történő hitelesítéshez.



Rendszer hitelesítés profil és harmadik fél hitelesítés profil Windows bejelentkezéshez

A Hitelesítési ügynök fiókok kezelése

Szükség van Hitelesítési ügynökre, ha a Kaspersky lemeztitkosítási (FDE) technológiával védett meghajtókkal kíván dolgozni. Az operációs rendszer betöltése előtt a felhasználónak el kell végeznie a hitelesítést az ügynökkel. A *Hitelesítési ügynök fiókok kezelése* feladat a felhasználóhitelesítési beállítások konfigurálására szolgál. Lehetősége van helyi feladatokat futtatni az egyes számítógépeken, valamint csoportfeladatokat különböző rendszergazdai csoportokból származó számítógépeken vagy kijelölt számítógépek csoportján.

Nem lehet időzítést beállítani a *Hitelesítési ügynök fiókok kezelése* feladathoz. Ugyanígy nincs mód a feladat kényszerített leállítására sem.

„Hitelesítési ügynök fiókok kezelése” feladat létrehozásának menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.
   Megnyílik a feladatok listája.
2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Hitelesítési ügynök fiókok kezelése** elemet.

2. lépés Hitelesítési ügynök-fiók kezelésére vonatkozó parancs kiválasztása

Hozza létre a „Hitelesítési ügynök fiókok kezelése” feladat parancsainak listáját. A kezelési parancsok segítségével felvehet, módosíthat és törölhet Hitelesítési ügynök-fiókokat (lásd az alábbi utasításokat). Csak a Hitelesítési ügynök-fiókkal rendelkező felhasználók tudják végrehajtani a hitelesítési eljárást, betölteni az operációs rendszert és hozzáférést szerezni a titkosított meghajtóhoz.

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés A feladat nevének megadása

Adjon nevet a feladatnak, például: *Rendszergazdai fiókok*.

5. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Ennek következtében, miután a feladat végrehajtása a számítógép következő rendszerindításával befejeződik, az új felhasználó befejezheti a hitelesítési eljárást, betöltheti az operációs rendszert, és hozzáférhet a titkosított meghajtóhoz.

A „Hitelesítési ügynök fiókok kezelése" feladat létrehozásának menete a Web Console-ban

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows (14.1)** lehetőséget.
2. A **Task type** legördülő listából válassza ki az **Manage Authentication Agent accounts** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például: *Adminisztrátori fiókok*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

2. lépés A Hitelesítési ügynök fiókok kezelése

Hozza létre a „Hitelesítési ügynök fiókok kezelése" feladat parancsainak listáját. A kezelési parancsok segítségével felvehet, módosíthat és törölhet Hitelesítési ügynök-fiókokat (lásd az alábbi utasításokat). Csak a Hitelesítési ügynök-fiókkal rendelkező felhasználók tudják végrehajtani a hitelesítési eljárást, betölteni az operációs rendszert és hozzáférést szerezni a titkosított meghajtóhoz.

3. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Egy új feladat jelenik meg a feladatok listájában.

A feladat futtatásához jelölje be a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra.

Ennek következtében, miután a feladat végrehajtása a számítógép következő rendszerindításával befejeződik, az új felhasználó befejezheti a hitelesítési eljárást, betöltheti az operációs rendszert, és hozzáférhet a titkosított meghajtóhoz.

Hitelesítési ügynök-fiók hozzáadásához speciális parancsot kell kiadnia a *Hitelesítési ügynök fiókok kezelése* feladatban. Érdemes csoportfeladatot használni, például ahhoz, hogy rendszergazdai fiókot adjon hozzá minden számítógéphez.

A Kaspersky Endpoint Security lehetővé teszi, hogy Ön automatikusan létrehozzon Hitelesítési ügynök-fiókokat a meghajtó titkosítása előtt. A Hitelesítési ügynök-fiókok automatikus létrehozását a teljes lemeztitkosítás rendszabályának beállításaiban engedélyezheti. Lehetősége van használni az egyszeri bejelentkezés (SSO) technológiát is.

Hitelesítési ügynök-fiók hozzáadásának menete az Adminisztrációs Konzolon (MMC) keresztül

1. Nyissa meg a *Hitelesítési ügynök fiókok kezelése* feladat tulajdonságait.
2. A feladat tulajdonságainál válassza a **Beállítások** részt.
3. Kattintson a **Hozzáadás → Fiók hozzáadása parancs** lehetőségre.
4. A megnyíló ablak **Windows fiók** mezőjében adja meg a Microsoft Windows-fiók nevét, amelyet a Hitelesítési ügynök-fiók létrehozásához fog használni.
5. Ha kézzel írta be a Windows-fiók nevét, kattintson az **Engedélyezés** gombra a fiók biztonsági azonosítójának (SID) megadásáért.

   Ha úgy dönt, hogy nem adja meg a biztonsági azonosítót (SID) az **Engedélyezés** gombra kattintva, akkor megállapítására a feladat számítógépen való elvégzésekor kerül sor.

   > Windows-fiók biztonsági azonosítójának megadása szükséges annak igazolásához, hogy a Windows-fiók neve helyesen van megadva. Ha a Windows-fiók nem létezik a számítógépen, a *Hitelesítési ügynök fiókok kezelése* feladat végrehajtása hibajelzéssel leáll.

6. Jelölje be a **Meglevő fiók felülírása** jelölőnégyzetet, ha azt szeretné, hogy a Hitelesítési ügynök számára korábban létrehozott fiókot a létrehozás alatt álló fiók lecserélje.

   > Ez a lépés akkor használható, ha a Hitelesítési ügynök-fiók létrehozási parancsát Hitelesítési ügynök-fiókok kezelésére szolgáló csoportos feladat tulajdonságaiban adja meg. Ez a lépés nem érhető el, ha a Hitelesítési ügynöki fiók létrehozási parancsát a *Hitelesítési ügynök fiókok kezelése* helyi feladat tulajdonságaiban adja meg.

7. Gépelje be a **Felhasználónév** mezőbe a Hitelesítési ügynök-fiók nevét, melyet a hitelesítés során a titkosított merevlemezekhez való hozzáféréshez meg kell adni.
8. Jelölje be a **Jelszóalapú hitelesítés engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a titkosított merevlemezekhez való hozzáférés céljából történő hitelesítés során a felhasználótól bekérje a Hitelesítési ügynök-fiók jelszavát. Adjon meg jelszót a Hitelesítési ügynök-fiókhoz. Ha szükséges, kérheti a felhasználótól, hogy állítson be új jelszót az első hitelesítés után.
9. Jelölje be a **Tanúsítványalapú hitelesítés engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a titkosított merevlemezekhez való hozzáférés céljából történő hitelesítés során felkérje a felhasználót, hogy csatlakoztasson a számítógéphez tokent vagy okoskártyát. Válasszon tanúsítványfájlt az okoskártya vagy token segítségével végzett hitelesítéshez.
10. Szükség esetén adja meg a **Parancs leírása** mezőben a Hitelesítési ügynök-fiók azon adatait, amelyek a parancs kezeléséhez szükségesek.
11. A **Hozzáférés a hitelesítéshez a Hitelesítési ügynökben** részen konfigurálja a parancsban megadott felhasználó a hitelesítéshez való hozzáférését a Hitelesítési ügynökben.
12. Mentse el a módosításokat.

Hitelesítési ügynök hozzáadásának menete a Web Console-on keresztül

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Manage Authentication Agent accounts** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. A Hitelesítési ügynök-fiókok listájában kattintson a **Add** gombra.

   Ezzel elindítja a Hitelesítési ügynök-fiókok kezelésének varázslóját.

5. Válassza a **Add** parancstípust.

6. Válasszon ki egy felhasználói fiókot. Fiókot választhat a tartományfiókok listájáról, de kézzel is megadhatja a fiók nevét. Lépjen a következő lépésre.

   A Kaspersky Endpoint Security meghatározza a fiók biztonsági azonosítóját (SID) is. Ez a fiók ellenőrzéséhez szükséges. Ha a felhasználónevet helytelenül adta meg, a Kaspersky Endpoint Security leállítja a feladat végrehajtását, és hibaállapotot jelez.

7. Konfigurálja a Hitelesítési ügynök-fiók beállításait.

   - **Create a new Authentication Agent account to replace the existing account**. A Kaspersky Endpoint Security megvizsgálja a létező fiókokat a számítógépen. Ha a felhasználó biztonsági azonosítója a számítógépen és a feladatban azonos, a Kaspersky Endpoint Security a feladatnak megfelelően módosítja a felhasználói fiókbeállításokat.

   - **User name**. A Hitelesítési ügynök-fiók alapértelmezett felhasználóneve megegyezik a felhasználó tartománynevével.

   - **Allow password-based authentication**. Adjon meg jelszót a Hitelesítési ügynök-fiókhoz. Ha szükséges, kérheti a felhasználótól, hogy állítson be új jelszót az első hitelesítés után. Így minden egyes felhasználó saját, egyedi jelszót kap. A rendszabályban beállíthat jelszóerősségi követelményeket is a Hitelesítési ügynök-fiókra vonatkozóan.

   - **Allow certificate-based authentication**. Válasszon tanúsítványfájlt az okoskártya vagy token segítségével végzett hitelesítéshez. Így a felhasználónak meg kell adnia az okoskártyához vagy tokenhez tartozó jelszót.

   - **Account access to encrypted data**. Konfigurálja a felhasználói hozzáférést a titkosított meghajtóhoz. Lehetősége van például ideiglenesen letiltani a felhasználói hitelesítést a Hitelesítési ügynök-fiók törlése helyett.

   - **Comment**. Ha szükséges, adjon meg fiókleírást.

8. Mentse el a módosításokat.

9. Tegyen jelölést a feladat melletti jelölőnégyzetbe, majd kattintson az **Start** gombra.

Ennek következtében, miután a feladat végrehajtása a számítógép következő rendszerindításával befejeződik, az új felhasználó befejezheti a hitelesítési eljárást, betöltheti az operációs rendszert, és hozzáférhet a titkosított meghajtóhoz.

A Hitelesítési ügynök-fiók jelszavának és más beállításainak módosításához hozzá kell adnia egy speciális parancsot a *Hitelesítési ügynök fiókok kezelése* feladathoz. Érdemes csoportfeladatot használni, például ahhoz, hogy lecserélje a rendszergazdai token tanúsítványát az összes számítógépen.

Hitelesítési ügynök-fiók módosításának menete az Adminisztrációs Konzolon (MMC) keresztül

1. Nyissa meg a *Hitelesítési ügynök fiókok kezelése* feladat tulajdonságait.
2. A feladat tulajdonságainál válassza a **Beállítások** részt.
3. Kattintson a **Hozzáadás → Fiók szerkesztése parancs** lehetőségre.
4. A megnyíló ablak **Windows fiók** mezőjében adja meg annak a Microsoft Windows felhasználói fióknak a nevét, amelyet szeretne megváltoztatni.
5. Ha kézzel írta be a Windows-fiók nevét, kattintson az **Engedélyezés** gombra a fiók biztonsági azonosítójának (SID) megadásáért.

   Ha úgy dönt, hogy nem adja meg a biztonsági azonosítót (SID) az **Engedélyezés** gombra kattintva, akkor megállapítására a feladat számítógépen való elvégzésekor kerül sor.

   > Windows-fiók biztonsági azonosítójának megadása szükséges annak igazolásához, hogy a Windows-fiók neve helyesen van megadva. Ha a Windows-fiók nem létezik a számítógépen, a *Hitelesítési ügynök fiókok kezelése* feladat végrehajtása hibajelzéssel leáll.

6. Jelölje be a **Felhasználónév módosítása** jelölőnégyzetet, és adja meg a Hitelesítési ügynök-fiók új nevét, ha azt szeretné, hogy a Kaspersky Endpoint Security a lenti mezőbe begépelt névre módosítsa a felhasználónevet minden olyan Hitelesítési ügynök-fióknál, amely a **Windows fiók** mezőben feltüntetett nevű Microsoft Windows fiók segítségével jött létre.
7. Jelölje be a **Jelszóalapú hitelesítés beállításainak módosítása** jelölőnégyzetet, ha a jelszóalapú hitelesítési beállításokat szerkeszthetővé szeretné tenni.
8. Jelölje be a **Jelszóalapú hitelesítés engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a titkosított merevlemezekhez való hozzáférés céljából történő hitelesítés során a felhasználótól bekérje a Hitelesítési ügynök-fiók jelszavát. Adjon meg jelszót a Hitelesítési ügynök-fiókhoz.
9. Jelölje be a **Jelszómódosítási szabály szerkesztése a Hitelesítési ügynökben való hitelesítéskor** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security a lent megadott értékre módosítsa a jelszómódosítási beállítás értékét minden olyan Hitelesítési ügynök-fióknál, amely a **Windows fiók** mezőben feltüntetett nevű Microsoft Windows fiók segítségével jött létre.
10. Adja meg a jelszómódosítási beállítás Hitelesítési ügynökben történő hitelesítés esetén felvett értékét.
11. Jelölje be a **Tanúsítványalapú hitelesítés beállításainak módosítása** jelölőnégyzetet, ha a token vagy okoskártya elektronikus tanúsítványa alapján történő hitelesítési beállításokat szerkeszthetővé szeretné tenni.
12. Jelölje be a **Tanúsítványalapú hitelesítés engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a titkosított merevlemezekhez való hozzáférés céljából történő hitelesítés során felkérje a felhasználót, hogy adja meg a számítógéphez csatlakoztatott token vagy okoskártya jelszavát. Válasszon tanúsítványfájlt az okoskártya vagy token segítségével végzett hitelesítéshez.
13. Jelölje be a **Parancsleírás szerkesztése** jelölőnégyzetet, és szerkessze a parancs leírását, ha azt szeretné, hogy a Kaspersky Endpoint Security módosítsa a parancs leírását minden olyan Hitelesítési ügynök-fióknál, amely a **Windows fiók** mezőben feltüntetett nevű Microsoft Windows fiók segítségével jött létre.

14. Jelölje be a **Hozzáférési szabály szerkesztése a Hitelesítési ügynökben végzett hitelesítéshez** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security a lent megadott értékre módosítsa a Hitelesítési ügynökben lévő hitelesítési párbeszédpanelhez való felhasználói hozzáférés szabályát minden olyan Hitelesítési ügynök-fióknál, amely a **Windows fiók** mezőben feltüntetett nevű Microsoft Windows fiók segítségével jött létre.

15. Adja meg a Hitelesítési ügynökben lévő hitelesítési párbeszédpanelhez való hozzáférési szabályt.

16. Mentse el a módosításokat.

A Hitelesítési ügynök-fiók megváltoztatásának menete a Web Console-on keresztül

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Manage Authentication Agent accounts** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. A Hitelesítési ügynök-fiókok listájában kattintson a **Add** gombra.

   Ezzel elindítja a Hitelesítési ügynök-fiókok kezelésének varázslóját.

5. Válassza a **Change** parancstípust.

6. Válasszon ki egy felhasználói fiókot. Fiókot választhat a tartományfiókok listájáról, de kézzel is megadhatja a fiók nevét. Lépjen a következő lépésre.

   A Kaspersky Endpoint Security meghatározza a fiók biztonsági azonosítóját (SID) is. Ez a fiók ellenőrzéséhez szükséges. Ha a felhasználónevet helytelenül adta meg, a Kaspersky Endpoint Security leállítja a feladat végrehajtását, és hibaállapotot jelez.

7. Tegyen jelölést a szerkeszteni kívánt beállítások melletti jelölőnégyzetbe.

8. Konfigurálja a Hitelesítési ügynök-fiók beállításait.

   - **Create a new Authentication Agent account to replace the existing account**. A Kaspersky Endpoint Security megvizsgálja a létező fiókokat a számítógépen. Ha a felhasználó biztonsági azonosítója a számítógépen és a feladatban azonos, a Kaspersky Endpoint Security a feladatnak megfelelően módosítja a felhasználói fiókbeállításokat.

   - **User name**. A Hitelesítési ügynök-fiók alapértelmezett felhasználóneve megegyezik a felhasználó tartománynevével.

   - **Allow password-based authentication**. Adjon meg jelszót a Hitelesítési ügynök-fiókhoz. Ha szükséges, kérheti a felhasználótól, hogy állítson be új jelszót az első hitelesítés után. Így minden egyes felhasználó saját, egyedi jelszót kap. A rendszabályban beállíthat jelszóerősségi követelményeket is a Hitelesítési ügynök-fiókra vonatkozóan.

   - **Allow certificate-based authentication**. Válasszon tanúsítványfájlt az okoskártya vagy token segítségével végzett hitelesítéshez. Így a felhasználónak meg kell adnia az okoskártyához vagy tokenhez tartozó jelszót.

- **Account access to encrypted data**. Konfigurálja a felhasználói hozzáférést a titkosított meghajtóhoz. Lehetősége van például ideiglenesen letiltani a felhasználói hitelesítést a Hitelesítési ügynök-fiók törlése helyett.

- **Comment**. Ha szükséges, adjon meg fiókleírást.

9. Mentse el a módosításokat.

10. Tegyen jelölést a feladat melletti jelölőnégyzetbe, majd kattintson az **Start** gombra.

Hitelesítési ügynök-fiók törléséhez speciális parancsot kell kiadnia a *Hitelesítési ügynök fiókok kezelése* feladatban. Érdemes csoportfeladatot használni, például ahhoz, hogy törölje egy elbocsátott alkalmazott fiókját.

Hitelesítési ügynök-fiók törlésének menete az Adminisztrációs Konzolon (MMC) keresztül

1. Nyissa meg a *Hitelesítési ügynök fiókok kezelése* feladat tulajdonságait.

2. A feladat tulajdonságainál válassza a **Beállítások** részt.

3. Kattintson a **Hozzáadás → Fiók törlése parancs** lehetőségre.

4. A megnyíló ablak **Windows fiók** mezőjében adja meg annak a Windows fióknak nevét, amelyet a törölni kívánt Hitelesítési ügynök-fiók létrehozásához használtak.

5. Ha kézzel írta be a Windows-fiók nevét, kattintson az **Engedélyezés** gombra a fiók biztonsági azonosítójának (SID) megadásáért.

   Ha úgy dönt, hogy nem adja meg a biztonsági azonosítót (SID) az **Engedélyezés** gombra kattintva, akkor megállapítására a feladat számítógépen való elvégzésekor kerül sor.

   > Windows-fiók biztonsági azonosítójának megadása szükséges annak igazolásához, hogy a Windows-fiók neve helyesen van megadva. Ha a Windows-fiók nem létezik a számítógépen, a *Hitelesítési ügynök fiókok kezelése* feladat végrehajtása hibajelzéssel leáll.

6. Mentse el a módosításokat.

Hitelesítési ügynök-fiók törlésének menete a Web Console-on keresztül

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **Manage Authentication Agent accounts** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. A Hitelesítési ügynök-fiókok listájában kattintson a **Add** gombra.

   Ezzel elindítja a Hitelesítési ügynök-fiókok kezelésének varázslóját.

5. Válassza a **Delete** parancstípust.

6. Válasszon ki egy felhasználói fiókot. Fiókot választhat a tartományfiókok listájáról, de kézzel is megadhatja a fiók nevét.

7. Mentse el a módosításokat.

8. Tegyen jelölést a feladat melletti jelölőnégyzetbe, majd kattintson az **Start** gombra.

Ennek következtében, miután a feladat végrehajtása befejeződik a számítógép következő rendszerindítása után, a felhasználó nem tudja elvégezni a hitelesítési eljárást, és betölteni az operációs rendszert. A Kaspersky Endpoint Security megtagadja a hozzáférést a titkosított adatokhoz.

A hitelesítést, valamint az operáció rendszer betöltését végrehajtani képes felhasználók listájának megtekintéséhez meg kell nyitni a kezelt számítógép tulajdonságait.

Hitelesítési ügynök-fiókok listájának megtekintése az Adminisztrációs Konzolon (MMC) keresztül

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Devices** lehetőséget.

3. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.

4. Válassza ki a számítógép tulajdonságainak ablakában a **Tasks** részt.

5. A feladatlistában válassza ki a **Manage Authentication Agent accounts** lehetőséget, és dupla kattintással nyissa meg a feladat tulajdonságait.

6. A feladat tulajdonságainál válassza a **Beállítások** részt.

Ennek eredményeképpen hozzáférhet az adott számítógépen jelen lévő Hitelesítési ügynök-fiókok listájához. Kizárólag a listán szereplő felhasználók tudják sikeresen végrehajtani a hitelesítést az ügynök segítségével, és betölteni az operációs rendszert.

Hitelesítési ügynök-fiókok listájának megtekintése a Web Console-on keresztül

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.

2. Kattintson annak a számítógépnek a nevére, amelyen szeretné megtekinteni a Hitelesítési ügynök-fiókok listáját.

3. A számítógép-tulajdonságokban válassza ki a **Tasks** lapot.

4. A feladatlistában válassza a **Manage Authentication Agent accounts** opciót.

5. A feladat tulajdonságainál válassza az **Application settings** lapot.

Ennek eredményeképpen hozzáférhet az adott számítógépen jelen lévő Hitelesítési ügynök-fiókok listájához. Kizárólag a listán szereplő felhasználók tudják sikeresen végrehajtani a hitelesítést az ügynök segítségével, és betölteni az operációs rendszert.

Token és okoskártya használata a Hitelesítési ügynökkel

A titkosított merevlemezekhez való hozzáféréshez token vagy okoskártya is használható. Ennek érdekében hozzá kell adnia egy token vagy okoskártya elektronikus tanúsítványának fájlját a *Hitelesítési ügynök fiókok kezelése* feladathoz.

Akkor lehet tokent vagy okoskártyát használni, ha a számítógép merevlemezeit az AES256 titkosítási algoritmus titkosította. Ha a számítógép merevlemezei az AES56 algoritmussal vannak titkosítva, a rendszer elutasítja az elektronikus tanúsítványfájl parancshoz való hozzáadását.

A Kaspersky Endpoint Security a következő tokeneket, okoskártya-olvasókat és okoskártyákat támogatja:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Ahhoz, hogy a token vagy okoskártya elektronikus tanúsítványának fájlját megadhassa a Hitelesítési ügynök-fiók létrehozására szolgáló parancsban, először harmadik féltől származó tanúsítványkezelő szoftverrel mentenie kell a fájlt.

A token vagy okoskártya tanúsítványainak a következő jellemzőkkel kell rendelkeznie:

- A tanúsítványnak meg kell felelnie az X.509 szabványnak, és a tanúsítványfájlban DER kódolást kell alkalmazni.
- A tanúsítvány legalább 1024 bit hosszúságú RSA kulcsot tartalmaz.

Ha a token vagy okoskártya elektronikus tanúsítványa nem felel meg ezen követelményeknek, nem lehet betölteni a tanúsítványfájlt a Hitelesítési ügynök-fiók létrehozására szolgáló parancs esetén.

A tanúsítvány `KeyUsage` paraméterének vagy `keyEncipherment` vagy `dataEncipherment` értékűnek kell lennie. A `KeyUsage` paraméter szabja meg a tanúsítvány célját. Ha a paraméternek más értéke van, a Kaspersky Security Center letölti a tanúsítványfájlt, de figyelmeztetést jelenít meg.

Ha egy felhasználó elvesztett egy tokent vagy okoskártyát, a rendszergazdának kötelező hozzáadnia a token vagy okoskártya elektronikus tanúsítványának fájlját a Hitelesítési ügynök-fiók létrehozására szolgáló parancshoz. Ezután a felhasználónak el kell végeznie a titkosított eszközökhöz való hozzáférés vagy a titkosított eszközökön lévő adatok visszaállítása folyamatot.

Merevlemez visszafejtése

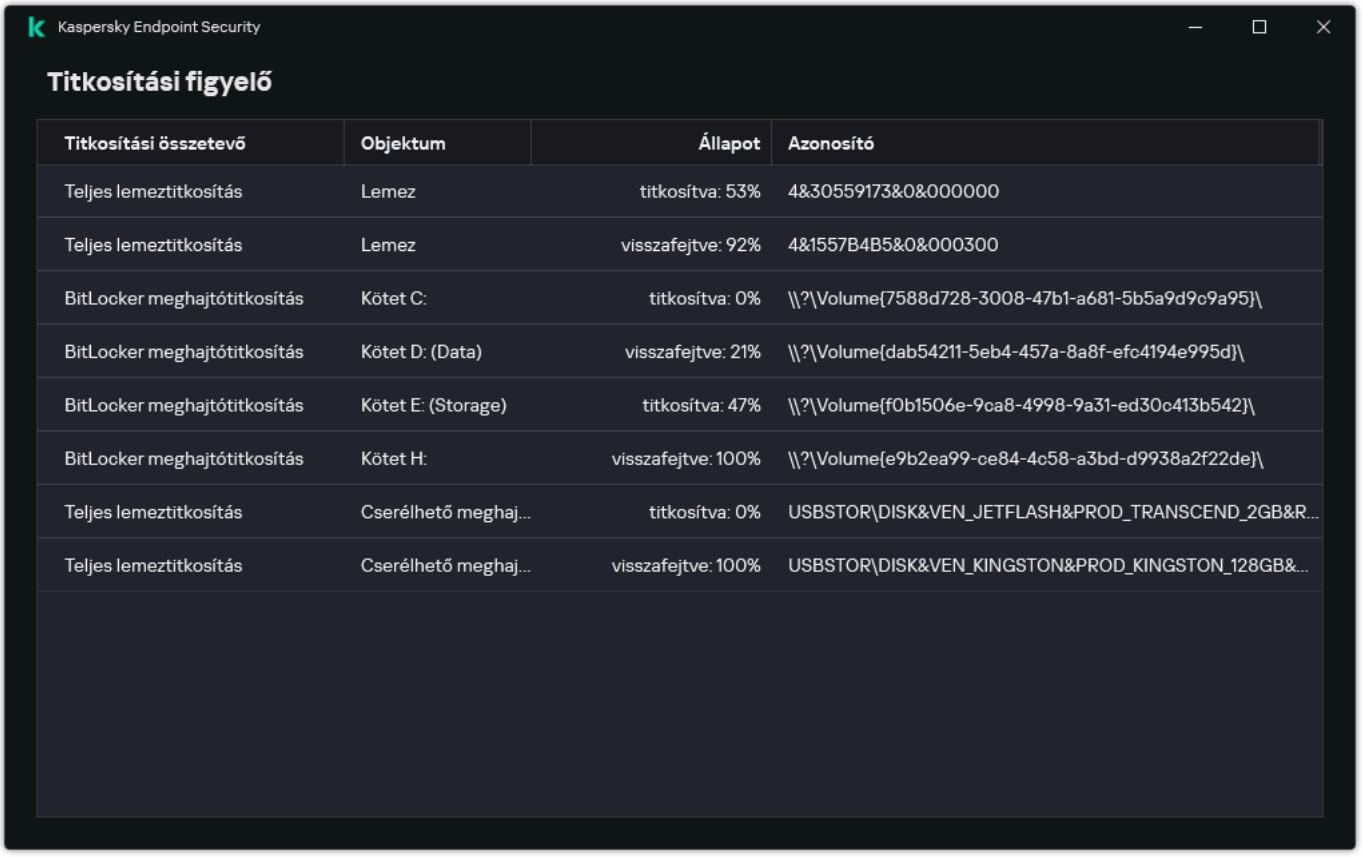
A merevlemezeket akkor is vissza lehet fejteni, ha nincs adattitkosítást lehetővé tevő aktuális licenc.

A merevlemezek visszafejtése:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
4. Válassza ki a **Titkosítási technológia** legördülő listán a merevlemezek titkosításához használt technológiát.
5. Végezze el az alábbiak egyikét:
   - Válassza ki a **Titkosítási mód** legördülő listán az **Összes merevlemez visszafejtése** lehetőséget, ha az összes titkosított merevlemezt vissza szeretné fejteni.
   - Adja hozzá a visszafejteni kívánt titkosított merevlemezeket **Ne titkosítsa a következő merevlemezeket** táblázathoz.

     Ez a lehetőség csak a Kaspersky lemeztitkosítási technológia esetén használható.
6. Mentse el a módosításokat.

A Titkosítási figyelő eszközzel vezérelheti a lemez titkosítási vagy visszafejtési folyamatát a felhasználó számítógépén. A Titkosítási figyelő eszközt a fő alkalmazásablakból futtathatja.



Titkosítási figyelő

Ha a Kaspersky lemeztitkosítási technológia segítségével titkosított merevlemez visszafejtése közben a felhasználó leállítja vagy újraindítja a számítógépet, a Hitelesítési ügynök betöltődik az operációs rendszer legközelebbi indulása előtt. A Kaspersky Endpoint Security a Hitelesítési ügynökben történő sikeres hitelesítést és az operációs rendszer elindulását követően folytatja a merevlemez visszafejtését.

Ha az operációs rendszer a Kaspersky lemeztitkosítási technológia segítségével titkosított merevlemezek visszafejtése közben hibernált módba vált, a Hitelesítési ügynök betöltődik, amikor az operációs rendszer kilép a hibernált módból. A Kaspersky Endpoint Security a Hitelesítési ügynökben történő sikeres hitelesítést és az operációs rendszer elindulását követően folytatja a merevlemez visszafejtését. A merevlemez visszafejtését követően a hibernált mód az operációs rendszer első újraindításáig nem áll rendelkezésre.

Ha az operációs rendszer a merevlemez visszafejtése közben alvó módba lép, a Kaspersky Endpoint Security a Hitelesítési ügynök betöltése nélkül folytatja a merevlemez visszafejtését, amikor az operációs rendszer kilép alvó módból.

A hozzáférés visszaállítása Kaspersky lemeztitkosítási technológiával védett meghajtóhoz

Ha egy felhasználó elfelejtette a hozzáférési jelszót egy Kaspersky lemeztitkosítási technológiával védett merevlemezhez, el kell indítania a visszaállítási eljárást (kérés–válasz). Használhatja a szolgáltatásfiókot a merevlemezhez való hozzáféréshez, ha ez a funkció engedélyezve van a lemeztitkosítási beállításokban.

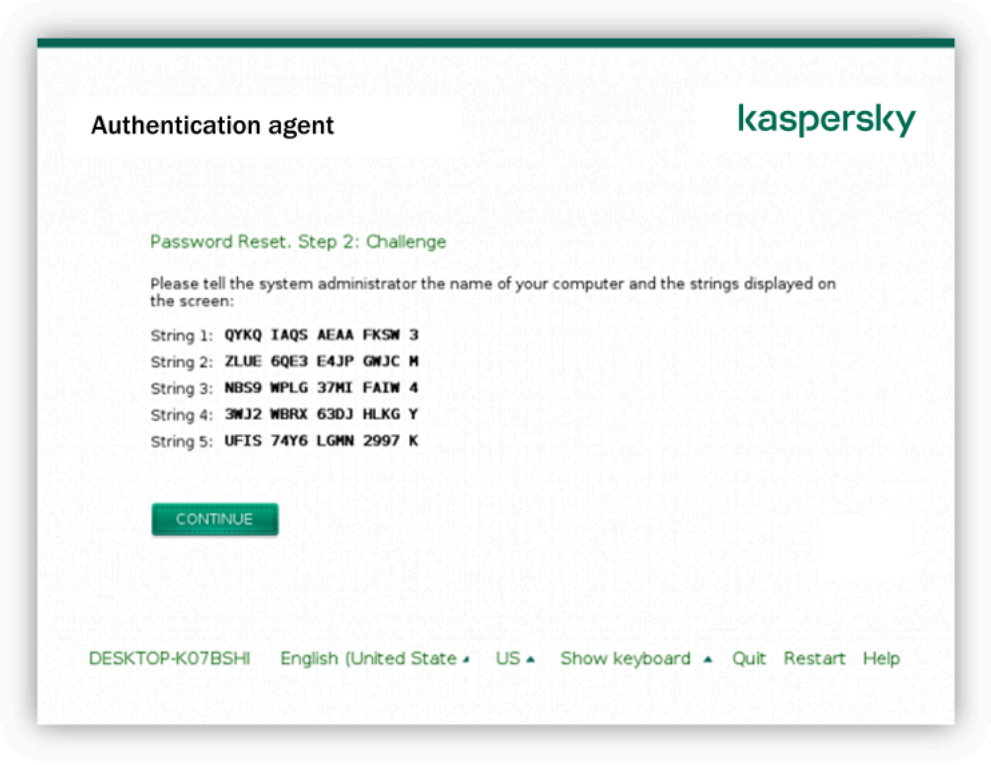
A rendszermerevlemez hozzáférésének visszaállítása

A Kaspersky lemeztitkosítási technológiával védett rendszermerevlemez elérésének visszaállítása a következő lépésekből áll:

1. A felhasználó jelenti a kérési blokkokat a rendszergazdának (részletek az alábbi ábrán).

2. A rendszergazda megadja a kérési blokkot a Kaspersky Security Centerben, megkapja a válaszblokkokat, majd jelenti a válaszblokkokat a felhasználónak.

3. A felhasználó megadja a válaszblokkokat a Hitelesítési ügynök kezelőfelületén, és hozzáférést kap a merevlemezhez.



A hozzáférés visszaállítása Kaspersky lemeztitkosítási technológiával védett rendszermerevlemezhez

A helyreállítási eljárás elindításához a felhasználónak a **Forgot your password** gombra kell kattintania a Hitelesítési ügynök kezelőfelületén.

Válaszblokkok beszerzése Kaspersky lemeztitkosítási technológiával védett rendszermerevlemezhez az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. A konzolfán válassza ki a **Devices** lehetőséget.

3. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.

4. A helyi menüben válassza ki a **Hozzáférés engedélyezése offline módban** elemet.

5. A megnyíló ablakban válassza a **Hitelesítési ügynök** lapot.

6. A **Használatban lévő titkosító algoritmus** területen válasszon titkosítási algoritmust: **AES56** vagy **AES256**.

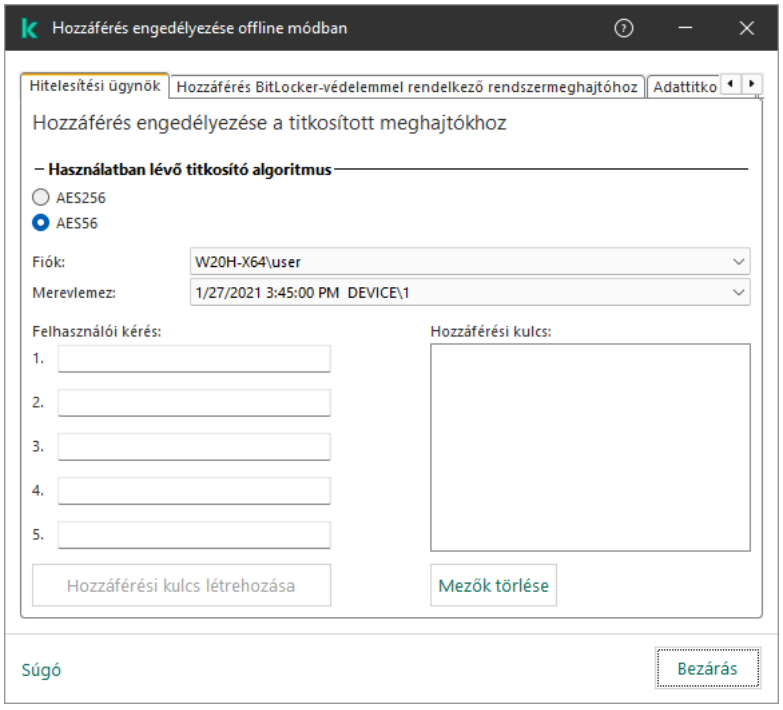
   Az adattitkosítási algoritmus az AES-titkosítási könyvtártól függ, amely a terjesztőcsomagba tartozik: *Strong encryption (AES256)* vagy *Lite encryption (AES56)*. Az AES-titkosítási könyvtár az alkalmazással együtt van telepítve.

7. A **Fiók** legördülő listán válassza ki annak a Hitelesítési ügynök-fióknak a nevét, amely a meghajtóhoz való hozzáférése visszaállítását kérő felhasználóhoz tartozik.

8. Válassza ki a **Merevlemez** legördülő listán azt a titkosított merevlemezt, amelyhez vissza szeretné állítani a hozzáférést.

9. Adja meg a **Felhasználói kérés** részben a felhasználó által bediktált kérésblokkokat.

Ekkor a rendszer a **Hozzáférési kulcs** mezőben megjeleníti azoknak a válaszblokkoknak a tartalmát, amelyek a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítására vonatkozó felhasználói kérésre válaszul érkeztek. Továbbítsa a válaszblokkok tartalmát a felhasználónak.



Hozzáférés engedélyezése offline módban

Válaszblokkok beszerzése Kaspersky lemeztitkosítási technológiával védett rendszermerevlemezhez a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.

2. Jelölje be annak a számítógépnek a neve melletti jelölőnégyzetet, amely számítógépben az ismét elérni kívánt meghajtó található.

3. Kattintson az **Grant access to the device in offline mode** gombra.

4. A megnyíló ablakban válassza a **Authentication Agent** szakaszt.

5. Válassza ki a **Account** legördülő listán azon felhasználó számára létrehozott Hitelesítési ügynök-fiók nevét, aki a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítását kéri.

6. Adja meg a felhasználó által továbbított kérésblokkokat.

A Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó helyreállítására vonatkozó, felhasználó által küldött kérésre válaszul küldött válaszblokkok tartalma az ablak alján jelenik meg. Továbbítsa a válaszblokkok tartalmát a felhasználónak.

A helyreállítási eljárás befejezését követően a Hitelesítési ügynök kéri a felhasználótól a jelszó megváltoztatását.

Hozzáférés visszaállítása rendszert nem futtató merevlemezhez

A Kaspersky lemeztitkosítási technológiával védett, rendszert nem futtató merevlemez hozzáférésének visszaállítása a következő lépésekből áll:

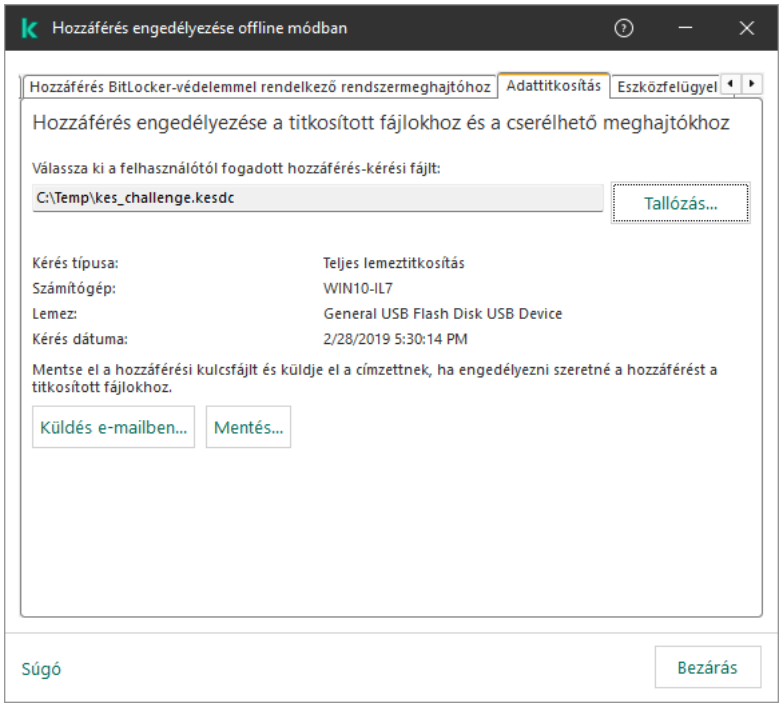
1. A felhasználó egy hozzáférés-kérési fájlt küld a rendszergazdának.
2. A rendszergazda hozzáadja a hozzáférés-kérési fájlt a Kaspersky Security Centerhez, létrehoz egy hozzáférésikulcs-fájlt, majd elküldi a fájlt a felhasználónak.
3. A felhasználó hozzáadja a hozzáférésikulcs-fájlt a Kaspersky Endpoint Security alkalmazáshoz, és hozzáférést kap a merevlemezhez.

A helyreállítási eljárás elindításához a felhasználónak meg kell kísérelnie egy merevlemez elérését. Ekkor a Kaspersky Endpoint Security létrehoz egy hozzáférés-kérési fájlt (KESDC kiterjesztéssel), amelyet a felhasználónak el kell küldenie a rendszergazdának, például e-mailben.

Hozzáférésikulcs-fájl beszerezése titkosított, rendszert nem futtató merevlemezhez az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Devices** lehetőséget.
3. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
4. A helyi menüben válassza ki a **Hozzáférés engedélyezése offline módban** elemet.
5. A megnyíló ablakban válassza az **Adattitkosítás** lapot.
6. Az **Adattitkosítás** lapon kattintson a **Browse** gombra.
7. A hozzáférés-kérési fájl kiválasztására szolgáló ablakban adja meg a felhasználótól kapott fájl elérési útját.

A felhasználó kérésére vonatkozó információ válik láthatóvá. A Kaspersky Security Center létrehoz egy kulcsfájlt. Küldje el e-mailben a létrehozott titkosítottadat-hozzáférési kulcsfájlt a felhasználónak. Másik megoldásként mentse a hozzáférési fájlt, és használjon tetszés szerinti módszert a fájl továbbításához.



Hozzáférés engedélyezése offline módban

Titkosított, rendszert nem futtató merevlemez hozzáférési kulcsfájljának beszerzése a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Tegyen jelölést annak a számítógépnek a neve mellé, amelynek adataihoz szeretné visszaállítani a hozzáférést.
3. Kattintson az **Grant access to the device in offline mode** gombra.
4. Válassza a **Data Encryption** lehetőséget.
5. Kattintson a **Select file** gombra, és válassza ki azt a hozzáférés-kérési (KESDC kiterjesztésű) fájlt, amelyet a felhasználótól kapott.

   A Web Console a kérésre vonatkozó információkat jelenít meg. Ezek között szerepel annak a számítógépnek a neve, amelyen a felhasználó hozzáférést kér a fájlhoz.
6. Kattintson a **Save key** gombra, és válassza ki azt a mappát, amelybe a titkosítottadat-hozzáférési (KESDR kiterjesztésű) kulcsfájlt menteni szeretné.

Ekkor beszerezheti titkosítottadat-hozzáférési kulcsot, amelyet továbbítania kell a felhasználónak.

Bejelentkezés a hitelesítési ügynöki szolgáltatásfiókkal

A Kaspersky Endpoint Security lehetővé teszi hitelesítési ügynöki szolgáltatásfiók hozzáadását a meghajtó titkosításakor. A szolgáltatásfiók szükséges a számítógéphez való hozzáféréshez, például ha a felhasználó elfelejti a jelszavát. A szolgáltatásfiókot tartalék fiókként is használhatja. Fiók hozzáadásához válasszon ki egy szolgáltatásfiókot a lemeztitkosítási beállításokban, és adja meg a felhasználói fiók nevét (alapértelmezés szerint `ServiceAccount`). Az ügynök használatával történő hitelesítéshez egyszeri jelszóra lesz szüksége.

Egyszeri jelszó megkeresése az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Devices** lehetőséget.
3. Kattintson duplán a számítógép-tulajdonságok ablak megnyitásához.
4. Válassza ki a számítógép tulajdonságainak ablakában a **Tasks** részt.
5. A feladatlistában válassza ki a **Manage Authentication Agent accounts** lehetőséget, és dupla kattintással nyissa meg a feladat tulajdonságait.
6. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.
7. A fiókok listájában válassza ki a hitelesítési ügynöki szolgáltatásfiókot (például `WIN10-USER\ServiceAccount`).
8. A **Művelet** legördülő listában válassza a **Fiók megtekintése** lehetőséget.
9. A fiók tulajdonságaiban jelölje be az **Eredeti jelszó megjelenítése** jelölőnégyzetet.
10. Másolja ki az egyszeri jelszót a szolgáltatásfiókkal való bejelentkezéshez.

Egyszeri jelszó megkeresése a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Assets (Devices)** lehetőséget.
2. Kattintson annak a számítógépnek a nevére, amelyen szeretné megtekinteni a Hitelesítési ügynök-fiókok listáját.
   Ez megnyitja a számítógép tulajdonságait.
3. A számítógép-tulajdonságokban válassza ki a **Tasks** lapot.
4. A feladatlistában válassza a **Manage Authentication Agent accounts** opciót.
5. A feladat tulajdonságainál válassza az **Application settings** lapot.
6. A fiókok listájában válassza ki a hitelesítési ügynöki szolgáltatásfiókot (például `WIN10-USER\ServiceAccount`).
7. A fiók tulajdonságainál jelölje be a **Show password** jelölőnégyzetet.
8. Másolja ki az egyszeri jelszót a szolgáltatásfiókkal való bejelentkezéshez.

A Kaspersky Endpoint Security automatikusan frissíti a jelszót minden alkalommal, amikor a felhasználó hitelesítést végez a szolgáltatásfiókkal. Az ügynök használatával történő hitelesítés után meg kell adnia a Windows-fiók jelszavát. Amikor bejelentkezik a szolgáltatásfiókkal, nem használhatja az SSO technológiát.

Az operációs rendszer frissítése

A Teljes lemeztitkosítással (FDE) védett számítógép operációs rendszerének frissítésekor számos dolgot figyelembe kell venni. Az operációs rendszer frissítése a következőképp zajlik: először frissítse az operációs rendszert az egyik számítógépen, majd a számítógépek egy részén, végül pedig a hálózat összes számítógépén.

Ha Kaspersky lemeztitkosítási technológiát használ, a Hitelesítési ügynök betöltődik az operációs rendszer indítása előtt. A Hitelesítési ügynök használatával a felhasználó bejelentkezhet a rendszerbe, és hozzáférhet a titkosított meghajtókhoz. Ezután az operációs rendszer megkezdi a betöltést. Ha egy Kaspersky lemeztitkosítási technológiával védett számítógép operációs rendszerét frissíti, az operációs rendszer frissítésvarázslója eltávolítja a Hitelesítési ügynököt. Ennek eredményeképp a számítógép zárolható, mivel az operációs rendszer betöltője nem tudja elérni a titkosított meghajtót.

Az operációs rendszer frissítésének jellemzői:

- **Az operációs rendszer frissítése a WSUS-on keresztül**. Az operációs rendszert a szokásos módon frissítheti.
- **Az operációs rendszer frissítése ISO-fájlból**. Az operációs rendszer frissítéséhez meg kell adnia a mappát a Kaspersky lemeztitkosító illesztőprogramokkal. Az alkalmazás automatikusan egy külön mappába másolja az illesztőprogramokat. Végezze el az alábbiakat:

  1. Csatlakoztassa az ISO-képet.
  2. Indítsa el a rendszerfrissítés telepítését a következő kulccsal:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.1\reflect_drivers
     ```

Az automatikus operációsrendszer-frissítés csak akkor érhető el, ha a számítógépen Windows 10 1607 (RS1) vagy újabb rendszer fut. Az operációs rendszer korábbi verzióinak frissítéséhez ajánlott először a lemez titkosításának feloldása, az operációs rendszer frissítésének végrehajtása, majd a lemez titkosítása.

Ha BitLocker meghajtótitkosítás technológiát használ, akkor a Windows 10 frissítéséhez nem kell visszafejtenie a merevlemezeket. A BitLocker működésének részleteiért lásd a Microsoft webhelyét.

A titkosítás funkció hibáinak elhárításával kapcsolatos frissítés

A Teljes lemeztitkosítás funkció frissítésére az alkalmazásnak a Kaspersky Endpoint Security for Windows 14.1 verzióra történő frissítésekor kerül sor.

A Teljes lemeztitkosítás funkció frissítésének elindításakor a következő hibák léphetnek fel:

- Nem lehet inicializálni a frissítést.
- Az eszköz a Hitelesítési ügynökkel nem kompatibilis.

Az új alkalmazásverzió Teljes lemeztitkosítás frissítési folyamatának elindításakor fellépő hibák elhárításához:

1. A merevlemezek visszafejtése.
2. A merevlemezek titkosítása ismét.

A Teljes lemeztitkosítás funkció frissítése alatt a következő hibák léphetnek fel:

- Nem lehet befejezni a frissítést.
- A Teljes lemeztitkosítás frissítési visszaállítása hibával végződött.

A Teljes lemeztitkosítás frissítési folyamata alatt fellépő hibák elhárításához

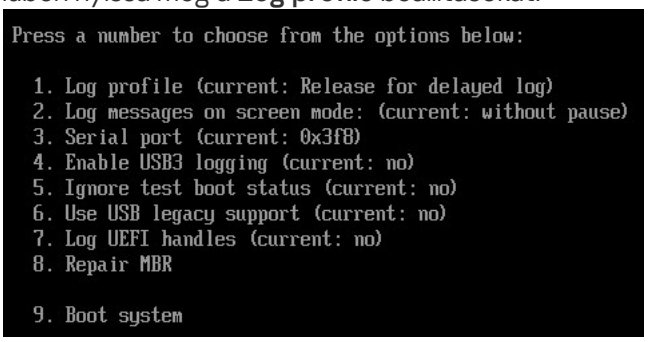
Állítsa vissza a titkosított eszközök hozzáférését a helyreállító segédprogrammal.

A Hitelesítési ügynök felkutatása

Az alkalmazás a nyomkövetési fájlban naplózza a Hitelesítési ügynök működéséről szóló szolgáltatásadatokat, valamint a felhasználó Hitelesítési ügynökkel végzett műveleteiről szóló információkat.

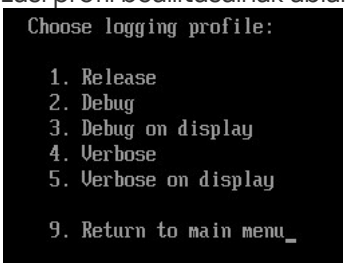
A Hitelesítési ügynök nyomkövetésének engedélyezése:

1. A Kaspersky Endpoint Security nyomkövetésének engedélyezése.
2. Indítsa újra a számítógépet.
3. Amint elindul a titkosított merevlemezeket tartalmazó számítógép, nyomja meg az **F3** billentyűt a Hitelesítési ügynök beállításainak megadására szolgáló ablak előhívásához.
4. Az FDE rendszertöltő elindulása után válassza ki a **KES (FDE <version>)** rendszertöltés-vezérlőt.
5. A rendszertöltés-vezérlő menüben nyissa meg a **Log profile** beállításokat.



Rendszertöltés-vezérlő menü

6. Válassza ki a nyomkövetési szintet a naplózási profil beállításainak ablakában:



A hitelesítési ügynök nyomkövetési szintjei

- **Release**. Ha ezt a lehetőséget választja, az alkalmazás nem naplózza a nyomkövetési fájlban a Hitelesítési ügynökre vonatkozó információkat.
- **Debug**. Ha ezt a lehetőséget választja, az alkalmazás a nyomkövetési fájlban naplózza a Hitelesítési ügynök működéséről szóló információkat, valamint a felhasználó Hitelesítési ügynökkel végzett műveleteiről szóló információkat.

- **Debug on display**. Ha ezt a lehetőséget választja, az alkalmazás a nyomkövetési fájlban naplózza a Hitelesítési ügynök működéséről szóló információkat, valamint a felhasználó Hitelesítési ügynökkel végzett műveleteiről szóló információkat, és mindezt a COM porton keresztül továbbítja.

  Ha a titkosított merevlemezeket tartalmazó számítógép a COM porton keresztül egy másik számítógéphez csatlakozik, akkor a Hitelesítési ügynök eseményeit e másik számítógépen meg lehet vizsgálni.

- **Verbose**. Ha ezt a lehetőséget választja, az alkalmazás a nyomkövetési fájlban részletesen naplózza a Hitelesítési ügynök működéséről szóló információkat, valamint a felhasználó Hitelesítési ügynökkel végzett műveleteiről szóló információkat.

  A bejegyzések részletességi szintje ennél a lehetőségnél magasabb, mint a **Debug** lehetőségnél. A magas részletességi szint lelassíthatja a Hitelesítési ügynök és az operációs rendszer indítását.

- **Verbose on display**. Ha ezt a lehetőséget választja, az alkalmazás a nyomkövetési fájlban részletesen naplózza a Hitelesítési ügynök működéséről szóló információkat, valamint a felhasználó Hitelesítési ügynökkel végzett műveleteiről szóló információkat, és mindezt a COM porton keresztül továbbítja.

  A bejegyzések részletességi szintje ennél a lehetőségnél magasabb, mint a **Debug on display** lehetőségnél. A magas részletességi szint lelassíthatja a Hitelesítési ügynök és az operációs rendszer indítását.

A nyomkövetési szint kiválasztása után a rendszertöltés-vezérlő ismét megjeleníti a menüt.

7. A Rendszertöltés-vezérlő menüben válassza ki a **Boot system** elemet.

   Az FDE rendszertöltő elindítja a hitelesítési ügynököt.

   Reprodukálja a problémát.

   Adatok akkor kerülnek rögzítésre a Hitelesítési ügynök nyomkövetési fájljába, ha a számítógépen vannak titkosított merevlemezek, illetve a teljes lemeztitkosítás folyamatban van.

8. A nyomkövetési folyamat leállításához térjen vissza a Támogató eszközök ablakba, és tiltsa le a nyomkövetést.

Ennek eredményeként a hitelesítési ügynök KES.SRV operációs nyomkövetési fájljai a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappában jönnek létre. Az alkalmazás nyomkövetési fájljaival ellentétben a Hitelesítési ügynök nyomkövetési fájlját nem kapja meg a Kaspersky. Szükség esetén elemzés céljából kézileg elküldheti a Hitelesítési ügynök nyomkövetési fájlját a Kaspersky részére.

Hitelesítési ügynök súgószövegeinek szerkesztése

A Hitelesítési ügynök súgóüzeneteinek szerkesztése előtt tekintse át a rendszerindítás előtti környezetben támogatott karakterek (lentebb elérhető) listáját.

A Hitelesítési ügynök súgóüzeneteinek szerkesztése:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza az **Adattitkosítás** → **Általános titkosítási beállítások** lehetőséget.

4. A megnyíló **Sablonok** részen kattintson a **Súgó** gombra.

5. A megnyíló ablakban tegye a következőket:

   - Válassza ki a **Hitelesítés** lapot a Hitelesítési ügynök ablakában akkor megjelenő súgószöveget, amikor a fiók bejelentkezési adatainak megadása folyik.

   - Válassza ki a **Jelszó módosítása** lapot a Hitelesítési ügynök ablakában akkor megjelenő súgószöveget, amikor a Hitelesítési ügynök-fiók jelszavának módosítása folyik.

   - Válassza ki a **Jelszó visszaállítása** lapot a Hitelesítési ügynök ablakában akkor megjelenő súgószöveget, amikor a Hitelesítési ügynök-fiók jelszavának visszaállítása folyik.

6. Szerkessze a súgóüzeneteket.

   Ha vissza szeretné állítani az eredeti szöveget, kattintson az **Alapértelmezett** gombra.

   > Legfeljebb 16 sorból álló súgószöveget adhat meg. Egy-egy sor legfeljebb 64 karakterből állhat.

7. Mentse el a módosításokat.

A Hitelesítési ügynök súgóüzenetiben lévő karakterek korlátozott támogatása

Rendszerindítás előtti környezetben az alábbi Unicode karakterek támogatottak:

- Alapszintű latin ábécé (0000–007F)
- Kiegészítő Latin-1 karakterek(0080–00FF)
- Kiterjesztett Latin-A (0100–017F)
- Kiterjesztett Latin-B (0180–024F)
- Nem kombinált kiterjesztett azonosító karakterek (02B0–02FF)
- Kombinált ékezetek (0300–036F)
- Görög és kopt ábécé (0370–03FF)
- Cirill (0400–04FF)
- Héber (0590–05FF)
- Arab írás (0600–06FF)
- Kiegészítő kiterjesztett latin (1E00–1EFF)
- Írásjelek (2000–206F)
- Pénznemek jelei (20A0–20CF)
- Betűszerű szimbólumok (2100–214F)

- Geometriai ábrák (25A0–25FF)
- Arab B írás bemutató formái (FE70–FEFF)

A listán nem szereplő karakterek a rendszerindítás előtti környezetben nem támogatottak. Ilyen karaktereket nem javasolt a Hitelesítési ügynök súgóüzeneteiben használni.

A Hitelesítési ügynök működésének tesztelése után hátramaradt objektumok és adatok eltávolítása

Ha az alkalmazás eltávolítása közben a Kaspersky Endpoint Security a rendszer merevlemezén a Hitelesítési ügynök tesztműködése után visszamaradt objektumokat és adatokat észlel, megszakad az alkalmazás eltávolítása, és az érintett objektumok és adatok eltávolításáig nem is folytatható.

A Hitelesítési ügynök tesztműködése után a rendszer merevlemezén csak kivételes esetekben maradhatnak objektumok és adatok. Akkor történhet például ilyen, ha a számítógép újraindítására titkosítási beállításokat tartalmazó Kaspersky Security Center rendszabály alkalmazását követően nem került sor, illetve ha az alkalmazás elindulása a Hitelesítési ügynök tesztműködése után nem sikerül.

A Hitelesítési ügynök tesztműködése után a rendszer merevlemezén maradt objektumokat és adatokat a következő módszerekkel távolíthatja el:

- a Kaspersky Security Center rendszabállyal;
- visszaállító segédprogrammal.

A Hitelesítési ügynök tesztműködése után megmaradt objektumok és adatok eltávolítása Kaspersky Security Center rendszabállyal:

1. Alkalmazzon a számítógépen olyan Kaspersky Security Center rendszabályt, amely úgy van beállítva, hogy a számítógép összes merevlemezét visszafejti.
2. Indítsa el a Kaspersky Endpoint Security alkalmazást.

A Hitelesítési ügynök tesztműködése után megmaradt objektumok és adatok eltávolítása Visszaállító segédprogrammal:

1. Futtassa az fdert.exe nevű fájlt, a visszaállító segédprogram végrehajtható fájlját. Ezt a fájlt a Kaspersky Endpoint Security hozza létre.
2. A Visszaállító segédprogram ablakában válassza ki a kívánt eszközt.
3. Kattintson a **Vizsgálat** gombra.
4. Ha a rendszer merevlemezének diagnosztizálása után olyan üzenetet kap, amely szerint objektumok és adatok maradtak vissza a Hitelesítési ügynök tesztműködéséből, kattintson az **AA-objektumok és -adatok törlése** gombra.

   Az **AA-objektumok és -adatok törlése** gomb csak akkor érhető el, ha a Hitelesítési ügynök tesztműködése után megmaradt objektumokat és adatokat észlel a rendszer.

Az alkalmazás Hitelesítési ügynökkel való inkompatibilitására vonatkozó adatok eltávolítása:

Gépelje be a parancssorba az `avp pbatestreset` parancsot.

BitLocker kezelés

A *BitLocker* a Windows operációs rendszerek beépített titkosítási technológiája. A Kaspersky Endpoint Security lehetővé teszi, hogy a Kaspersky Next infrastruktúra segítségével vezérelje és kezelje a Bitlockert. A BitLocker logikai köteteket titkosít. A BitLocker használatával nem lehet cserélhető meghajtókat titkosítani. A BitLocker részleteiért lásd a Microsoft dokumentációját.

A lemez titkosításakor a BitLocker a system partition helyre helyezi a rendszerbetöltőt és az egyéb segédfájlokat. Ez a partíció nem titkosított. Az operációs rendszer a Windows telepítése során automatikusan létrehozza a rendszerpartíciót. Ha a lemez teljesen particionálva van a Windows telepítése előtt, az operációs rendszer nem tud rendszerpartíciót létrehozni. Ebben az esetben a BitLocker-lemeztitkosítás indításakor az operációs rendszer arra kéri Önt, hogy particionálja újra a lemezt, és hozzon létre rendszerpartíciót. A rendszerpartíció létrehozása után az operációs rendszer elindítja a BitLocker titkosítást.

A BitLocker titkosítási algoritmus nem függ a terjesztőcsomagban található AES-függvénytár verziójától (AES256 vagy AES56). A titkosítás az operációs rendszer beépített titkosítási függvénytárát használja.

Alapértelmezés szerint az alkalmazás a BitLocker titkosítási algoritmust használja, amelynek tényleges kulcshossza 256 bit a korábban nem titkosított eszközök titkosításához. Azoknál az eszközöknél, amelyeket az alkalmazás telepítése előtt titkosítottak, a titkosítási algoritmus eltérő lehet. A titkosítási algoritmus kiválasztásával kapcsolatos részletes információkat a Microsoft terméktámogatásának webhelyén találja. A 12.9-es verziótól kezdve a Kaspersky Endpoint Security elküldi a Kaspersky Security Centernek az eredeti helyreállítási kulcsot azoknak az eszközöknek az esetében, amelyeket korábban külső alkalmazások titkosítottak.

A BitLocker egy Trusted Platform Module segítségével a hozzáférési kulcsok biztonságos tárolását biztosítja. A *Trusted Platform Module* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapján helyezkedik el, és a rendszer többi összetevőjével a hardverbuszon keresztül lép kapcsolatba. A TPM-ek használatával lehet a legbiztonságosabb módon tárolni a BitLocker hozzáférési kulcsokat, mivel a TPM indítás előtti rendszerintegráció-hitelesítést nyújt. A számítógépen továbbra is titkosíthat meghajtókat TPM nélkül. Ilyen esetben a hozzáférési kulcs jelszó nélkül lesz titkosítva. A BitLocker a következő hitelesítési módszereket használja:

- TPM.
- TPM és PIN-kód.
- Jelszó.

Miután titkosítja a rendszer merevlemezét, a felhasználónak végig kell mennie a BitLocker hitelesítések, hogy elindítsa az operációs rendszert. Hitelesítés után a BitLocker lehetővé teszi a felhasználó számára a bejelentkezést. A BitLocker nem támogatja az egyszeri bejelentkezési technológiát (SSO).

Egy meghajtó titkosítása után a BitLocker létrehoz egy helyreállítási kulcsot. A Kaspersky Endpoint Security elküldi a helyreállítási kulcsot a Kaspersky Security Centernek, hogy visszaállíthassa a lemezhez való hozzáférést, például ha egy felhasználó elfelejtette a jelszavát.

Ha egy felhasználó BitLocker használatával titkosít egy lemezt, a Kaspersky Endpoint Security elküldi a helyreállítási kulcsot és a lemeztitkosítással kapcsolatos információkat a Kaspersky Security Centernek.

Ha Windows csoportrendszabályokat használ, kapcsolja ki a BitLocker kezelést a rendszabály-beállításokban. A Windows rendszabály-beállítások összeférhetetlenek lehetnek a Kaspersky Endpoint Security rendszabály-beállításaival. Meghajtó titkosításakor hiba léphet fel.

BitLocker meghajtótitkosítás indítása

Teljes lemeztitkosítás megkezdése előtt célszerű meggyőződni arról, hogy a számítógép nem fertőzött. Ehhez indítsa el a Teljes vizsgálat vagy a Kritikus területek vizsgálata feladatot. Ha rootkittel fertőzött számítógépen teljes lemeztitkosítást végez, akkor a számítógép működésképtelenné válhat.

Ahhoz, hogy a BitLocker meghajtótitkosítást olyan számítógépeken is használhassa, melyek a szerverekhez Windows operációs rendszert futtatnak, előfordulhat, hogy telepíteni kell a BitLocker meghajtótitkosítás összetevőt. Telepítse az összetevőt az operációs rendszer eszközeivel (Szerepek és összetevők hozzáadása varázsló). A BitLocker meghajtótitkosítás telepítéséről szóló további információkat a Microsoft dokumentációban találhat.

A BitLocker meghajtótitkosítás futtatásának menete az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
4. A **Titkosítási technológia** legördülő listán válassza ki az **BitLocker meghajtótitkosítás** lehetőséget.
5. A **Titkosítási mód** legördülő listán válassza ki az **Összes merevlemez titkosítása** elemet.

   Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak azon operációs rendszer tölthető be, melyen a titkosítás el lett végezve.

6. Konfigurálja a fejlett BitLocker meghajtótitkosítás opciókat (lásd az alábbi táblázatot).
7. Mentse el a módosításokat.

A BitLocker meghajtótitkosítás futtatásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption** → **Full Disk Encryption** elemet.

5. Válassza a **BitLocker Disk Encryption** technológiát.

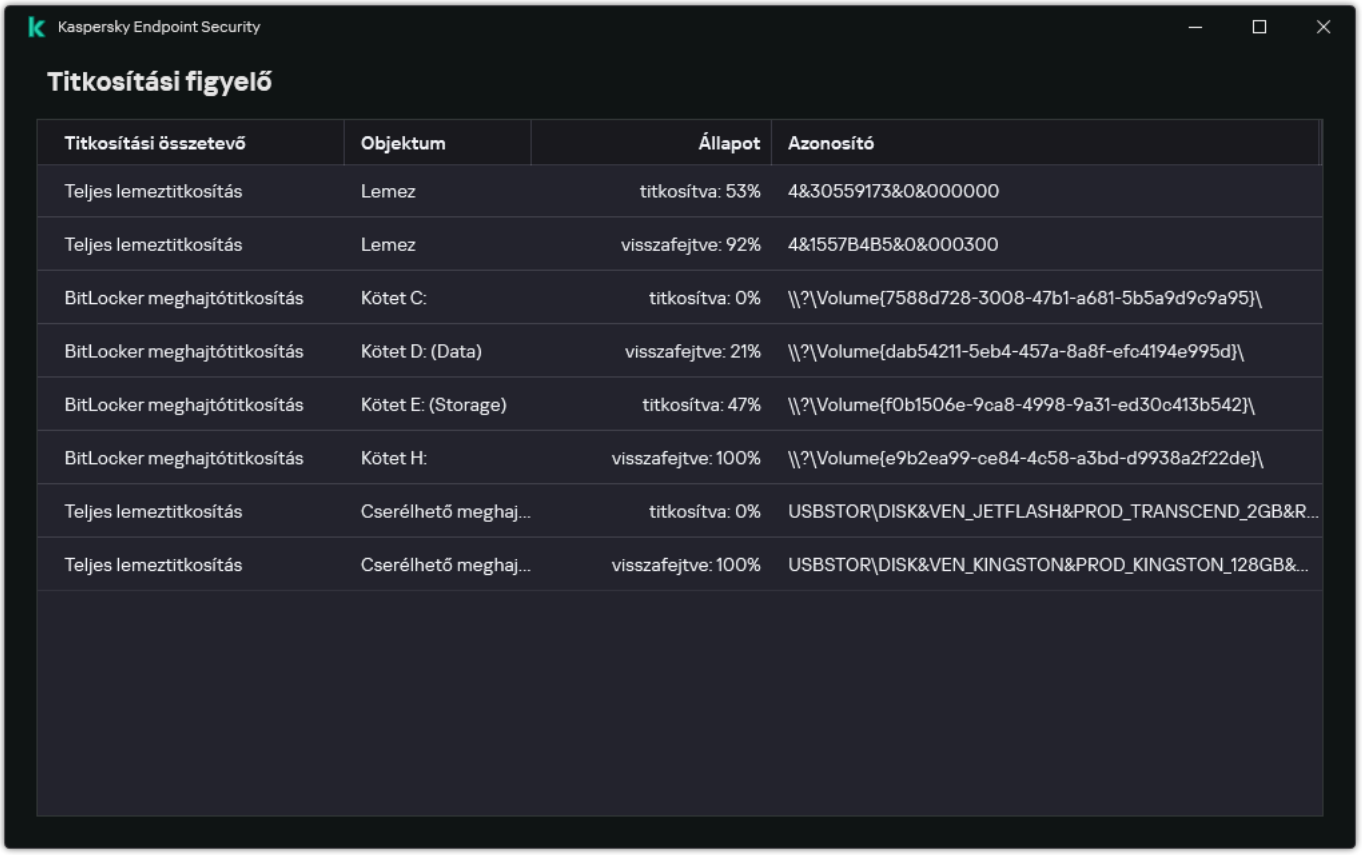
6. A **Action on devices** területen válassza az **Encrypt all hard drives** opciót.

Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak azon operációs rendszer tölthető be, melyen a titkosítás el lett végezve.

7. Konfigurálja a fejlett BitLocker meghajtótitkosítás opciókat (lásd az alábbi táblázatot).

8. Mentse el a módosításokat.

A Titkosítási figyelő eszközzel vezérelheti a lemez titkosítási vagy visszafejtési folyamatát a felhasználó számítógépén. A Titkosítási figyelő eszközt a fő alkalmazásablakból futtathatja.



Titkosítási figyelő

A házirend alkalmazása után az alkalmazás a hitelesítési beállításoktól függően a következő lekérdezéseket jeleníti meg:

- Csak TPM. Nincs szükség felhasználói beavatkozásra. A lemez a számítógép újraindításakor lesz titkosítva.
- TPM + PIN / jelszó. Ha van elérhető TPM modul, megjelenik a PIN-kódot kérő ablak. Ha nincs elérhető TPM modul, megjelenik az rendszerindítás előtti hitelesítés jelszókérő ablaka.
- Csak jelszó. A rendszerindítás előtti hitelesítéskor egy jelszókérő ablak jelenik meg.

Ha a számítógép operációs rendszeréhez be van kapcsolva a be van kapcsolva a Federal Information Processing szabványú kompatibilitási mód, akkor a Windows 8 és korábbi operációs rendszerek esetében megjelenik egy kérelem, ami a tárolóeszközhöz való csatlakozásról szól, hogy elmentse a visszaállítási kulcsfájlt. Több visszaállítási kulcsot is elmenthet egy tárolóeszközön.

PIN-kód vagy jelszó megadása után a BitLocker a számítógép újraindítását fogja kérni a titkosítás befejezése érdekében. Ezután a felhasználónak végig kell mennie a BitLocker hitelesítési folyamaton. A hitelesítési folyamat után a felhasználónak be kell jelentkeznie a rendszerbe. Az operációs rendszer betöltődését követően a BitLocker befejezi a titkosítást.

Ha nem lehet elérni a titkosítási kulcsokat, a felhasználó kérheti visszaállítási kulcs megadását a helyi hálózat rendszergazdájától (ha a visszaállítási kulcsot nem mentette korábban a tárolóeszközre, vagy elvesztette).

A BitLocker meghajtótitkosítás összetevő beállításai

Paraméter	Leírás
Rendszerindítás előtt, billentyűzeten keresztül történő BitLocker hitelesítés bekapcsolása táblagépeken	Adatbevitelt igénylő hitelesítés használata rendszerindítás előtti környezetben, még akkor is, ha a platformon nem lehetséges a bevitel rendszerindítás előtt (például táblagépek érintőképernyős billentyűzetei esetén). A táblagépek érintőképernyője nem érhető el rendszerindítás előtt. Ahhoz, hogy a felhasználó befejezze a BitLocker hitelesítést a táblagépeken, először csatlakoztatnia kell egy USB-billentyűzetet például. Ha a jelölőnégyzet be van jelölve, a rendszerindítás előtti bevitelt igénylő hitelesítés engedélyezve van. Javasoljuk, hogy ezt a beállítást csak olyan eszközöknél használja, amelyek az érintőképernyős billentyűzeteken kívül alternatív adatbeviteli eszközöket – például USB-billentyűzetet – is tartalmaznak a rendszerindítás előtti környezetben. Ha a jelölőnégyzet üres, a BitLocker meghajtótitkosítás nem érhető el táblagépeken.
Hardveres titkosítás használata (Windows 8 és újabb verziók)	Ha a jelölőnégyzet be van jelölve, az alkalmazás hardveres titkosítást használ. Ennek köszönhetően felgyorsul a titkosítás, és kevesebb számítógépes erőforrásra lesz szükség.

Paraméter	Leírás
Csak a felhasznált lemezterület titkosítása (Windows 8 és újabb verziók)	Ez a jelölőnégyzet engedélyezi/letiltja azt a lehetőséget, amely a titkosítási területet kizárólag a foglalt merevlemez-szektorokra korlátozza. A korlátozás révén csökkentheti a titkosítási időt. A **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemezek visszafejtése. A titkosítás megkezdése előtt kell a jelölőnégyzetet bejelölni, illetve törölni. Ha a jelölőnégyzet be van jelölve, akkor a merevlemeznek csak a fájlok által elfoglalt részei kerülnek titkosításra. A Kaspersky Endpoint Security az új adatokat hozzáadásukkor automatikusan titkosítja. Ha a jelölőnégyzet nincs bejelölve, a teljes merevlemez titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit. Ez a lehetőség új merevlemezek esetén javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha már használatban lévő merevlemezen alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről, még a törölt, esetlegesen helyreállítható adatokról is. Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.
Hitelesítési módszer	**Csak jelszó (Windows 8 és újabb verziók)** Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security jelszót kér a felhasználótól, ha a felhasználó megpróbál egy titkosított meghajtóhoz hozzáférni. Ezt a lehetőséget akkor lehet kiválasztani, ha nincs használatban Trusted Platform Module (TPM). **Trusted Platform Module (TPM)** Ha ez a lehetőség van kiválasztva, a BitLocker Trusted Platform Module-t (TPM) használ. A *Trusted Platform Module* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapján helyezkedik el, és a rendszer többi összetevőjével a hardverbuszon keresztül lép kapcsolatba. A Windows 7 vagy Windows Server 2008 R2 rendszert futtató számítógépeknél csak TPM-modul használata érhető el. Ha nincs telepítve TPM-modul, akkor a BitLocker titkosítás nem lehetséges. Az ilyen számítógépeken nem támogatott a jelszó használata. A Trusted Platform Module-lal rendelkező eszköz olyan titkosítási kulcsokat tud előállítani, amelyeket csak az adott eszközzel lehet visszafejteni. A Trusted Platform Module a titkosítási kulcsokat saját gyökértárolási kulcsával titkosítja. A gyökértárolási kulcs tárolása a Trusted Platform Module-on belül történik. Ez további védelmi szintet nyújt a titkosítási kulcsok feltörési próbálkozásai ellen. Alapértelmezésben ez a művelet van kiválasztva. A titkosítási kulcshoz való hozzáféréshez további védelmi szintet állíthat be, és a kulcsot jelszóval vagy PIN-kóddal titkosíthatja: • **PIN-kód használata a TPM-nél**. Ennek a négyzetnek a bejelölésével a felhasználó használhatja a PIN-kódot a Trusted Platform Module-ban (TPM) tárolt titkosítási kulcshoz való hozzáférés megszerzéséhez. Ha a jelölőnégyzet törölve van, a felhasználók nem használhatják a PIN-kódokat. A titkosítási kulcs eléréséhez a felhasználónak meg kell adnia a jelszót. • **Trusted Platform Module (TPM) vagy jelszó, ha a TPM nem érhető el**. Ha ez az opció van kiválasztva, a felhasználó jelszó segítségével férhet hozzá a titkosítási kulcshoz, ha nem áll rendelkezésre Trusted Platform Module (TPM). Ha a jelölőnégyzet törölve van és a TPM nem érhető el, nem indul el a teljes lemeztitkosítás. A kiválasztott hitelesítési módszert jelszó- vagy PIN-kódkövetelmények megadásával kell konfigurálni: • **PIN-kód minimális hossza (karakter)**. • **Jelszó minimális hossza (karakter)**. • **A jelszó/PIN-kód érvényességi idejének korlátozása a TPM-nél (nap)**. • **Bővített PIN-kód használata (betűk és számok)**. A *bővített PIN-kód* lehetővé teszi a számokon kívül más karakterek használatát is: latin nagy- és kisbetűket, speciális karaktereket és szóközöket.
Helyreállítási kulcs automatikus újragenerálása (nap)	A jelszó automatikus frissítése a BitLocker által védett meghajtóhoz való hozzáférés visszaállításához. Ha a jelölőnégyzet be van jelölve, adja meg a helyreállítási kulcs jelszavának érvényességi idejét. Ez segít megelőzni a helyreállítási kulcs jelszavának ismételt használatát.

BitLocker által védett merevlemez visszafejtése

A felhasználók az operációs rendszer segítségével fejthetik vissza a lemezt (a *BitLocker kikapcsolása* funkció). Ezután a Kaspersky Endpoint Security figyelmezteti a felhasználót, hogy titkosítsa újra a lemezt. A Kaspersky Endpoint Security figyelmeztetni fog a lemez titkosítására, kivéve akkor, ha rendszabályban engedélyezi a lemeztitkosítást.

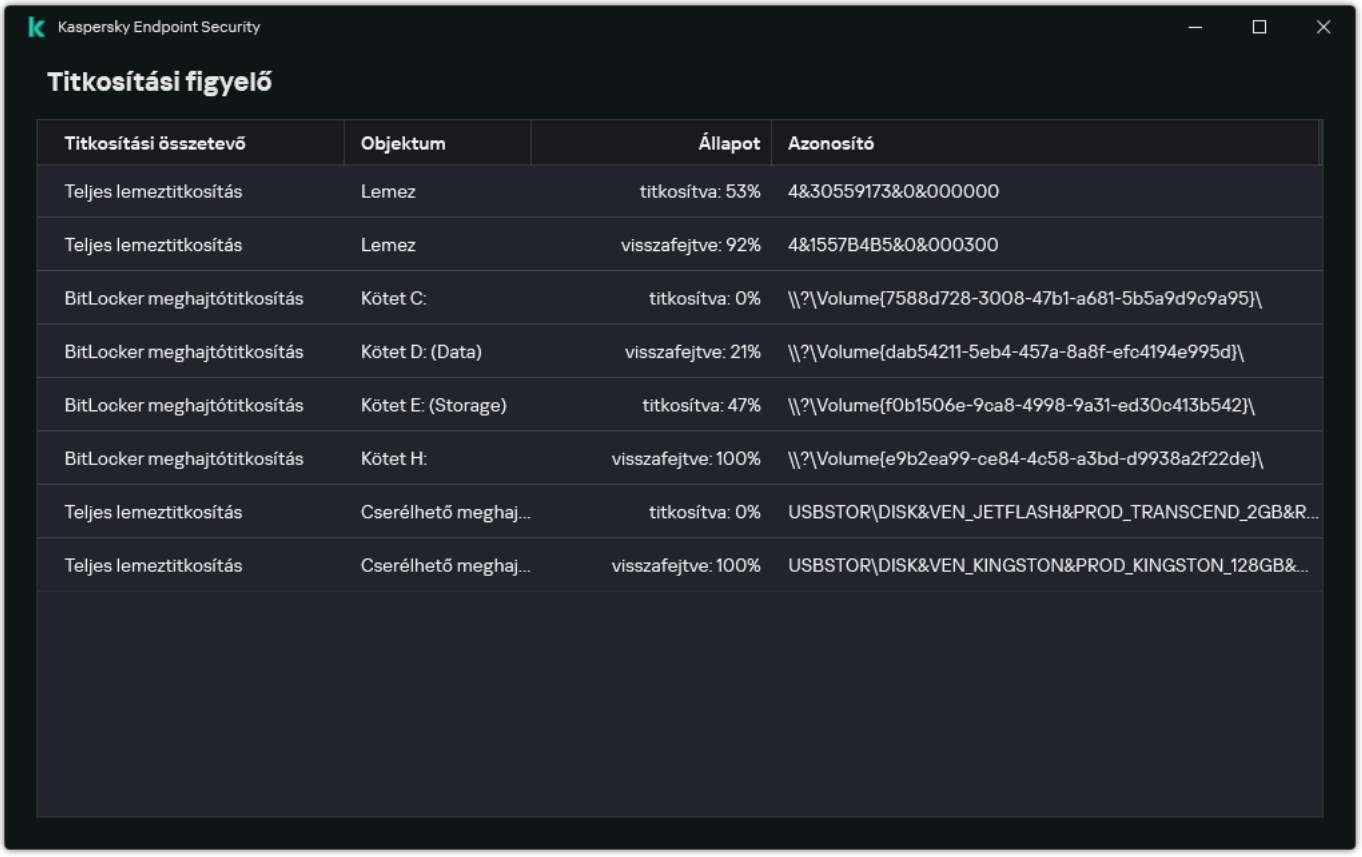
Hogyan kell visszafejteni a BitLocker által védett merevlemezt az Adminisztrációs konzolon (MMC) keresztül

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
4. A **Titkosítási technológia** legördülő listán válassza ki az **BitLocker meghajtótitkosítás** lehetőséget.
5. A **Titkosítási mód** legördülő listán válassza ki az **Összes merevlemez visszafejtése** elemet.
6. Mentse el a módosításokat.

A BitLocker által titkosított merevlemez visszafejtésének menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption** → **Full Disk Encryption** elemet.
5. Válassza a **BitLocker Disk Encryption** technológiát.
6. A **Action on devices** területen válassza az **Decrypt all hard drives** opciót.
7. Mentse el a módosításokat.

A Titkosítási figyelő eszközzel vezérelheti a lemez titkosítási vagy visszafejtési folyamatát a felhasználó számítógépén. A Titkosítási figyelő eszközt a fő alkalmazásablakból futtathatja.



Titkosítási figyelő

A hozzáférés visszaállítása BitLockerrel védett merevlemezhez

Ha egy felhasználó elfelejtette a hozzáférési jelszót egy BitLockerrel titkosított merevlemezhez, el kell indítania a visszaállítási eljárást (kérés–válasz).

Ha a számítógép operációs rendszeréhez be van kapcsolva a Federal Information Processing szabványú kompatibilitási mód, akkor a Windows 8 és a korábbi verziók esetében a visszaállítási kulcsfájl a titkosítás előtt lesz mentve a cserélhető meghajtóra. A meghajtóhoz való hozzáférés visszaállításához helyezze be a cserélhető meghajtót, és kövesse a képernyőn látható utasításokat.

A BitLockerrel titkosított merevlemez hozzáférhetőségének visszaállítása a következő lépésekből áll:

1. A felhasználó közli a rendszergazdával a visszaállítási kulcs azonosítóját (részletek az alábbi ábrán).
2. A rendszergazda ellenőrzi a visszaállítási kulcs azonosítóját a számítógép tulajdonságai között, a Kaspersky Security Centerben. A felhasználó által megadott azonosítónak egyeznie kell a számítógép tulajdonságai között megjelenő azonosítóval.
3. Ha a visszaállításikulcs-azonosítók megegyeznek, a rendszergazda elküldi a felhasználónak a visszaállítási kulcsot vagy a visszaállításikulcs-fájlt.

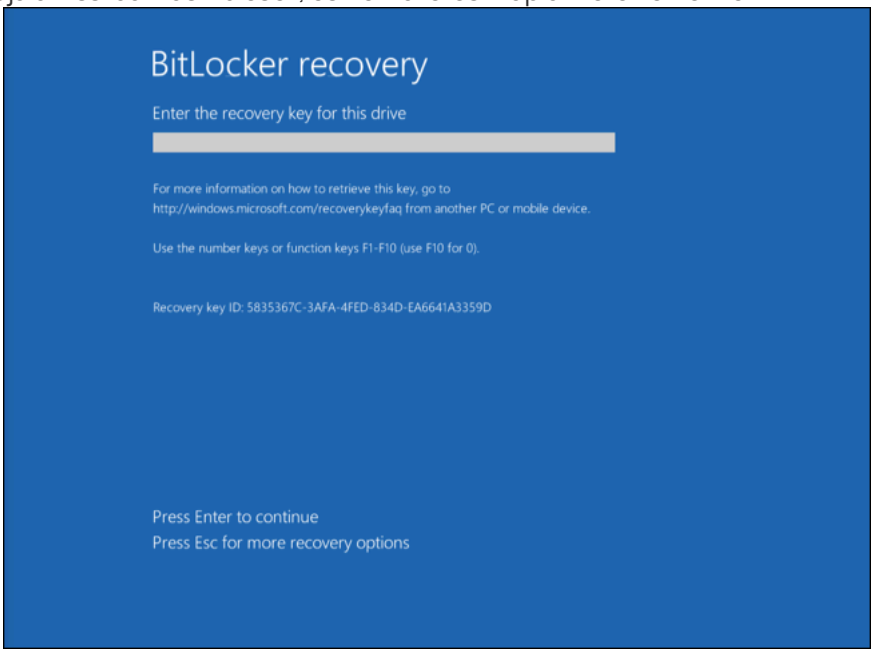
Visszaállításikulcs-fájl használata a következő operációs rendszert futtató számítógépek esetében indokolt:

- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2011
- Windows Server 2012

Minden egyéb operációs rendszer esetén visszaállítási kulcs használatos.

A visszaállítási kulcs jelszavának ismételt használatának megakadályozása céljából a házirend beállításaiban beállíthatja az automatikus jelszófrissítést.

4. A felhasználó megadja a visszaállítási kulcsot, és hozzáférést kap a merevlemezhez.



A hozzáférés visszaállítása BitLockerrel titkosított merevlemezhez

Rendszermeghajtó hozzáférésének visszaállítása

A helyreállítási eljárást elindításához a felhasználónak a rendszerindítás előtti hitelesítéskor meg kell nyomnia az **Esc** billentyűt.

A BitLockerrel titkosított rendszermeghajtó visszaállítási kulcsának megtekintése az Adminisztrációs Konzolon (MMC)

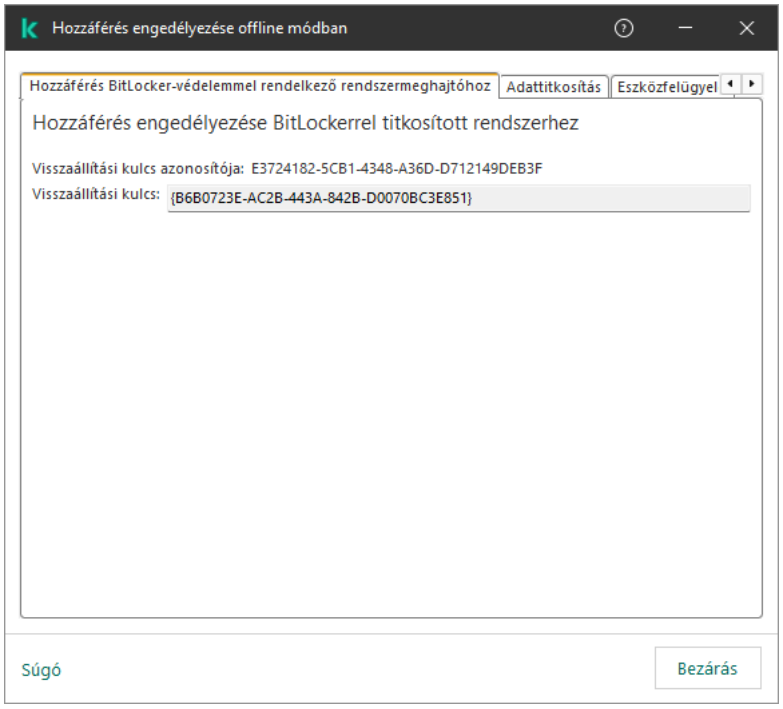
1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Managed devices** lehetőséget.
3. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
4. A helyi menüben válassza ki a **Hozzáférés engedélyezése offline módban** elemet.

5. A megnyíló ablakban válassza a **Hozzáférés BitLocker-védelemmel rendelkező rendszermeghajtóhoz** lapot.

6. Kérje be a felhasználótól a BitLocker jelszóbeviteli ablakban jelzett visszaállítási kulcsazonosítót, és vesse össze a **Recovery key ID** mezőben lévő azonosítóval.

> Ha az azonosítók nem egyeznek, a kulcs nem használható a megadott rendszermeghajtóhoz való hozzáférés visszaállítására. Győződjön meg arról, hogy a kiválasztott számítógép neve egyezik a felhasználó számítógépének nevével.

Ekkor hozzáférést kap a visszaállítási kulcshoz vagy a visszaállítási kulcs fájljához, amelyet továbbítania kell a felhasználónak.



Hozzáférés visszaállítása BitLockerrel titkosított meghajtóhoz

BitLockerrel titkosított rendszermeghajtó visszaállítási kulcsának megtekintése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.

2. Jelölje be annak a számítógépnek a neve melletti jelölőnégyzetet, amely számítógépben az ismét elérni kívánt meghajtó található.

3. Kattintson az **Grant access to the device in offline mode** gombra.

4. A megnyíló ablakban válassza a **BitLocker** szakaszt.

5. Ellenőrizze a visszaállítási kulcs azonosítóját. A felhasználó által megadott azonosítónak egyeznie kell a számítógép beállításai között megjelenő azonosítóval.

   Ha az azonosítók nem egyeznek, a kulcs nem használható a megadott rendszermeghajtóhoz való hozzáférés visszaállítására. Győződjön meg arról, hogy a kiválasztott számítógép neve egyezik a felhasználó számítógépének nevével.

6. Kattintson az **Receive key** gombra.

   Ekkor hozzáférést kap a visszaállítási kulcshoz vagy a visszaállítási kulcs fájljához, amelyet továbbítania kell a felhasználónak.

Az operációs rendszer betöltése után a Kaspersky Endpoint Security felszólítja a felhasználót a jelszó vagy a PIN-kód módosítására. Miután beállított egy új jelszót vagy PIN-kódot, a BitLocker létrehoz egy új helyreállítási kulcsot, és elküldi azt a Kaspersky Security Centernek. Ennek eredményeképpen a helyreállítási kulcs és a helyreállítási kulcsfájl is frissítésre kerül. Ha a felhasználó nem módosította a jelszavát, használhatja a régi visszaállítási kulcsot az operációs rendszer következő betöltését követően.

A Windows 7 rendszerű számítógépek nem engedélyezik a jelszó vagy a PIN-kód megváltoztatását. A visszaállítási kulcs megadása és az operációs rendszer betöltése után a Kaspersky Endpoint Security nem szólítja fel a felhasználót a jelszó vagy a PIN-kód módosítására. Így nem lehet új jelszót vagy PIN-kódot beállítani. A probléma az operációs rendszer sajátosságaiból származik. A folytatáshoz újra kell titkosítania a merevlemezt.

Hozzáférés visszaállítása rendszert nem futtató meghajtóhoz

A helyreállítási eljárás elindításához a felhasználónak rá kell kattintania a **Elfelejtette jelszavát** hivatkozásra a meghajtó elérését kínáló ablakban. Miután megkapta a hozzáférést a titkosított meghajtóhoz, a felhasználó a BitLocker beállításaiban engedélyezheti a meghajtó automatikus feloldását a Windows-hitelesítés során.

A BitLockerrel titkosított, rendszert nem futtató meghajtó visszaállítási kulcsának megtekintése az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

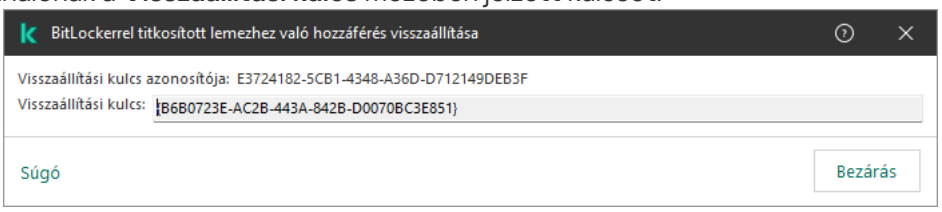
2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Data encryption and protection** → **Encrypted drives** mappát.

3. Válassza ki a munkaterületen azt a titkosított eszközt, amelyhez hozzáférésikulcs-fájlt szeretne létrehozni, majd az eszköz helyi menüjében kattintson a **Hozzáférés az eszközhöz a Kaspersky Endpoint Security alkalmazásban** lehetőségre.

4. Kérje be a felhasználótól a BitLocker jelszóbeviteli ablakban jelzett visszaállítási kulcsazonosítót, és vesse össze a **Recovery key ID** mezőben lévő azonosítóval.

   Ha az azonosítók nem egyeznek, a kulcs nem használható a megadott meghajtóhoz való hozzáférés visszaállítására. Győződjön meg arról, hogy a kiválasztott számítógép neve egyezik a felhasználó számítógépének nevével.

5. Küldje el a felhasználónak a **Visszaállítási kulcs** mezőben jelzett kulcsot.



Hozzáférés visszaállítása BitLockerrel titkosított meghajtóhoz

BitLockerrel titkosított, rendszert nem futtató meghajtó visszaállítási kulcsának megtekintése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza az **Operations** → **Data encryption and protection** → **Encrypted drives** lehetőséget.

2. Jelölje be annak a számítógépnek a neve melletti jelölőnégyzetet, amely számítógépben az ismét elérni kívánt meghajtó található.

3. Kattintson az **Grant access to the device in offline mode** gombra.

   Ezzel elindítja az eszközelérést biztosító varázslót.

4. Kövesse az eszközelérést biztosító varázsló utasításait:

   a. Válassza ki a **Kaspersky Endpoint Security for Windows** bővítményt

   b. Ellenőrizze a visszaállítási kulcs azonosítóját. A felhasználó által megadott azonosítónak egyeznie kell a számítógép beállításai között megjelenő azonosítóval.

   > Ha az azonosítók nem egyeznek, a kulcs nem használható a megadott rendszermeghajtóhoz való hozzáférés visszaállítására. Győződjön meg arról, hogy a kiválasztott számítógép neve egyezik a felhasználó számítógépének nevével.

   c. Kattintson az **Receive key** gombra.

Ekkor hozzáférést kap a visszaállítási kulcshoz vagy a visszaállítási kulcs fájljához, amelyet továbbítania kell a felhasználónak.

A BitLocker védelem szüneteltetése a szoftver frissítéséhez

Az operációs rendszer frissítése, az operációs rendszerhez tartozó frissítőcsomagok telepítése vagy más, BitLocker-védelemmel rendelkező szoftver frissítése során számos speciális szempontot kell figyelembe venni. A frissítések telepítéséhez szükség lehet a számítógép többszöri újraindítására. Minden újraindítás után a felhasználónak be kell fejeznie a BitLocker hitelesítést. Annak érdekében, hogy a frissítések megfelelően települjenek, ideiglenesen kikapcsolhatja a BitLocker-hitelesítést. Ebben az esetben a lemez titkosítva marad, és a felhasználó hozzáférhet az adatokhoz, miután bejelentkezett a rendszerbe. A BitLocker-hitelesítés kezeléséhez használja a *BitLocker-védelem felügyelete* feladatot. Ezzel a feladattal megadhatja a számítógép olyan újraindításainak számát, amelyek nem igényelnek BitLocker-hitelesítést. Ily módon a frissítések telepítése és a *BitLocker-védelem felügyelete* feladat befejezése után a BitLocker-hitelesítés automatikusan engedélyezve lesz. A BitLocker-hitelesítést bármikor engedélyezheti.

A BitLocker-védelem szüneteltetése az Adminisztrációs Konzol (MMC) használatával

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **BitLocker-védelem felügyelete** elemet.

2. lépés. BitLocker-védelem felügyelete

A BitLocker-hitelesítés konfigurálása. A BitLocker-védelem szüneteltetéséhez válassza **A BitLocker-hitelesítés kihagyásának ideiglenes engedélyezése** lehetőséget, és adja meg a BitLocker-hitelesítés nélküli újraindítások számát (1–15 alkalom). Ha szükséges, adja meg a feladat lejárati dátumát és időpontját. A megadott időpontban a feladat automatikusan kikapcsol, és a felhasználónak el kell végeznie a BitLocker-hitelesítést a számítógép újraindításakor.

3. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

4. lépés A feladat nevének megadása

Írja be a feladat nevét, pl. *Frissítés Windows 10-re*.

5. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

A BitLocker-védelem szüneteltetése a Web Console használatával

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** legördülő listából válassza ki a **Kaspersky Endpoint Security** elemet.
2. A **Task type** legördülő listából válassza ki az **BitLocker Protection Management** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például *Frissítés Windows 10-re*.
4. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

2. lépés. BitLocker-védelem felügyelete

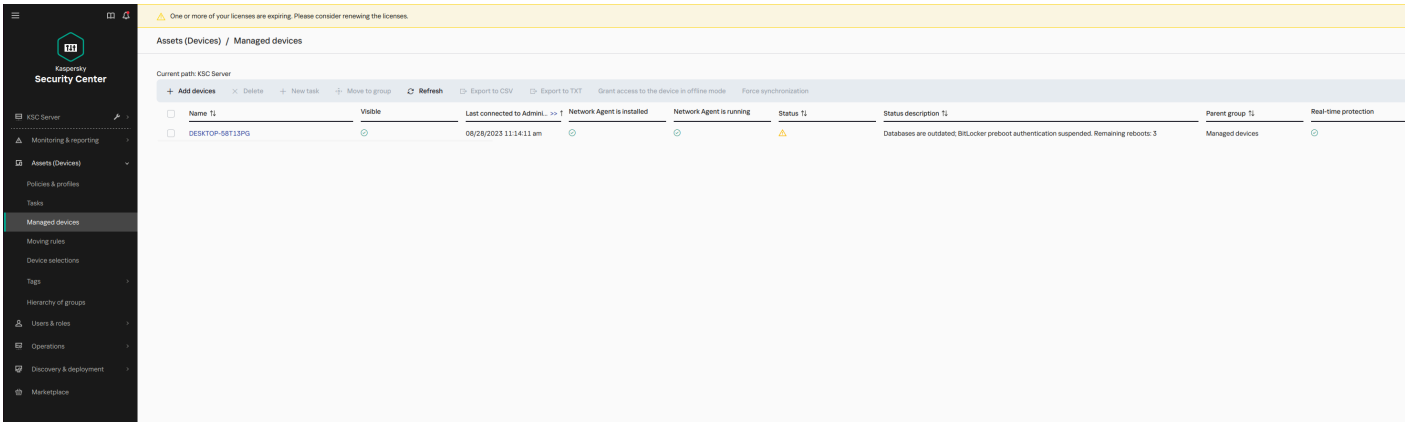
A BitLocker-hitelesítés konfigurálása. A BitLocker-védelem szüneteltetéséhez válassza **Temporarily allow skipping BitLocker authentication** lehetőséget, és adja meg a BitLocker-hitelesítés nélküli újraindítások számát (1–15 alkalom). Ha szükséges, adja meg a feladat lejárati dátumát és időpontját. A megadott időpontban a feladat automatikusan kikapcsol, és a felhasználónak el kell végeznie a BitLocker-hitelesítést a számítógép újraindításakor.

3. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Egy új feladat jelenik meg a feladatok listájában.

A feladat futtatásához jelölje be a feladattal szemben lévő jelölőnégyzetet, majd kattintson a **Start** gombra.

Ennek eredményeként, amikor a feladat fut, a számítógép következő újraindítása után a BitLocker nem kéri fel a felhasználót a hitelesítésre. A számítógép minden, BitLocker-hitelesítés nélküli újraindítása után a Kaspersky Endpoint Security létrehozza a megfelelő eseményt, és rögzíti a fennmaradó újraindítások számát. A Kaspersky Endpoint Security ezután elküldi az eseményt a Kaspersky Security Centernek a rendszergazda általi felügyeletre. A hátralévő újraindítások számát is megtekintheti a Kaspersky Security Center konzol **Managed devices** mappájában az eszköz állapotleírásában.



A felügyelt eszközök listája

Amikor eléri a megadott számú újraindítást vagy a feladat lejárati idejét, a BitLocker-hitelesítés automatikusan bekapcsol. Az adatokhoz való hozzáféréshez a felhasználónak el kell végeznie a BitLocker-hitelesítést.

A Windows 7 rendszert futtató számítógépeken a BitLocker nem képes nyilvántartani a számítógép újraindításainak számát. Az újraindítások számlálását a Windows 7 rendszerű számítógépeken a Kaspersky Endpoint Security végzi. Így a BitLocker-hitelesítés automatikus bekapcsolásához minden újraindítás után el kell indítani a Kaspersky Endpoint Security alkalmazást.

A BitLocker-hitelesítés idő előtti bekapcsolásához nyissa meg a *BitLocker-védelem felügyelete* feladat tulajdonságait, és válassza a **Minden alkalommal kérjen hitelesítést rendszerindítás előtti állapotban** lehetőséget.

Fájl szintű titkosítás a számítógép helyi meghajtóin

A fájltitkosítás nem támogatott az ARM-alapú számítógépeken.

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

A fájltitkosítás a következő speciális tulajdonságokkal rendelkezik:

- A Kaspersky Endpoint Security csak az operációs rendszer helyi felhasználói profiljai esetén titkosítja és fejti vissza az előre megadott mappákban lévő fájlokat. A Kaspersky Endpoint Security a barangoló felhasználói profilok, a kötelező felhasználói profilok, az ideiglenes felhasználói profilok előre megadott mappáiban és az átirányított mappákban lévő fájlokat nem titkosítja és nem fejti vissza.

- A Kaspersky Endpoint Security nem végzi el a fájlok titkosítását, ha módosításuk kárt tehet az operációs rendszerben és a telepített alkalmazásokban. Az alábbi fájlok és mappák az összes beágyazott mappával együtt a titkosítási kizárások listáján vannak:

  - %WINDIR%;

  - %PROGRAMFILES% és %PROGRAMFILES(X86)%;

  - Windows beállításjegyzékfájlok.

  A titkosítási kizárások listája nem tekinthető meg és nem szerkeszthető. Noha a titkosítási kizárások listáján szereplő fájlokat és mappákat fel lehet venni a titkosítási listára, a fájltitkosítási feladat végrehajtásakor nem kerül sor a titkosításukra.

Fájlok titkosítása a számítógép helyi meghajtóin

A Kaspersky Endpoint Security nem titkosítja azokat a fájlokat, amelyek a OneDrive felhőalapú tárhelyen vagy más olyan mappákban találhatók, amelyek neve OneDrive. A Kaspersky Endpoint Security blokkolja a titkosított fájlok OneDrive mappákba másolását is, ha ezeket a fájlokat nem adják hozzá a visszafejtési szabályhoz.

Fájlok titkosítása helyi meghajtókon:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza ki az **Data Encryption** → **File Level Encryption** lehetőséget.

4. A **Titkosítási mód** legördülő listában válassza ki **A szabályoknak megfelelően** elemet.

5. Kattintson a **Titkosítás** lapon a **Hozzáadás** gombra, a legördülő listán pedig válassza ki valamelyiket az alábbi elemek közül:

   a. Válassza ki az **Előre megadott mappák** elemet a Kaspersky szakértői által javasolt helyi felhasználói profilok mappáiban lévő fájlok titkosítási szabályhoz való hozzáadásához.

      - **Dokumentumok**. Az operációs rendszer szokványos *Dokumentumok* mappájában, valamint az azon belüli almappákban található fájlok.

      - **Kedvencek**. Az operációs rendszer szokványos *Kedvencek* mappájában, valamint az azon belüli almappákban található fájlok.

      - **Asztal**. Az operációs rendszer szokványos *Asztal* mappájában, valamint az azon belüli almappákban található fájlok.

- **Ideiglenes fájlok**. A számítógépre telepített alkalmazások működéséhez kapcsolódó ideiglenes fájlok. Például a Microsoft Office alkalmazások olyan ideiglenes fájlokat hoznak létre, amelyek a dokumentumok biztonsági mentését tartalmazzák.

  Nem ajánlott az ideiglenes fájlok titkosítása, mert ez adatvesztést okozhat. Például a Microsoft Word ideiglenes fájlokat hoz létre egy dokumentum feldolgozása során. Ha az ideiglenes fájlok titkosítottak, de az eredeti fájl nem, a felhasználó *Hozzáférés megtagadva* hibát kaphat a dokumentum mentésekor. Az is előfordulhat, hogy a Microsoft Word menti a fájlt, de a következő alkalommal nem lehet megnyitni, tehát elvész az adat.

- **Outlook fájlok**. Az Outlook levelezőprogram működéséhez kapcsolódó fájlok: adatfájlok (PST), offline adatfájlok (OST), offline címjegyzékfájlok (OAB) és személyes címjegyzékfájlok (PAB).

b. Válassza ki az **Egyéni mappa** elemet kézileg beírt mappa elérési útvonalának titkosítási szabályhoz való hozzáadásához.

Mappa elérési útjának megadásakor tartsa be a következő szabályokat:

- Használjon környezeti változót (például: `%FOLDER%\UserFolder\`). Egy környezeti változót csak egyszer lehet használni, és kizárólag az elérési út kezdetén.
- Ne használjon relatív útvonalat.
- Ne használja a `*` (csillag) és a `?` (kérdőjel) karaktert.
- Ne használjon UNC-útvonalat.
- Használjon `;` (pontosvessző) vagy `,` (vessző) karaktert elválasztókarakterként.

c. Válassza a **Fájlok kiterjesztés alapján** elemet, és egyenként hozzáadhatja a fájlkiterjesztéseket a titkosítási szabályhoz. A Kaspersky Endpoint Security csak a megadott kiterjesztésű új és módosult fájlokat titkosítja a számítógépen lévő összes helyi meghajtón.

d. Válassza a **Fájlok kiterjesztéscsoportok alapján** lehetőséget, ha fájlkiterjesztések csoportjait kívánja hozzáadni a titkosítási szabályhoz (például: *Microsoft Office-dokumentumok*). A Kaspersky Endpoint Security a kiterjesztéscsoportok listáján szereplő kiterjesztéssel rendelkező fájlokat titkosítja a számítógépen lévő összes helyi meghajtón.

6. Mentse el a módosításokat.

A rendszabály alkalmazását követően a Kaspersky Endpoint Security azonnal titkosítja a titkosítási szabályban szereplő, a visszafejtési szabályban pedig nem szereplő fájlokat.

A fájltitkosítás a következő speciális tulajdonságokkal rendelkezik:

- Ha ugyanaz a fájl titkosítási szabályban és visszafejtési szabályban is szerepel, a Kaspersky Endpoint Security a következő műveleteket végzi el:
  - Ha a fájl nincs titkosítva, a Kaspersky Endpoint Security nem titkosítja a fájlt.
  - Ha a fájl titkosítva van, a Kaspersky Endpoint Security visszafejti a fájlt.
- A Kaspersky Endpoint Security folytatja az új fájlok titkosítását, ha azok megfelelnek a titkosítási szabály kritériumainak. Például, ha módosítja a titkosítatlan fájl (útvonal vagy kiterjesztés) tulajdonságait, a fájl megfelel a titkosítási szabály kritériumainak. A Kaspersky Endpoint Security titkosítja a fájlt.

- Ha a felhasználó egy olyan új fájlt állít elő, amelynek a tulajdonságai megfelelnek a titkosítási szabály feltételeinek, a Kaspersky Endpoint Security a fájlt megnyitásakor azonnal titkosítja.
- A Kaspersky Endpoint Security a megnyitott fájlok titkosítását bezárásukig elhalasztja.
- Ha egy titkosított fájlt a helyi meghajtón egy másik mappába helyez át, a fájl attól függetlenül titkosítva marad, hogy az új mappa szerepel-e a titkosítási szabályban.
- Ha visszafejt egy fájlt és egy olyan helyi mappába másolja, amely nincs a visszafejtési szabályban, a fájl másolata titkosítva lehet. Ahhoz, hogy a másolt fájl ne legyen titkosítva, hozzon létre egy titkosítási szabályt a célmappához.

A titkosított fájlok hozzáférési szabályainak kialakítása az alkalmazások számára

Alapértelmezés szerint az összes alkalmazás visszafejtett állapotú titkosított fájlokkal működik. Ha gyakran használ bizonyos alkalmazásokat (például böngészőket vagy szövegszerkesztőket), az információk védelme érdekében titkosított fájlhozzáférési szabályokat hozhat létre.

Javasoljuk, hogy hozzon létre egy titkosított fájl-hozzáférési szabályt a Microsoft Internet Explorer és a Microsoft Edge böngészők számára. E böngészők működése miatt, ha titkosított fájlt tölt fel egy webhelyre (például felhőtárhelyre), a fájl titkosítása automatikusan feloldódik. Ez adatszivárgást okozhat. Ezekkel a böngészőkkel nem lehet titkosított fájlokat feltölteni. Javasoljuk, hogy állítsa be a **Hozzáférés engedélyezése a titkosított fájlokhoz csak rejtjelezett szövegként** szabályt. Nem kell szabályt létrehoznia más böngészőkhöz (például a Google Chrome-hoz).

A titkosított fájlok hozzáférési szabályainak kialakítása az alkalmazások számára:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki az **Data Encryption** → **File Level Encryption** lehetőséget.
4. A **Titkosítási mód** legördülő listában válassza ki **A szabályoknak megfelelően** elemet.

   A hozzáférési szabályok alkalmazására kizárólag **A szabályoknak megfelelően** módban kerül sor. Ha a hozzáférési szabályok **A szabályoknak megfelelően** módban történő alkalmazását követően átvált **Maradjon változatlan** módba, a Kaspersky Endpoint Security minden hozzáférési szabályt figyelmen kívül hagy. Minden alkalmazás minden titkosított fájlhoz hozzáfér.

5. Az ablak jobb oldalán válassza ki az **Alkalmazások szabályai** lapot.
6. Ha kizárólag a Kaspersky Security Center listájáról szeretne alkalmazásokat választani, kattintson a **Hozzáadás** gombra, és a legördülő listán válassza ki az **Alkalmazások a Kaspersky Security Center listából** elemet.
   a. Adjon meg szűrőket a táblázatban lévő alkalmazások listájának szűkítéséhez. Ehhez adja meg az **Alkalmazás**, **Forgalmazó** és **Időtartam felvéve** paramétereket, valamint a **Csoport** rész összes jelölőnégyzetét.
   b. Kattintson a **Frissítés**.

c. A táblázatban megjelennek alkalmazott szűrőknek megfelelő alkalmazások.

d. Jelölje be az **Alkalmazás** oszlopban azokkal az alkalmazásokkal szemben lévő jelölőnégyzeteket, amelyekhez titkosított fájlokra vonatkozó hozzáférési szabályt szeretne kialakítani.

e. Válassza ki a **Szabály az alkalmazásokhoz** legördülő listán azt a szabályt, amely az alkalmazások titkosított fájlokhoz való hozzáférését megszabja.

f. Válassza ki a **Műveletek a korábban kiválasztott alkalmazásokhoz** legördülő listán azt a műveletet, amelyet a Kaspersky Endpoint Security az ilyen alkalmazásokhoz korábban kialakított, titkosított fájlokra vonatkozó hozzáférési szabályokon végez.

Az alkalmazások titkosított fájlokhoz való hozzáférési szabályainak adatai az **Alkalmazások szabályai** lapon lévő táblázatban jelennek meg.

7. Ha kézileg szeretne alkalmazásokat választani, kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki az **Egyéni alkalmazások** elemet.

a. Gépelje be a beviteli mezőbe az alkalmazások végrehajtható fájljainak nevét, illetve a nevek listáját kiterjesztésükkel együtt.

Az alkalmazások végrehajtható fájljainak neveit megadhatja a Kaspersky Security Center listájáról is, ha a **Hozzáadás a Kaspersky Security Center listából** gombra kattint.

b. Szükség esetén a **Leírás** mezőben adja meg az alkalmazások listájának leírását.

c. Válassza ki a **Szabály az alkalmazásokhoz** legördülő listán azt a szabályt, amely az alkalmazások titkosított fájlokhoz való hozzáférését megszabja.

Az alkalmazások titkosított fájlokhoz való hozzáférési szabályainak adatai az **Alkalmazások szabályai** lapon lévő táblázatban jelennek meg.

8. Mentse el a módosításokat.

Adott alkalmazások által létrehozott és módosított fájlok titkosítása

Létrehozhat olyan szabályt, mely alapján a Kaspersky Endpoint Security a szabályban megadott alkalmazások által létrehozott és módosított összes fájlt titkosítja.

A megadott alkalmazások által a titkosítási szabály alkalmazását megelőzően létrehozott, illetve módosított fájlok titkosítására nem kerül sor.

Adott alkalmazások által létrehozott és módosított fájlok titkosításának beállítása:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza ki az **Data Encryption** → **File Level Encryption** lehetőséget.

4. A **Titkosítási mód** legördülő listában válassza ki **A szabályoknak megfelelően** elemet.

   A titkosítási szabályok alkalmazására kizárólag **A szabályoknak megfelelően** módban kerül sor. Ha a titkosítási szabályok **A szabályoknak megfelelően** módban történő alkalmazását követően átvált **Maradjon változatlan** módba, a Kaspersky Endpoint Security minden titkosítási szabályt figyelmen kívül hagy. A korábban titkosított fájlok titkosított állapotban maradnak.

5. Az ablak jobb oldalán válassza ki az **Alkalmazások szabályai** lapot.

6. Ha kizárólag a Kaspersky Security Center listájáról szeretne alkalmazásokat választani, kattintson a **Hozzáadás** gombra, és a legördülő listán válassza ki az **Alkalmazások a Kaspersky Security Center listából** elemet.

   a. Adjon meg szűrőket a táblázatban lévő alkalmazások listájának szűkítéséhez. Ehhez adja meg az **Alkalmazás**, **Forgalmazó** és **Időtartam felvéve** paramétereket, valamint a **Csoport** rész összes jelölőnégyzetét.

   b. Kattintson a **Frissítés**.

      A táblázatban megjelennek alkalmazott szűrőknek megfelelő alkalmazások.

   c. Az **Alkalmazás** oszlopban tegyen jelölést azon alkalmazások jelölőnégyzetébe, amelyek létrehozott fájljait titkosítani szeretné.

   d. A **Szabály az alkalmazásokhoz** legördülő listán válassza ki az **Összes létrehozott fájl titkosítása** elemet.

   e. Válassza ki a **Műveletek a korábban kiválasztott alkalmazásokhoz** legördülő listán azt a műveletet, amelyet a Kaspersky Endpoint Security az ilyen alkalmazásokhoz korábban kialakított, titkosítási szabályokon végez.

   A kiválasztott alkalmazások által létrehozott és módosított fájlok titkosítási szabályára vonatkozó információk az **Alkalmazások szabályai** lapon lévő táblázatban láthatók.

7. Ha kézileg szeretne alkalmazásokat választani, kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki az **Egyéni alkalmazások** elemet.

   a. Gépelje be a beviteli mezőbe az alkalmazások végrehajtható fájljainak nevét, illetve a nevek listáját kiterjesztésükkel együtt.

      Az alkalmazások végrehajtható fájljainak neveit megadhatja a Kaspersky Security Center listájáról is, ha a **Hozzáadás a Kaspersky Security Center listából** gombra kattint.

   b. Szükség esetén a **Leírás** mezőben adja meg az alkalmazások listájának leírását.

   c. A **Szabály az alkalmazásokhoz** legördülő listán válassza ki az **Összes létrehozott fájl titkosítása** elemet.

   A kiválasztott alkalmazások által létrehozott és módosított fájlok titkosítási szabályára vonatkozó információk az **Alkalmazások szabályai** lapon lévő táblázatban láthatók.

8. Mentse el a módosításokat.

Visszafejtési szabály előállítása

Visszafejtési szabály előállítása:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki az **Data Encryption** → **File Level Encryption** lehetőséget.
4. A **Titkosítási mód** legördülő listában válassza ki **A szabályoknak megfelelően** elemet.
5. Kattintson a **Visszafejtés** lapon a **Hozzáadás** gombra, a legördülő listán pedig válassza ki valamelyiket az alábbi elemek közül:
   a. Válassza ki az **Előre megadott mappák** elemet a Kaspersky szakértői által javasolt helyi felhasználói profilok mappáiban lévő fájlok visszafejtési szabályhoz való hozzáadásához.
   b. Válassza ki az **Egyéni mappa** elemet kézileg beírt mappa elérési útvonalának visszafejtési szabályhoz való hozzáadásához.
   c. Válassza a **Fájlok kiterjesztés alapján** elemet, és egyenként hozzáadhatja a fájlkiterjesztéseket a visszafejtési szabályhoz. A Kaspersky Endpoint Security nem titkosítja a megadott kiterjesztésű fájlokat a számítógépen lévő összes helyi meghajtón.
   d. Válassza a **Fájlok kiterjesztéscsoportok alapján** lehetőséget, ha fájlkiterjesztések csoportjait kívánja hozzáadni a visszafejtési szabályhoz (például: *Microsoft Office-dokumentumok*). A Kaspersky Endpoint Security a kiterjesztéscsoportok listáján szereplő kiterjesztéssel rendelkező fájlokat nem titkosítja a számítógép összes helyi meghajtóján.
6. Mentse el a módosításokat.

Ha ugyanaz a fájl bekerült a titkosítási és a visszafejtési szabályba is, a Kaspersky Endpoint Security nem titkosítja, ha nincs titkosítva, és visszafejti, ha titkosítva van.

A számítógép helyi meghajtóin lévő fájlok visszafejtése

Fájlok visszafejtése helyi meghajtókon:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki az **Data Encryption** → **File Level Encryption** lehetőséget.
4. Az ablak bal oldalán válassza ki a **Titkosítás** fület.

5. Távolítsa el a visszafejteni kívánt fájlokat és mappákat a titkosítási listáról. Ehhez válassza ki a fájlokat, majd válassza ki a **Szabály törlése és fájlok visszafejtése** elemet a **Törlés** gomb helyi menüjében.

   A titkosítási listáról eltávolított fájlok és mappák automatikusan a visszafejtési listára kerülnek.

6. Fájlvisszafejtési lista kialakítása.

7. Mentse el a módosításokat.

A rendszabály alkalmazását követően a Kaspersky Endpoint Security azonnal visszafejti a visszafejtési szabályba felvett titkosított fájlokat.

A Kaspersky Endpoint Security akkor fejti vissza a titkosított fájlokat, ha paramétereik (fájl elérési útvonala/neve/kiterjesztése) megváltoznak, és így egyeznek a visszafejtési listára felvett objektumok paramétereivel.

A Kaspersky Endpoint Security a megnyitott fájlok visszafejtését bezárásukig elhalasztja.

Titkosított csomagok létrehozása

Ahhoz, hogy védje az adatait, amikor fájlokat küld a vállalati hálózaton kívül tartózkodó felhasználóknak, használhat titkosított csomagokat. A titkosított csomagok hasznosak lehetnek olyan esetekben, ha nagy méretű fájlokat szeretne átvinni cserélhető meghajtókon, mivel a levelező alkalmazások rendelkezhetnek bizonyos méretkorlátozásokkal.

A titkosított csomagok létrehozása előtt a Kaspersky Endpoint Security jelszót fog kérni a felhasználótól. Az adatai védelme érdekében engedélyezheti a jelszóerősség-meghatározást, illetve megadhatja a jelszóerősség követelményeit. Ez megelőzi, hogy a felhasználók olyan rövid és egyszerű jelszavakat használjanak, mint az `1234`.

A jelszóerősség-meghatározás engedélyezése, ha titkosított archívumokat hoz létre az Adminisztrációs konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza az **Adattitkosítás → Általános titkosítási beállítások** lehetőséget.

4. A **Jelszóbeállítások** területen kattintson a **Beállítások** gombra.

5. A megnyíló ablakban válassza a **Titkosított csomagok** lapot.

6. Adja meg a jelszóösszetettség beállításait, ha létrehoz titkosított csomagokat.

A jelszóerősség-meghatározás engedélyezése, ha titkosított archívumokat hoz létre a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Data Encryption** → **File Level Encryption** elemet.

5. A(z) **Encrypted package password settings** területen konfigurálja a titkosított csomagok létrehozásához szükséges jelszóerősségi feltételeket.

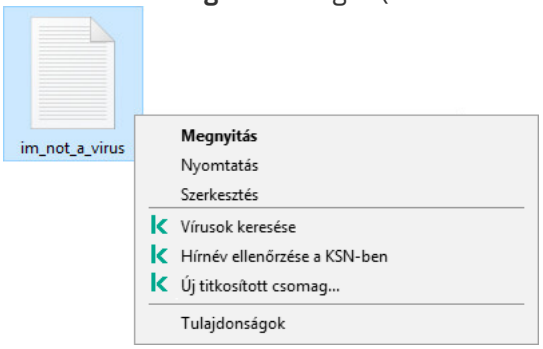
A titkosított csomagokat olyan számítógépeken hozhatja létre, melyek Fájlszintű titkosítást alkalmazó Kaspersky Endpoint Security alkalmazással rendelkeznek.

Egy fájl olyan titkosított csomaghoz történő hozzáadásánál, ami tartalma a OneDrive felhőtárhelyen van, a Kaspersky Endpoint Security letölti a fájl tartalmát, majd végrehajtja a titkosítást.

Titkosított csomag létrehozása:

1. Egy Ön által választott fájlkezelőben válassza ki a fájlokat vagy mappákat, melyeket hozzá kíván adni a titkosított csomaghoz. Az egér jobb gombjával kattintva nyissa meg a helyi menüt.

2. Válassza ki a helyi menüben a **Új titkosított csomag** lehetőséget (lásd az alábbi ábrát).



Titkosított csomag létrehozása

3. A megnyíló ablakban adja meg a jelszót, majd erősítse meg azt.

   A jelszónak meg kell felelnie a rendszabályban meghatározott összetettségi kritériumoknak.

4. Kattintson a **Létrehozás** lehetőségre.

   Elindul a titkosított csomag létrehozásának folyamata. A Kaspersky Endpoint Security nem végez fájltömörítést a titkosított csomagok létrehozása során. Ha a folyamat befejeződik, az önkicsomagoló, jelszóval védett titkosított csomag (egy futtatható fájl .exe kiterjesztéssel –) létre lesz hozva a kiválasztott célmappába.

Ahhoz, hogy elérje a titkosított csomagban lévő fájlokat, kattintson rá duplán, hogy elindítsa a Kicsomagoló varázslót, majd adja meg a jelszót. Ha elfelejtette vagy elvesztette jelszavát, akkor nem lehet visszaállítani azt, illetve a titkosított csomagban lévő fájlokhoz való hozzáférést. Újra létrehozhatja a titkosított csomagot.

Titkosított fájlok hozzáférésének helyreállítása

Ha a fájlok titkosítva vannak, a Kaspersky Endpoint Security megkapja a titkosított fájlok közvetlen eléréséhez szükséges titkosítási kulcsot. A titkosítási kulcs segítségével a fájltitkosítás közben aktív bármely Windows felhasználói fiókban dolgozó felhasználó közvetlenül hozzáférhet a titkosított fájlokhoz. A fájltitkosítás közben inaktív Windows fiókokban dolgozó felhasználóknak a titkosított fájlokhoz való hozzáféréshez kapcsolódniuk kell a Kaspersky Security Centerhez.

Az alábbi körülmények esetén előfordulhat, hogy a titkosított fájlok nem hozzáférhetők:

- A felhasználó számítógépe tárolja a titkosítási kulcsokat, de nincs kapcsolat a Kaspersky Security Centerrel, ami a kezelésükhöz lenne szükséges. Ilyenkor a felhasználónak a titkosított fájlokhoz hozzáférést kell kérnie a helyi hálózati rendszergazdától.

  Ha a Kaspersky Security Center nem elérhető, az alábbi a teendő:

  - hozzáférési kulcs kérése a számítógép merevlemezein lévő titkosított fájlokhoz való hozzáféréshez;
  - a cserélhető meghajtókon tárolt titkosított fájlokhoz való hozzáféréshez az egyes cserélhető meghajtókon lévő titkosított fájlokhoz külön-külön hozzáférési kulcsot kell kérni.

- A titkosítási összetevők törlődnek a felhasználó számítógépéről. Ilyenkor a felhasználó a helyi és cserélhető lemezeken lévő titkosított fájlokat megnyithatja, de tartalmuk titkosítottan jelenik meg.

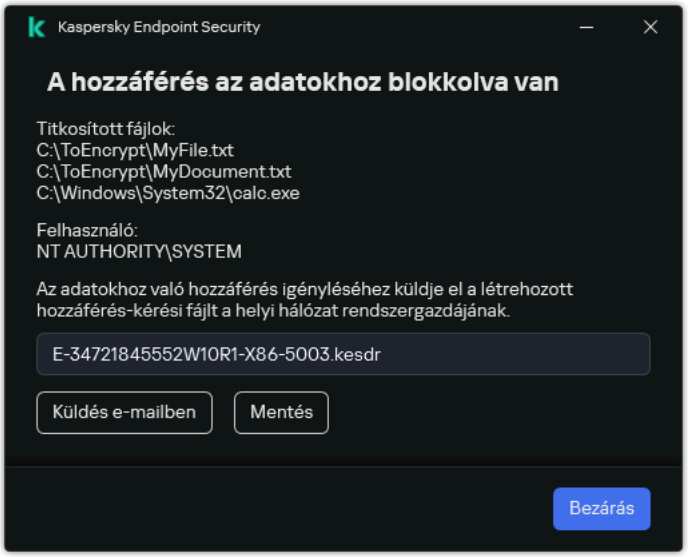
  A felhasználó az alábbi körülmények esetén dolgozhat titkosított fájlokkal:

  - Olyan számítógépen létrehozott titkosított csomagokba helyezett fájlok, amelyeken telepítve van a Kaspersky Endpoint Security.
  - A fájlok olyan cserélhető meghajtókra kerülnek mentésre, amelyeken engedélyezve van a hordozható mód.

A titkosított fájlokhoz való hozzáférés érdekében a felhasználónak el kell indítania a helyreállítási eljárást (kérelem–válasz).

A titkosított fájlok hozzáférhetőségének helyreállítása a következő lépésekből áll:

1. A felhasználó hozzáférés-kérési fájlt küld a rendszergazdának (részletek az alábbi ábrán).
2. A rendszergazda hozzáadja a hozzáférés-kérési fájlt a Kaspersky Security Centerhez, létrehoz egy hozzáférésikulcs-fájlt, majd elküldi a fájlt a felhasználónak.
3. A felhasználó a hozzáférésikulcs-fájlt hozzáadja a Kaspersky Endpoint Security alkalmazáshoz, és hozzáférést kap a fájlokhoz.



Titkosított fájlok hozzáférésének helyreállítása

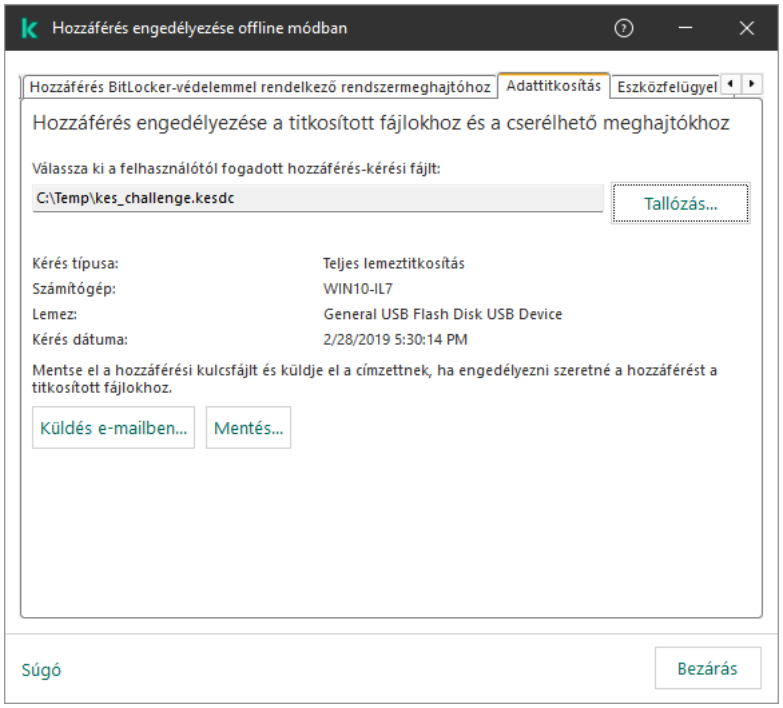
A helyreállítási eljárás elindításához a felhasználónak meg kell kísérelnie hozzáférni egy fájlhoz. Ekkor a Kaspersky Endpoint Security létrehoz egy hozzáférés-kérési fájlt (KESDC kiterjesztéssel), amelyet a felhasználónak el kell küldenie a rendszergazdának, például e-mailben.

A Kaspersky Endpoint Security hozzáférés-kérési fájlt hoz létre a számítógép (helyi vagy cserélhető) meghajtóján tárolt titkosított fájlok mindegyikéhez tartozóan.

Titkosítottadat-hozzáférési kulcsfájl beszerzésének menete az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Devices** lehetőséget.
3. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
4. A helyi menüben válassza ki a **Hozzáférés engedélyezése offline módban** elemet.
5. A megnyíló ablakban válassza az **Adattitkosítás** lapot.
6. Az **Adattitkosítás** lapon kattintson a **Browse** gombra.
7. A hozzáférés-kérési fájl kiválasztására szolgáló ablakban adja meg a felhasználótól kapott fájl elérési útját.

A felhasználó kérésére vonatkozó információ válik láthatóvá. A Kaspersky Security Center létrehoz egy kulcsfájlt. Küldje el e-mailben a létrehozott titkosítottadat-hozzáférési kulcsfájlt a felhasználónak. Másik megoldásként mentse a hozzáférési fájlt, és használjon tetszés szerinti módszert a fájl továbbításához.



Hozzáférés engedélyezése offline módban

Titkosítottadat-hozzáférési kulcsfájl beszerezésének menete a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Assets (Devices)** lehetőséget.
2. Tegyen jelölést annak a számítógépnek a neve mellé, amelynek adataihoz szeretné visszaállítani a hozzáférést.

3. Kattintson az **Grant access to the device in offline mode** gombra.

4. Válassza a **Data Encryption** lehetőséget.

5. Kattintson a **Select file** gombra, és válassza ki azt a hozzáférés-kérési (KESDC kiterjesztésű) fájlt, amelyet a felhasználótól kapott.

   A Web Console a kérésre vonatkozó információkat jelenít meg. Ezek között szerepel annak a számítógépnek a neve, amelyen a felhasználó hozzáférést kér a fájlhoz.

6. Kattintson a **Save key** gombra, és válassza ki azt a mappát, amelybe a titkosítottadat-hozzáférési (KESDR kiterjesztésű) kulcsfájlt menteni szeretné.

Ekkor beszerezheti titkosítottadat-hozzáférési kulcsot, amelyet továbbítania kell a felhasználónak.

A titkosítottadat-hozzáférési fájl megszerzését követően a felhasználónak – dupla kattintással – futtatnia kell a fájlt. Ezt követően a Kaspersky Endpoint Security hozzáférést biztosít a meghajtón tárolt összes titkosított fájlhoz. A más meghajtókon tárolt titkosított fájlokhoz eléréséhez meghajtónként külön hozzáférési kulcsfájlt kell beszerezni.

Titkosított adatokhoz való hozzáférés visszaállítása az operációs rendszer hibáját követően

Operációs rendszerhiba után csak fájlszintű titkosítás (FLE) esetén állíthatja vissza az adatokat. Nem állíthatja vissza az adatok elérését, ha teljes lemeztitkosítást (FDE) használ.

Titkosított adatokhoz való hozzáférés visszaállításához az operációs rendszer hibáját követően:

1. Telepítse újra az operációs rendszert a merevlemez formázása nélkül.

2. Telepítse a Kaspersky Endpoint Security alkalmazást.

3. Kapcsolat létrehozása a számítógép és a számítógép által vezérelt Kaspersky Security Center felügyeleti kiszolgálója között, amikor az adatok titkosítva voltak.

A titkosított adatokhoz való hozzáférés megadásának ugyanazok a feltételei, mint amelyek az operációs rendszer hibája előtt voltak érvényben.

A titkosított fájlokhoz való hozzáférés üzenetsablonjainak szerkesztése

A titkosított fájlokhoz való hozzáférés üzenetsablonjainak szerkesztése:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabály ablakában válassza az **Adattitkosítás → Általános titkosítási beállítások** lehetőséget.

4. A megnyíló **Sablonok** részen kattintson a **Sablonok** gombra.

5. A megnyíló ablakban tegye a következőket:

   - Ha a felhasználói üzenetsablont szeretné szerkeszteni, válassza ki a **Felhasználó üzenete** lapot. A következő ablak akkor jelenik meg, ha a felhasználó egy titkosított fájlhoz próbál hozzáférni úgy, hogy a számítógépen nem található a titkosított fájlokhoz való hozzáféréshez szükséges kulcs (lásd az alábbi ábrát). A **Küldés e-mailben** gombra kattintva automatikusan létrehozhat egy felhasználói üzenetet. Ezt az üzenetet a vállalati helyi hálózati rendszergazda kapja meg a titkosított fájlokhoz való hozzáférést kérő fájllal együtt.

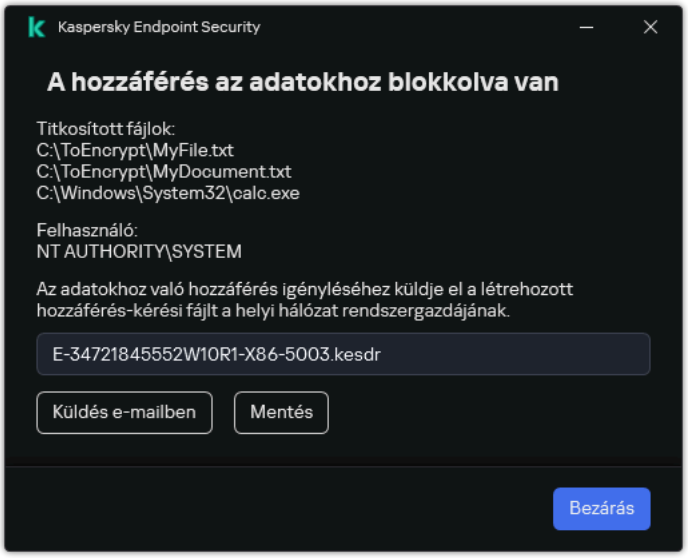
   - Ha a rendszergazdai üzenetsablont szeretné szerkeszteni, válassza ki a **Rendszergazda üzenete** lapot. Ezt az üzenetet a felhasználó a titkosított fájlokhoz való hozzáférés engedélyezése után kapja meg.

6. Szerkessze az üzenetsablonokat.

   Ha változót szeretne hozzáadni a sablon szövegéhez, vigye a kurzort a kívánt helyre, és kattintson a **Változó** gombra, majd válassza ki a kívánt változót az elérhető opciók listájából.

   Az alapértelmezett sablonszöveget az **Alapértelmezés szerint** gombra kattintva is visszaállíthatja.

7. Mentse el a módosításokat.



Titkosított fájlok hozzáférésének helyreállítása

Cserélhető meghajtók titkosítása

Az ARM-alapú számítógépek nem támogatják a cserélhető meghajtók titkosítását.

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

A Kaspersky Endpoint Security a FAT32 fájlok és az NTFS fájlrendszerek titkosítását támogatja. Ha egy nem támogatott fájlrendszerű cserélhető meghajtó van csatlakoztatva a számítógéphez, a cserélhető meghajtó titkosítási feladata hibás lesz, a Kaspersky Endpoint Security pedig csak olvasható állapotot rendel a cserélhető meghajtóhoz.

A cserélhető meghajtón tárolt adatok védelme érdekében a következő titkosítási típusokat használhatja:

- Full Disk Encryption (FDE).

  A teljes cserélhető meghajtó titkosítása, annak fájlrendszerét is beleértve.

  > Nincs mód a titkosított adatok elérésére a vállalati hálózaton kívülről. A titkosított adatok elérése a vállalti hálózaton belül sem lehetséges, ha a számítógép nincs csatlakoztatva a Kaspersky Security Centerhez (pl „vendég" számítógépen).

- File Level Encryption (FLE).

  Csak a fájlok titkosítása egy cserélhető meghajtón. A fájlrendszer változatlan marad.

  > A cserélhető meghajtón tárolt fájlok titkosítása lehetőséget biztosít az adatok elérésére a vállalati hálózaton kívülről egy speciális mód, az úgynevezett *hordozható mód* segítségével.

A titkosítási folyamat során a Kaspersky Endpoint Security főkulcsot hoz létre. A Kaspersky Endpoint Security a következő tárhelyekre menti a főkulcsot:

- Kaspersky Security Center.
- A felhasználó számítógépe.

  A főkulcs titkosítása a felhasználó titkos kulcsával történik.

- Cserélhető meghajtó.

  A főkulcs titkosítása a Kaspersky Security Center nyilvános kulcsával történik.

A titkosítás befejezését követően a cserélhető meghajtón tárolt adatok a vállalati hálózaton belülről úgy érhetők el, mintha szokványos cserélhető meghajtóról lenne szó, titkosítás nélkül.

A titkosított adatok elérése

Titkosított adatokat tartalmazó cserélhető meghajtó csatlakoztatásakor a Kaspersky Endpoint Security a következő műveleteket hajtja végre:

1. Ellenőrzi a főkulcs meglétét a felhasználó számítógépének helyi adattárolóján.

   Ha a főkulcs megtalálható, a felhasználó hozzáférést kap a cserélhető meghajtón tárolt adatokhoz.

   Ha nem található a főkulcs, a Kaspersky Endpoint Security a következő műveleteket hajtja végre:

   a. Kérelmet küld a Kaspersky Security Center felé.

      A kérelem beérkezését követően a Kaspersky Security Center választ küld, amely tartalmazza a főkulcsot.

   b. A Kaspersky Endpoint Security menti a főkulcsot a felhasználó számítógépének helyi adattárolójában a titkosított cserélhető meghajtón később végzett műveletekhez.

2. Visszafejti az adatokat.

A cserélhető meghajtó titkosításának speciális jellemzői

A cserélhető meghajtók titkosításának folyamata a következő speciális jellemzőkkel bír:

- A cserélhető meghajtók titkosításának előre megadott beállításait tartalmazó rendszabály a kezelt számítógépek egy adott csoportja számára van kialakítva. Emiatt a cserélhető meghajtók titkosításához és visszafejtéséhez beállított Kaspersky Security Center-rendszabály alkalmazásának eredménye attól a számítógéptől függ, amelyhez a cserélhető meghajtót csatlakoztatja.
- A Kaspersky Endpoint Security a cserélhető meghajtókon tárolt csak olvasható fájlokat nem titkosítja és nem fejti vissza.
- Az alábbi eszköztípusok cserélhető meghajtókként vannak támogatva:
  - USB buszon keresztül csatlakoztatott adathordozók
  - USB és FireWire buszokon keresztül csatlakoztatott merevlemezek
  - USB és FireWire buszokon keresztül csatlakoztatott SSD-meghajtók

Cserélhető meghajtók titkosításának megkezdése

Lehetősége van rendszabály segítségével visszafejteni egy cserélhető meghajtó tartalmát. A rendszer létrehoz rendszabályt egy adott adminisztrációs csoport számára, amelyben a cserélhető meghajtók titkosítására vonatkozó beállítások szerepelnek. Emiatt az adatvisszafejtés eredménye cserélhető meghajtókon attól a számítógéptől függ, amelyhez a cserélhető meghajtót csatlakoztatja.

A Kaspersky Endpoint Security a FAT32 fájlok és az NTFS fájlrendszerek titkosítását támogatja. Ha egy nem támogatott fájlrendszerű cserélhető meghajtó van csatlakoztatva a számítógéphez, a cserélhető meghajtó titkosítási feladata hibás lesz, a Kaspersky Endpoint Security pedig csak olvasható állapotot rendel a cserélhető meghajtóhoz.

Mielőtt titkosítaná a fájlokat egy cserélhető meghajtón, győződjön meg arról, hogy a meghajtó formázva van, és nincsenek rejtett partíciók (például EFI rendszerpartíció). Ha a meghajtó formázatlan vagy rejtett partíciókat tartalmaz, előfordulhat, hogy a fájltitkosítás hibával meghiúsul.

Cserélhető meghajtók titkosítása:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás → Cserélhető meghajtók titkosítása** lehetőséget.

4. A **Titkosítási mód** legördülő listából válassza ki azt az alapértelmezett tevékenységet, amit a Kaspersky Endpoint Security alkalmazásnak a cserélhető meghajtókon kell elvégeznie:

   - **Teljes cserélhető meghajtó titkosítása** (FDE). A Kaspersky Endpoint Security szektoronként titkosítja a cserélhető meghajtó tartalmát. Ezért az alkalmazás nem csak a tárolt fájlokat titkosítja a cserélhető meghajtókon, de a fájlrendszereket is, köztük a cserélhető meghajtón lévő neveket és mappaszerkezeteket is.

   - **Összes fájl titkosítása** (FLE). A Kaspersky Endpoint Security minden fájlt titkosít a cserélhető meghajtókon. Az alkalmazás nem titkosítja a cserélhető meghajtók fájlrendszereit, köztük fájlok neveit és a mappaszerkezeteket.

   - **Csak az új fájlok titkosítása** (FLE). A Kaspersky Endpoint Security csak azon fájlokat titkosítja, amik hozzá lettek adva a cserélhető meghajtókhoz, vagy ott voltak tárolva, és a legutóbbi Kaspersky Security Center rendszabály alkalmazása után módosítva voltak.

   A Kaspersky Endpoint Security a már titkosított cserélhető meghajtókat nem titkosítja ismét.

5. Ha a hordozható módot használná a cserélhető meghajtók titkosításához, tegyen jelölést a **Hordozható mód** jelölőnégyzetbe.

   A *Hordozható mód* a fájlok titkosításának egy módja (FLE) olyan cserélhető meghajtók esetében, amely az adatok elérését a szervezeti hálózaton kívülről biztosítja. A hordozható mód azt is lehetővé teszi, hogy a titkosított adatokkal olyan számítógépen dolgozzon, amelyen nincs telepítve Kaspersky Endpoint Security.

6. Ha egy új cserélhető meghajtót szeretne titkosítani, akkor javasolt kijelölni a **Csak a használt lemezterület titkosítása** jelölőnégyzetet. A jelölőnégyzet törlése esetén a Kaspersky Endpoint Security minden fájlt titkosít, köztük a törölt vagy módosított fájlok fennmaradt részeit.

7. Ha konfigurálni szeretné az egyéni cserélhető meghajtót titkosítását, akkor adjon meg titkosítási szabályokat.

8. Ha a cserélhető meghajtók teljes lemeztitkosítását offline módban szeretné elvégezni, jelölje be a **Cserélhető meghajtók titkosításának engedélyezése offline módban** jelölőnégyzetet.

   Az *Offline titkosítási mód* a cserélhető meghajtók titkosítását (FDE) jelenti, ha nincs kapcsolat a Kaspersky Security Centerrel. A titkosítás során a Kaspersky Endpoint Security csak a felhasználói számítógépen menti el a főkulcsot. A Kaspersky Endpoint Security elküldi a főkulcsot a Kaspersky Security Center számára a következő titkosítás során.

   Ha a számítógép, amin a főkulcs el van mentve, fertőzött, és az adatok nem lettek elküldve a Kaspersky Security Center számára, akkor nem lehetséges elérni a cserélhető meghajtókat.

   Ha eltávolítja a **Cserélhető meghajtók titkosításának engedélyezése offline módban** jelölőnégyzet bejelölését, és nincs kapcsolat a Kaspersky Security Centerrel, akkor a cserélhető meghajtók titkosítása nem lehetséges.

9. Mentse el a módosításokat.

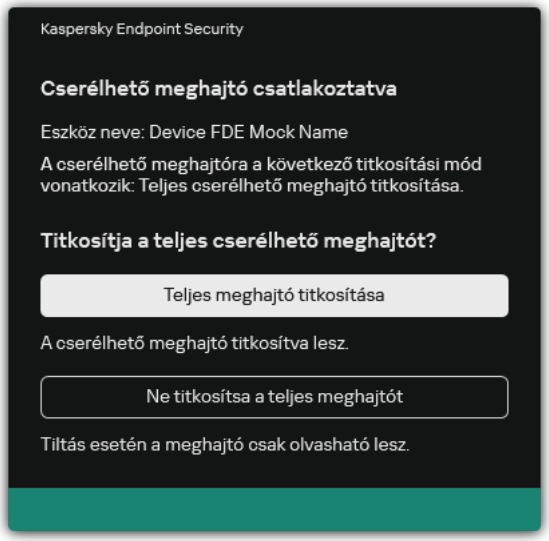
A rendszabály alkalmazása után, ha a felhasználó csatlakozik egy cserélhető meghajtóhoz, vagy egy cserélhető meghajtó már csatlakoztatva van, a Kaspersky Endpoint Security a felhasználó megerősítését kéri, hogy titkosítási műveletet végezzen el (lásd az alábbi ábrát).

Az alkalmazás a következő műveletek elvégzését teszi lehetővé:

- Ha a felhasználó megerősíti a titkosítási kérelmet, a Kaspersky Endpoint Security titkosítja az adatokat.
- Ha a felhasználó elutasítja a titkosítási kérelmet, a Kaspersky Endpoint Security változatlanul hagyja az adatokat, és csak olvasható elérést ad a cserélhető meghajtónak.
- Ha a felhasználó nem válaszol a titkosítási kérelemre, a Kaspersky Endpoint Security változatlanul hagyja az adatokat, és csak olvasható elérést ad a cserélhető meghajtónak. Az alkalmazás ismét megerősítést kér, ha újabb rendszabályt alkalmaz, vagy ha legközelebb csatlakoztatja a jelen cserélhető meghajtót.

Ha az adatok titkosítása közben a felhasználó a cserélhető meghajtó biztonságos eltávolítását kezdeményezi, a Kaspersky Endpoint Security megszakítja az adattitkosítási folyamatot, és a titkosítási művelet befejezése előtt lehetővé teszi a cserélhető meghajtó eltávolítását. Az adattitkosítás folytatódik, ha legközelebb csatlakozik a számítógéphez ez a cserélhető meghajtó.

Ha sikertelen egy cserélhető meghajtó titkosítása, tekintse meg az **Adattitkosítás** jelentését a Kaspersky Endpoint Security felületén. A fájlok elérését blokkolhatja egy másik alkalmazás. Ebben az esetben próbálja meg kihúzni a cserélhető meghajtót a számítógépből, majd dugja be újra.



Cserélhető meghajtó titkosítási kérelem

Titkosítási szabály megadása cserélhető meghajtóknál

Titkosítási szabály megadása cserélhető meghajtóknál:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.

4. Kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki valamelyiket az alábbi elemek közül:

   - Ha olyan cserélhető meghajtóknál szeretne titkosítási szabályokat megadni, amelyek szerepelnek az Eszközfelügyelő összetevő megbízható eszközök listáján, válassza ki az **Ezen házirend megbízható eszközeinek listájából** lehetőséget.

   - Ha olyan cserélhető meghajtóknál szeretne titkosítási szabályokat megadni, amelyek szerepelnek a Kaspersky Security Center listáján, válassza ki a **A Kaspersky Security Center eszközlistájából** lehetőséget.

5. Válassza ki a **Titkosítási mód a kiválasztott eszközökhöz** legördülő listán azt a műveletet, amelyet a Kaspersky Endpoint Security a kiválasztott cserélhető meghajtókon tárolt fájlokon végez.

6. Jelölje be a **Hordozható mód** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security a titkosítás előtt készítse elő a cserélhető meghajtókat, és így hordozható módban is használni lehessen a rajtuk tárolt fájlokat.

   A hordozható mód révén használhatja az olyan cserélhető meghajtókon tárolt titkosított fájlokat, amelyeket titkosítási funkcióval nem rendelkező számítógépekhez csatlakoztat.

7. Jelölje be a **Csak a használt lemezterület titkosítása** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security csak a fájlok által elfoglalt lemezszektorokat titkosítsa.

   Ha már használatban lévő meghajtón alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről – még a korábban törölt, de esetleg visszanyerhető információt hordozó adatokéról is. A **Csak a használt lemezterület titkosítása** funkció új, korábban nem használt meghajtók esetén javasolt.

   Ha egy eszköz titkosítására korábban már sor került a **Csak a használt lemezterület titkosítása** funkcióval, akkor a **Teljes cserélhető meghajtó titkosítása** módú rendszabály alkalmazását követően a fájlok által el nem foglalt szektorok továbbra sem lesznek titkosítva.

8. Válassza ki a **Műveletek a korábban kiválasztott eszközökhöz** legördülő listán azt a műveletet, amelyet a Kaspersky Endpoint Security a cserélhető meghajtókhoz korábban megadott titkosítási szabályok szerint végez:

   - Ha azt szeretné, hogy a cserélhető meghajtó korábban létrehozott titkosítási szabálya változatlanul maradjon, válassza a **Átugrás** lehetőséget.

   - Ha azt szeretné, hogy a cserélhető meghajtó korábban létrehozott titkosítási szabályát az új szabály felváltsa az új, válassza a **Frissítés** lehetőséget.

9. Mentse el a módosításokat.

A cserélhető meghajtóra vonatkozóan hozzáadott titkosítási szabályokat a rendszer minden olyan cserélhető meghajtóra alkalmazza, amelyet a szervezet bármely számítógépéhez csatlakoztatnak.

Cserélhető meghajtók titkosítási szabályait tartalmazó lista exportálása és importálása

A cserélhető meghajtók titkosítási szabályainak listáját exportálhatja egy XML-fájlba. Ezután módosíthatja a fájlt, például nagyszámú szabály hozzáadásával azonos típusú cserélhető meghajtókhoz. Használhatja az exportálás/importálás funkciót a szabályok biztonsági mentésének létrehozásához, vagy a szabályok egy másik kiszolgálóra való áttelepítéséhez is.

A cserélhető meghajtó titkosítási szabályait tartalmazó lista exportálása és importálása az Adminisztrációs konzolban (MMC)

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption** → **Encryption of removable drives** elemet.
5. A **Encryption rules for selected devices** részen kattintson a **<N> rules** hivatkozásra.

   Ez megnyitja a cserélhető meghajtók titkosítási szabályainak listáját.
6. Cserélhető meghajtók titkosítási szabályait tartalmazó lista exportálása:

   a. Jelölje ki az exportálni kívánt szabályokat.

   b. Kattintson az **Export** gombra.

   c. Erősítse meg, hogy csak a kijelölt szabályokat, vagy a teljes listáját szeretné exportálni.

   d. Mentse a fájlt.

   A Kaspersky Endpoint Security a szabályok listáját egy XML-fájlba exportálja az alapértelmezett letöltési mappában.
7. A szabályok listájának importálása:

   a. Kattintson a **Import** hivatkozásra.

   A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.

   b. Nyissa meg a fájlt.

   Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.
8. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.
4. Cserélhető meghajtók titkosítási szabályait tartalmazó lista exportálása:

   a. Jelölje ki az exportálni kívánt szabályokat. Több port kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.

   Ha nem jelölt ki szabályt, a Kaspersky Endpoint Security az összes szabályt exportálja.

   b. Kattintson az **Exportálás** hivatkozásra.

   c. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a szabályok listáját, és válassza a fájl mentésére kiszemelt mappát.

d. Mentse a fájlt.

A Kaspersky Endpoint Security exportálja a szabályok listáját az XML-fájlba.

5. Cserélhető meghajtók titkosítási szabályait tartalmazó lista importálása:

a. Kattintson az **Import** hivatkozásra.

A megnyíló ablakban válassza ki azt az XML-fájlt, amelyből importálni szeretné a szabályok listáját.

b. Nyissa meg a fájlt.

Ha a számítógépen már létezik egy lista a szabályokról, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba a XML-fájlból.

6. Mentse el a módosításokat.

Hordozható mód a cserélhető meghajtókon lévő titkosított fájlok eléréséhez

A *Hordozható mód* a fájlok titkosításának egy módja (FLE) olyan cserélhető meghajtók esetében, amely az adatok elérését a szervezeti hálózaton kívülről biztosítja. A hordozható mód azt is lehetővé teszi, hogy a titkosított adatokkal olyan számítógépen dolgozzon, amelyen nincs telepítve Kaspersky Endpoint Security.

A hordozható mód kényelmes használatot biztosít a következő esetekben:

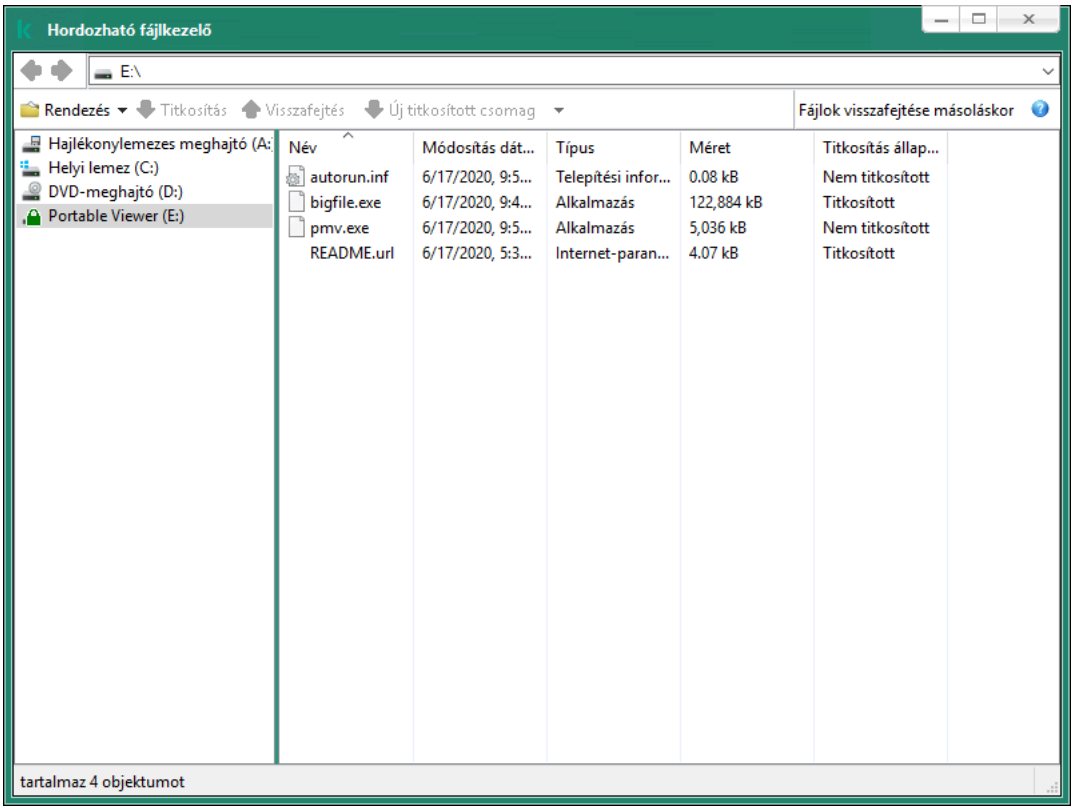
- ha nincs kapcsolat a számítógép és a Kaspersky Security Center felügyeleti kiszolgáló között;
- ha megváltozott az infrastruktúra a Kaspersky Security Center felügyeleti kiszolgáló módosításakor;
- ha a Kaspersky Endpoint Security nincs telepítve a számítógépre.

Hordozható fájlkezelő

A hordozható módban történő munkavégzéshez a Kaspersky Endpoint Security egy speciális, *Hordozható fájlkezelő* nevű titkosítási modult telepít egy cserélhető meghajtóra. A Hordozható fájlkezelő kezelőfelületet biztosít a titkosított adatokkal végzett munkához arra az esetre, ha a számítógépre nincs telepítve Kaspersky Endpoint Security (részletek az alábbi ábrán). Ha a Kaspersky Endpoint Security telepítve van a számítógépre, dolgozhat a titkosított cserélhető meghajtó tartalmán a szokványos fájlkezelő (például az Intéző) segítségével.

A Hordozható fájlkezelő egy kulcsot tárol a cserélhető meghajtón található fájlok titkosításához. A kulcs titkosítása a felhasználó jelszavával történik. A felhasználó beállít egy jelszót a cserélhető meghajtón tárolt fájlok titkosítása előtt.

A Hordozható fájlkezelő automatikusan elindul, amikor a cserélhető meghajtót csatlakoztatják olyan számítógéphez, amelyen nincs telepítve Kaspersky Endpoint Security. Ha az alkalmazások automatikus indítása le van tiltva a számítógépen, kézzel indítsa el a Hordozható fájlkezelőt. Ehhez futtassa a cserélhető meghajtón tárolt pmv.exe nevű fájlt.



Hordozható fájlkezelő

A hordozható mód támogatása a titkosított fájlokkal végzett munkához

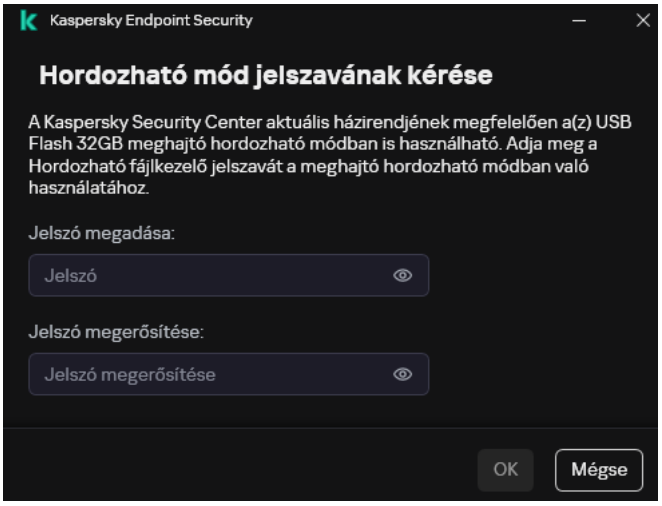
A hordozható mód támogatásának bekapcsolása cserélhető meghajtón tárolt, titkosított fájlokkal végzett munka érdekében az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.
4. A **Titkosítási mód a kiválasztott eszközökhöz** legördülő listában válassza az **Összes fájl titkosítása** vagy a **Csak az új fájlok titkosítása** lehetőséget.

   A hordozható mód kizárólag a fájlszintű titkosítás (FLE) esetében érhető el. Nincs mód a hordozható mód támogatására aktiválására FDE (Full Disk Encryption – Teljes lemeztitkosítás) esetén.

5. Jelölje be a **Hordozható mód** jelölőnégyzetet.
6. Ha szükséges, adjon hozzá titkosítási szabályokat az egyes cserélhető meghajtókhoz.
7. Mentse el a módosításokat.
8. A rendszabály alkalmazását követően csatlakoztassa a cserélhető meghajtót a számítógéphez.
9. Erősítse meg a cserélhető meghajtó titkosítási műveletét.

Ekkor megnyílik egy ablak, amelyben jelszót hozhat létre a Hordozható fájlkezelő számára.



Hordozható mód jelszavának kérése

10. Adjon meg a jelszóerősségi követelményeknek megfelelő jelszót, és erősítse meg.
11. Mentse el a módosításokat.

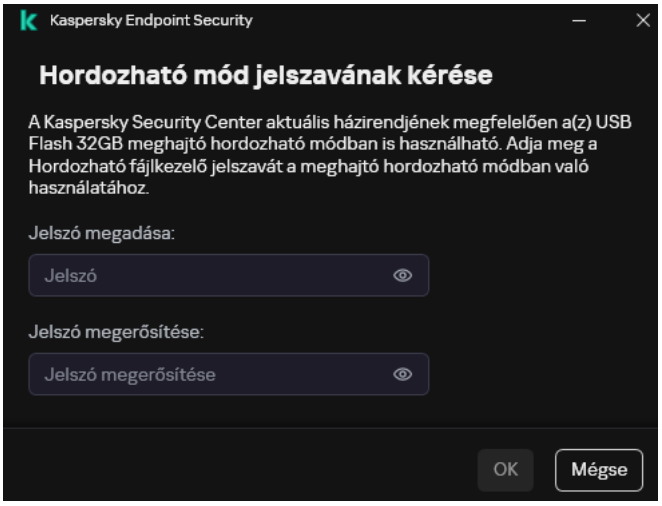
A hordozható mód támogatásának bekapcsolása a Web Console-ban a cserélhető meghajtón tárolt, titkosított fájlokkal végzett munka érdekében.

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Data Encryption** → **Encryption of removable drives** elemet.
5. Az **Default action** területen válassza a **Encrypt all files** vagy a **Encrypt new files only** opciót.

   A hordozható mód kizárólag a fájlszintű titkosítás (FLE) esetében érhető el. Nincs mód a hordozható mód támogatására aktiválására FDE (Full Disk Encryption – Teljes lemeztitkosítás) esetén.

6. Tegyen jelölést a **Portable mode** jelölőnégyzetbe.
7. Ha szükséges, adjon hozzá titkosítási szabályokat az egyes cserélhető meghajtókhoz.
8. Mentse el a módosításokat.
9. A rendszabály alkalmazását követően csatlakoztassa a cserélhető meghajtót a számítógéphez.
10. Erősítse meg a cserélhető meghajtó titkosítási műveletét.

Ekkor megnyílik egy ablak, amelyben jelszót hozhat létre a Hordozható fájlkezelő számára.



Hordozható mód jelszavának kérése

11. Adjon meg a jelszóerősségi követelményeknek megfelelő jelszót, és erősítse meg.

12. Mentse el a módosításokat.

A Kaspersky Endpoint Security titkosítja a fájlokat a cserélhető meghajtón. A rendszer a titkosított fájlokkal való munkavégzéshez használt Hordozható fájlkezelőt is felveszi a cserélhető meghajtóra. Ha már eleve van titkosított fájl a cserélhető meghajtón, a Kaspersky Endpoint Security újra titkosítja azokat a saját kulcsával. Ez lehetővé teszi a felhasználó számára, hogy hordozható módban hozzáférjen minden fájlhoz.

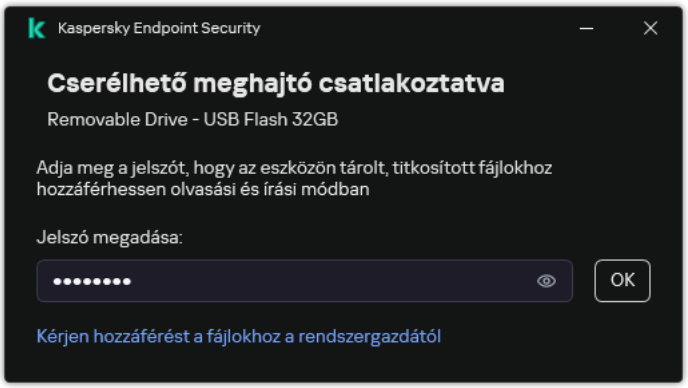
Titkosított fájlok elérése cserélhető meghajtón

Ha megtörtént a fájlok titkosítása a cserélhető meghajtón a hordozható mód támogatása mellett, a következő hozzáférési módok állnak rendelkezésre:

- Ha a Kaspersky Endpoint Security nincs telepítve a számítógépre, a Hordozható fájlkezelő párbeszédpanelben kéri jelszó megadását. Minden alkalommal meg kell adnia jelszót, ha újraindítja a számítógépet vagy újracsatlakoztatja a cserélhető meghajtót.

- Ha a számítógép fizikailag nem része a vállalati hálózatnak, és a Kaspersky Endpoint Security telepítve van a számítógépre, az alkalmazás arra kéri, hogy adjon meg jelszót, vagy küldjön fájlhozzáférési kérelmet a rendszergazdának. A cserélhető meghajtón található fájlok elérhetővé válását követően a Kaspersky Endpoint Security menti a titkos kulcsot a számítógép kulcstárolójában. Ez lehetővé teszi a fájlok későbbi elérését a jelszó megadása, illetve a rendszergazdának küldött kérés nélkül (lásd az alábbi ábrát).

- Ha a számítógép fizikailag csatlakozik a vállalati hálózathoz, és a Kaspersky Endpoint Security telepítve van a számítógépre, Ön hozzáférhet az eszközhöz jelszó megadása nélkül. A Kaspersky Endpoint Security megkapja a titkos kulcsot a Kaspersky Security Center felügyeleti kiszolgálótól, amelyhez a számítógép csatlakoztatva van.



Titkosított fájlok elérése cserélhető meghajtón

A hordozható módban történő munkavégzés jelszavának helyreállítása

Ha elfelejtette a hordozható módban történő munkavégzéshez szükséges jelszót, csatlakoztatnia kell a cserélhető meghajtót a vállalati hálózat olyan számítógépéhez, amelyre telepítve van a Kaspersky Endpoint Security. Ezzel hozzáférést kap a fájlokhoz, ugyanis a titkos kulcs megtalálható a számítógép kulcstárolójában vagy az adminisztrációs kiszolgálón. Visszafejtheti és újra titkosíthatja a fájlokat új jelszóval.

A hordozható mód funkciói, ha a cserélhető meghajtót másik hálózatról származó számítógéphez csatlakoztatja

Ha a számítógép nem csatlakozik a vállalati hálózathoz, és a Kaspersky Endpoint Security telepítve van a számítógépre, Ön hozzáférhet az eszközhöz jelszó megadása nélkül.

- **Jelszóalapú hozzáférés**

  A jelszó megadása után lehetősége lesz megtekinteni, módosítani és menteni a cserélhető meghajtó fájljait (*átlátható hozzáférés*). A Kaspersky Endpoint Security megszabhat „csak olvasható” hozzáférési jogosultságot a cserélhető meghajtó esetében, ha a következő paraméterek vannak beállítva a cserélhető meghajtók titkosítására vonatkozó házirend-beállításokban:

  - A hordozható mód támogatása ki van kapcsolva.
  - Az **Összes fájl titkosítása** vagy **Csak az új fájlok titkosítása** üzemmód van kiválasztva.

  Minden más esetben teljes körű hozzáférést kap a cserélhető meghajtó fájljaihoz (olvasás/írás jogosultságot). Lehetősége lesz fájlok hozzáadására és törlésére is.

  Ön olyankor is módosíthatja a cserélhető meghajtó hozzáférési jogosultságait, amikor a cserélhető meghajtó a számítógéphez van csatlakoztatva. Ha a cserélhető meghajtó hozzáférési jogosultságai megváltoznak, a Kaspersky Endpoint Security letiltja a hozzáférést a fájlokhoz és felszólítja Önt a jelszó ismételt megadására.

  A jelszó megadása után nem fogja tudni a titkosítási házirendek beállításait alkalmazni a cserélhető meghajtóra. Ebben az esetben nem lehetséges a cserélhető meghajtó fájljainak a visszafejtése és az ismételt titkosítása.

- **A fájlokhoz a rendszergazdától kérjen hozzáférést**

Ha elfelejtette a hordozható módban történő munkavégzéshez szükséges jelszót, kérjen hozzáférést a fájlokhoz a rendszergazdától. A fájlok eléréséhez a felhasználónak hozzáférés-kérési fájlt (egy KESDC kiterjesztésű fájlt) kell küldenie a rendszergazdának. A hozzáférés-kérési fájlt el lehet küldeni például e-mailben. A rendszergazda válaszul küld egy titkosítottadat-hozzáférési fájlt (egy KESDR kiterjesztésű fájlt).

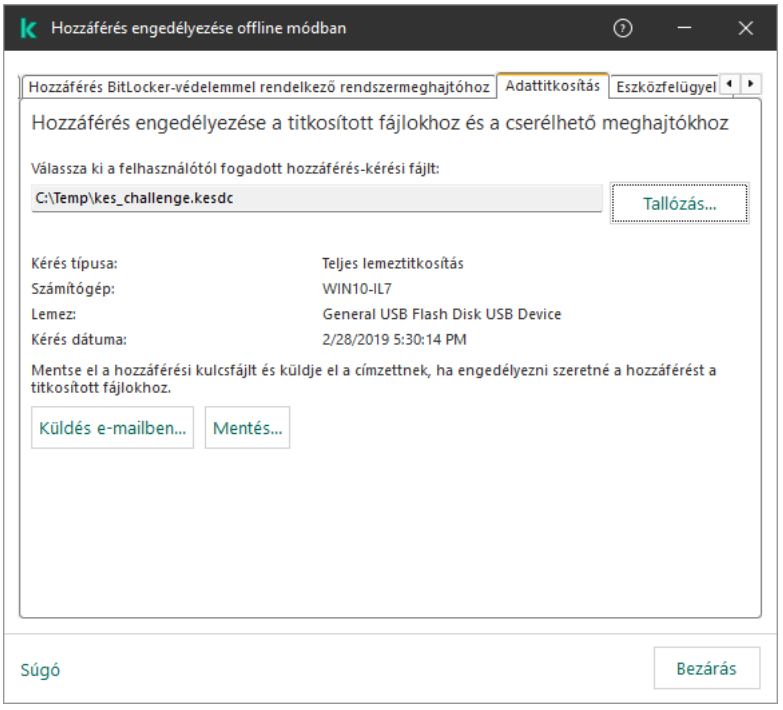
Miután elvégezte a kérelem-válasz jellegű jelszó-visszaállítási folyamatot, általános hozzáférést kap a cserélhető meghajtó fájljaihoz és teljes körű hozzáférést a cserélhető meghajtóhoz (írás/olvasás jogosultságok).

Alkalmazhatja a cserélhető meghajtó titkosítási házirendjeit, például fájlok visszafejtésére. A jelszó visszaállítását vagy a rendszabály frissítését követően a Kaspersky Endpoint Security kéri a módosítások megerősítését.

Titkosítottadat-hozzáférési fájl beszerezésének menete az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Devices** lehetőséget.
3. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
4. A helyi menüben válassza ki a **Hozzáférés engedélyezése offline módban** elemet.
5. A megnyíló ablakban válassza az **Adattitkosítás** lapot.
6. Az **Adattitkosítás** lapon kattintson a **Browse** gombra.
7. A hozzáférés-kérési fájl kiválasztására szolgáló ablakban adja meg a felhasználótól kapott fájl elérési útját.

A felhasználó kérésére vonatkozó információ válik láthatóvá. A Kaspersky Security Center létrehoz egy kulcsfájlt. Küldje el e-mailben a létrehozott titkosítottadat-hozzáférési kulcsfájlt a felhasználónak. Másik megoldásként mentse a hozzáférési fájlt, és használjon tetszés szerinti módszert a fájl továbbításához.



Hozzáférés engedélyezése offline módban

Titkosítottadat-hozzáférési fájl beszerezésének menete a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Assets (Devices)** lehetőséget.
2. Tegyen jelölést annak a számítógépnek a neve mellé, amelynek adataihoz szeretné visszaállítani a hozzáférést.
3. Kattintson az **Grant access to the device in offline mode** gombra.
4. Válassza a **Data Encryption** lehetőséget.
5. Kattintson a **Select file** gombra, és válassza ki azt a hozzáférés-kérési (KESDC kiterjesztésű) fájlt, amelyet a felhasználótól kapott.

   A Web Console a kérésre vonatkozó információkat jelenít meg. Ezek között szerepel annak a számítógépnek a neve, amelyen a felhasználó hozzáférést kér a fájlhoz.
6. Kattintson a **Save key** gombra, és válassza ki azt a mappát, amelybe a titkosítottadat-hozzáférési (KESDR kiterjesztésű) kulcsfájlt menteni szeretné.

Ekkor beszerezheti titkosítottadat-hozzáférési kulcsot, amelyet továbbítania kell a felhasználónak.

Cserélhető meghajtók visszafejtése

Lehetősége van rendszabály segítségével visszafejteni egy cserélhető meghajtó tartalmát. A rendszer létrehoz rendszabályt egy adott adminisztrációs csoport számára, amelyben a cserélhető meghajtók titkosítására vonatkozó beállítások szerepelnek. Emiatt az adatvisszafejtés eredménye cserélhető meghajtókon attól a számítógéptől függ, amelyhez a cserélhető meghajtót csatlakoztatja.

Cserélhető meghajtók visszafejtése:

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabály ablakában válassza az **Adattitkosítás → Cserélhető meghajtók titkosítása** lehetőséget.
4. Ha a cserélhető meghajtókon lévő összes titkosított fájlt vissza szeretné fejteni, válassza a **Titkosítási mód** legördülő listán a **Teljes cserélhető meghajtó visszafejtése** lehetőséget.

5. Ha egyes cserélhető meghajtókon lévő adatokat szeretne visszafejteni, szerkessze azon cserélhető meghajtók titkosítási szabályait, amelynek az adatait vissza szeretné fejteni. Ehhez:

   a. Válassza ki azon cserélhető meghajtók listáján, amelyekhez titkosítási szabályok vannak beállítva, a kívánt cserélhető meghajtóhoz tartozó bejegyzést.

   b. Kattintson a **Szabály beállítása** gombra a kiválasztott cserélhető meghajtó titkosítási szabályának szerkesztéséhez.

   c. A **Szabály beállítása** gomb helyi menüjében válassza ki a **Teljes cserélhető meghajtó visszafejtése** elemet.

6. Mentse el a módosításokat.

Ennek következtében, ha egy felhasználó csatlakoztat egy cserélhető meghajtót, vagy ha már csatlakoztatva van egy, a Kaspersky Endpoint Security visszafejti a cserélhető meghajtó tartalmát. Az alkalmazás figyelmezteti a felhasználót, hogy a visszafejtés folyamata eltarthat egy ideig. Ha az adatok visszafejtése közben a felhasználó a cserélhető meghajtó biztonságos eltávolítását kezdeményezi, a Kaspersky Endpoint Security megszakítja az adatvisszafejtési folyamatot, és a visszafejtési művelet befejezése előtt lehetővé teszi a cserélhető meghajtó eltávolítását. Az adatok visszafejtése folytatódik, amikor az adott cserélhető meghajtót legközelebb csatlakoztatják a számítógéphez.

Ha sikertelen egy cserélhető meghajtó visszafejtése, tekintse meg az **Adattitkosítás** jelentését a Kaspersky Endpoint Security felületén. A fájlok elérését blokkolhatja egy másik alkalmazás. Ebben az esetben próbálja meg kihúzni a cserélhető meghajtót a számítógépből, majd dugja be újra.

Az adattitkosítási részletek megtekintése

A titkosítás, illetve visszafejtés folyamata közben a Kaspersky Endpoint Security adatokat ad tovább az ügyfélszámítógépekre alkalmazott titkosítási paraméterekről a Kaspersky Security Center részére.

A titkosítási állapot megtekintése

Az adattitkosítás ellenőrzéséhez megnézheti az állapotot. A Kaspersky Endpoint Security a következő titkosítási állapotokat rendeli hozzá:

- **Does not meet the policy; canceled by user**. A felhasználó megszakította az adattitkosítást.
- **Does not meet the policy due to an error**. Adattitkosítási hiba, például hiányzik a licenc.
- **Applying the policy; restart is required**. Az adattitkosítás folyamatban van a számítógépen. Az adattitkosítás befejezéséhez indítsa újra a számítógépet.
- **No encryption policy specified**. Az adattitkosítás ki van kapcsolva a házirend-beállításokban.
- **Not supported**. Az adattitkosítási összetevők nincsenek telepítve a számítógépre.
- **Applying the policy**. A számítógépen adattitkosítás és / vagy -visszafejtés zajlik.

A számítógép adatai titkosítási állapotának megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Managed devices** lehetőséget.
3. A munkaterület **Devices** lapján csúsztassa a görgetősávot a jobb szélső állásba. Ha az **Encryption status** oszlop nem jelenik meg, adja hozzá ezt az oszlopot a Kaspersky Security Center konzolbeállításaiban.

   A **Encryption status** oszlopban a kiválasztott adminisztrációs csoportba tartozó számítógépek adatainak titkosítási állapota látható. Az állapot a számítógép helyi meghajtóin lévő fájlok titkosítására, valamint a teljes lemeztitkosításra vonatkozó információkból áll össze.
4. Ha a számítógép adattitkosításának állapota **Applying policy**, figyelemmel kísérheti a titkosítás folyamatának paneljét:
   a. Nyissa meg a számítógép tulajdonságait az **Applying policy** állapotra duplán kattintva.
   b. Válassza ki a számítógép tulajdonságainak ablakában a **Applications** részt.
   c. A számítógépre telepített Kaspersky-alkalmazások listájában válassza a **Kaspersky Endpoint Security for Windows** lehetőséget.
   d. Kattintson az **Statistics** gombra.
   e. Az **Encryption of devices** részen százalékban láthatja az adattitkosítás aktuális állapotát.

A titkosítási statisztikák megtekintése a Kaspersky Security Center irányítópanelein

A Kaspersky Security Center irányítópanelén a titkosítási állapotok megtekintéséhez:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki a konzolfában az **Administration Server** csomópontot.
3. Az Adminisztrációs Konzol fájától jobbra lévő munkaterületen válassza ki a **Statistics** lapot.
4. Hozzon létre új oldalt, melyen az adattitkosítási statisztikát tartalmazó részletes ablaktáblák találhatók. Ehhez:
   a. A **Statistics** lapon kattintson a **Customize view** gombra.
   b. Az ablakban kattintson a **Add** gombra.
   c. Ekkor megnyílik egy ablak, amelyben a **General** részbe írja be az oldal nevét.
   d. A **Information panels** részben kattintson a **Add** gombra.
   e. A megnyíló ablakban a **Protection status** csoportban válassza ki az **Encryption of devices** elemet.
   f. Kattintson az **OK** gombra.
   g. Szükség esetén szerkessze a részletes ablaktábla beállításait. Ehhez használja a **View** és **Devices** szakaszt.

h. Kattintson az **OK** gombra.

i. Ismételje meg az utasítások d–h lépését, ehhez válassza ki a **Encryption of removable drives** elemet a **Protection status** részben.

A hozzáadott részletes ablaktáblák az **Information panels** listában jelennek meg.

j. Kattintson az **OK** gombra.

Az előző lépésekben létrehozott részletes ablaktáblákat tartalmazó oldal neve a **Pages** listában jelenik meg.

k. Kattintson az **Close** gombra.

5. Nyissa meg a **Statistics** lapon az utasítások előző lépéseiben létrehozott oldalt.

Megjelennek a részletes ablaktáblák, melyekben a számítógépek és cserélhető meghajtók titkosítási állapota látható.

A számítógép helyi meghajtóin lévő fájlok titkosítási hibáinak megtekintése

A számítógép helyi meghajtóin lévő fájlok titkosítási hibáinak megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Managed devices** lehetőséget.
3. A **Devices** lapon válassza ki a számítógép nevét a listán, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
4. A számítógép helyi menüjében válassza ki a **Properties** elemet. A megnyíló ablakban válassza a **Protection** szakaszt.
5. A **View data encryption errors** hivatkozásra kattintva megnyílik a **Data encryption errors** menü.

Ebben az ablakban megjelennek a számítógép helyi meghajtóin lévő fájlok titkosítási hibái. Ha sor kerül egy hiba kijavítására, a Kaspersky Security Center a hiba adatait eltávolítja az **Data encryption errors** ablakból.

Az adattitkosítási jelentés megtekintése

A Kaspersky Security Center lehetővé teszi adattitkosítási jelentések létrehozását:

- **Report on encryption status of managed devices**. A jelentés információkat tartalmaz arról, hogy a számítógép titkosítási állapota megfelel-e a titkosítási házirendnek.
- **Report on encryption status of mass storage devices**. A jelentés információkat tartalmaz a külső eszközök és tárolóeszközök titkosítási állapotáról.
- **Report on rights to access encrypted drives**. A jelentés információkat tartalmaz a titkosított meghajtókhoz hozzáféréssel rendelkező fiókok állapotáról.

- **Report on file encryption errors**. A jelentés információkat tartalmaz a számítógépeken végzett adattitkosítási vagy visszafejtési feladatok végrehajtása során fellépő hibákról.
- **Report on blockage of access to encrypted files**. A jelentés információkat tartalmaz arról, hogy az alkalmazások nem férhetnek hozzá a titkosított fájlokhoz.

Az adattitkosítási jelentés megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki az **Reports** lapot.
3. Kattintson az **New report template** gombra.

   Ekkor elindul az új Jelentéssablon varázsló.
4. Kövesse a Jelentéssablon-varázsló utasításait. A **Selecting the report template type** ablak **Other** szakaszában válasszon egyet az adattitkosítási jelentések közül.

   Miután végzett az Új jelentéssablon varázslóval, az új jelentéssablon megjelenik a **Reports** lapon lévő táblázatban.
5. Válassza ki az utasítások előző lépéseiben létrehozott jelentéssablont.
6. A sablon helyi menüjében válassza ki a **Show report** elemet.

Megkezdődik a jelentés előállítási folyamata. A jelentés egy új ablakban jelenik meg.

Munkavégzés titkosított eszközökkel, ha nincs hozzájuk hozzáférés

Titkosított eszközökhöz való hozzáférés megszerzése

Az alábbi esetekben fordulhat elő, hogy a felhasználónak titkosított eszközökhöz való hozzáférést kell kérelmeznie:

- A merevlemez titkosítása egy másik számítógépen történt.
- Az eszköz titkosítási kulcsa nem található a számítógépen (például az adott számítógépen titkosított cserélhető meghajtóhoz való első hozzáférési kísérlet esetén), és a számítógép nem kapcsolódik a Kaspersky Security Centerhez.

  Miután a felhasználó a hozzáférési kulcsot alkalmazta a titkosított eszközön, a Kaspersky Endpoint Security menti a titkosítási kulcsot a felhasználó számítógépén, és engedélyezi az eszközhöz való hozzáférést a további hozzáférési próbálkozások során, még akkor is, ha nincs kapcsolat a Kaspersky Security Centerrel.

Az alábbiak szerint lehet hozzáférést szerezni a titkosított eszközökhöz:

1. A felhasználó a Kaspersky Endpoint Security alkalmazás felhasználói felülete segítségével hozzáférés-kérési fájlt hoz létre (kesdc kiterjesztéssel), és elküldi azt a vállalati LAN rendszergazdájának.
2. A rendszergazda a Kaspersky Security Center Adminisztrációs Konzol segítségével hozzáférési kulcsfájlt készít (kesdr kiterjesztéssel), és elküldi a felhasználónak.
3. A felhasználó alkalmazza a hozzáférési kulcsot.

Titkosított eszközökön lévő adatok visszaállítása

A felhasználó a Titkosított eszköz helyreállító segédprogram (a továbbiakban: visszaállító segédprogram) segítségével dolgozhat titkosított eszközökkel. Ez az alábbi esetekben lehet szükséges:

- A hozzáférési kulcs alkalmazása a hozzáférés megszerzése érdekében nem volt sikeres.
- A titkosított eszközt tartalmazó számítógépen nincsenek telepítve a titkosítási összetevők.

A titkosított eszközökhöz való hozzáférés visszaállító segédprogram segítségével történő visszaállításához szükséges adatok a felhasználó számítógépének memóriájában valamennyi ideig titkosítatlan formában találhatók. Az ilyen adatok illetéktelen elérésének kockázata csökkentése érdekében javasoljuk, hogy a titkosított eszközökhöz való hozzáférést megbízható számítógépeken állítsa vissza.

Az alábbiak szerint lehet visszaállítani a titkosított eszközökön lévő adatokat:

1. A felhasználó a visszaállító segédprogrammal hozzáférés-kérési fájlt készít (fdertc kiterjesztéssel), és elküldi a vállalati LAN rendszergazdájának.
2. A rendszergazda a Kaspersky Security Center Adminisztrációs Konzol segítségével hozzáférési kulcsfájlt készít (fdertr kiterjesztéssel), és elküldi a felhasználónak.
3. A felhasználó alkalmazza a hozzáférési kulcsot.

Titkosított rendszermerevlemezeken lévő adatok visszaállításához a felhasználó a Visszaállító segédprogramban megadhatja a Hitelesítési ügynök-fiók hitelesítési adatait is. Ha a Hitelesítési ügynök-fiók metaadatai megsérültek, a felhasználónak hozzáférés-kérési fájl segítségével kell elvégeznie a visszaállítási eljárást.

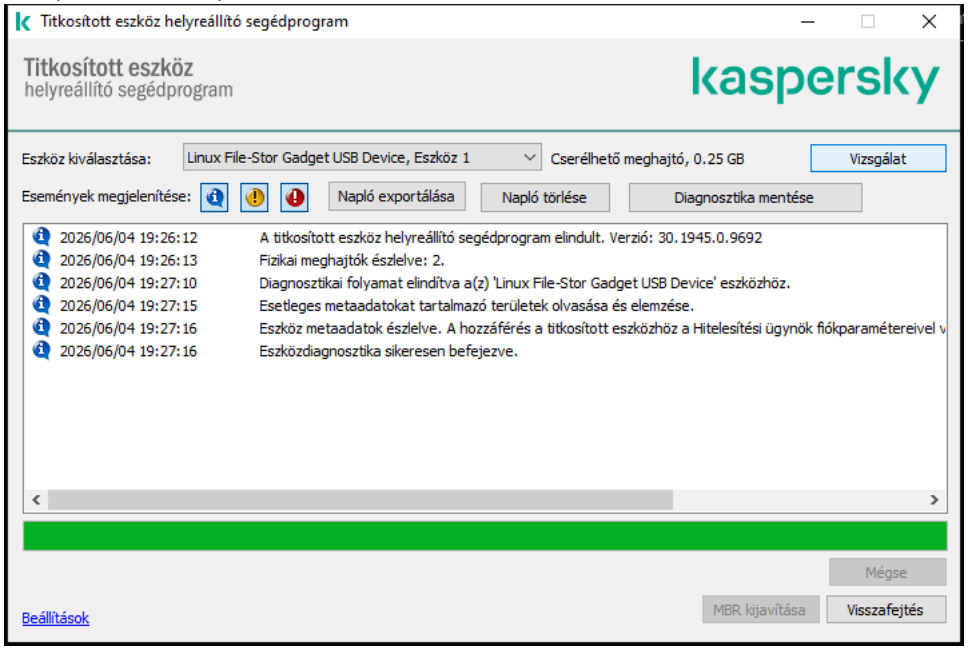
Javasoljuk, hogy a titkosított eszközökön lévő adatok visszaállítása előtt szakítsa meg azon a számítógépen a Kaspersky Security Center titkosítási rendszabályát, illetve tiltsa le a titkosítást a Kaspersky Security Center rendszabály-beállításaiban, amelyen a műveletet elvégzi. Ez megakadályozza az eszköz ismételt titkosítását.

Az adatok helyreállítása az FDERT visszaállító segédprogrammal

Ha a merevlemez hibásan működik, sérült lehet a fájlrendszer. Ilyen esetben a Kaspersky lemeztitkosítási technológiával védett adatok elérhetetlenek. Lehetősége van visszafejteni, majd új meghajtóra másolni az adatokat.

A Kaspersky lemeztitkosítási technológiával védett meghajtón tárolt adatok visszaállítása a következő lépésekből áll:

1. Hozzon létre önálló helyreállító segédprogramot (részletek a lentebbi ábrán).
2. Csatlakoztasson egy meghajtót olyan számítógéphez, amelyre nincs telepítve Kaspersky Endpoint Security titkosítási összetevő.
3. Futtassa a visszaállító segédprogramot, és vizsgálja meg a merevlemezt.
4. Érje el a meghajtón tárolt adatokat. Ehhez adja meg a Hitelesítési ügynök bejelentkezési adatait, vagy indítsa el a visszaállítási eljárást (kérés–válasz).



FDERT visszaállító segédprogram

Önálló helyreállító segédprogram létrehozása

A Visszaállító segédprogram végrehajtható fájljának létrehozása:

1. Kattintson a fő alkalmazásablakban a gombra.
2. A megnyíló ablakban kattintson a **Titkosított eszköz visszaállítása** gombra.

   Elindul a Titkosított eszköz helyreállító segédprogramja.

3. Kattintson a Visszaállító segédprogram ablakában az **Önálló helyreállító segédprogram létrehozása** gombra.

4. Mentse az önálló helyreállító segédprogramot a számítógép memóriájába.

   Ekkor a rendszer a visszaállító segédprogram végrehajtható fájlját (fdert.exe) a megadott mappába menti. Másolja a visszaállító segédprogramot olyan számítógépre, amelyre nincs telepítve Kaspersky Endpoint Security titkosítási összetevő. Ez megakadályozza a meghajtó ismételt titkosítását.

A titkosított eszközökhöz való hozzáférés visszaállító segédprogram segítségével történő visszaállításához szükséges adatok a felhasználó számítógépének memóriájában valamennyi ideig titkosítatlan formában találhatók. Az ilyen adatok illetéktelen elérésének kockázata csökkentése érdekében javasoljuk, hogy a titkosított eszközökhöz való hozzáférést megbízható számítógépeken állítsa vissza.

Adatok visszaállítása merevlemezen

Titkosított eszközhöz való hozzáférés helyreállítása a Visszaállító segédprogrammal:

1. Futtassa az fdert.exe nevű fájlt, a visszaállító segédprogram végrehajtható fájlját. Ezt a fájlt a Kaspersky Endpoint Security állítja elő.

2. A visszaállítási segédprogram ablakában válassza ki azt a titkosított eszközt, amelyhez vissza szeretné állítani a hozzáférést.

3. Kattintson a **Vizsgálat** gombra annak engedélyezéséhez, hogy a segédprogram meghatározza, melyik műveleteket kell elvégezni az eszközön: feloldani vagy visszafejteni kell-e.

   A Visszaállító segédprogram akkor kínálja fel az eszköz feloldását, ha a Kaspersky Endpoint Security titkosítási funkciója a számítógépen rendelkezésre áll. Noha az eszköz feloldásakor nem kerül sor visszafejtésre, a feloldás eredményeként közvetlenül hozzáférhetővé válik. Ha a Kaspersky Endpoint Security titkosítási funkciójához a számítógép nem fér hozzá, a Visszaállító segédprogram felkínálja az eszköz visszafejtését.

4. Ha diagnosztikai információt kíván importálni, kattintson a **Diagnosztika mentése** gombra.

   A segédprogram archívumként menti a diagnosztikai adatokat tartalmazó fájlokat.

5. Kattintson az **MBR kijavítása** gombra, ha a titkosított rendszermerevlemez diagnosztikája üzenetet jelenített meg az eszköz fő rendszerindító rekordjával (MBR) kapcsolatos problémákról.

   Az eszköz fő rendszerindító rekordjának kijavítása felgyorsíthatja az eszköz feloldásához, illetve visszafejtéséhez szükséges adatok megszerzésének folyamatát.

6. A diagnosztika eredményeitől függően kattintson a **Feloldás** vagy a **Visszafejtés** gombra.

7. Ha az adatokat a Hitelesítési ügynök-fiók segítségével szeretné visszaállítani, válassza a **Hitelesítési ügynök fiókbeállításainak használata** lehetőséget, és adja meg a Hitelesítési ügynökhöz tartozó bejelentkezési adatokat.

   Ez a módszer csak rendszermerevlemezen lévő adatok visszaállításakor használható. Ha a rendszermerevlemez megsérült, és a Hitelesítési ügynök-fiók adatai elvesztek, akkor a titkosított eszközön lévő adatok visszaállításához hozzáférési kulcsot kell beszereznie a vállalati hálózati rendszergazdától.

8. A visszaállítási eljárás elindításához tegye a következőket:

   a. Válassza ki az **Eszköz-hozzáférési kulcs manuális megadása** lehetőséget.

   b. Kattintson a **Hozzáférési kulcs fogadása** gombra, és mentse a hozzáférés-kérési (FDERTC kiterjesztésű) fájlt a számítógép memóriájába.

   c. Küldje el a hozzáférés-kérési fájlt a vállalati hálózati rendszergazdának.

   > Addig ne zárja be az **Eszköz-hozzáférési kulcs fogadása** ablakot, amíg meg nem kapta a hozzáférési kulcsot. Ha az ablakot ismét megnyitja, a korábban a rendszergazda által készített hozzáférési kulcsot már nem tudja alkalmazni.

   d. Fogadja és mentse a vállalati helyi hálózat rendszergazdája által létrehozott és elküldött, FDERTR kiterjesztésű hozzáférési fájlt (részletek a lentebbi ábrán).

   e. Töltse le a hozzáférési fájlt az **Eszköz-hozzáférési kulcs fogadása** ablakban.

9. Ha eszköz visszafejtését végzi, további visszafejtési beállításokat is meg kell adnia:

   - Adja meg a visszafejteni kívánt területet:
     - Ha a teljes eszközt vissza szeretné fejteni, válassza a **Teljes eszköz visszafejtése** lehetőséget.
     - Ha az eszközön lévő adatoknak csak egy részét szeretné visszafejteni, válassza az **Egyedi eszközterületek visszafejtése** lehetőséget, és adja meg a visszafejteni kívánt terület határait.
   - Válassza ki a visszafejtett adatok írásának helyét:
     - Ha az eredeti eszközön lévő adatokat felül szeretné írni a visszafejtett adatokkal, törölje az **Visszafejtés lemezképfájlba** jelölőnégyzetet.
     - Ha a visszafejtett adatokat az eredeti titkosított adatoktól elkülönítve szeretné menteni, jelölje be az **Visszafejtés lemezképfájlba** jelölőnégyzetet, és adja meg az adatok mentésének elérési útját a **Tallózás** gombra kattintva.

10. Kattintson az **OK** gombra.

Megkezdődik az eszköz feloldási/visszafejtési folyamata.

Titkosítottadat-hozzáférési fájl létrehozásának menete az Adminisztrációs Konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Válassza ki az Adminisztrációs Konzol fájában az **Advanced** → **Data encryption and protection** → **Encrypted drives** mappát.

3. Válassza ki a munkaterületen azt a titkosított eszközt, amelyhez hozzáférésikulcs-fájlt szeretne létrehozni, majd az eszköz helyi menüjében kattintson a **Hozzáférés az eszközhöz a Kaspersky Endpoint Security alkalmazásban** lehetőségre.

   Ha nem biztos abban, hogy a hozzáférés-kérési fájl melyik számítógéphez készült, válassza ki a Felügyeleti konzol fájában a **Advanced → Data encryption and protection** mappát, és a munkaterületen kattintson az **Eszköztitkosítási kulcs beszerzése a Kaspersky Endpoint Security alkalmazásban** elemre.

4. A megnyíló ablakban válassza ki a használni kívánt titkosítási algoritmust: AES256 vagy AES56.

   Az adattitkosítási algoritmus az AES-titkosítási könyvtártól függ, amely a terjesztőcsomagba tartozik: *Strong encryption (AES256)* vagy *Lite encryption (AES56)*. Az AES-titkosítási könyvtár az alkalmazással együtt van telepítve.

5. Kattintson **Tallózás** gombra egy ablak megnyitásához, amelyben megadhatja a felhasználótól kapott fdertc kiterjesztésű kérésfájl elérési útját.

6. Kattintson a **Feloldás** gombra.

A felhasználó kérésére vonatkozó információ válik láthatóvá. A Kaspersky Security Center létrehoz egy kulcsfájlt. Küldje el e-mailben a létrehozott titkosítottadat-hozzáférési kulcsfájlt a felhasználónak. Másik megoldásként mentse a hozzáférési fájlt, és használjon tetszés szerinti módszert a fájl továbbításához.

Titkosítottadat-hozzáférési fájl létrehozásának menete a Web Console-ban

1. A Web Console fő ablakában válassza az **Operations → Data encryption and protection → Encrypted drives** lehetőséget.

2. Tegyen jelölést annak a számítógépnek a neve melletti jelölőnégyzetbe, amelyen számítógépen adatok visszaállítását tervezi.

3. Kattintson az **Grant access to the device in offline mode** gombra.

   Ezzel elindítja az eszközelérést biztosító varázslót.

4. Kövesse az eszközelérést biztosító varázsló utasításait:

   a. Válassza ki a Kaspersky Endpoint Security for Windows bővítményt.

   b. Válassza ki a használni kívánt titkosítási algoritmust: AES256 vagy AES56.

      Az adattitkosítási algoritmus az AES-titkosítási könyvtártól függ, amely a terjesztőcsomagba tartozik: *Strong encryption (AES256)* vagy *Lite encryption (AES56)*. Az AES-titkosítási könyvtár az alkalmazással együtt van telepítve.

   c. Válassza ki a felhasználótól kapott hozzáférés-kérési (FDERTC kiterjesztésű) fájlt.

   d. Válassza ki azt a mappát, amelybe a titkosítottadat-hozzáférési (FDERTR kiterjesztésű) kulcsfájlt menteni szeretné.

Ekkor beszerezheti titkosítottadat-hozzáférési kulcsot, amelyet továbbítania kell a felhasználónak.

Operációs rendszer helyreállító lemezének létrehozása

Az operációs rendszer helyreállító lemeze akkor jöhet jól, ha egy titkosított merevlemezhez valamilyen okból nem fér hozzá, és az operációs rendszer nem töltődik be.

A helyreállító lemezzel betöltheti a Windows operációs rendszer lemezképét, és visszaállíthatja a titkosított merevlemezhez való hozzáférést az operációs rendszer lemezképén lévő Visszaállító segédprogram segítségével.

Operációs rendszer helyreállító lemezének létrehozása:

1. Titkosított eszköz helyreállító segédprogram futtatható fájljának létrehozása.

2. A Windows rendszerindítás előtti környezet egyéni lemezképének létrehozása. A Windows rendszerindítás előtti környezet egyéni lemezképének létrehozása közben a Visszaállító segédprogram futtatható fájljának hozzáadása a lemezképhez.

3. A Windows rendszerindítás előtti környezet egyéni lemezképének mentése rendszerindításra alkalmas adathordozóra, például CD-re vagy cserélhető meghajtóra.

   A Windows rendszerindítás előtti környezet egyéni lemezképének létrehozására vonatkozó utasítások a Microsoft súgófájlokban találhatók (például a Microsoft TechNet erőforrásban).

Detection and Response-megoldások

A Kaspersky Detection and Response megoldások olyan biztonsági rendszerek, amelyek a vállalat infrastruktúrájának különböző szintjein észlelik a fejlett fenyegetéseket és a támadásra utaló jeleket. A Detection és Response megoldások információt nyújtanak az észlelt fenyegetésről, és lehetővé teszik a fenyegetésre adott válasz műveleteinek kezelését.

Így a Detection and Response megoldás az alábbiakat teszi:

- Információk fogadása egy számítógép, kiszolgáló vagy más eszköz működéséről (telemetria).
- Az információk automatikus elemzése a fenyegetések észleléséhez.
- A riasztási részleteket a fenyegetés-fejlődési lánc oszlopaiként generálja az elemzéshez és a fenyegetésre adott válasz műveleteinek kiválasztásához.
- Végrehajtja a fenyegetésre adott válasz műveleteit (például a számítógép hálózati leválasztását).

A Kaspersky Endpoint Security beépített ügynök használatával támogatja a Detection and Response-megoldásokat. A beépített ügynök telemetriai adatokat küld a megoldások kiszolgálóinak, és végrehajtja a fenyegetésre adott válasz műveleteit. A beépített ügynök a következőket támogatja:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) 7.1 vagy korábbi verzió
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

A Kaspersky Endpoint Security Detection and Response megoldást különféle konfigurációkban használhatja, például: [EDR Optimum+MDR].

MDR és EDR Optimum licencelése

A Kaspersky Endpoint Security támogatja a Kaspersky Managed Detection and Response (MDR) és a Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) megoldások funkcióit. Ezekkel a megoldásokkal különféle konfigurációkban használhatja a Kaspersky Endpoint Security alkalmazást, és olyan egyéni védelmi rendszert hozhat létre, amely megfelel az Ön egyedi követelményeinek. Ahhoz, hogy ezt megtehesse, minden egyes megoldáshoz licencet kell vásárolnia. A licenc kiterjedhet egyetlen megoldás (például csak MDR kiegészítő) vagy több megoldás, pl. [EDR Optimum+MDR] kiegészítő használati jogára.

Az MDR és az EDR Optimum a következő licencelési módszereket támogatja:

- A Kaspersky Endpoint Security for Windows licence tartalmazza az MDR vagy EDR Optimum funkciót.

  A funkció a Kaspersky Endpoint Security for Windows aktiválása után azonnal elérhetővé válik. Csak egy kulcsot kell hozzáadnia.

- Külön licencek az MDR vagy az EDR Optimum számára (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  A funkció az MDR kiegészítő, az EDR Optimum kiegészítő vagy az [EDR Optimum+MDR] kiegészítő külön kulcsának hozzáadása után válik elérhetővé. Ennek eredményeképpen két kulcs kerül hozzáadásra a számítógépen: egy kulcs a Kaspersky Endpoint Security és egy kulcs az MDR vagy EDR Optimum számára. A Kaspersky Endpoint Security kulcsát kell elsőként hozzáadni.

A Kaspersky Endpoint Security csak egy *aktív kulcs* hozzáadását teszi lehetővé az MDR és EDR Optimum licenchez. Ezért ha mindkét megoldást aktiválni szeretné, akkor egy [EDR Optimum+MDR] Add-on kulcsot kell hozzáadnia, nem pedig külön kulcsot mindkét megoldáshoz. Egy *tartalék kulcsot* is hozzáadhat.

Ha BLOB fájlt használt az MDR telepítésekor, nincs szükség külön kulcsra az MDR aktiválásához. A BLOB fájl már tartalmazza a licencinformációkat.

A megoldások kezdeti licencelése

Az MDR és az EDR Optimum első telepítésekor a megoldások aktiválása ugyanúgy történik, mint a Kaspersky Endpoint Security alkalmazásé. Hozzáadhat kulcsot a *Kulcs hozzáadása* feladat segítségével, vagy használhatja az automatikus kulcsterjesztés funkciót. A licenckulcs második aktív kulcsként vagy tartalék kulcsként kerül hozzáadásra az alkalmazáshoz, ha bejelöli a megfelelő jelölőnégyzetet.

Váltás egyik licencről a másikra

Ha a vállalat már telepítette valamelyik ilyen megoldást, és a megfelelő kulcsot hozzáadták az alkalmazáshoz, az új konfiguráció licencelésével kapcsolatban néhány különleges szempontot kell figyelembe venni. Másik licencre való váltáskor az alkalmazás nem adja hozzá az új kulcsot az alkalmazáshoz, hanem lecseréli az aktuális kulcsot az új kulcsra. Ennek oka az a korlátozás, amely lehetővé teszi, hogy az alkalmazás csak egy kulcsot adjon hozzá az MDR és az EDR Optimum aktiválásához.

Tegyük fel például, hogy a vállalat az [EDR Optimum+MDR] megoldást telepítette, és Ön úgy döntött, hogy vált az MDR kiegészítő konfigurációra. Az új konfigurációra való áttéréshez a(z) [EDR Optimum+MDR] Add-on kulcsot az MDR bővítményi kulcsra kell cserélni.

Az EDR Optimum és az MDR ([EDR Optimum+MDR] kiegészítő) külön licence már nem érhető el. Ha mindkét megoldást használni szeretné, aktiválnia kell az MDR-t egy BLOB fájllal, az EDR Optimumot pedig egy licenckulccsal.

Az automatikus kulcsterjesztési funkcióval az alkalmazás elutasítja az azonos számú megoldásra vonatkozó licenckulcsokat. Ez azt jelenti, hogy ha EDR Optimum kiegészítői kulcsot adott hozzá, azt nem cserélheti le MDR bővítménykulcsra. Az EDR Optimum kiegészítői kulcsot azonban lecserélheti egy [EDR Optimum+MDR] kiegészítői kulcsra. Az alkalmazás akkor is elutasítja a kulcsokat, ha egy MDR kiegészítői kulcsot EDR kiegészítői kulcsra próbál meg lecserélni. Kulcs cseréjéhez futtathatja a *Kulcs hozzáadása* feladatot. A *Kulcs hozzáadása* feladat lehetővé teszi a licenckulcsok tetszőleges számú megoldással való lecserélését.

Ha egy [EDR Optimum+MDR] Add-on tartalék licenckulcsot adott hozzá, az EDR Optimum vagy MDR bővítmény aktív kulcsának megfelelő hozzáadásához először le kell cserélnie a tartalék licenckulcsot egy EDR Optimum vagy MDR bővítményi kulcsra, vagy távolítsa el a tartalék kulcsot, majd cserélje le az aktív kulcsot.

Kompatibilitás harmadik féltől származó EDR-megoldásokkal

A Kaspersky Endpoint Security segítségével külső gyártók EDR-megoldásaival együtt védheti a munkaállomásokat és a kiszolgálókat. A vakriasztások kiküszöböléséhez ajánlott hozzáadni a Kaspersky Endpoint Security és a Network Agent futtatható fájljait a harmadik féltől származó EDR-megoldás megbízható zónájához.

Megbízható zóna a harmadik féltől származó EDR megoldásokkal való kompatibilitáshoz

	Kaspersky Endpoint Security for Windows	Kaspersky Security Center Network Agent
Munkamappa	`C:\Program Files (x86)\Kaspersky Lab\KES.14.1.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Végrehajtható fájlok	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent támogatja az alkalmazás és más Kaspersky megoldás közötti kapcsolatot a fejlett fenyegetések felismerése érdekében (pl. Kaspersky Sandbox). A Kaspersky megoldások a Kaspersky Endpoint Agent adott verzióival kompatibilisek.

Ha a Kaspersky-megoldások részeként kívánja használni a Kaspersky Endpoint Agent végponti ügynököt, a megoldásokat aktiválnia kell a megfelelő licenckulccsal.

Az Ön által használt szoftveres megoldás részét képező Kaspersky Endpoint Agenttel és az önálló megoldással kapcsolatos részletes információkért olvassa el a megfelelő termék súgóját:

- A Kaspersky Anti Targeted Attack Platform súgója
- A Kaspersky Sandbox súgója
- A Kaspersky Endpoint Detection and Response Optimum súgója
- A Kaspersky Managed Detection and Response súgója

A Kaspersky Endpoint Security 11.2.0 – 11.8.0 verzióihoz készült terjesztőkészlet tartalmazza a Kaspersky Endpoint Agent megoldást. A Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows telepítésekor választható ki. Ennek eredményeként két alkalmazás települ a számítógépére: KEA és KES. A Kaspersky Endpoint Security 11.9.0 verziójában a Kaspersky Endpoint Agent terjesztőcsomag már nem része a Kaspersky Endpoint Security terjesztőkészletének.

A KEA verziók (a KES részeként) megfeleltetése a KES verzióknak

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

A Kaspersky a Kaspersky Endpoint Agent helyett a beépített Kaspersky Endpoint Security ügynökre állítja át az összes Detection and Response megoldást. A Kaspersky fokozatosan támogatja ezeket a megoldásokat, és fokozatosan megszünteti a Kaspersky Endpoint Agent szolgáltatást (lásd az alábbi táblázatot). A 12.1 verziótól kezdve az alkalmazás támogatja az összes Detection and Response megoldást. Ezenkívül a 12.1 verziótól kezdődően az alkalmazás már nem kompatibilis a Kaspersky Endpoint Agenttel, és a két alkalmazás egymás melletti telepítése már nem lehetséges ugyanazon a számítógépen.

A Kaspersky Endpoint Security verziója	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (Endpoint Detection and Response összetevő)	Kaspersky Anti Targeted Attack Platform (Network Detection and Response összetevő)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	Kaspersky Endpoint Agent
12.6	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**	**Beépített ügynök**

A [KES+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra

A Kaspersky Endpoint Security a Detection and Response megoldásokhoz készült beépített ügynökökkel rendelkezik. Az ezekkel a megoldásokkal való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra. Amikor olyan számítógépeken telepíti a Kaspersky Endpoint Security alkalmazást, amelyekre telepítve van a Kaspersky Endpoint Agent, a Detection and Response megoldások továbbra is együttműködnek a Kaspersky Endpoint Security termékkel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről.

A Kaspersky Endpoint Security 11.2.0 – 11.8.0 verzióihoz készült terjesztőkészlet tartalmazza a Kaspersky Endpoint Agent megoldást. A Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows telepítésekor választható ki. Ennek eredményeként két alkalmazás települ a számítógépére: KEA és KES. A Kaspersky Endpoint Security 11.9.0 verziójában a Kaspersky Endpoint Agent terjesztőcsomag már nem része a Kaspersky Endpoint Security terjesztőkészletének.

A [KES+KEA] konfiguráció [KES+beépített ügynök] konfigurációra történő áttelepítése a következő lépéseket foglalja magában:

1. **A Kaspersky Security Center frissítése**

   Frissítse a Kaspersky Security Center összes összetevőjét a 13.2 vagy újabb verzióra, beleértve a felhasználói számítógépeken lévő hálózati ügynököt és a Web Console-t is.

2. **A Kaspersky Endpoint Security webes bővítmény frissítése**

A Kaspersky Security Center Web Console-ban frissítse a Kaspersky Endpoint Security webes bővítményt a 11.7.0 vagy újabb verzióra. Az EDR Optimum és a Kaspersky Sandbox összetevők kezeléséhez a Web Console-t kell használnia.

A Kaspersky Anti Targeted Attack Platform (EDR) használatához webbővítményre lesz szükség a Kaspersky Endpoint Security 12.1 vagy újabb verzió esetében.

A Kaspersky Anti Targeted Attack Platform (NDR) használatához webbővítményre lesz szükség a Kaspersky Endpoint Security 12.7 vagy újabb verzió esetében.

3. **A házirend és a feladatok áttelepítése**

A Kaspersky Endpoint Agent házirendet és feladatokat áttelepítő varázslójával áttelepítheti a Kaspersky Endpoint Agent beállításait a Kaspersky Endpoint Security for Windows rendszerbe.

Ez létrehoz egy új Kaspersky Endpoint Security szabályzatot. Az új házirend *Inactive* állapotot kap. A házirend alkalmazásához nyissa meg a házirend tulajdonságait, fogadja el a Kaspersky Security Network nyilatkozatot, és állítsa az állapotot *Active* értékre.

4. **Licencelési funkcionalitás**

Ha egy közös Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security licencet használ a Kaspersky Endpoint Security for Windows és a Kaspersky Endpoint Agent aktiválásához, az EDR Optimum funkció automatikusan aktiválódik az alkalmazás 11.7.0 verzióra történő frissítése után. Semmi mást nem kell tennie.

Ha önálló Kaspersky Endpoint Detection and Response Optimum bővítményi licencet használ az EDR Optimum funkció aktiválásához, akkor győződjön meg arról, hogy az EDR Optimum bővítményi kulcsot hozzáadta a Kaspersky Security Center tárolójához, és engedélyezte az automatikus licenckulcs-szolgáltatói funkciót. Az alkalmazás 11.7.0 verzióra történő frissítése után az EDR Optimum funkció automatikusan aktiválódik.

Ha Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security licencet használ a Kaspersky Endpoint Agent aktiválásához, és egy másik licencet a Kaspersky Endpoint Security for Windows aktiválásához, akkor a Kaspersky Endpoint Security for Windows kulcsot a közös Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security kulcsra kell cserélnie. A kulcsot a *Add key* feladat segítségével cserélheti ki.

A Kaspersky Sandbox funkciót nem kell aktiválnia. A Kaspersky Sandbox funkció a Kaspersky Endpoint Security for Windows frissítése és aktiválása után azonnal elérhetővé válik.

Csak a Kaspersky Anti Targeted Attack Platform licence használható a Kaspersky Endpoint Security aktiválására a Kaspersky Anti Targeted Attack Platform megoldás részeként. Az alkalmazás 12.1 verzióra történő frissítése után az EDR (KATA) funkció automatikusan aktiválódik. Semmi mást nem kell tennie.

5. **A Kaspersky Endpoint Security alkalmazás frissítése**

Az alkalmazás frissítéséhez és az EDR Optimum és a Kaspersky Sandbox funkciók áttelepítéséhez távoli telepítési feladat ajánlott.

Az alkalmazás távoli telepítési feladattal történő frissítéséhez a következő beállításokat kell módosítania:

- Válassza ki a Detection and Response megoldások összetevőit a telepítőcsomag beállításainál.
- Zárja ki a Kaspersky Endpoint Agent összetevőt a telepítőcsomag beállításaiból (a Kaspersky Endpoint Security for Windows 11.2.0 – 11.8.0 verziói esetében).
- Ha a jelszóvédelem engedélyezve van a Kaspersky Endpoint Agenthez való hozzáférés korlátozása céljából, adja meg az alkalmazás eltávolítási jelszavát az *Install application remotely* feladat beállításaiban. Az eltávolítási jelszót a Kaspersky Security Center Linux 15.1 verziótól kezdve adhatja meg.

Az alkalmazást a következő módszerekkel is frissítheti:

- A Kaspersky frissítési szolgáltatás használatával (zökkenőmentes frissítés – SMU).
- Helyben, a Telepítővarázsló segítségével.

A Kaspersky Endpoint Security támogatja az összetevők automatikus kiválasztását az alkalmazásfrissítés során az olyan számítógép esetében, amelyre a Kaspersky Endpoint Agent alkalmazás telepítve van. Az összetevők automatikus kiválasztása az alkalmazás frissítését végző felhasználói fiók engedélyeitől függ.

Ha a Kaspersky Endpoint Security frissítése a rendszerfiók (SYSTEM) alatt található EXE- vagy MSI-fájl használatával történik, a Kaspersky Endpoint Security hozzáférést kap a Kaspersky-megoldások aktuális licenceihez. Ezért ha a számítógépen például a telepített Kaspersky Endpoint Agent mellett az EDR Optimum megoldás aktiválva van, a Kaspersky Endpoint Security telepítője automatikusan konfigurálja az összetevőket, és kiválasztja az EDR Optimum összetevőt. Ezáltal a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt. Az MSI-telepítő rendszerfiók (SYSTEM) alatti futtatása általában a Kaspersky frissítési szolgáltatása (SMU) keretében történő frissítéskor vagy egy telepítőcsomag Kaspersky Security Centerrel végzett telepítésekor zajlik.

Ha a Kaspersky Endpoint Security frissítése emelt szintű jogosultsággal nem rendelkező felhasználói fiók alatt található MSI-fájl használatával történik, a Kaspersky Endpoint Security nem kap hozzáférést a Kaspersky-megoldások aktuális licenceihez. Ilyenkor a Kaspersky Endpoint Security automatikusan választja ki az összetevőket a Kaspersky Endpoint Agent konfigurációja alapján. Ezután a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt.

6. **A számítógép újraindítása**

   A számítógép újraindítása a beépített ügynökkel az alkalmazás frissítésének befejezéséhez. Amikor az alkalmazás frissül, a telepítő a számítógép újraindítása előtt eltávolítja a Kaspersky Endpoint Agent eszközt. A számítógép újraindítása után a telepítő hozzáadja a beépített ügynököt. Ez azt jelenti, hogy a Kaspersky Endpoint Security nem látja el az EDR és Kaspersky Sandbox funkcióit a számítógép újraindításáig.

7. **A Kaspersky Endpoint Detection and Response Optimum és a Kaspersky Sandbox állapotának ellenőrzése**

   Ha a frissítés után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

   - Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
   - Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal.
   - Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.

   - Győződjön meg arról, hogy az EDR Optimum funkció aktiválva van az *Report on status of application components* segítségével. Ha egy összetevőnél a *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy az EDR Optimum automatikus licenckulcs-szolgáltatói funkciója be van kapcsolva.

Szabályzatok és feladatok áttelepítése a Kaspersky Endpoint Agent számára

A Kaspersky Endpoint Security for Windows tartalmaz egy varázslót a Kaspersky Endpoint Agent megoldásról a Kaspersky Endpoint Security termékre való áttéréshez. A szabályzat- és feladatbeállításokat a következő megoldások esetén telepítheti át:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

A Kaspersky Endpoint Agent megoldásról a Kaspersky Endpoint Security termékre áttérő varázsló csak a Web Console-ban és a Cloud Console-ban működik. A Felügyeleti konzolban (MMC), csak a Kaspersky Anti Targeted Attack Platform (EDR) megoldás beállításait tudja áttelepíteni a Kaspersky Security Center standard szabályzat- és feladatáttelepítési varázslójával.

Javasoljuk, hogy egyetlen számítógépen kezdje el a Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security szolgáltatásra való áttelepítést, majd végezze el egy számítógépcsoporton, ezután fejezze be az áttelepítést a vállalat összes számítógépén.

A szabályzat- és feladatbeállítások áttelepítése a Kaspersky Endpoint Agent szolgáltatásból a Kaspersky Endpoint Security szolgáltatásba,

a Web Console fő ablakában válassza az **Operations → Migration from Kaspersky Endpoint Agent** lehetőséget.

Ezzel futtatja a szabályzat- és feladatáttelepítési varázslót. Kövesse a varázsló utasításait.

1. lépés. Szabályzat áttelepítése

Az áttelepítési varázsló új szabályzatot hoz létre, amely egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent szabályzatainak beállításait. A listában válassza ki azokat a Kaspersky Endpoint Agent szabályzatokat, amelyek beállításait egyesíteni szeretné a Kaspersky Endpoint Security szabályzatával. Kattintson a Kaspersky Endpoint Agent szabályzatára, és válassza ki azt a Kaspersky Endpoint Security szabályzatot, amellyel egyesíteni szeretné a beállításokat. Győződjön meg arról, hogy a megfelelő szabályzatokat választotta, és folytassa a következő lépéssel.

2. lépés. Feladatok áttelepítése

Az áttelepítési varázsló új feladatokat hoz létre a Kaspersky Endpoint Security számára. A feladatlistában válassza ki azokat a Kaspersky Endpoint Agent feladatokat, amelyeket létre szeretné hozni a Kaspersky Endpoint Security szabályzatához. A varázsló támogatja a Kaspersky Endpoint Detection and Response és a Kaspersky Sandbox feladatait. Lépjen a következő lépésre.

3. lépés. A varázsló befejezése

Lépjen ki a varázslóból. Ennek eredményeként a varázsló a következőket teszi:

- Létrehoz egy új Kaspersky Endpoint Security szabályzatot.

  A szabályzat egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent beállításait. A szabályzat neve *<Kaspersky Endpoint Security policy name> és <Kaspersky Endpoint Agent policy name>*. Az új házirend *Inactive* állapotot kap. A folytatáshoz módosítsa a Kaspersky Endpoint Agent és a Kaspersky Endpoint Security szabályzatok állapotát *Inactive* értékre, és aktiválja az új egyesített szabályzatot.

  A Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security for Windows szolgáltatásra történő áttérés után győződjön meg arról, hogy az új házirendben be van-e állítva az Adatátvitel az adminisztrációs kiszolgálóra funkció (karanténfájl-adatok és fenyegetés-fejlődési lánc adatai). Az adatátviteli paraméterek értékei nem lesznek áttelepítve a Kaspersky Endpoint Agent házirendjéből.

  A Kaspersky Endpoint Agent megoldásról a Kaspersky Endpoint Security for the Kaspersky Anti Targeted Attack Platform (EDR) megoldásra történő áttérés során előfordulhat, hogy a számítógép Central Node kiszolgálóihoz való csatlakoztatáskor hibák lépnek fel. Ennek oka, hogy a Web Console áttelepítési varázslója kihagyja a következő házirend-beállításokat, és nem telepíti át őket:

  - Beállítások módosításának tiltása **Connection to KATA servers** („zárolás”).

    Alapértelmezés szerint a beállítások módosíthatók (a „lakat” nyitva van). Ezért a beállítások nem kerülnek alkalmazásra a számítógépen. Meg kell tiltania a beállítások módosítását, és be kell zárnia a „lakatot”.

  - Kriptotároló.

    Ha kétirányú hitelesítést használ a Central Node kiszolgálóihoz való csatlakozáshoz, akkor újra fel kell vennie a kriptotárolót. Az áttelepítési varázsló helyesen telepíti át a kiszolgáló TLS-tanúsítványát.

  Az Adminisztrációs konzol (MMC) Házirend és feladatok áttelepítési varázslója áttelepíti a Kaspersky Anti Targeted Attack Platform (EDR) megoldás összes beállítását.

- Létrehozza a Kaspersky Endpoint Security új feladatait.

  Az új feladatok a Kaspersky Endpoint Agent feladatok másolatai a Kaspersky Endpoint Detection and Response és a Kaspersky Sandbox számára. Emellett a varázsló változatlanul hagyja a Kaspersky Endpoint Agent feladatait.

A szabályzat- és feladatbeállítások áttelepítése a Kaspersky Endpoint Agent szolgáltatásból a Kaspersky Endpoint Security szolgáltatásba a felügyeleti konzolon (MMC) (csak KATA (EDR) esetében)

1. A Felügyeleti konzolon válassza a Felügyeleti kiszolgáló lehetőséget, és kattintson a jobb gombbal a helyi menü megnyitásához.
2. Válassza az **All tasks** → **Policies and tasks batch conversion wizard** lehetőséget.

A Házirendek és feladatok kötegelt átalakítása varázsló elindul. Kövesse a varázsló utasításait.

1. lépés: Válassza ki azt az alkalmazást, amelyhez házirendeket és feladatokat kell konvertálnia

Ennél a lépésnél a Kaspersky Endpoint Security for Windows lehetőséget kell választania. Lépjen a következő lépésre.

2. lépés: Házirendek átalakítása

Az áttelepítési varázsló egy új Kaspersky Endpoint Security házirendet hoz létre, amelybe a Kaspersky Endpoint Agent házirend-beállításait áttelepíti. A házirendek listájában válassza ki azokat a Kaspersky Endpoint Agent házirendeket, amelyek beállításait egyesíteni szeretné a Kaspersky Endpoint Security házirendjével. Lépjen a következő lépésre.

Az áttelepítési varázsló ezután elkezdi a házirendek átalakítását. A házirend-átalakítás során az Áttelepítési varázsló felkéri a Kaspersky Security Network nyilatkozatának elfogadására. Az új házirendek neve *<Házirend neve> (átalakítva)* lesz.

3. lépés: Feladatok átalakítása

Átugorhatja ezt a lépést. A varázsló csak a Kaspersky Endpoint Detection and Response Optimum és a Kaspersky Sandbox feladatait támogatja. Ezen összetevők kezelése csak a Web Console-on érhető el. Lépjen a következő lépésre.

4. lépés. A varázsló befejezése

Lépjen ki a varázslóból. A varázsló eredményeként egy új Kaspersky Endpoint Security házirend jön létre.

Endpoint Detection and Response Agent (EDR Agent)

A Kaspersky Endpoint Security 12.3 for Windows verziótól kezdve az alkalmazás tartalmazza az Endpoint Detection and Response Agent (EDR Agent) konfigurációt. Az *Endpoint Detection and Response Agent* egy olyan alkalmazás, amely a vállalat informatikai infrastruktúrájában az egyes munkaállomásokra és kiszolgálókra telepítve támogatja a Kaspersky alábbi Detection and Response megoldásait:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (12.6 verziótól kezdve)

- Kaspersky Anti Targeted Attack Platform (NDR) (12.7 verziótól kezdve)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (a 12.11 verziótól)

Az EDR Agent nem támogatja az integrációt a Kaspersky Endpoint Detection and Response Expert (cloud) megoldással.

Az EDR Agent folyamatosan figyeli az ezeken a számítógépeken futó folyamatokat, a nyílt hálózati kapcsolatokat és a módosítandó fájlokat. Az EDR Agenthez nem állnak rendelkezésre az alkalmazás védelmi és felügyeleti összetevői.

Az EDR Agent kompatibilis harmadik féltől származó EPP alkalmazásokkal. Ez lehetővé teszi harmadik féltől származó infrastruktúra-biztonsági eszközök használatát a Kaspersky Detection and Response mellett.

Az EDR Agent telepítéséhez a számítógépen telepíteni kell a Network Agentet, és a számítógépet hozzá kell adni a Kaspersky Security Center konzolon. Az EDR Agent és a Kaspersky Security Center közötti interakció engedélyezéséhez telepítenie kell a Kaspersky Endpoint Security for Windows adminisztrációs bővítményt. Az EDR Agent beállításait csoportházirend segítségével adhatja meg. Az EDR Agent integrálásához konfigurálnia kell az integrációt a megfelelő házirend-szakaszokban.

A Kaspersky Detection and Response megoldásainak támogatásához a következő Kaspersky-alkalmazásokat kell telepíteni az infrastruktúrára:

	• Network Agent • EDR Agent
Endpoint	
	Kaspersky Endpoint Security for Windows adminisztrációs bővítmény
Kaspersky Security Center	
	
Detection and Response-megoldások: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Az EDR Agent telepítése

Az Endpoint Detection and Response Agent (EDR Agent) konfigurációjában a Kaspersky Detection and Response megoldások esetében a Kaspersky Endpoint Security telepítése ugyanúgy történik.

Az EDR Agent az alábbi módok egyikén telepíthető a számítógépre:

- Távolról a Kaspersky Security Centeren keresztül.
- Helyileg a Telepítővarázsló segítségével.
- Helyileg, a parancssorból (csak a KATA (EDR) és az EDR Expert (on-premises) esetén).

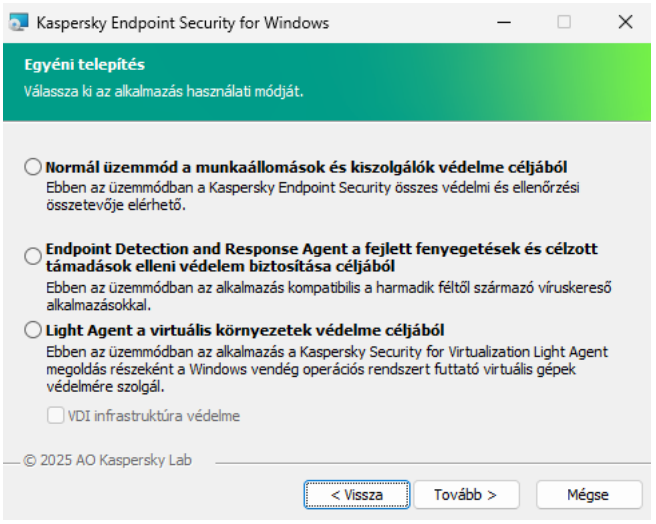
Az EDR Agent telepítéséhez ki kell választania a megfelelő konfigurációt telepítőcsomag beállításaiban vagy a Telepítővarázslóban.

Az EDR Agent telepítése a Telepítővarázsló segítségével

1. Másolja a terjesztőkészlet mappáját a felhasználó számítógépére.
2. Futtassa a setup_kes.exe fájlt.

   A Telepítővarázsló elindul.

A Kaspersky Endpoint Security konfigurációja



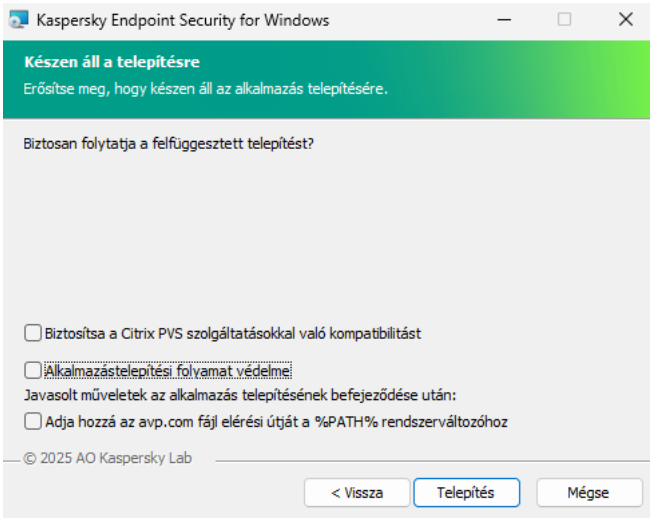
Az alkalmazás konfigurációjának kiválasztása

Jelölje be az **Endpoint Detection and Response Agent** konfigurációt. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.

Kaspersky Endpoint Security összetevők

Válassza ki a telepíteni kívánt összetevőket. Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket. Ehhez futtatnia kell a Telepítővarázslót, és ki kell választania az elérhető összetevőket.

Speciális beállítások



Alkalmazás telepítési beállításai

Alkalmazástelepítési folyamat védelme. A telepítési védelembe tartozik a terjesztőcsomagok rosszindulatú alkalmazásokkal való kicserélése elleni védelem, a Kaspersky Endpoint Security telepítési mappái elérésének blokkolása, valamint az alkalmazáskulcsokat tartalmazó beállításjegyzék-rész elérésének blokkolása. Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni.

A Citrix PVS kompatibilitás biztosítása. Engedélyezheti a Citrix Provisioning Services támogatását, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre telepítse.

Adja hozzá az avp.com fájl elérési útját a %PATH% rendszerváltozóhoz. A parancssori felület kényelmes használata érdekében hozzáadhatja a telepítés elérési útvonalát a %PATH% változóhoz.

Az EDR Agent telepítése a parancssorból (csak a KATA (EDR) és az EDR Expert (on-premises) esetén)

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security terjesztőcsomagja telepítve van.
3. Futtassa a következő parancsot:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

vagy

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

Ennek eredményeként a Kaspersky Anti Targeted Attack Platform (EDR) vagy a Kaspersky Endpoint Detection and Response Expert (on-premises) integrálására szolgáló EDR Agent alkalmazás települ a számítógépen. A `status` paranccsal ellenőrizheti az alkalmazásbeállításokat, illetve hogy az alkalmazás telepítve van-e.

Az EDR Agent telepítése az adminisztrációs konzol (MMC) használatával

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki a konzolfán az **Advanced** → **Remote installation** → **Installation packages** mappát.

   Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.
3. Nyissa meg a telepítőcsomag tulajdonságait.

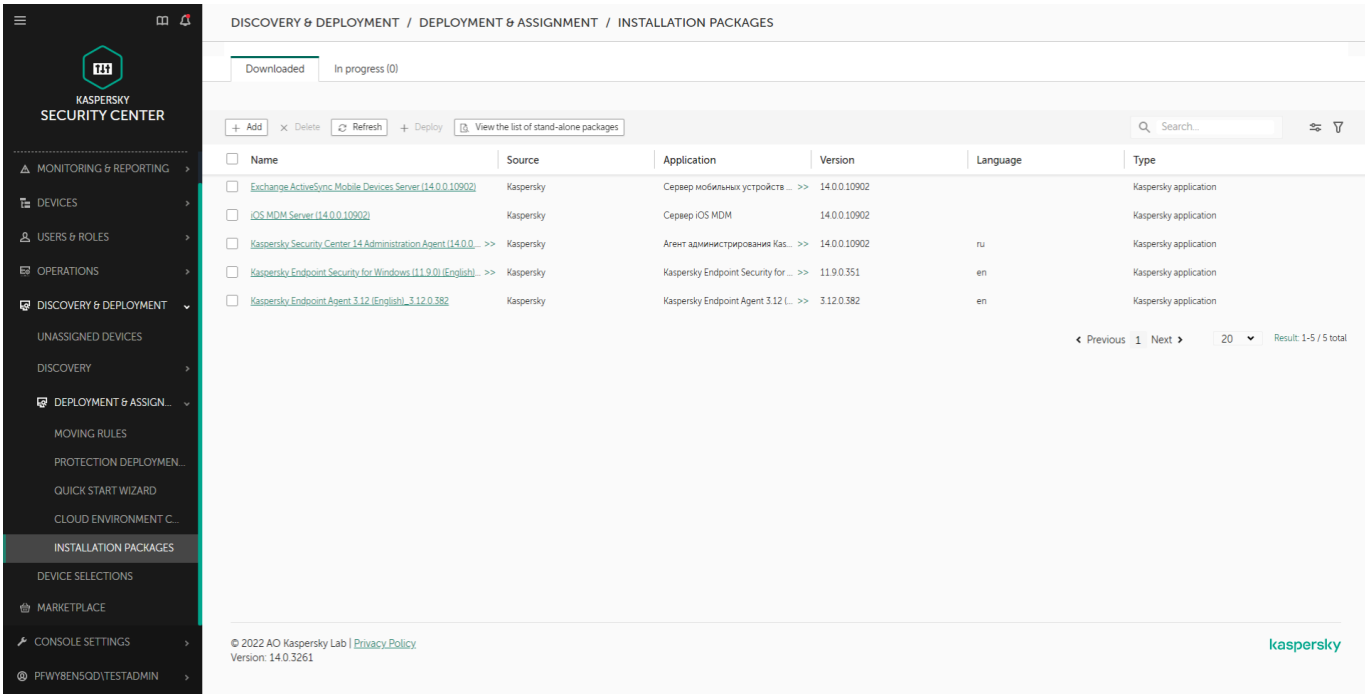
   Ha szükséges, hozzon létre egy új telepítőcsomagot.
4. Nyissa meg a **Protection components** szakaszt.
5. Válassza ki az **Endpoint Detection and Response Agent a speciális fenyegetések és a célzott támadások elleni védelemhez** konfigurációt. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.
6. Válassza ki a telepíteni kívánt összetevőket.

   Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket.
7. Mentse el a módosításokat.
8. Hozzon létre egy távoli telepítési feladatot. A feladat tulajdonságaiban válassza ki a létrehozott telepítőcsomagot.

Az EDR Agent telepítése a Web Console segítségével

1. A Web Console fő ablakában válassza az **Discovery & deployment** → **Deployment & assignment** → **Installation packages** lehetőséget.

   Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.



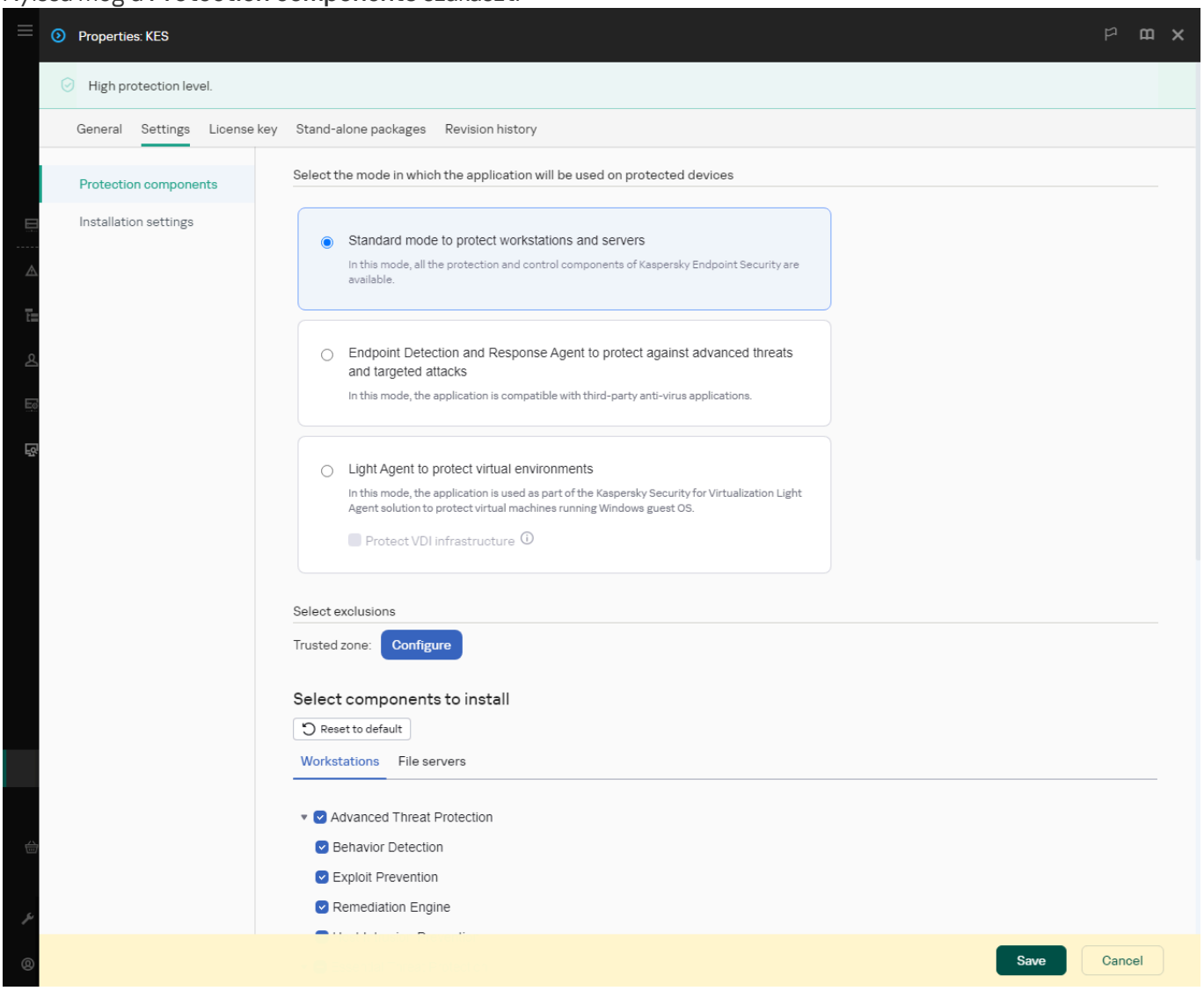
A telepítőcsomagok listája

2. Nyissa meg a telepítőcsomag tulajdonságait.

   Ha szükséges, hozzon létre egy új telepítőcsomagot.

3. Válassza ki az **Settings** lapot.

4. Nyissa meg a **Protection components** szakaszt.



A telepítőcsomagban található összetevők

5. Válassza a **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks** konfigurációt. Ebben a konfigurációban csak azokat az összetevőket telepítheti, amelyek támogatást nyújtanak az észlelési és válaszadási megoldásokhoz: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), valamint KUMA. Erre a konfigurációra akkor van szükség, ha a Kaspersky Detection and Response megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.

6. Válassza ki a telepíteni kívánt összetevőket.

   Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket.

7. Mentse el a módosításokat.

8. Hozzon létre egy távoli telepítési feladatot. A feladat tulajdonságaiban válassza ki a létrehozott telepítőcsomagot.

Ennek eredményeként az EDR Agent telepítve lesz a felhasználó számítógépére. Használhatja az alkalmazás felületét, és az alkalmazás ikonja megjelenik az értesítési területen .

A Kaspersky Security Center megoldásban az EDR Agent konfigurációjú telepített alkalmazást tartalmazó számítógép *Critical* állapottal rendelkezik – . A számítógépnek ez az állapota, mert hiányzik a Fájl védelem összetevő. Nem kell semmilyen intézkedést tennie.

Ha az EDR Agentet nem tudta telepíteni egy harmadik féltől származó EPP alkalmazást tartalmazó számítógépre, mert a telepítőprogram inkompatibilis szoftvert talált a számítógépen, akkor kihagyhatja az inkompatibilis szoftverek ellenőrzését.



Az EDR Agent főablaka

Most konfigurálnia kell az integrációt a Kaspersky Managed Detection and Response, a Kaspersky Anti Targeted Attack (EDR) vagy a Kaspersky Anti Targeted Attack (NDR) megoldással. Megadhat speciális alkalmazásbeállításokat is, és például létrehozhat egy megbízható zónát, vagy elrejtheti az alkalmazás felületét. A következő szakaszok beállításai érhetők el:

- Kaspersky Security Network
- Alkalmazásbeállítások
- Hálózati beállítások
- Kizárások
- Jelentések

- Felület
- Beállítások kezelése

Az EDR Agent integrálása az MDR megoldással

Az EDR Agent a vállalat informatikai infrastruktúrájában lévő munkaállomásokra és kiszolgálókra települ. Az EDR Agent feldolgozza az adatokat, és a Kaspersky Security Network adatfolyamain keresztül továbbítja azokat a Kaspersky Managed Detection and Response számára.

Ahhoz, hogy a Kaspersky Managed Detection and Response együtt tudjon működni a Felügyeleti kiszolgálóval a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos *háttérkapcsolatot*. A Kaspersky Managed Detection and Response a megoldás telepítésekor rákérdez a háttérkapcsolat létrehozására. Győződjön meg arról, hogy létrejött a háttérkapcsolat.

Háttérkapcsolat létrehozása a Web Console-ban

1. A Web Console fő ablakában válassza a **Settings** → **Integration** lehetőséget.
2. Nyissa meg a **Integration** szakaszt.
3. Kapcsolja be az **Background connection for integration Enabled** kapcsolót.
4. Mentse el a módosításokat.

A Kaspersky Managed Detection and Response integrálása a következő lépéseket foglalja magában:

1. **A Managed Detection and Response összetevő telepítése**

   A MDR összetevőt telepítés vagy frissítés közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

   > Ahhoz, hogy az *Alkalmazás-összetevők módosítása feladat* segítségével a számítógép újraindítása nélkül telepíthesse a Managed Detection and Response összetevőt, a feladat beállításaiban ki kell kapcsolnia az **Inkompatibilis, harmadik féltől származó alkalmazások ellenőrzése** opciót.

2. **A Privát Kaspersky Security Network konfigurálása**

   > Hagyja ki ezt a lépést, ha a Kaspersky Security Center Cloud Console-t használja. A Kaspersky Security Center Cloud Console automatikusan konfigurálja a Privát Kaspersky Security Network szolgáltatást az MDR bővítmény telepítésekor.

   A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről.

   Töltse fel a Kaspersky Security Network konfigurációs fájlját az adminisztrációs kiszolgálói tulajdonságokban. A Kaspersky Security Network konfigurációs fájlja az MDR konfigurációs fájljának ZIP-archívumában található. A ZIP-archívumot a Kaspersky Managed Detection and Response konzoljában szerezheti be. A Privát Kaspersky Security Network konfigurálásával kapcsolatos részletekért olvassa el a Kaspersky Security Center súgóját. A Kaspersky Security Network konfigurációs fájlját a parancssorból is feltöltheti a számítógépre (lásd az alábbi utasításokat).

A Privát Kaspersky Security Network konfigurálása a parancssorból

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.
3. Futtassa a következő parancsot:

```
avp.com KSN /private <file name>
```

ahol a `<file name>` a Privát Kaspersky Security Network beállításait tartalmazó konfigurációs fájl neve (PKCS7 vagy PEM fájlformátum).

Példa:
`avp.com KSN /private C:\kpsn_config.pkcs7`

Ennek eredményeként a Kaspersky Endpoint Security a Privát Kaspersky Security Network-öt használja a fájlok, az alkalmazások és a webhelyek megbízhatóságának meghatározására. A házirend-beállítások **Kaspersky Security Network** szakaszában a következő működési állapot jelenik meg: *Infrastruktúra: Kaspersky Private Security Network*.

Engedélyeznie kell a kiterjesztett KSN módot a Managed Detection and Response használatához.

3 A Kaspersky Managed Detection and Response aktiválása

A Kaspersky Endpoint Security for Windows 12.10 verziótól kezdődően a Managed Detection and Response funkció aktiválásához az aktiváló kód helyett kulcsfájlt is használhat.

Külön licenc vásárlására van szükség az MDR számára (Kaspersky Managed Detection and Response bővítmény).

A funkció a Kaspersky Managed Detection and Response bővítmény külön kulcsának hozzáadását követően lesz elérhető. Az önálló Managed Detection and Response funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

Győződjön meg arról, hogy az MDR funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén működik.

4 A Managed Detection and Response összetevő engedélyezése

Töltse be a BLOB konfigurációs fájlt a Kaspersky Endpoint Security házirendjébe (lásd az alábbi utasításokat). A BLOB fájl tartalmazza az ügyfélazonosítót és a Kaspersky Managed Detection and Response licencére vonatkozó információkat. A BLOB fájl az MDR konfigurációs fájl ZIP-archívumában található. A ZIP-archívumot a Kaspersky Managed Detection and Response konzoljában szerezheti be. A BLOB fájlról részletes információt a Kaspersky Managed Detection and Response súgójában találhat.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve BLOB fájl hozzáadása nem kötelező a Kaspersky Managed Detection and Response bérlők nélküli használatához, ha rendelkezik aktuális licenccel.

A Managed Detection and Response összetevő engedélyezének menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki a **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** lehetőséget.

4. Jelölje be a **Managed Detection and Response (Industrial CyberSecurity)** jelölőnégyzetet.

5. A **Beállítások** területen kattintson az **Feltöltés** elemre, és válassza ki a Kaspersky Managed Detection and Response konzoljában kapott BLOB fájlt. A fájl P7 kiterjesztéssel rendelkezik.

   Alapértelmezés szerint a felhasználó kezelheti az alkalmazásbeállításokat (a „lakat” nyitva van). A házirend számítógépeken való alkalmazásához zárolja a lakatokat .

6. Mentse el a módosításokat.

A Managed Detection and Response összetevő engedélyezének menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration** → **Managed Detection and Response** elemet.

5. Kapcsolja be az **Managed Detection and Response ENABLED** kapcsolót.

6. Kattintson az **Upload** elemre, és válassza ki a Kaspersky Managed Detection and Response konzoljában kapott BLOB fájlt. A fájl P7 kiterjesztéssel rendelkezik.

   Alapértelmezés szerint a felhasználó kezelheti a házirend-beállításokat (a „lakat” nyitva van). A házirend számítógépeken való alkalmazásához zárolja a lakatokat .

7. Mentse el a módosításokat.

A Managed Detection and Response összetevő engedélyezének menete a parancssorból

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.

2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

3. Futtassa a következő parancsot:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Alkalmazásbeállítások konfigurálása** jogosultsággal.

Ennek eredményeként a Kaspersky Endpoint Security ellenőrizni fogja a BLOB fájlt. A BLOB fájl ellenőrzése magában foglalja a digitális aláírás és a licenc időtartamának ellenőrzését. Ha a BLOB fájl ellenőrzése sikerült, a Kaspersky Endpoint Security leltölti a fájlt, és elküldi azt a számítógépre a Kaspersky Security Centerrel való következő szinkronizálás során. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. A **Managed Detection and Response** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

5. **Az alkalmazás egyéb összetevőinek konfigurálása telemetria fogadására**

   Engedélyeznie kell a következő összetevőket a Managed Detection and Response használatához:

   - Kaspersky Security Network (kiterjesztett mód).
   - Viselkedésészlelés.
   - Biztonsági rések kihasználásának megelőzése.
   - Web védelem.
   - Levelezés védelem.
   - Fájl védelem.
   - Hálózati védelem.
   - Tűzfal.
   - AMSI védelem.
   - Vizsgálat a háttérben.

     1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
     2. Kattintson a Kaspersky Endpoint Security házirend nevére.

        Megnyílik a rendszabályok tulajdonságai ablak.
     3. Válassza ki az **Application settings** lapot.
     4. Nyissa meg a **Built-in Agents Configuration** → **Managed Detection and Response** elemet.
     5. Kapcsolja be az **Managed Detection and Response ENABLED** kapcsolót.
     6. Mentse el a módosításokat.

     1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
     2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
     3. A házirend ablakban válassza ki a **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** lehetőséget.
     4. Jelölje be a **Managed Detection and Response (Industrial CyberSecurity)** jelölőnégyzetet.
     5. Mentse el a módosításokat.

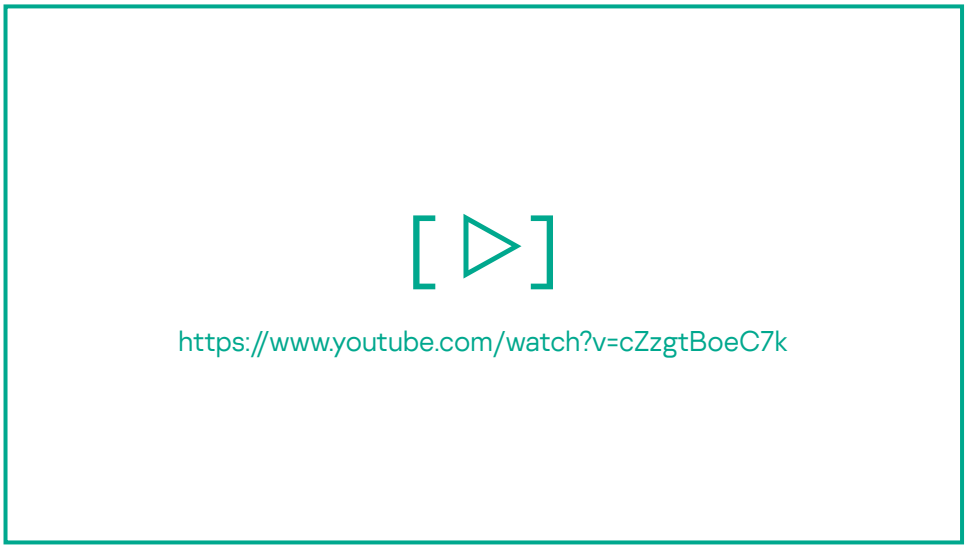
Az EDR Agent integrálása a EDR (KATA) megoldással

Az EDR Agent a vállalat informatikai infrastruktúrájában lévő munkaállomásokra és kiszolgálókra települ. Ezeken a számítógépeken az EDR Agent folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítandó fájlokat, és felügyeleti adatokat küld a Central Node összetevőt tartalmazó kiszolgálónak.

Az EDR (KATA) integrálásához engedélyeznie kell az Endpoint Detection and Response (KATA) összetevőt, és konfigurálnia kell az EDR Agentet.

A következő feltételeknek kell teljesülniük ahhoz, hogy az Endpoint Detection and Response (KATA) működjön:

- A Kaspersky Anti Targeted Attack Platform 5.0–7.1 verziói.
- Kaspersky Security Center 14.2 vagy újabb verzió. A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az Endpoint Detection and Response (KATA) szolgáltatást.



Az Endpoint Detection and Response (KATA) integrálása a következő lépéseket foglalja magában:

1. **Az Endpoint Detection and Response (KATA) aktiválása**

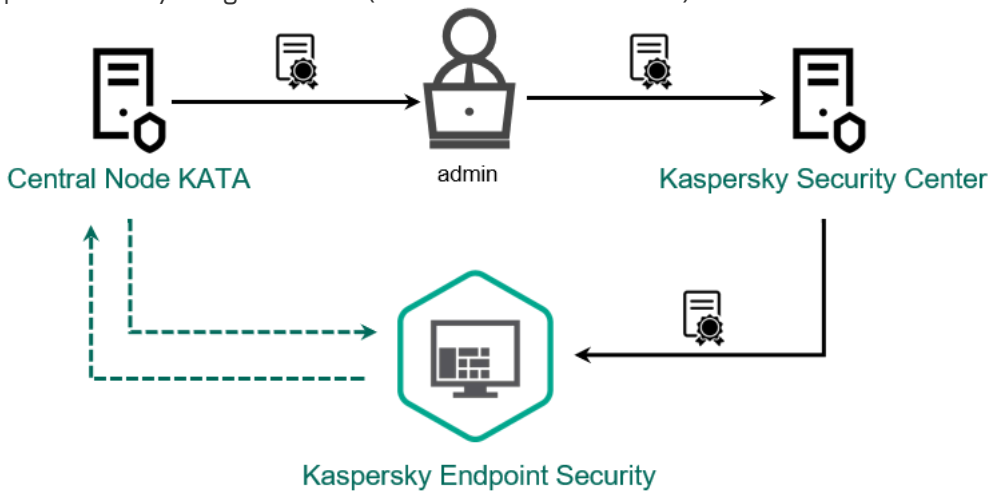
   Külön licenc vásárlására van szükség az EDR (KATA) számára (Kaspersky Endpoint Detection and Response (KATA) bővítmény).

   A funkció a Kaspersky Endpoint Detection and Response (KATA) külön kulcsának hozzáadását követően lesz elérhető. Az önálló Endpoint Detection and Response (KATA) funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

   Győződjön meg arról, hogy az EDR (KATA) funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén fut.

2. **Csatlakozás a Central Node-hoz**

A Kaspersky Anti Targeted Attack Platform megbízható kapcsolatot létesít a Kaspersky Endpoint Security és a Central Node összetevő között. A megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell használnia. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). Ezután hozzá kell adnia a TLS-tanúsítványt a Kaspersky Endpoint Security szolgáltatáshoz (lásd az alábbi utasításokat).



A TLS-tanúsítvány hozzáadása a Kaspersky Endpoint Security szolgáltatáshoz

Alapértelmezés szerint a Kaspersky Endpoint Security csak a Central Node TLS-tanúsítványát ellenőrzi. A kapcsolat biztonságosabbá tétele céljából ezenkívül engedélyezheti a számítógép ellenőrzését a Central Node-on (kétirányú hitelesítés). Az ellenőrzés engedélyezéséhez be kell kapcsolnia a kétirányú hitelesítést a Central Node és a Kaspersky Endpoint Security beállításaiban. A kétirányú hitelesítés használatához kriptotárolóra is szüksége lesz. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Central Node-hoz az adminisztrációs konzol (MMC) segítségével

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A házirend ablakban válassza a **Detection and Response → Endpoint Detection and Response Expert (on-premises)** lehetőséget.
5. Jelölje be az **Endpoint Detection and Response Expert (on-premises)** négyzetet.
6. Kattintson a **Kiszolgáló kapcsolódási beállításai** lehetőségre.
7. Konfigurálja a kiszolgálói kapcsolatot:
   - **Időtúllépés (mp)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz.
   - **Kiszolgálói TLS-tanúsítvány hibája**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

- **Kétirányú hitelesítés használata**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

  A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

8. Kattintson az **OK** gombra.
9. Central Node-kiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

   Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
10. Ha szükséges, konfigurálja a telemetriát.
11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Central Node-hoz a Web Console segítségével

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)** elemet.
5. Kapcsolja be az **Endpoint Detection and Response Expert (on-premises) ENABLED** kapcsolót.
6. Az EDR (KATA) beállításához válassza ki az **Endpoint Detection and Response Expert (version 7.1 or earlier)**lehetőséget a megoldások listájából.
7. Kattintson az **Connection settings** gombra.
8. Konfigurálja a kiszolgálói kapcsolatot:

   - **Timeout (sec)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz.
   - **Server certificate**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

- **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

  A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

9. Kattintson az **OK** gombra.
10. Central Node-kiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

    Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
11. Ha szükséges, konfigurálja a telemetriát.
12. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Ennek eredményeként a számítógép hozzá lesz adva a Kaspersky Anti Targeted Attack Platform konzolhoz. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Endpoint Detection and Response Expert (on-premises)** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

Az EDR Agent integrálása a NDR (KATA) megoldással

Az EDR Agent a vállalat informatikai infrastruktúrájában lévő munkaállomásokra és kiszolgálókra települ. Ezeken a számítógépeken az EDR Agent folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítandó fájlokat, és felügyeleti adatokat küld a Central Node összetevőt tartalmazó kiszolgálónak.

Az NDR (KATA) integrálásához engedélyeznie kell a Network Detection and Response (KATA) összetevőt, és konfigurálnia kell az EDR Agentet.

A következő feltételeknek kell teljesülniük ahhoz, hogy a Network Detection and Response (KATA) működjön:

- Kaspersky Anti Targeted Attack Platform 7.0 vagy újabb verzió.
- Kaspersky Security Center 14.2 vagy újabb verzió. A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni a Network Detection and Response (KATA) szolgáltatást.

https://www.youtube.com/watch?v=gd-rySv0ThQ

A Network Detection and Response (KATA) integrálása a következő lépéseket foglalja magában:

1. **A Network Detection and Response (KATA) aktiválása**

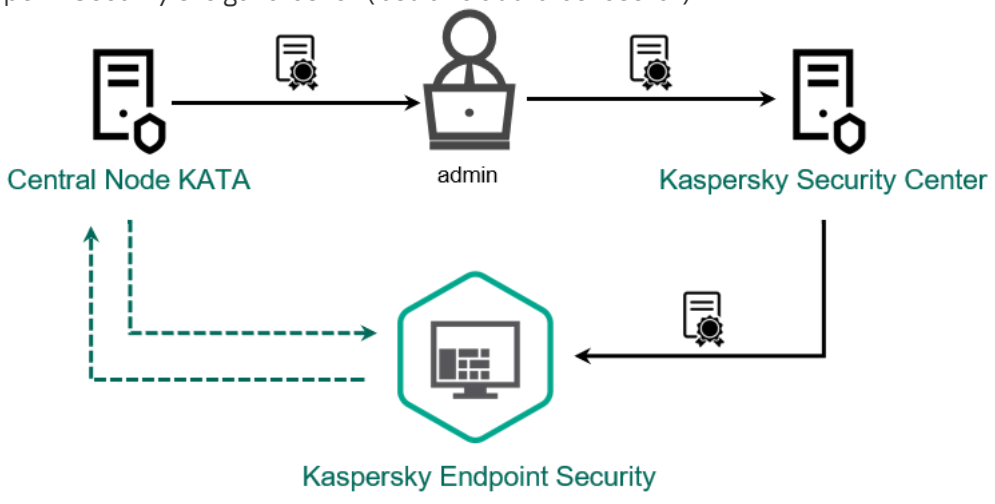
   Külön licenc vásárlására van szükség az NDR (KATA) számára (Kaspersky Network Detection and Response (KATA) bővítmény).

   A funkció a Kaspersky Network Detection and Response (KATA) külön kulcsának hozzáadását követően lesz elérhető. Az önálló Network Detection and Response (KATA) funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

   Győződjön meg arról, hogy az NDR (KATA) funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén fut.

2. **Csatlakozás a Central Node-hoz**

   A Kaspersky Anti Targeted Attack Platform megbízható kapcsolatot létesít a Kaspersky Endpoint Security és a Central Node összetevő között. A megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell használnia. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). Ezután hozzá kell adnia a TLS-tanúsítványt a Kaspersky Endpoint Security szolgáltatáshoz (lásd az alábbi utasításokat).



A TLS-tanúsítvány hozzáadása a Kaspersky Endpoint Security szolgáltatáshoz

Alapértelmezés szerint a Kaspersky Endpoint Security csak a Central Node TLS-tanúsítványát ellenőrzi. A kapcsolat biztonságosabbá tétele céljából ezenkívül engedélyezheti a számítógép ellenőrzését a Central Node-on (kétirányú hitelesítés). Az ellenőrzés engedélyezéséhez be kell kapcsolnia a kétirányú hitelesítést a Central Node és a Kaspersky Endpoint Security beállításaiban. A kétirányú hitelesítés használatához kriptotárolóra is szüksége lesz. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Central Node-hoz az adminisztrációs konzol (MMC) segítségével

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki a **Detection and Response → Network Detection and Response (KATA)** lehetőséget.
4. Jelölje be az **Network Detection and Response (KATA)** jelölőnégyzetet.
5. Kattintson az **Connection settings** gombra.
6. Konfigurálja a kiszolgálói kapcsolatot:
   - **Timeout (sec)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz.
   - **Server certificate**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).
   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.
7. Kattintson az **OK** gombra.
8. Central Node-kiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.
9. Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
10. Ha szükséges, konfigurálja a telemetriát.
11. Mentse el a módosításokat.

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Central Node-hoz a Web Console segítségével

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Network Detection and Response (KATA)** elemet.
5. Kapcsolja be az **Network Detection and Response (KATA) ENABLED** kapcsolót.
6. Kattintson az **Connection settings** gombra.
7. Konfigurálja a kiszolgálói kapcsolatot:

   - **Timeout (sec)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz.
   - **Server certificate**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).
   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.
8. Kattintson az **OK** gombra.
9. Central Node-kiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.
10. Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
11. Ha szükséges, konfigurálja a telemetriát.
12. Mentse el a módosításokat.

Ennek eredményeként a számítógép hozzá lesz adva a Kaspersky Anti Targeted Attack Platform konzolhoz. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Network Detection and Response (KATA)** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

EDR Agent integrálása az EDR Expert (on-premises) szolgáltatásba

Az EDR Agent a vállalat informatikai infrastruktúrájában lévő munkaállomásokra és kiszolgálókra települ. Ezeken a számítógépeken az EDR Agent folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítandó fájlokat, és felügyeleti adatokat küld az EDR Expert (on-premises) kiszolgálónak.

Az EDR Expert (on-premises) integrálásához engedélyeznie kell az Endpoint Detection and Response Expert (on-premises) összetevőt, és konfigurálnia kell az EDR Agentet.

Az Endpoint Detection and Response Expert (on-premises) integrálása a következő lépéseket foglalja magában:

1. **A Kaspersky Endpoint Detection and Response Expert (on-premises) aktiválása**

   Külön licenc vásárlására van szükség az EDR Expert (on-premises) számára (Kaspersky Endpoint Detection and Response Expert (on-premise) bővítmény).

   A szolgáltatás a Kaspersky Endpoint Detection and Response Expert (on-premises) külön kulcsának hozzáadását követően válik elérhetővé. Az önálló Endpoint Detection and Response Expert (on-premises) funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

   Győződjön meg arról, hogy az EDR Expert (on-premises) funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén fut.

2. **Csatlakozás a telemetriagyűjtő kiszolgálóhoz és a válaszkiszolgálóhoz**

   A Kaspersky Endpoint Detection and Response Expert (on-premises) megoldásnak megbízható kapcsolatra van szüksége a Kaspersky Endpoint Security és két kiszolgáló között:

   - A *telemetriagyűjtő kiszolgáló* egy olyan SIEM-megoldás részét képező kiszolgáló, amely a számítógépen bekövetkező eseményekre vonatkozó információkat gyűjti, normalizálja, korrelálja, elemzi és tárolja.
   - A *válaszkiszolgáló* egy olyan kiszolgáló, amely adatokat fogad és vizsgál, tanulmányozza az objektumok viselkedését, és közzéteszi az ilyen tanulmányok eredményeit.

   A megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell használnia. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). Ezután hozzá kell adnia a TLS-tanúsítványt a Kaspersky Endpoint Security szolgáltatáshoz (lásd az alábbi utasításokat).

   Alapértelmezés szerint a Kaspersky Endpoint Security csak a kiszolgálók TLS-tanúsítványát ellenőrzi. A kapcsolat biztonságosabbá tétele céljából ezenkívül engedélyezheti a számítógép ellenőrzését a kiszolgálón (kétirányú hitelesítés). Az ellenőrzés engedélyezéséhez be kell kapcsolnia a kétirányú hitelesítést a kiszolgálón és a Kaspersky Endpoint Security beállításaiban. A kétirányú hitelesítés használatához kriptotárolóra is szüksége lesz. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja).

   A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Expert (on-premises) megoldáshoz a Web Console segítségével

   1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
   2. Kattintson a Kaspersky Endpoint Security házirend nevére.

      Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)** elemet.

5. Kapcsolja be az **Endpoint Detection and Response Expert (on-premises) ENABLED** kapcsolót.

6. Az EDR Expert (on-premises) beállításához válassza ki az **Endpoint Detection and Response Expert (version 8.0 or later)**lehetőséget a megoldások listájából.

7. Konfigurálja a *telemetriagyűjtő kiszolgálók* csatlakozását:

   a. A **Connection to telemetry collection servers** részen kattintson a **Connection settings** hivatkozásra.

   b. A telemetriagyűjtő kiszolgálók csatlakozásának konfigurálása:

   - **Timeout (sec)**. A kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik kiszolgálóhoz.

   - **Server certificate**. TLS-tanúsítvány a kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja).

   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). A kiszolgáló beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

   c. Kattintson az **OK** gombra.

   d. Telemetria-gyűjtőkiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

      Több telemetriagyűjtő kiszolgáló címét is hozzáadhatja. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

   e. Ha szükséges, konfigurálja a telemetriát.

8. A *válaszkiszolgálók* kapcsolatának konfigurálása:

   a. Az **Connection to response servers** területen konfigurálhatja a **Send sync request to server every (min)** beállítást. A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security fogadja a fenyegetésre adott válasz feladatait, és elküldi a feladatok eredményeit.

   b. Kattintson a **Connection settings** hivatkozásra.

c. A válaszkiszolgálók kapcsolatának konfigurálása:

- **Timeout (sec)**. A kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik kiszolgálóhoz.
- **Server certificate**. TLS-tanúsítvány a kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja).
- **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). A kiszolgáló beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

  A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

d. Kattintson az **OK** gombra.

e. Adja hozzá a válaszkiszolgálókat. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

Több válaszkiszolgáló-címet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Ennek eredményeként a számítógép felkerül az Open Single Management Platform (OSMP) rendszerre. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Endpoint Detection and Response Expert (on-premises)** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

Kompatibilitás harmadik féltől származó EPP alkalmazásokkal

Az EDR Agent támogatja a Kaspersky Detection and Response megoldásainak funkcionalitását. Az EDR Agenthez nem állnak rendelkezésre védelmi és felügyeleti szolgáltatások. Ez a konfiguráció lehetővé teszi harmadik féltől származó EPP alkalmazások telepítését és a Kaspersky Detection and Response megoldások telepítését a vállalat infrastruktúrájában. Az EDR Agent támogatja a Kaspersky Managed Detection and Response, a Kaspersky Anti Targeted Attack Platform (EDR) és a Kaspersky Anti Targeted Attack Platform (NDR) megoldásokkal való együttműködést.

Az EDR Agent a következő gyártók EPP alkalmazásaival kompatibilis:

- **Dr.Web**

  Az EDR Agent kompatibilis a Dr.Web Agent for Windows 13.0.1 vagy újabb verziójával és a Dr.Web Server (x64) 13.0.0.10200 verzióval.

- **Dallas Lock**

  Az EDR Agent kompatibilis a Dallas Lock 8.0-C 11.4.2.843 vagy újabb verziójával.

Ahhoz, hogy az EDR Agent futhasson olyan számítógépen, amelyen telepítve van a Dallas Lock szoftver, a tűzfalmodul beállításaiban engedélyeznie kell a Kaspersky külső szolgáltatásaihoz való kapcsolatot.

- **Secret Net Studio**

  Az EDR Agent kompatibilis a Secret Net Studio 8.11 vagy újabb verziójával.

  Az alkalmazás nem telepíthető olyan számítógépre, amelyen a Secret Net Studio a víruskereső összetevővel van telepítve. Az együttműködés lehetővé tételéhez el kell távolítania a víruskereső összetevőt a Secret Net Studio-ból.

- **Trend Micro**

  Az EDR Agent kompatibilis a Trend Micro Apex One 14.0.12994 vagy újabb verziójával (beleértve a Security Agent megoldást is).

  Az EDR Agent kompatibilis a Trend Micro Deep Security 20.0.2-4960 vagy újabb verziójával (beleértve a Security Agent megoldást is).

- **Windows Defender**

- **Sophos**

  Az EDR Agent kompatibilis a Sophos Intercept X 2024.1.2 vagy újabb verziójával (beleértve az Endpoint Agent megoldást) és a Sophos Core Agent 2024.3.2.3 verziójával.

- **Bitdefender**

  Az EDR Agent kompatibilis a Bitdefender Endpoint Security Tools 7.9.21.523 vagy újabb verziójával.

- **ESET**

  Az EDR Agent kompatibilis az ESET Endpoint Security 12.0.2049.0 vagy újabb verziójával és az ESET Management Agent 12.0 vagy újabb verziójával.

A Windows 11 for Arm64 rendszert futtató számítógépeken az EDR Agent nem kompatibilis a következővel: Bitdefender Endpoint Security Tools.

Az alkalmazásokat a következő sorrendben kell telepíteni: először telepítse az EPP alkalmazást, majd a Kaspersky Security Center Network Agentet, majd az EDR Agentet. Erre azért van szükség, mert az EPP alkalmazás telepítője inkompatibilis szoftverként észlelheti az EDR Agentet és a Network Agentet, és eltávolíthatja őket. Az EDR Agent és a Network Agent működését a harmadik féltől származó EPP alkalmazás frissítése után is ellenőrizni kell, mert a telepítő újra átvizsgálhatja a számítógépet, hogy inkompatibilis szoftvereket keressen, és eltávolíthatja az alkalmazásokat.

Ha az EDR Agentet nem tudta telepíteni egy harmadik féltől származó EPP alkalmazást tartalmazó számítógépre, mert a telepítőprogram inkompatibilis szoftvert talált a számítógépen, akkor kihagyhatja az inkompatibilis szoftverek ellenőrzését.

Managed Detection and Response

A Kaspersky Endpoint Security for Windows támogatja a Managed Detection and Response megoldással való integrációt. A *Kaspersky Managed Detection and Response (MDR)* megoldás automatikusan észleli és elemzi az infrastruktúrában bekövetkező biztonsági incidenseket. Ehhez az MDR a végpontoktól és a gépi tanulásból kapott telemetriai adatokat használja. Az MDR incidensadatokat küld a Kaspersky szakértőinek. A szakértők ezután feldolgozhatják az incidenst, és például új bejegyzést adhatnak hozzá a vírusadatbázisokhoz. Alternatív megoldásként a szakértők javaslatokat tehetnek az incidens feldolgozására, és például javasolhatják a számítógép leválasztását a hálózatról. A megoldás működéséről részletes információt a Kaspersky Managed Detection and Response súgójában talál.

A Kaspersky Endpoint Security konfigurációi az MDR-hez való integrációhoz

A következő konfigurációk használhatók az MDR-hez:

- **[KES+beépített ügynök]**. Ebben a konfigurációban a Kaspersky Endpoint Security a számítógép biztonságát garantáló alkalmazásként és az MDR-rel való munkavégzéshez is használható alkalmazásként működik. A beépített ügynök a Kaspersky Endpoint Security 11.6.0 for Windows vagy újabb verziójában érhető el.
- **[külső EPP+EDR Agent]**. Ebben a konfigurációban az IT-infrastruktúra biztonságát a harmadik féltől származó Endpoint Protection Platform (EPP) garantálja. Az MDR-rel való interakciót a Kaspersky Endpoint Security biztosítja az Endpoint Detection and Response Agent (EDR Agent) konfigurációban. Ebben a konfigurációban az EDR Agent kompatibilis a harmadik féltől származó EPP-alkalmazásokkal. Az EDR Agent a Kaspersky Endpoint Security 12.3 for Windows vagy újabb verzióban érhető el.

A Kaspersky Endpoint Security korábbi verzióinak támogatása

A Kaspersky Endpoint Security 11-es és újabb verziói támogatják az MDR megoldást. A Kaspersky Endpoint Security 11–11.5.0 verziója csak telemetriai adatokat küld a Kaspersky Managed Detection and Response számára, hogy lehetővé tegye a fenyegetések észlelését. A Kaspersky Endpoint Security 11.6.0 verziója a beépített ügynök (Kaspersky Endpoint Agent) minden funkciójával rendelkezik.

Ha a Kaspersky Endpoint Security 11–11.5.0 verziót használja, akkor az MDR megoldás használatához frissítenie kell az adatbázisokat a legújabb verzióra. Telepítenie kell a Kaspersky Endpoint Agent szolgáltatást is.

Ha a Kaspersky Endpoint Security 11.6.0 vagy újabb verzióját használja, az MDR megoldás használatához nem kell telepítenie a Kaspersky Endpoint Agentet.

Ha a Kaspersky Endpoint Security házirendje olyan számítógépekre is vonatkozik, amelyeken nincs telepítve a Kaspersky Endpoint Security 11–11.5.0, akkor először létre kell hoznia egy külön Kaspersky Endpoint Agent-házirendet ezekhez a számítógépekhez. Az új házirendben konfigurálhatja az integrációt a Kaspersky Managed Detection and Response szolgáltatással.

A beépített ügynök integrációja az MDR megoldással

A Kaspersky Managed Detection and Response integrációjának beállításához engedélyeznie kell a Managed Detection and Response összetevőt, és konfigurálnia kell a Kaspersky Endpoint Security alkalmazást.

Ahhoz, hogy a Kaspersky Managed Detection and Response együtt tudjon működni a Felügyeleti kiszolgálóval a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos *háttérkapcsolatot*. A Kaspersky Managed Detection and Response a megoldás telepítésekor rákérdez a háttérkapcsolat létrehozására. Győződjön meg arról, hogy létrejött a háttérkapcsolat.

Háttérkapcsolat létrehozása a Web Console-ban

1. A Web Console fő ablakában válassza a **Settings** → **Integration** lehetőséget.
2. Nyissa meg a **Integration** szakaszt.
3. Kapcsolja be az **Background connection for integration Enabled** kapcsolót.
4. Mentse el a módosításokat.

A Kaspersky Managed Detection and Response integrálása a következő lépéseket foglalja magában:

1. **A Managed Detection and Response összetevő telepítése**

   A MDR összetevőt telepítés vagy frissítés közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

   > Ahhoz, hogy az *Alkalmazás-összetevők módosítása feladat* segítségével a számítógép újraindítása nélkül telepíthesse a Managed Detection and Response összetevőt, a feladat beállításaiban ki kell kapcsolnia az **Inkompatibilis, harmadik féltől származó alkalmazások ellenőrzése** opciót.

2. **A Privát Kaspersky Security Network konfigurálása**

   > Hagyja ki ezt a lépést, ha a Kaspersky Security Center Cloud Console-t használja. A Kaspersky Security Center Cloud Console automatikusan konfigurálja a Privát Kaspersky Security Network szolgáltatást az MDR bővítmény telepítésekor.

   A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről.

   Töltse fel a Kaspersky Security Network konfigurációs fájlját az adminisztrációs kiszolgálói tulajdonságokban. A Kaspersky Security Network konfigurációs fájlja az MDR konfigurációs fájljának ZIP-archívumában található. A ZIP-archívumot a Kaspersky Managed Detection and Response konzoljában szerezheti be. A Privát Kaspersky Security Network konfigurálásával kapcsolatos részletekért olvassa el a Kaspersky Security Center súgóját. A Kaspersky Security Network konfigurációs fájlját a parancssorból is feltöltheti a számítógépre (lásd az alábbi utasításokat).

A Privát Kaspersky Security Network konfigurálása a parancssorból

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.
3. Futtassa a következő parancsot:

   ```
   avp.com KSN /private <file name>
   ```

   ahol a `<file name>` a Privát Kaspersky Security Network beállításait tartalmazó konfigurációs fájl neve (PKCS7 vagy PEM fájlformátum).

   Példa:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Ennek eredményeként a Kaspersky Endpoint Security a Privát Kaspersky Security Network-öt használja a fájlok, az alkalmazások és a webhelyek megbízhatóságának meghatározására. A házirend-beállítások **Kaspersky Security Network** szakaszában a következő működési állapot jelenik meg: *Infrastruktúra: Kaspersky Private Security Network*.

Engedélyeznie kell a kiterjesztett KSN módot a Managed Detection and Response használatához.

3 A Kaspersky Managed Detection and Response aktiválása

A Kaspersky Endpoint Security for Windows 12.10 verziótól kezdődően a Managed Detection and Response funkció aktiválásához az aktiváló kód helyett kulcsfájlt is használhat.

A Kaspersky Managed Detection and Response a következő licencelési módszereket támogatja:

- A Kaspersky Endpoint Security for Windows licenc tartalmazza a Managed Detection and Response funkciót.

  A funkció a Kaspersky Endpoint Security for Windows aktiválása után azonnal elérhetővé válik.

- Az MDR (Kaspersky Managed Detection and Response bővítmény) külön licencet használ.

  A funkció a Kaspersky Managed Detection and Response bővítmény külön kulcsának hozzáadását követően lesz elérhető. Ennek eredményeképpen két kulcs kerül hozzáadásra a számítógépen: egy kulcs a Kaspersky Endpoint Security és egy kulcs a Kaspersky Managed Detection and Response számára.

  Az önálló Managed Detection and Response funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

Győződjön meg arról, hogy az MDR funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén működik.

4 A Managed Detection and Response összetevő engedélyezése

Töltse be a BLOB konfigurációs fájlt a Kaspersky Endpoint Security házirendjébe (lásd az alábbi utasításokat). A BLOB fájl tartalmazza az ügyfélazonosítót és a Kaspersky Managed Detection and Response licencére vonatkozó információkat. A BLOB fájl az MDR konfigurációs fájl ZIP-archívumában található. A ZIP-archívumot a Kaspersky Managed Detection and Response konzoljában szerezheti be. A BLOB fájlról részletes információt a Kaspersky Managed Detection and Response súgójában találhat.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve BLOB fájl hozzáadása nem kötelező a Kaspersky Managed Detection and Response bérlők nélküli használatához, ha rendelkezik aktuális licenccel.

A Managed Detection and Response összetevő engedélyezének menete az Adminisztrációs Konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki a **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** lehetőséget.
4. Jelölje be a **Managed Detection and Response (Industrial CyberSecurity)** jelölőnégyzetet.
5. A **Beállítások** területen kattintson az **Feltöltés** elemre, és válassza ki a Kaspersky Managed Detection and Response konzoljában kapott BLOB fájlt. A fájl P7 kiterjesztéssel rendelkezik.

   Alapértelmezés szerint a felhasználó kezelheti az alkalmazásbeállításokat (a „lakat" nyitva van). A házirend számítógépeken való alkalmazásához zárolja a lakatokat .
6. Mentse el a módosításokat.

A Managed Detection and Response összetevő engedélyezének menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration → Managed Detection and Response** elemet.
5. Kapcsolja be az **Managed Detection and Response ENABLED** kapcsolót.
6. Kattintson az **Upload** elemre, és válassza ki a Kaspersky Managed Detection and Response konzoljában kapott BLOB fájlt. A fájl P7 kiterjesztéssel rendelkezik.

   Alapértelmezés szerint a felhasználó kezelheti a házirend-beállításokat (a „lakat" nyitva van). A házirend számítógépeken való alkalmazásához zárolja a lakatokat .
7. Mentse el a módosításokat.

A Managed Detection and Response összetevő engedélyezének menete a parancssorból

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

3. Futtassa a következő parancsot:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Alkalmazásbeállítások konfigurálása** jogosultsággal.

Ennek eredményeként a Kaspersky Endpoint Security ellenőrizni fogja a BLOB fájlt. A BLOB fájl ellenőrzése magában foglalja a digitális aláírás és a licenc időtartamának ellenőrzését. Ha a BLOB fájl ellenőrzése sikerült, a Kaspersky Endpoint Security leltölti a fájlt, és elküldi azt a számítógépre a Kaspersky Security Centerrel való következő szinkronizálás során. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. A **Managed Detection and Response** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

5. **Az alkalmazás egyéb összetevőinek konfigurálása telemetria fogadására**

Engedélyeznie kell a következő összetevőket a Managed Detection and Response használatához:

- Kaspersky Security Network (kiterjesztett mód).
- Viselkedésészlelés.
- Biztonsági rések kihasználásának megelőzése.
- Web védelem.
- Levelezés védelem.
- Fájl védelem.
- Hálózati védelem.
- Tűzfal.
- AMSI védelem.
- Vizsgálat a háttérben.

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Managed Detection and Response** elemet.

5. Kapcsolja be az **Managed Detection and Response ENABLED** kapcsolót.

6. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza ki a **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** lehetőséget.

4. Jelölje be a **Managed Detection and Response (Industrial CyberSecurity)** jelölőnégyzetet.

5. Mentse el a módosításokat.

KEA-KES migrációs útmutató az MDR számára

A Kaspersky Endpoint Security for Windows tartalmaz egy beépített ügynököt a Kaspersky Managed Detection and Response megoldáshoz. Az MDR-rel való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra. A Kaspersky Endpoint Agent minden funkcióját a Kaspersky Endpoint Security végzi.

Amikor olyan számítógépeken telepíti a Kaspersky Endpoint Security alkalmazást, amelyekre telepítve van a Kaspersky Endpoint Agent, a Kaspersky Managed Detection and Response megoldás továbbra is együttműködik a Kaspersky Endpoint Security termékkel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről. A Kaspersky Endpoint Security 11.6.0 vagy újabb verzióra történő frissítésekor a rendszer ugyanígy viselkedik.

A Kaspersky Endpoint Security nem kompatibilis a Kaspersky Endpoint Agent szolgáltatással. Ezeket az alkalmazásokat nem telepítheti ugyanarra a számítógépre.

A következő feltételeknek kell teljesülniük ahhoz, hogy a Kaspersky Endpoint Security a Kaspersky Managed Detection and Response részeként működjön:

- Kaspersky Security Center 13.2 vagy újabb verzió (beleértve a Network Agentet is). A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az Managed Detection and Response szolgáltatást.
- Létrejön a háttérkapcsolat a Kaspersky Security Center Web Console és a Felügyeleti kiszolgáló között. Ahhoz, hogy az MDR működni tudjon az Administration Serverrel a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos kapcsolatot, egy *háttérkapcsolatot*.

A [KES+KEA] konfiguráció [KES+beépített ügynök] MDR-be történő migrálásának lépései

1. **A Kaspersky Endpoint Security felügyeleti bővítményének frissítése**

   Az MDR összetevő a Kaspersky Endpoint Security adminisztrációs bővítmény 11.6 vagy újabb verziójával felügyelhető. A Kaspersky Security Center konzol típusától függően frissítse a felügyeleti bővítményt az adminisztrációs konzolon (MMC) vagy a webes bővítményt a Web Console-on.

2. **Házirendek és a feladatok áttelepítése**

A Kaspersky Endpoint Agent beállításainak átvitele a Kaspersky Endpoint Security for Windows megoldásba. A következők közül választhat:

- Varázsló a Kaspersky Endpoint Agent termékről a Kaspersky Endpoint Security termékre történő áttelepítéshez. A Kaspersky Endpoint Agent termékről a Kaspersky Endpoint Security termékre történő áttelepítést segítő varázsló csak a Web Console-ban működik

  A szabályzat- és feladatbeállítások áttelepítése a Kaspersky Endpoint Agent szolgáltatásból a Kaspersky Endpoint Security szolgáltatásba a Web Console-on

  A Web Console fő ablakában válassza a **Operations → Migration from Kaspersky Endpoint Agent** lehetőséget.

  Ezzel futtatja a szabályzat- és feladatáttelepítési varázslót. Kövesse a varázsló utasításait.

  1. lépés. Szabályzat áttelepítése

  Az áttelepítési varázsló új szabályzatot hoz létre, amely egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent szabályzatainak beállításait. A listában válassza ki azokat a Kaspersky Endpoint Agent szabályzatokat, amelyek beállításait egyesíteni szeretné a Kaspersky Endpoint Security szabályzatával. Kattintson a Kaspersky Endpoint Agent szabályzatára, és válassza ki azt a Kaspersky Endpoint Security szabályzatot, amellyel egyesíteni szeretné a beállításokat. Győződjön meg arról, hogy a megfelelő szabályzatokat választotta, és folytassa a következő lépéssel.

  2. lépés. Feladatok áttelepítése

  Az áttelepítési varázsló nem támogatja az MDR feladatokat. Átugorhatja ezt a lépést.

  3. lépés. A varázsló befejezése

  Lépjen ki a varázslóból. A varázsló eredményeként egy új Kaspersky Endpoint Security házirend jön létre. A szabályzat egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent beállításait. A szabályzat neve *<Kaspersky Endpoint Security policy name> és <Kaspersky Endpoint Agent policy name>*. Az új házirend *Inactive* állapotot kap. A folytatáshoz módosítsa a Kaspersky Endpoint Agent és a Kaspersky Endpoint Security szabályzatok állapotát *Inactive* értékre, és aktiválja az új egyesített szabályzatot.

- A standard Házirend és feladatok kötegelt konvertálási varázslója. A Házirendek és feladatok kötegelt konvertálási varázslója csak az Adminisztrációs konzolon (MMC) érhető el. A Házirendek és feladatok kötegelt konvertálási varázslójával kapcsolatos további részletekért olvassa el a következőt: Kaspersky Security Center Súgó.

3. **Az MDR funkció licencelése**

   A Kaspersky Endpoint Security aktiválásához a Kaspersky Managed Detection and Response megoldás részeként külön licenc szükséges a Kaspersky Managed Detection and Response kiegészítőhöz. A kulcsot a *Add key* feladat segítségével veheti fel. Ennek eredményeképpen a rendszer két kulcsot ad hozzá az alkalmazáshoz: *Kaspersky Endpoint Security* és *Kaspersky Managed Detection and Response*.

4. **A Kaspersky Endpoint Security alkalmazás telepítése/frissítése**

Az alkalmazás telepítése vagy frissítése során az MDR funkciók áttelepítéséhez ajánlott a távoli telepítési feladat használata. Távoli telepítési feladat létrehozásakor a telepítőcsomag beállításaiban ki kell választania az MDR összetevőt.

Az alkalmazást a következő módszerekkel is frissítheti:

- A Kaspersky frissítési szolgáltatás használatával.
- Helyben, a Telepítővarázsló segítségével.

A Kaspersky Endpoint Security támogatja az összetevők automatikus kiválasztását az alkalmazásfrissítés során az olyan számítógép esetében, amelyre a Kaspersky Endpoint Agent alkalmazás telepítve van. Az összetevők automatikus kiválasztása az alkalmazás frissítését végző felhasználói fiók engedélyeitől függ.

Ha a Kaspersky Endpoint Security frissítése a rendszerfiók (SYSTEM) alatt található EXE- vagy MSI-fájl használatával történik, a Kaspersky Endpoint Security hozzáférést kap a Kaspersky-megoldások aktuális licenceihez. Ezért ha a számítógépen telepítve van a Kaspersky Endpoint Agent és aktiválva van az MDR megoldás, a Kaspersky Endpoint Security telepítője automatikusan konfigurálja az összetevők készletét, és kiválasztja az MDR összetevőt. Ezáltal a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt. Az MSI-telepítő rendszerfiók (SYSTEM) alatti futtatása általában a Kaspersky frissítési szolgáltatása keretében történő frissítéskor vagy egy telepítőcsomag Kaspersky Security Centerrel végzett telepítésekor zajlik.

Ha a Kaspersky Endpoint Security frissítése emelt szintű jogosultsággal nem rendelkező felhasználói fiók alatt található MSI-fájl használatával történik, a Kaspersky Endpoint Security nem kap hozzáférést a Kaspersky-megoldások aktuális licenceihez. Ebben az esetben a Kaspersky Endpoint Security automatikusan kiválasztja az összetevőket a Kaspersky Endpoint Agent összetevőinek készlete alapján. Ezután a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt.

A Kaspersky Endpoint Security támogatja a frissítést a számítógép újraindítása nélkül. Az alkalmazásfrissítési módot a házirend tulajdonságaiban választhatja ki.

5. **Az alkalmazás működésének ellenőrzése**

Ha az alkalmazás telepítése vagy frissítése után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

- Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
- Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal. Ha egy összetevőnél *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy aktiválta a beépített ügynök funkciót.
- Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.

Endpoint Detection and Response

A Kaspersky Endpoint Security for Windows beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Optimum megoldáshoz (a továbbiakban: „EDR Optimum"). A 11.8.0 verzióval kezdődően a Kaspersky Endpoint Security for Windows beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Expert megoldáshoz (a továbbiakban: „EDR Expert"). A *Kaspersky Endpoint Detection and Response* megoldáscsomag a vállalat informatikai infrastruktúrájának védelmét biztosítja a fejlett számítógépes fenyegetések ellen. A megoldások ötvözik a fenyegetések különböző automatikus észlelését, és képesek reagálni ezekre a fenyegetésekre, hogy ellensúlyozzák a speciális támadásokat, beleértve az új biztonsági réseket, a zsarolóprogramokat, a fájlmentes támadásokat, valamint a legitim rendszereszközöket használó módszereket. Az EDR Expert több fenyegetésfigyelési és reagálási funkciót kínál, mint az EDR Optimum. A megoldásokról részletesen a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban olvashat.

Fenyegetés-felderítési eszközök

A Kaspersky Endpoint Detection and Response a következő Threat Intelligence eszközöket használja:

- Integráció a Kaspersky Threat Intelligence Portállal, amely információkat tartalmaz és jelenít meg fájlok és webcímek megbízhatóságáról.
- Kaspersky Threats adatbázis.
- Kaspersky Security Network (a továbbiakban: KSN) felhőszolgáltatási infrastruktúra, amely hozzáférést biztosít a Kaspersky tudásbázisából származó valós idejű fájl-, webhely- és szoftver-megbízhatósági információkhoz. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban képes reagálni a fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken.
- Cloud Sandbox technológia, amely lehetővé teszi, hogy észlelt fájlokat futtasson elszigetelt környezetben és ellenőrizze azok megbízhatóságát.

A megoldás működési elve

A Kaspersky Endpoint Detection and Response felügyeli és elemzi a fenyegetések fejlődését, és olyan információkat szolgáltat a *biztonsági személyzetnek* vagy a *rendszergazdának* a lehetséges támadásról, amely szükséges az időben történő reagáláshoz. A Kaspersky Endpoint Detection and Response külön ablakban jeleníti meg az észlelés részleteit. A *riasztás* olyan esemény a vállalati IT-infrastruktúrában, amelyet az alkalmazás szokatlan vagy gyanús eseményként azonosított, és amely biztonsági fenyegetést jelenthet a vállalati IT-infrastruktúrára. Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

A Kaspersky Endpoint Security korábbi verzióinak támogatása

Ha a Kaspersky Endpoint Security 11.2.0–11.6.0 verzióját használja a Kaspersky Endpoint Detection and Response Optimummal való együttműködésre, akkor az alkalmazás magában foglalja a Kaspersky Endpoint Agent szolgáltatást. A Kaspersky Endpoint Agent szolgáltatást a Kaspersky Endpoint Security szolgáltatással együtt telepítheti. A Kaspersky Endpoint Security 11.9.0 verziójában a Kaspersky Endpoint Agent terjesztőcsomag már nem része a Kaspersky Endpoint Security terjesztőkészletének.

A Kaspersky Endpoint Detection and Response Expert megoldás nem támogatja az átjárhatóságot a Kaspersky Endpoint Agent megoldással. A Kaspersky Endpoint Detection and Response Expert megoldás a beépített ügynököt tartalmazó Kaspersky Endpoint Security-t használja (11.8.0 vagy újabb verzió).

A beépített ügynök integrációja az EDR Optimum / EDR Expert megoldással

A Kaspersky Endpoint Detection and Response integrációjának beállításához hozzá kell adnia az Endpoint Detection and Response Optimum vagy az Endpoint Detection and Response Expert (cloud) összetevőt, és konfigurálnia kell a Kaspersky Endpoint Security-t.

Az Endpoint Detection and Response Optimum, az Endpoint Detection and Response Expert (cloud) és az Endpoint Detection and Response Expert (on-premises) összetevők nem kompatibilisek egymással.

A következő feltételeknek kell teljesülniük ahhoz, hogy az Endpoint Detection and Response működjön:

- Kaspersky Security Center 13.2 vagy újabb verzió. A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az Endpoint Detection and Response szolgáltatást.
- Kaspersky Endpoint Detection and Response felügyeleti bővítmény.

  A Kaspersky Endpoint Security 12.6-os verziójától kezdve a riasztások részleteinek megjelenítése a Kaspersky Endpoint Security felügyeleti bővítményből az EDR felügyeleti bővítménybe került át. Az EDR felügyeleti bővítmény egyetlen bővítmény a Windows, Mac és Linux operációs rendszereken futó ügynökökkel való munkavégzéshez. Mostantól az EDR Optimummal való munkavégzés során a Kaspersky Endpoint Security adminisztrációs bővítményre van szükség a fenyegetéselhárítási feladatok létrehozásához, valamint az EDR adminisztrációs bővítményre a riasztások részleteinek megtekintéséhez.
- A Kaspersky Endpoint Security részeként az Endpoint Detection and Response Optimum összetevő támogatja az interakciót a Kaspersky Endpoint Detection and Response Optimum 2.0 megoldással. A Kaspersky Endpoint Detection and Response Optimum 1.0 verzióval való kommunikáció nem támogatott.
- Az EDR Optimum a Kaspersky Security Center Web Console-on és a Kaspersky Security Center Cloud Console-on keresztül kezelhető.

  Az EDR Expert funkcióit csak a Kaspersky Security Center Cloud Console használatával lehet felügyelni. Ezt a funkciót nem felügyelheti az Adminisztrációs Konzol (MMC) használatával.
- Az alkalmazás aktiválva van, és a funkciójára a licenc kiterjed.
- Az Endpoint Detection and Response összetevő be van kapcsolva.
- Azok az alkalmazásösszetevők, amelyektől az Endpoint Detection and Response függ, engedélyezve vannak és működőképesek. Az Endpoint Detection and Response a következő összetevőktől függ:
  - Fájl védelem.
  - Web védelem.
  - Levelezés védelem.
  - Biztonsági rések kihasználásának megelőzése.
  - Viselkedésészlelés.
  - Behatolásmegelőző rendszer.

- Kármentesítő motor.
- Adaptív Anomáliafelügyelő.

A Kaspersky Endpoint Detection and Response integrálása a következő lépéseket foglalja magában:

1. **Az Endpoint Detection and Response összetevők telepítése**

   A Endpoint Detection and Response Optimum vagy a Endpoint Detection and Response Expert (cloud) összetevőt kiválaszthatja a telepítés vagy a frissítés során, valamint a *Alkalmazásösszetevők módosítása* feladat használatával.

   > Újra kell indítania a számítógépét az alkalmazás új elemekkel történő frissítésének befejezéséhez.

2. **A Kaspersky Endpoint Detection and Response aktiválása**

   A Kaspersky Endpoint Detection and Response használatára vonatkozó licencet a következő módokon szerezheti be:

   - A Kaspersky Endpoint Security for Windows licenc tartalmazza az Endpoint Detection and Response funkciót.

     A funkció a Kaspersky Endpoint Security for Windows aktiválása után azonnal elérhetővé válik.

   - Külön licenc vásárlása az EDR Optimum vagy az EDR Expert számára (Kaspersky Endpoint Detection and Response bővítmény).

     A funkció a Kaspersky Endpoint Detection and Response külön kulcsának hozzáadását követően lesz elérhető. Ennek eredményeképpen két kulcs kerül hozzáadásra a számítógépen: egy kulcs a Kaspersky Endpoint Security és egy kulcs a Kaspersky Endpoint Detection and Response számára.

     Az önálló Endpoint Detection and Response funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

   Győződjön meg arról, hogy az EDR Optimum vagy EDR Expert szolgáltatás szerepel a licencben, és az alkalmazás helyi felületén fut.

   Az EDR Optimum Végfelhasználói Licencszerződéssel kapcsolatos további információkért olvassa el a Kaspersky Endpoint Detection and Response Optimum súgót.

3. **Az Endpoint Detection and Response összetevők engedélyezése**

   Engedélyezheti vagy letilthatja az összetevőt a Kaspersky Endpoint Security for Windows házirend-beállításaiban.

   Az Endpoint Detection and Response összetevő engedélyezése vagy letiltása a Web Console-ban és a Cloud Console-ban

   1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
   2. Kattintson a Kaspersky Endpoint Security házirend nevére.

      Megnyílik a rendszabályok tulajdonságai ablak.
   3. Válassza ki az **Application settings** lapot.
   4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response** elemet.
   5. Kapcsolja be az **Endpoint Detection and Response ENABLED** kapcsolót.
   6. Mentse el a módosításokat.

A Kaspersky Endpoint Detection and Response összetevő engedélyezve van. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Endpoint Detection and Response Optimum** vagy az **Endpoint Detection and Response Expert (cloud)** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevőinek listájához.

4. **Adatátvitel engedélyezése az adminisztrációs kiszolgálóra**

   Az Endpoint Detection and Response összes funkciójának engedélyezéséhez az adatátvitelt a következő adattípusok esetében kell engedélyezni:

   - Karanténba helyezett fájlok adatai.

     Az adatokra a számítógépen karanténba helyezett fájlokkal kapcsolatos információk megszerzéséhez van szükség a Web Console-on és a Cloud Console-on keresztül. Letölthet például egy fájlt a karanténból a Web Console-ban és a Cloud Console-ban történő elemzéshez.

   - Fenyegetés-fejlődési lánc adatai.

     Az adatokra a számítógépen észlelt fenyegetésekről szóló információk megszerzéséhez van szükség a Web Console-on és a Cloud Console-on keresztül. A Web Console-ban és a Cloud Console-ban megtekintheti az észlelés részleteit, és válaszlépéseket tehet.

   Útmutató az adatátvitel az adminisztrációs kiszolgálóra funkció engedélyezéséhez a Web Console-ban és a Cloud Console-ban

   1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
   2. Kattintson a Kaspersky Endpoint Security házirend nevére.

      Megnyílik a rendszabályok tulajdonságai ablak.
   3. Válassza ki az **Application settings** lapot.
   4. Nyissa meg a **General Settings** → **KSC Integration** elemet.
   5. A **Data transfer to Administration Server** részen kattintson a **Advanced settings** hivatkozásra.
   6. A megnyíló ablakban jelölje be a következő jelölőnégyzeteket:

      - **About Quarantine files**.
      - **About a threat development chain**.
   7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Biztonsági sérülési indikátorok vizsgálata (szabványos feladat)

A *biztonsági sérülési indikátor (IOC)* egy olyan objektumra vagy tevékenységre vonatkozó adathalmaz, amely jogosulatlan hozzáférést jelez a számítógéphez (adatok veszélyeztetése). Például sok sikertelen bejelentkezési kísérlet a rendszerbe biztonsági sérülésre utalhat. Az *IOC Scan* feladat lehetővé teszi a biztonsági sérülési indikátorok (IOC) megtalálását a számítógépen, valamint biztosítja a fenyegetésre reagáló intézkedések megtételét.

A Kaspersky Endpoint Security IOC-fájlok segítségével keresi a biztonsági sérülés indikátorait. Az *IOC-fájlok* olyan fájlok, amelyek az indikátorkészleteket tartalmazzák, és amelyekkel az alkalmazás egyezést próbál találni észlelés esetén. Az IOC-fájloknak meg kell felelniük az OpenIOC szabványnak.

Az IOC Scan feladat futásmódja

A Kaspersky Endpoint Detection and Response lehetővé teszi a standard IOC vizsgálati feladatok létrehozását a feltört adatok észleléséhez. A *Szabványos IOC vizsgálati feladat* egy olyan csoportos vagy helyi feladat, amelyet manuálisan hoznak létre és konfigurálnak a Web Console-ban. A feladatok a felhasználó által előkészített IOC-fájlok használatával futnak. Ha manuálisan szeretne hozzáadni egy biztonsági sérülési indikátort, olvassa el az IOC-fájlokra vonatkozó követelményeket.

Az alábbi hivatkozásra kattintva letölthető fájl egy táblázatot tartalmaz az OpenIOC szabvány IOC-feltételeinek teljes listájával.

TÖLTSE LE AZ IOC_TERMS.XLSX FÁJLT

A Kaspersky Endpoint Security támogatja az önálló IOC vizsgálati feladatokat is, ha az alkalmazást a Kaspersky Sandbox megoldás részeként használják.

IOC-fájl létrehozása

A Kaspersky Endpoint Security 12.10 for Windows verziótól kezdve az IOC-fájlokat közvetlenül a feladatbeállításokban hozhatja létre. IOC-fájl létrehozásához el kell készítenie egy TXT-fájlt a fertőzöttségi mutatók listájával. A következő objektumok listáját adhatja hozzá fertőzöttségi mutatóként:

- Fájlkivonatok (MD5 / SHA256).

  Az alkalmazás előkészít egy IOC-fájlt FileItem/Md5sum vagy FileItem/Sha256sum vizsgálati hatókörrel.

- IP-címek (IPv4, IPv6).

  Az alkalmazás előkészít egy IOC-fájlt PortItem/RemoteIP vizsgálati hatókörrel.

- DNS-nevek.

  Az alkalmazás előkészít egy IOC-fájlt DnsEntryItem/RecordName vizsgálati hatókörrel.

IOC-fájl létrehozása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Válassza ki az **IOC Scan** feladatot.

   Megnyílik a feladatok tulajdonságai ablak. Ha szükséges, hozza létre a(z) **IOC Scan** feladatot.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Threat Scan** szakaszt.

5. Kattintson az **Redefine IOC files** gombra.

6. Ezzel megnyitja az IOC-fájl létrehozására szolgáló űrlapot:

   a. A **IOC files source** részen válassza a **Generate from file** elemet.

   b. Adja meg az IOC-fájl nevét.

   c. Válasszon ki egy TXT fájlt, amely tartalmazza a fertőzöttségi mutatók listáját.

   d. Válassza ki az IOC-fájl típusát: **DNS names**, **File hashes**, **IP addresses**.

   e. Kattintson az **Generate** gombra.

   A Kaspersky Endpoint Security hozzáadja az IOC-fájlokat az IOC-gyűjteményhez. Ha szükséges, ideiglenesen kizárhatja az IOC-fájlokat a feladat hatóköréből.

7. Mentse el a módosításokat.

IOC Scan feladat létrehozása

Létrehozhat *IOC Scan* feladatokat manuálisan:

- A riasztás részleteiben (csak az EDR Optimum esetében).

  Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

- A Feladat varázsló használata.

Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.

IOC Scan feladat létrehozása:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **IOC Scan** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Lépjen a következő lépésre.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Lépjen a következő lépésre.

   Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

   A rendszerfiók (SYSTEM) nem rendelkezik jogosultsággal az *IOC Scan* feladat végrehajtásához a hálózati meghajtókon. Ha a feladatot hálózati meghajtón szeretné futtatni, válassza ki annak a felhasználónak a fiókját, aki hozzáfér a meghajtóhoz.

   A hálózati meghajtókon végzendő önálló IOC vizsgálati feladatok esetében a feladat tulajdonságaiban manuálisan kell kiválasztania azt a felhasználói fiókot, amely hozzáféréssel rendelkezik a meghajtóhoz.

6. Fejezze be a varázslót.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. Nyissa meg a **Threat Scan** szakaszt.

10. Töltse fel az IOC-fájlokat fertőzöttségi mutatók kereséséhez.

    Az IOC-fájlok feltöltése után az alkalmazás összefoglaló információkat jelenít meg a fájlról, beleértve azon mutatók listáját, amelyek nem mentek át az ellenőrzésen. Az IOC-fájlok feltöltése után manuálisan szerkesztheti a fájlokat a beépített szerkesztőben közvetlenül a feladat tulajdonságaiban. A Kaspersky Endpoint Security az OpenIOC 1.1 szabványnak megfelelő IOC-fájlok szerkesztését támogatja. Az OpenIOC 1.0 verziójával kompatibilis IOC fájlok tartalma nem módosítható.

    A Kaspersky Endpoint Security hozzáadja az IOC-fájlokat az IOC-gyűjteményhez. Ha szükséges, ideiglenesen kizárhatja az IOC-fájlokat a feladat hatóköréből.

    Az IOC-fájlok hozzáadása vagy eltávolítása a feladat futtatása után nem javasolt. Ez azt okozhatja, hogy az IOC vizsgálat eredményei helytelenül jelennek meg a feladat korábbi futtatásakor. Az új IOC-fájlok biztonsági sérülési indikátorainak kereséséhez ajánlott új feladatokat hozzáadni.

11. Ha szükséges, tegyen jelölést a **Retrospective IOC Scan** jelölőnégyzetbe. A *Visszamenőleges IOC vizsgálat* az *IOC Scan* egyik módja, amelyben a Kaspersky Endpoint Security egy bizonyos időszak adatai alapján a sérülésekre utaló jelek után kutat. Ez az üzemmód arra szolgál, hogy a védett számítógép telemetriai adatai – például a hálózati tevékenység, a folyamatok, a fájlok és egyéb telemetriai adatok – alapján felderítse a biztonsági incidensekre utaló jeleket. A Kaspersky Endpoint Security elemzi az operációs rendszer naplóiban és a böngésző naplóiban található adatokat a számítógépen. A Visszamenőleges IOC vizsgálat a következő böngészők naplófájljait elemzi: Google Chrome, Mozilla Firefox, Microsoft Edge (79-es vagy újabb verzió).

12. Az IOC-észlelésre vonatkozó műveletek konfigurálása:

- **Isolate device from the network**. Ha ezt az opciót választja, a Kaspersky Endpoint Security elkülöníti a számítógépet a hálózattól, hogy megakadályozza a fenyegetés terjedését. Beállíthatja az elkülönítés időtartamát az Endpoint Detection and Response összetevő beállításaiban.

  Ha a jelölőnégyzet nincs bejelölve, a feladat kézi futtatása után leválaszthatja a számítógépet a hálózatról. Ha az *IOC Scan* feladat fertőzöttségi mutatót észlel, a számítógépet elkülönítheti a hálózattól közvetlenül az IOC használatával (*IOC Scan* tulajdonságai → **Application settings** → **IOC Scan results** feladat). A Kaspersky Endpoint Security lehetővé teszi további beállítások azonnali kezelését is: hálózatelkülönítés letiltásának időtartama és hálózatelkülönítési kivételek.

- **Move copy to Quarantine, delete object**. Ha ezt az opciót választja, a Kaspersky Endpoint Security törli a számítógépen talált rosszindulatú objektumot. Az objektum törlése előtt a Kaspersky Endpoint Security biztonsági másolatot készít arra az esetre, ha az objektumot később vissza kell állítani. A Kaspersky Endpoint Security a biztonsági másolatot karanténba helyezi.

  Ha a jelölőnégyzet nincs bejelölve, a feladat kézi futtatása után manuálisan is karanténba helyezheti a fájlt. Ha az *IOC Scan* feladat olyan fájlt észlel, amely veszélyeztetheti az adatokat, akkor ezt a fájlt közvetlenül az IOC vizsgálat eredményeiből helyezheti karanténba (**Application settings** → **IOC Scan results**). Ennek eredményeként a Kaspersky Endpoint Security elindítja a feladat létrehozásának varázslóját az észlelt fájl előre beállított adataival. Csak a további feladatbeállításokat kell kezelnie, például beállítani a feladat ütemezését.

- **Run Critical Areas Scan**. Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a *Critical Areas Scan* feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.

13. Nyissa meg a **Advanced** szakaszt.

14. Válassza ki az adattípusokat (IOC-dokumentumok), amelyeket a feladat részeként elemezni kell.

> A Kaspersky Endpoint Security automatikusan kiválasztja az adattípusokat (IOC-dokumentumokat) az *IOC Scan* feladathoz a betöltött IOC-fájlok tartalmának megfelelően. Nem ajánlott megszüntetni az adattípusok kijelölését.

Ezenkívül konfigurálhatja a vizsgálati hatóköröket a következő adattípusokhoz:

- **Files - FileItem**. Beállítja az IOC vizsgálat hatókörét a számítógépen az előre beállított hatókörök használatával.

  Alapértelmezés szerint a Kaspersky Endpoint Security csak a számítógép fontos területein keresi a biztonsági sérülési indikátorokat, például a Letöltések mappában, az asztalon, az operációs rendszer ideiglenes fájljait tartalmazó mappában stb. Manuálisan is hozzáadhatja a vizsgálati hatóköröket.

- **Windows Event Log - EventLogItem**. Adja meg azt az időszakot, amikor az események naplózva lettek. Azt is kiválaszthatja, hogy mely Windows eseménynaplókat kell használni az IOC vizsgálathoz. Alapértelmezés szerint a következő eseménynaplók vannak kiválasztva: alkalmazási eseménynapló, rendszer-eseménynapló és biztonsági eseménynapló.

- **Windows Registry - RegistryItem**. Konfigurálja az IOC vizsgálat hatókörét a beállításjegyzékben.

  Alapértelmezés szerint a Kaspersky Endpoint Security átvizsgálja a beállításkulcsok készletét.

15. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.

16. Állítsa be a feladat ütemezését.

A Wake-on-LAN nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.

17. Mentse el a módosításokat.

18. Válassza ki a feladat melletti jelölőnégyzetet.

19. Kattintson az **Start** gombra.

Ennek eredményeként a Kaspersky Endpoint Security futtatja a biztonsági sérülési indikátorok keresését a számítógépen. A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Results** szakaszban. Az észlelt biztonsági sérülési indikátorokra vonatkozó információkat a feladat tulajdonságaiban tekintheti meg: **Application settings** → **IOC Scan results**. Az IOC vizsgálat eredményeiben manuálisan is karanténba helyezheti az észlelt fájlt, vagy elszigetelheti a számítógépet a hálózattól.

A Kaspersky Endpoint Security ismétlődéseket keres az ugyanahhoz az IOC-fájlhoz létrehozott rekordok között, és csak az egyedi rekordokat tárolja a feladatok eredményeiben. A másodpéldányok olyan azonos típusú rekordok, amelyeknek az összes összehasonlított mezőjében azonos érték szerepel. Előfordulhat, hogy az alkalmazás nem hoz létre rekordot, ha egy vagy több mezőben hiányzik az érték (lásd az alábbi táblázatot).

Típus	Összehasonlított mezők	A rekord létrehozásának elmulasztásának feltétele
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• A FullPath, a Md5sum és a Sha256sum mező értéke hiányzik. • A) FullPath mező értéke hiányzik, és azonos érték szerepel a Md5sum és a Sha256sum mezőben.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Hiányzik az érték az alábbi mezők közül legalább egyből: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	A startTime vagy a PID mező értéke hiányzik.

A **Alert Details** ablakban megjelenhetnek az azonos mezőértékekkel rendelkező RegistryItem rekordok. Az ilyen rekordok nem ismétlődések, mert eltérő értékkel rendelkeznek a Szöveg mezőben, amely nem jelenik meg a felületen.

Az IOC vizsgálat eredményeinek megőrzése 30 napig történik. Ezt követően a Kaspersky Endpoint Security automatikusan törli a legrégebbi bejegyzéseket.

Kiterjesztett telemetria az IOC vizsgálathoz

Javasoljuk, hogy engedélyezze a kiterjesztett telemetriát a számítógépen az utólagos IOC-vizsgálathoz. A kiterjesztett telemetria javítja az IOC-észlelés pontosságát, de a számítógép ilyenkor több erőforrást használ.

A kiterjesztett telemetria a következő kiegészítő feltételek támogatását is tartalmazza:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Ha a kiterjesztett telemetria le van tiltva, a Kaspersky Endpoint Security rotálhatja az észlelt sérülési indikátorokra vonatkozó információkat.

A kiterjesztett telemetria engedélyezése:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response** elemet.
5. Tegyen jelölést a **Enable advanced system activity logging** jelölőnégyzetbe.
6. Mentse el a módosításokat.

Fájl áthelyezése a Karanténba

A fenyegetésekre reagálva a Kaspersky Endpoint Detection and Response létrehozhat *Move file to Quarantine* feladatokat. Erre azért van szükség, hogy minimalizáljuk a fenyegetés következményeit. A *karantén* egy speciális helyi tároló a számítógépen. A felhasználó karanténba helyezheti azokat a fájlokat, amelyeket veszélyesnek ítél meg a számítógépen. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha az integrálva van a Kaspersky Detection and Response megoldásokkal. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a Biztonsági mentésbe helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért olvassa el a Kaspersky Sandbox súgót, a Kaspersky Endpoint Detection and Response Optimum súgót, a Kaspersky Endpoint Detection and Response Expert súgót, a Kaspersky Anti Targeted Attack Platform súgót és a Kaspersky Endpoint Detection and Response Expert (on-premises) súgót.

Move file to Quarantine feladatokat a következő módokon hozhat létre:

- A riasztás részleteiben (csak az EDR Optimum esetében).

  Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

- A Feladat varázsló használata.

  Meg kell adnia a fájl elérési útját vagy kivonatát (SHA256 vagy MD5), vagy a fájl elérési útját és a fájl kivonatát is.

- Az *IOC Scan* feladat beállításaiban.

  Ha az *IOC Scan* feladat olyan fájlt észlel, amely veszélyeztetheti az adatokat, akkor ezt a fájlt közvetlenül az IOC vizsgálat eredményeiből helyezheti karanténba (**Application settings** → **IOC Scan results**). Ennek eredményeként a Kaspersky Endpoint Security elindítja a feladat létrehozásának varázslóját az észlelt fájl előre beállított adataival. Csak a további feladatbeállításokat kell kezelnie, például beállítani a feladat ütemezését.

A *Move file to Quarantine* feladatnak a következő korlátai vannak:

1. A fájl mérete nem haladhatja meg a 100 MB-ot.
2. A kritikus rendszerobjektumok (SCO) nem helyezhetők karanténba. Az SCO-k olyan fájlok, amelyek futtatásához az operációs rendszernek és a Kaspersky Endpoint Security for Windows alkalmazásnak szüksége van.
3. Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.
4. A *Move file to Quarantine* feladat miatt nem vizsgálhat karanténba helyezett objektumot.

Move file to Quarantine feladat létrehozásához:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Move file to Quarantine** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Kattintson az **Next** gombra.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Kattintson az **Next** gombra.

   Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Fejezze be a varázslót a **Finish** gombra való kattintással.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. A fájlok listájában kattintson az **Add** elemre.

   Elindul a fájlhozzáadási varázsló.

10. A fájl hozzáadásához meg kell adnia a fájl teljes elérési útját, vagy a fájlkivonatot és az elérési utat egyszerre.

    Ha a fájl hálózati meghajtón található, adja meg a fájl elérési útját, amely a meghajtó betűjele helyett `\\` értékkel kezdődjön. Például: `\\server\shared_folder\file.exe`. Ha a fájl elérési útja tartalmazza a hálózati meghajtó betűjelét, akkor *A fájl nem található* hibaüzenetet fog kapni.

11. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.

12. Állítsa be a feladat ütemezését.

    A Wake-on-LAN nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.

13. Mentse el a módosításokat.

14. Válassza ki a feladat melletti jelölőnégyzetet.

15. Kattintson az **Start** gombra.

    Ennek eredményeként a Kaspersky Endpoint Security karanténba helyezi a fájlt.

Ha a fájlt egy másik folyamat zárolja, a feladat *Completed* állapotúként jelenik meg, de maga a fájl csak a számítógép újraindítása után fog karanténba kerülni. A számítógép újraindítása után győződjön meg arról, hogy a fájl törlődött.

A *Move file to Quarantine* feladat *Hozzáférés megtagadva* hibaüzenettel is végződhet, ha egy éppen futó végrehajtható fájlt próbál karanténba helyezni. Hozzon létre egy folyamatmegszakítási feladatot a fájlhoz, és próbálkozzon újra.

A *Move file to Quarantine* feladat befejeződhet a *Nincs elegendő hely a karanténként szolgáló tárhelyen* hibával, ha túl nagy fájlt próbál karanténba helyezni. Ürítse ki a Karantént, vagy növelje meg a Karantén méretét. Ezután próbálja újra.

A fájlokat visszaállíthatja a karanténból, vagy kiürítheti a karantént a Web Console használatával. Az objektumokat a számítógépen helyileg visszaállíthatja a parancssor használatával.

Fájl lekérése

Lekérhet fájlokat a felhasználói számítógépekről. Például beállíthatja egy harmadik féltől származó alkalmazás által létrehozott eseménynaplófájl lekérését. A feladat végrehajtásának eredményeként a fájl a karanténban mentésre kerül. A *karantén* egy speciális helyi tároló a számítógépen. Letöltheti ezt a fájlt a karanténból a számítógépére a Web Console segítségével (**Műveletek** → **Tárolók** → **Karantén**). A felhasználó számítógépén a fájl az eredeti mappában marad.

A fájl mérete nem haladhatja meg a 100 MB-ot.

Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.

Fájl lekérése feladat létrehozása:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Get file** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Kattintson az **Next** gombra.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Kattintson az **Next** gombra.

   Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Fejezze be a varázslót a **Finish** gombra való kattintással.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.
9. A fájlok listájában kattintson az **Add** elemre.

   Elindul a fájlhozzáadási varázsló.
10. A fájl hozzáadásához meg kell adnia a fájl teljes elérési útját, vagy a fájlkivonatot és az elérési utat egyszerre.

    Ha a fájl hálózati meghajtón található, adja meg a fájl elérési útját, amely a meghajtó betűjele helyett `\\` értékkel kezdődjön. Például: `\\server\shared_folder\file.exe`. Ha a fájl elérési útja tartalmazza a hálózati meghajtó betűjelét, akkor *A fájl nem található* hibaüzenetet fog kapni.
11. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.
12. Állítsa be a feladat ütemezését.

    A Wake-on-LAN nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.
13. Mentse el a módosításokat.
14. Válassza ki a feladat melletti jelölőnégyzetet.
15. Kattintson az **Start** gombra.

    Ennek eredményeként a Kaspersky Endpoint Security létrehoz egy másolatot a fájlról, és áthelyezi azt a Karanténba. Letöltheti a fájlt a Web Console karanténjából.

Fájl törlése

A távolról törölhet fájlokat a *Delete file* feladattal. Például távolról törölhet egy fájlt fenyegetésre történő reagálás során.

A *Delete file* feladatnak a következő korlátai vannak:

- A System Critical Object (SCO) nem törölhető. Az SCO-k olyan fájlok, amelyek futtatásához az operációs rendszernek és a Kaspersky Endpoint Security alkalmazásnak szüksége van.
- Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.

Delete file feladat létrehozásához:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.
2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Delete file** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Kattintson az **Next** gombra.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Kattintson az **Next** gombra.

   Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Fejezze be a varázslót a **Finish** gombra való kattintással.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. A fájlok listájában kattintson az **Add** elemre.

   Elindul a fájlhozzáadási varázsló.

10. A fájl hozzáadásához meg kell adnia a fájl teljes elérési útját, vagy a fájlkivonatot és az elérési utat egyszerre.

    Ha a fájl hálózati meghajtón található, adja meg a fájl elérési útját, amely a meghajtó betűjele helyett `\\` értékkel kezdődjön. Például: `\\server\shared_folder\file.exe`. Ha a fájl elérési útja tartalmazza a hálózati meghajtó betűjelét, akkor *A fájl nem található* hibaüzenetet fog kapni.

11. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.

12. Állítsa be a feladat ütemezését.

    A Wake-on-LAN nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.

13. Mentse el a módosításokat.

14. Válassza ki a feladat melletti jelölőnégyzetet.

15. Kattintson az **Start** gombra.

Ennek eredményeként a Kaspersky Endpoint Security törli a fájlt a számítógépről. Ha a fájlt egy másik folyamat

zárolja, a feladat *Done* állapotúként jelenik meg, de maga a fájl csak a számítógép újraindítása után fog törlődni. A számítógép újraindítása után győződjön meg arról, hogy a fájl törlődött.

A *Delete file* feladat *Access denied or file not found* hibaüzenettel is végződhet, ha egy éppen futó futtatható fájlt próbál törölni. Hozzon létre egy folyamatmegszakítási feladatot a fájlhoz, és próbálkozzon újra.

Folyamat indítása

A távolról futtathat fájlokat a *Process start* feladattal. Például távolról futtathat egy segédprogramot, amely létrehozza a számítógép konfigurációs fájlját. Ezután használhatja a *Receive file from device* feladatot a létrehozott fájl fogadásához a Kaspersky Security Center Web Console-ban.

Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.

Process start feladat létrehozásához:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Process start** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Kattintson az **Next** gombra.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Kattintson az **Next** gombra.

   Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Fejezze be a varázslót a **Finish** gombra való kattintással.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

8. Megnyílik a feladatok tulajdonságai ablak.

9. Válassza ki az **Application settings** lapot.

10. Írja be a folyamatindítási parancsot.

    Tegyük fel, hogy egy segédprogramot szeretne futtatni (`utility.exe`), amely menti a számítógép konfigurációjával kapcsolatos információkat egy `conf.txt` nevű fájlba az aktuális mappában (alapértelmezés szerint). A segédprogram a `C:\Users\admin\Diagnostic\` mappában található. A konfigurációs fájlt a `C:\Users\admin\Documents\Configuration` mappába mentse. Adja meg a következő értékeket:

    - **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Command line arguments (optional)** – `/R conf.txt`
    - **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`

11. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.

12. Állítsa be a feladat ütemezését.

    A Wake-on-LAN nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.

13. Mentse el a módosításokat.

14. Válassza ki a feladat melletti jelölőnégyzetet.

15. Kattintson az **Start** gombra.

    Ennek eredményeként a Kaspersky Endpoint Security csendes módban futtatja a parancsot, és elindítja a folyamatot. A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Execution results** szakaszban.

Folyamat megszakítása

Távolról is leállíthat folyamatokat a *Terminate process* feladattal. Például távolról leállíthat egy internetes sebességtesztelő segédprogramot, amelyet a *Folyamat futtatása* feladattal indítottak el.

Ha meg szeretné tiltani egy fájl futtatását, konfigurálhatja a végrehajtásmegelőzési összetevőt. Letilthatja futtatható fájlok, szkriptek, Office formátumú fájlok végrehajtását is.

A *Terminate process* feladatnak a következő korlátai vannak:

- A kritikus rendszerobjektumok (SCO) folyamatai nem leállíthatók. Az SCO-k olyan fájlok, amelyek futtatásához az operációs rendszernek és a Kaspersky Endpoint Security alkalmazásnak szüksége van.
- Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.

Terminate process feladat létrehozásához:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson az **Add** gombra.

   Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

   a. A **Application** legördülő listából válassza ki az **Kaspersky Endpoint Security for Windows 14.1.0** lehetőséget.

   b. A **Task type** legördülő listából válassza ki az **Terminate process** lehetőséget.

   c. A **Task name** mezőben adjon meg egy rövid leírást.

   d. A **Devices to which the task will be assigned** blokkban válassza ki a feladathatókört.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Kattintson az **Next** gombra.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Kattintson az **Next** gombra.

   Alapértelmezés szerint a Kaspersky Endpoint Security rendszerfelhasználóként (SYSTEM) indítja el a feladatot.

6. Fejezze be a varázslót a **Finish** gombra való kattintással.

   Egy új feladat jelenik meg a feladatok listájában.

7. Kattintson az új feladatra.

   Megnyílik a feladatok tulajdonságai ablak.

8. Válassza ki az **Application settings** lapot.

9. A folyamat befejezéséhez ki kell választania a leállítani kívánt fájlt. Egy fájlt az alábbi módokon választhat ki:

   - Írja be a fájl teljes nevét.
   - Adja meg a fájl hash értékét és a fájl elérési útját.
   - Adja meg a folyamat PID-jét (csak helyi feladatok esetén).

   Ha a fájl hálózati meghajtón található, adja meg a fájl elérési útját, amely a meghajtó betűjele helyett `\\` értékkel kezdődjön. Például: `\\server\shared_folder\file.exe`. Ha a fájl elérési útja tartalmazza a hálózati meghajtó betűjelét, akkor *A fájl nem található* hibaüzenetet fog kapni.

10. Válassza ki a számítógép tulajdonságainak ablakában az **Schedule** lapot.

11. Állítsa be a feladat ütemezését.

    A Wake-on-LAN nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.

12. Kattintson az **Save** gombra.

13. Válassza ki a feladat melletti jelölőnégyzetet.

14. Kattintson az **Start** gombra.

    Ennek eredményeként a Kaspersky Endpoint Security megszakítja a folyamatot a számítógépen. Például, ha egy GAME alkalmazás fut, és leállítja a game.exe folyamatot, az alkalmazás adatmentés nélkül bezárul. A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Results** szakaszban.

Végrehajtás megelőzése

A végrehajtás megakadályozása lehetővé teszi a futtatható fájlok és a parancsfájlok futtatásának, valamint az Office formátumú fájlok megnyitásának kezelését. Ilyen módon például megakadályozhatja az Ön által nem biztonságosnak ítélt alkalmazások végrehajtását. Ennek eredményeként a fenyegetés terjedése megállítható. A végrehajtás megakadályozása támogatja az Office-fájlkiterjesztések és a szkriptértelmezők készletét.

Végrehajtás megelőzésének szabálya

A végrehajtás megakadályozása megelőzési szabályokkal kezeli a felhasználók hozzáférését a fájlokhoz. A *végrehajtás-megelőzési szabály* olyan kritériumok összessége, amelyeket az alkalmazás figyelembe vesz, amikor egy objektum végrehajtására reagál, például amikor blokkolja az objektum végrehajtását. Az alkalmazás elérési utak vagy az MD5 és SHA256 kivonatolási algoritmusokkal kiszámított ellenőrzőösszegek alapján azonosítja a fájlokat.

Létrehozhat végrehajtásmegelőzési szabályokat:

- A riasztás részleteiben (csak az EDR Optimum esetében).

  Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

- Csoportházirend vagy helyi alkalmazásbeállítások használata.

  Meg kell adnia a fájl elérési útját vagy kivonatát (SHA256 vagy MD5), vagy a fájl elérési útját és a fájl kivonatát is.

A végrehajtásmegelőzést helyben is kezelheti a parancssor használatával.

A Végrehajtás megelőzése a következő korlátozásokkal rendelkezik:

1. A megelőzési szabályok nem terjednek ki CD-n vagy ISO-lemezképeken található fájlokra. Az alkalmazás nem blokkolja ezen fájlok végrehajtását vagy megnyitását.

2. Nem lehet a rendszerkritikus objektumokat (SCO) blokkolni. Az SCO-k olyan fájlok, amelyek futtatásához az operációs rendszernek és a Kaspersky Endpoint Security alkalmazásnak szüksége van.

3. Nem ajánlott 5000-nél több futtatás-megakadályozási szabályt létrehozni, mivel ez a rendszer instabilitását okozhatja.

Végrehajtás megelőzésének szabályai – üzemmódok

A végrehajtásmegelőzési összetevő két módban működhet:

- **Csak statisztika**

  Ebben az üzemmódban a Kaspersky Endpoint Security közzétesz egy eseményt a Windows eseménynaplójában és a Kaspersky Security Center eseménynaplójában a végrehajtható objektumok futtatására vagy a megelőzési szabály kritériumainak megfelelő dokumentumok megnyitására tett kísérletről, de nem blokkolja az objektum vagy a dokumentum futtatási vagy megnyitási kísérletét. Alapértelmezésben ez a mód van kiválasztva.

- **Aktív**

  Ebben az üzemmódban az alkalmazás blokkolja a megelőzési szabály kritériumainak megfelelő objektumok végrehajtását vagy dokumentumok megnyitását. Az alkalmazás egy eseményt is közzétesz az objektumok végrehajtására vagy dokumentumok megnyitására irányuló kísérletekről a Windows eseménynaplójában és a Kaspersky Security Center eseménynaplójában.

A végrehajtás megakadályozásának kezelése

Az összetevői beállítások csak a webkonzolon keresztül konfigurálhatók.

A végrehajtás megakadályozása:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response** elemet.
5. Válassza ki az **Execution Prevention** lapot.
6. Kapcsolja be az **Execution Prevention ENABLED** kapcsolót.
7. A(z) **Action on execution or opening of forbidden object** területen válassza ki az összetevő működési módját:

   - **Block and add to event log**. Ebben az üzemmódban az alkalmazás blokkolja a megelőzési szabály kritériumainak megfelelő objektumok végrehajtását vagy dokumentumok megnyitását. Az alkalmazás egy eseményt is közzétesz az objektumok végrehajtására vagy dokumentumok megnyitására irányuló kísérletekről a Windows eseménynaplójában és a Kaspersky Security Center eseménynaplójában.

   - **Add to event log**. Ebben az üzemmódban a Kaspersky Endpoint Security közzétesz egy eseményt a Windows eseménynaplójában és a Kaspersky Security Center eseménynaplójában a végrehajtható objektumok futtatására vagy a megelőzési szabály kritériumainak megfelelő dokumentumok megnyitására tett kísérletről, de nem blokkolja az objektum vagy a dokumentum futtatási vagy megnyitási kísérletét. Alapértelmezésben ez a mód van kiválasztva.

8. Végrehajtásmegelőzési szabályok listájának létrehozása:

   a. Kattintson az **Add** gombra.

   b. Ezzel megnyit egy ablakot; ebben az ablakba írja be a végrehajtásmegelőzési szabály nevét (például *A alkalmazás*).

   c. A(z) **Type** legördülő listából válassza ki a blokkolni kívánt objektumot: **Executable file**, **Script**, **Microsoft Office document**.

   Ha rossz objektumtípust választ, a Kaspersky Endpoint Security nem blokkolja a fájlt vagy a szkriptet.

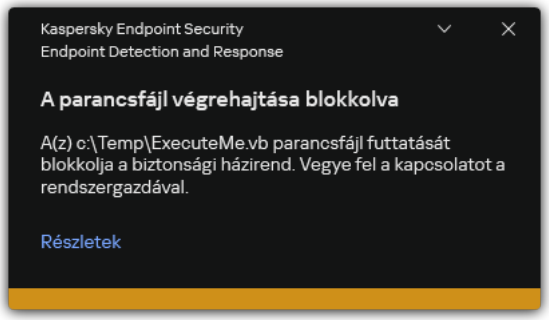
   d. A fájl hozzáadásához meg kell adnia a fájl kivonatát (SHA256 vagy MD5), a fájl teljes elérési útját, vagy a kivonatot és az elérési utat egyszerre.

   > Ha a fájl hálózati meghajtón található, adja meg a fájl elérési útját, amely a meghajtó betűjele helyett `\\` értékkel kezdődjön. Például: `\\server\shared_folder\file.exe`. Ha a fájl elérési útja hálózati meghajtó betűjelét tartalmazza, a Kaspersky Endpoint Security nem blokkolja a fájlt vagy a szkriptet.

   A végrehajtás megakadályozása támogatja az Office-fájlkiterjesztések és a szkriptértelmezők készletét.

9. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Endpoint Security blokkolja az objektumok végrehajtását: futtatható fájlok és szkriptek futtatása, Office-formátumú fájlok megnyitása. Azonban megnyithat például egy parancsfájlt egy szövegszerkesztőben, még akkor is, ha a szkript futtatása meg van akadályozva. Amikor blokkolja egy objektum végrehajtását, a Kaspersky Endpoint Security szabványos értesítést jelenít meg (lásd az alábbi ábrát), ha az értesítések engedélyezve vannak az alkalmazás beállításaiban.



Értesítés a végrehajtás megakadályozásáról

Számítógép hálózatelkülönítése

A számítógép hálózatelkülönítése lehetővé teszi a számítógép automatikus leválasztását a hálózatról, válaszul a biztonsági sérülési indikátorok (IOC) észlelésére – ez az *automatikus mód*. Az észlelt fenyegetés tanulmányozása közben manuálisan is bekapcsolhatja a hálózatelkülönítést – ez a *manuális mód*.

Amikor a Hálózatelkülönítés be van kapcsolva, az alkalmazás leválaszt minden aktív kapcsolatot, és blokkol minden új TCP/IP-hálózati kapcsolatot a számítógépen az alábbi kapcsolatok kivételével:

- A Hálózatelkülönítés kizárásaiban felsorolt kapcsolatok.
- A Kaspersky Endpoint Security szolgáltatásai által kezdeményezett kapcsolatok.

- A Kaspersky Security Center Network Agent által kezdeményezett kapcsolatok.
- Csatlakozások az SVM-hez és az Integrációs kiszolgálóhoz, ha az alkalmazást Light Agent üzemmódban használják.
- Kapcsolódások a KSN-hez az alkalmazásnak a Kaspersky Managed Detection and Response szolgáltatással való integrálásakor.

Az összetevői beállítások csak a webkonzolon keresztül konfigurálhatók.

Automatikus hálózatelkülönítési mód

Beállíthatja, hogy a Hálózatelkülönítés automatikusan bekapcsoljon az IOC észlelésre adott válaszként. Az automatikus hálózatelkülönítési mód csoportházirenddel konfigurálható.

A Hálózatelkülönítés beállítása, hogy automatikusan bekapcsoljon az IOC észlelésre adott válaszként

1. A Web Console fő ablakában válassza a **Asset management** → **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **IOC Scan** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

   Ha szükséges, hozza létre a(z) *IOC Scan* feladatot.

3. Válassza ki az **Application settings** lapot.

4. A **Action on IOC detection** részen jelölje be a **Take response actions after an IOC is found** és a **Isolate computer from the network** jelölőnégyzetet.

5. Mentse el a módosításokat.

   Ennek eredményeként IOC észlelésekor az alkalmazás elkülöníti a számítógépet a hálózattól, hogy megakadályozza a fenyegetés terjedését.

Beállíthatja, hogy az automatikus hálózatelkülönítés egy bizonyos idő elteltével le legyen tiltva. Alapértelmezés szerint az alkalmazás kikapcsolja a Hálózatelkülönítést a bekapcsolástól számított 8 óra elteltével. A hálózatelkülönítést manuálisan is kikapcsolhatja (lásd az alábbi utasításokat). A Hálózatelkülönítés kikapcsolása után a számítógép korlátozások nélkül használhatja a hálózatot.

A számítógép hálózatelkülönítésének automatikus módban történő kikapcsolásához szükséges késleltetés beállítása

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response** elemet.

5. Válassza ki az **Network Isolation** lapot.
6. Válassza ki a késleltetést a Hálózatelkülönítés kikapcsolásához.
7. Mentse el a módosításokat.

Manuális hálózatelkülönítési mód

A hálózatelkülönítést manuálisan be- és kikapcsolhatja. A manuális hálózatelkülönítési módot a Kaspersky Security Center konzol számítógép-tulajdonságaiban állíthatja be.

A Hálózatelkülönítés funkciót bekapcsolhatja:

- A riasztás részleteiben (csak az EDR Optimum esetében).

  Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

- Helyi alkalmazásbeállítások használata.
- Az *IOC Scan* feladat beállításaiban.

  Ha az *IOC Scan* feladat fertőzöttségi mutatót észlel, a számítógépet elkülönítheti a hálózattól közvetlenül az IOC használatával (*IOC Scan* tulajdonságai → **Application settings** → **IOC Scan results** feladat). A Kaspersky Endpoint Security lehetővé teszi további beállítások azonnali kezelését is: hálózatelkülönítés letiltásának időtartama és hálózatelkülönítési kivételek.

A számítógép hálózatelkülönítésének manuális bekapcsolása

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.

   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.

   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
7. Az **Network isolation** blokkban kattintson a **Isolate computer from the network** lehetőségre.

Beállíthatja, hogy az automatikus hálózatelkülönítés egy bizonyos idő elteltével le legyen tiltva. Alapértelmezés szerint az alkalmazás kikapcsolja a Hálózatelkülönítést a bekapcsolástól számított 8 óra elteltével. A Hálózatelkülönítés kikapcsolása után a számítógép korlátozások nélkül használhatja a hálózatot.

A számítógép hálózatelkülönítésének manuális módban történő kikapcsolásához szükséges késleltetés beállítása

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.
   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Tasks** lapot.
   Ez megjeleníti a számítógépen elérhető feladatok listáját.
4. Válassza ki az **Network isolation** feladatot.
5. Válassza ki az **Application settings** lapot.
6. Ez megnyit egy ablakot; ebben az ablakban válassza ki a hálózatelkülönítés kikapcsolásának késleltetését.
7. Mentse el a módosításokat.

A számítógép hálózatelkülönítésének manuális kikapcsolása

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.
   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.
   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
7. Az **Network isolation** blokkban kattintson a **Unblock computer isolated from the network** lehetőségre.

Helyileg is letilthatja a Hálózatelkülönítést a command line használatával.

A Kaspersky Endpoint Security 12.10 for Windows verziótól kezdve a hálózatelkülönítést a riasztás részleteinél kezelheti. Ezenkívül a riasztás részleteiben megadhatja a számítógép hálózatelkülönítésének időtartamát. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

Network isolation exclusions

Beállíthatja a Hálózatelkülönítés kizárásait. Az e szabályoknak megfelelő hálózati kapcsolatok nincsenek blokkolva a számítógépen, ha a Hálózatelkülönítés be van kapcsolva.

A Hálózatelkülönítés kizárásainak konfigurálásához használhatja a *szabványos hálózati profilok* listáját. Alapértelmezés szerint a kizárások közé tartoznak azok a hálózati profilok, amelyek a DNS-/DHCP-kiszolgálóval és a DNS-/DHCP-ügyfélszerepkörrel rendelkező eszközök zavartalan működését biztosító szabályokat tartalmazzák. Módosíthatja a szabványos hálózati profilok beállításait, vagy manuálisan is megadhat kizárásokat (lásd az alábbi utasításokat).

A házirend tulajdonságaiban megadott kizárások csak akkor alkalmazhatók, ha a hálózatelkülönítés automatikusan bekapcsol az észlelt fenyegetés hatására. A számítógép tulajdonságaiban megadott kizárások csak akkor érvényesek, ha a hálózatelkülönítést a Kaspersky Security Center konzoljának számítógép-tulajdonságaiban vagy a riasztási részletekben manuálisan kapcsolják be.

Egy aktív szabályzat nem akadályozza meg a számítógéptulajdonságokban konfigurált Hálózatelkülönítésből történő kizárások alkalmazását, mivel ezek a paraméterek eltérő használati forgatókönyvekkel rendelkeznek.

Hálózatelkülönítési kizárás hozzáadása automatikus módban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response** elemet.
5. Válassza ki az **Network Isolation** lapot.
6. Az **Network isolation exclusions** blokkban kattintson a **Exclusions** lehetőségre.
7. Megnyílik egy ablak. Ebben az ablakban kattintson a(z) **Add** → **Add from profile** elemre, és válassza ki a szabványos hálózati profilokat a kizárások konfigurálásához.

   A profilból származó hálózatelkülönítési kizárások hozzáadódnak a Hálózatelkülönítés kizárásainak listájához. Megtekintheti a hálózati kapcsolatok tulajdonságait. Ha szükséges, módosíthatja a hálózati kapcsolatok beállításait.
8. Ha szükséges, adjon hozzá manuálisan egy hálózatelkülönítési kizárást. Ehhez a kizárások listáját tartalmazó ablakban kattintson a **Add** → **Add** gombra, és manuálisan szerkessze a hálózati kapcsolat beállításait.
9. Mentse el a módosításokat.

Hálózatelkülönítési kizárás hozzáadása manuális módban

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.

   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Tasks** lapot.

   Ez megjeleníti a számítógépen elérhető feladatok listáját.
4. Válassza ki az **Network isolation** feladatot.

5. Válassza ki az **Application settings** lapot.
6. A megnyíló ablakban kattintson a **Exclusions** gombra.
7. A megnyíló ablakban kattintson a **Add from profile** elemre, és válassza ki a szabványos hálózati profilokat a kizárások konfigurálásához.

   A profilból származó hálózatelkülönítési kizárások hozzáadódnak a Hálózatelkülönítés kizárásainak listájához. Megtekintheti a hálózati kapcsolatok tulajdonságait. Ha szükséges, módosíthatja a hálózati kapcsolatok beállításait.
8. Ha szükséges, adjon hozzá manuálisan egy hálózatelkülönítési kizárást. Ehhez a kizárások listáját tartalmazó ablakban kattintson a **Add** gombra, és manuálisan szerkessze a hálózati kapcsolat beállításait.
9. Mentse el a módosításokat.

A Hálózatelkülönítés kizárásainak listáját helyben is megtekintheti a parancssor használatával. Ebben az esetben a számítógépet el kell különíteni.

A Kaspersky Endpoint Security 12.10 for Windows verziótól kezdődően a riasztás részleteinél megadhatja a hálózatelkülönítés kizárásait. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

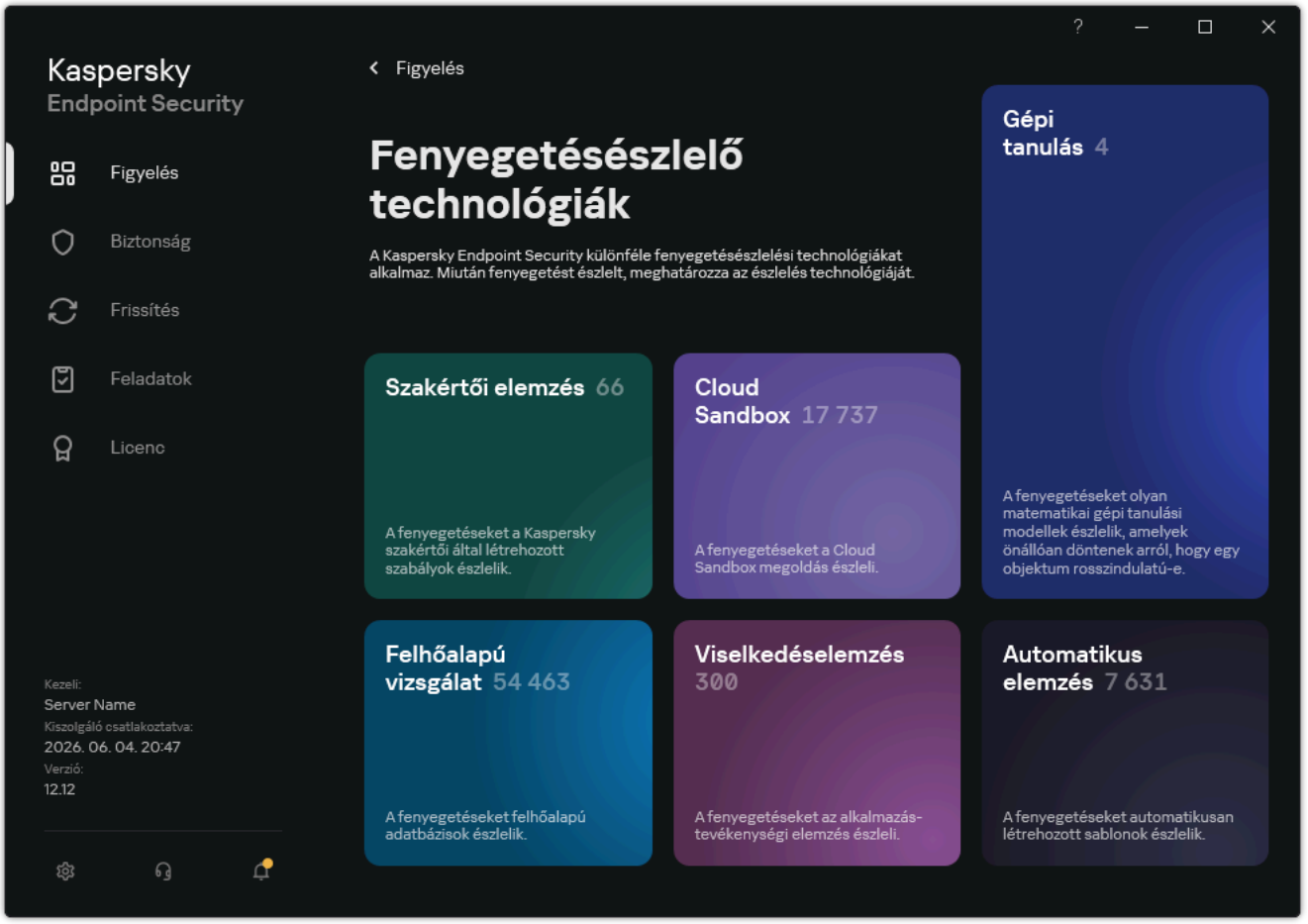
Cloud Sandbox

Cloud Sandbox egy olyan technológia, amely lehetővé teszi a speciális fenyegetések észlelését egy számítógépen. A Kaspersky Endpoint Security elemzés céljából automatikusan továbbítja az észlelt fájlokat a Cloud Sandbox részére. A Cloud Sandbox elszigetelt környezetben futtatja ezeket a fájlokat, hogy azonosítsa a rosszindulatú tevékenységeket és döntsön a megbízhatóságukról. Ezen fájlok adatai ezután Kaspersky Security Network részére elküldésre kerülnek. Ezért, ha a Cloud Sandbox rosszindulatú fájlt észlelt, a Kaspersky Endpoint Security, a fenyegetésnek a megszüntetése érdekében az összes olyan számítógépen el fogja végezni a megfelelő műveletet, amelyen ez a fájl észlelhető.

A Cloud Sandbox működéséhez engedélyeznie kell a Kaspersky Security Network használatát.

Ha Kaspersky Private Security Networköt használ, a Cloud Sandbox technológia nem érhető el.

A Cloud Sandbox technológia folyamatosan engedélyezve van és minden Kaspersky Security Network felhasználó számára elérhető, függetlenül attól, milyen típusú licencet használnak. Ha már telepítette az Endpoint Detection and Response Optimum megoldást, engedélyezhet egy külön számlálót a Cloud Sandbox által észlelt fenyegetésekhez. Ezzel a számlálóval statisztikákat állíthat össze az észlelt fenyegetések elemzésekor. A Kaspersky Endpoint Security a Cloud Sandbox fenyegetésészlelő technológiát a Kaspersky Security Center konzol *Report on threats* jelentésében jelzi.



Fenyegetésszámlálók

A Cloud Sandbox számláló engedélyezéséhez:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response** elemet.
5. Válassza ki az **Cloud Sandbox** lapot.
6. Kapcsolja be az **Cloud Sandbox ENABLED** kapcsolót.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Fenyegetés esetén, a Kaspersky Endpoint Security aktiválja a Cloud Sandbox segítségével észlelt fenyegetések számlálóját a fő alkalmazásablaknak a **Fenyegetésészlelő technológiák** alatt. A Kaspersky Endpoint Security a Cloud Sandbox fenyegetésészlelő technológiát a Kaspersky Security Center konzol *Report on threats* jelentésében is jelzi.

KEA-KES migrációs útmutató az EDR Optimum számára

A Kaspersky Endpoint Security for Windows beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Optimum megoldáshoz. Az EDR Optimummal való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra. A Kaspersky Endpoint Agent minden funkcióját a Kaspersky Endpoint Security végzi.

Amikor olyan számítógépeken telepíti a Kaspersky Endpoint Security alkalmazást, amelyekre telepítve van a Kaspersky Endpoint Agent, a Kaspersky Endpoint Detection and Response Optimum megoldás továbbra is együttműködik a Kaspersky Endpoint Security termékkel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről. A Kaspersky Endpoint Security 11.7.0 vagy újabb verzióra történő frissítésekor a rendszer ugyanígy viselkedik.

A Kaspersky Endpoint Security nem kompatibilis a Kaspersky Endpoint Agent szolgáltatással. Ezeket az alkalmazásokat nem telepítheti ugyanarra a számítógépre.

A következő feltételeknek kell teljesülniük ahhoz, hogy a Kaspersky Endpoint Security az Kaspersky Endpoint Detection and Response Optimum részeként működjön:

- Kaspersky Endpoint Detection and Response Optimum 2.0 vagy újabb verzió.
- Kaspersky Security Center 13.2 vagy újabb verzió (beleértve a Network Agentet is). A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az EDR Optimum szolgáltatást.
- Az EDR Optimum funkcióit csak a Kaspersky Security Center Web Console használatával lehet felügyelni.
- Az adatátvitel a felügyeleti kiszolgálóra engedélyezett. Az adatokra a számítógépen karanténba helyezett fájlokkal kapcsolatos információk megszerzéséhez van szükség a Web Console-on keresztül.
- Létrejön a háttérkapcsolat a Kaspersky Security Center Web Console és a Felügyeleti kiszolgáló között. Ahhoz, hogy a EDR Optimum működni tudjon a Felügyeleti kiszolgálóval a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos kapcsolatot, egy *háttérkapcsolatot*.

A [KES+KEA] konfiguráció [KES+beépített ügynök] EDR Optimum megoldásba történő migrálásának lépései

1. **A Kaspersky Endpoint Security webes bővítmény frissítése**

   Az EDR Optimum összetevő a Kaspersky Endpoint Security webes bővítmény 11.7.0 vagy újabb verziójával felügyelhető.

2. **Házirendek és a feladatok áttelepítése**

   A Kaspersky Endpoint Agent beállításainak átvitele a Kaspersky Endpoint Security for Windows megoldásba. Ehhez használja a varázslót a Kaspersky Endpoint Agentből való migráláshoz a Web Console-ban.

   A szabályzat- és feladatbeállítások áttelepítése a Kaspersky Endpoint Agent szolgáltatásból a Kaspersky Endpoint Security szolgáltatásba a Web Console-on

   A Web Console fő ablakában válassza a **Operations** → **Migration from Kaspersky Endpoint Agent** lehetőséget.

Ezzel futtatja a szabályzat- és feladatáttelepítési varázslót. Kövesse a varázsló utasításait.

1. lépés. Szabályzat áttelepítése

Az áttelepítési varázsló új szabályzatot hoz létre, amely egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent szabályzatainak beállításait. A listában válassza ki azokat a Kaspersky Endpoint Agent szabályzatokat, amelyek beállításait egyesíteni szeretné a Kaspersky Endpoint Security szabályzatával. Kattintson a Kaspersky Endpoint Agent szabályzatára, és válassza ki azt a Kaspersky Endpoint Security szabályzatot, amellyel egyesíteni szeretné a beállításokat. Győződjön meg arról, hogy a megfelelő szabályzatokat választotta, és folytassa a következő lépéssel.

2. lépés. Feladatok áttelepítése

Az áttelepítési varázsló új feladatokat hoz létre a Kaspersky Endpoint Security számára. A feladatlistában válassza ki azokat a Kaspersky Endpoint Agent feladatokat, amelyeket létre szeretné hozni a Kaspersky Endpoint Security szabályzatához. Lépjen a következő lépésre.

3. lépés. A varázsló befejezése

Lépjen ki a varázslóból. Ennek eredményeként a varázsló a következőket teszi:

- Létrehoz egy új Kaspersky Endpoint Security szabályzatot.

  A szabályzat egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent beállításait. A szabályzat neve *<Kaspersky Endpoint Security policy name> és <Kaspersky Endpoint Agent policy name>*. Az új házirend *Inactive* állapotot kap. A folytatáshoz módosítsa a Kaspersky Endpoint Agent és a Kaspersky Endpoint Security szabályzatok állapotát *Inactive* értékre, és aktiválja az új egyesített szabályzatot.

  > A Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security for Windows szolgáltatásra történő áttérés után győződjön meg arról, hogy az új házirendben be van-e állítva az Adatátvitel az adminisztrációs kiszolgálóra funkció (karanténfájl-adatok és fenyegetés-fejlődési lánc adatai). Az adatátviteli paraméterek értékei nem lesznek áttelepítve a Kaspersky Endpoint Agent házirendjéből.

- Létrehozza a Kaspersky Endpoint Security új feladatait.

  Az új feladatok a Kaspersky Endpoint Agent feladatainak másolatai. Emellett a varázsló változatlanul hagyja a Kaspersky Endpoint Agent feladatait.

3 Az EDR Optimum funkció licencelése

Ha egy közös Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security licencet használ a Kaspersky Endpoint Security for Windows és a Kaspersky Endpoint Agent aktiválásához, az EDR Optimum funkció automatikusan aktiválódik az alkalmazás 11.7.0 vagy újabb verzióra történő frissítése után. Semmi mást nem kell tennie.

Ha önálló Kaspersky Endpoint Detection and Response Optimum bővítményi licencet használ az EDR Optimum funkció aktiválásához, akkor győződjön meg arról, hogy az EDR Optimum kulcsot hozzáadta a Kaspersky Security Center tárolójához, és engedélyezte az automatikus licenckulcs-szolgáltatói funkciót. Az alkalmazás 11.7.0 vagy újabb verzióra történő frissítése után az EDR Optimum funkció automatikusan aktiválódik.

Ha Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security licencet használ a Kaspersky Endpoint Agent aktiválásához, és egy másik licencet a Kaspersky Endpoint Security for Windows aktiválásához, akkor a Kaspersky Endpoint Security for Windows kulcsot a közös Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security kulcsra kell cserélnie. A kulcsot a *Add key* feladat segítségével cserélheti ki.

4 A Kaspersky Endpoint Security alkalmazás telepítése/frissítése

Az alkalmazás telepítése vagy frissítése során az EDR Optimum funkciók áttelepítéséhez ajánlott a távoli telepítési feladat használata. Távoli telepítési feladat létrehozásakor a telepítőcsomag beállításaiban ki kell választania az EDR Optimum összetevőt.

Az alkalmazást a következő módszerekkel is frissítheti:

- A Kaspersky frissítési szolgáltatás használatával.
- Helyben, a Telepítővarázsló segítségével.

A Kaspersky Endpoint Security támogatja az összetevők automatikus kiválasztását az alkalmazásfrissítés során az olyan számítógép esetében, amelyre a Kaspersky Endpoint Agent alkalmazás telepítve van. Az összetevők automatikus kiválasztása az alkalmazás frissítését végző felhasználói fiók engedélyeitől függ.

Ha a Kaspersky Endpoint Security frissítése a rendszerfiók (SYSTEM) alatt található EXE- vagy MSI-fájl használatával történik, a Kaspersky Endpoint Security hozzáférést kap a Kaspersky-megoldások aktuális licenceihez. Ezért ha a számítógépen például a telepített Kaspersky Endpoint Agent mellett az EDR Optimum megoldás aktiválva van, a Kaspersky Endpoint Security telepítője automatikusan konfigurálja az összetevőket, és kiválasztja az EDR Optimum összetevőt. Ezáltal a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt. Az MSI-telepítő rendszerfiók (SYSTEM) alatti futtatása általában a Kaspersky frissítési szolgáltatása keretében történő frissítéskor vagy egy telepítőcsomag Kaspersky Security Centerrel végzett telepítésekor zajlik.

Ha a Kaspersky Endpoint Security frissítése emelt szintű jogosultsággal nem rendelkező felhasználói fiók alatt található MSI-fájl használatával történik, a Kaspersky Endpoint Security nem kap hozzáférést a Kaspersky-megoldások aktuális licenceihez. Ilyenkor a Kaspersky Endpoint Security automatikusan választja ki az összetevőket a Kaspersky Endpoint Agent konfigurációja alapján. Ezután a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt.

A Kaspersky Endpoint Security támogatja a frissítést a számítógép újraindítása nélkül. Az alkalmazásfrissítési módot a házirend tulajdonságaiban választhatja ki.

5 Az alkalmazás működésének ellenőrzése

Ha az alkalmazás telepítése vagy frissítése után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

- Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
- Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal. Ha egy összetevőnél *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy aktiválta a beépített ügynök funkciót.
- Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.

Kaspersky Sandbox



A Kaspersky Endpoint Security for Windows tartalmaz egy beépített ügynököt a Kaspersky Sandbox megoldással való integrációhoz. *A Sandbox* összetevő észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (a Sandbox-kiszolgálók). A megoldás részleteivel kapcsolatos információkat a Kaspersky Sandbox súgóban és a Kaspersky Anti Targeted Attack Platform súgóban találja.

A beépített ügynök integrációja a Kaspersky Sandbox megoldással

A Sandbox összetevővel való integrációhoz a Kaspersky Sandbox összetevő hozzáadása szükséges. A Sandbox összetevőt telepítés vagy frissítés közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

Az összetevő használatához az alábbi feltételeknek kell teljesülniük:

- Kaspersky Security Center 13.2. A Kaspersky Security Center korábbi verziói nem teszik lehetővé önálló IOC vizsgálati feladatok létrehozását fenyegetésre adott válaszként.
- Az összetevőt csak a Web Console használatával lehet felügyelni. Ezt az összetevőt nem felügyelheti az Adminisztrációs Konzol (MMC) használatával.
- Az alkalmazás aktiválva van, és a funkciójára a licenc kiterjed.
- Az adatátvitel a felügyeleti kiszolgálóra engedélyezett.

  A Kaspersky Sandbox összes funkciójának használatához ellenőrizze, hogy a karanténba helyezett fájlok adatátvitele engedélyezve van-e. Az adatokra a számítógépen karanténba helyezett fájlokkal kapcsolatos információk megszerzéséhez van szükség a Web Console-on keresztül. Letölthet például egy fájlt a karanténból a Web Console-ban történő elemzéshez.

  Útmutató az adatátvitel az adminisztrációs kiszolgálóra funkció engedélyezéséhez a Web Console-ban

  1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
  2. Kattintson a Kaspersky Endpoint Security házirend nevére.

     Megnyílik a rendszabályok tulajdonságai ablak.
  3. Válassza ki az **Application settings** lapot.
  4. Nyissa meg a **General Settings** → **KSC Integration** elemet.
  5. A **Data transfer to Administration Server** részen jelölje be az **About Quarantine files** jelölőnégyzetet.
  6. Mentse el a módosításokat.
- Létrejön a háttérkapcsolat a Kaspersky Security Center Web Console és a Felügyeleti kiszolgáló között

Ahhoz, hogy a Kaspersky Sandbox működni tudjon a Felügyeleti kiszolgálóval a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos kapcsolatot, egy *háttérkapcsolatot*. A Kaspersky Security Center és más Kaspersky-megoldások integrálásával kapcsolatos részletekért tekintse meg a Kaspersky Security Center súgót.

Háttérkapcsolat létrehozása a Web Console-ban

1. A Web Console fő ablakában válassza a **Settings** → **Integration** lehetőséget.
2. Nyissa meg a **Integration** szakaszt.
3. Kapcsolja be az **Background connection for integration Enabled** kapcsolót.
4. Mentse el a módosításokat.

Ha nem jön létre háttérkapcsolat a Kaspersky Security Center Web Console és a Felügyeleti kiszolgáló között, akkor önálló IOC vizsgálati feladatok nem hozhatók létre a fenyegetésre adott válasz részeként.

- Ha megbízható kapcsolatot szeretne konfigurálni a Sandbox-kiszolgálóval, elő kell készítenie egy TLS-tanúsítványt. Ezután hozzá kell adnia a tanúsítványt a számítógéphez egy házirend segítségével. A tanúsítványt a Sandbox-kiszolgálóhoz is hozzá kell adnia.

  > A kriptokonténerrel történő kétirányú hitelesítés nem érhető el a Kaspersky Sandbox esetében.

  TLS-tanúsítványt helyileg is hozzáadhat a Web Console-ban vagy helyileg a parancssor segítségével.

- A Kaspersky Sandbox összetevő engedélyezve van.
- A Sandbox működését biztosító alkalmazásösszetevők engedélyezve vannak és működőképesek. A Sandbox működését a következő összetevők biztosítják:
  - Fájl védelem.
  - Behatolásmegelőző rendszer.
  - Tűzfal.
  - AMSI védelem.
  - Vizsgálat a háttérben.

A Kaspersky Sandbox-szal való integráció engedélyezése vagy letiltása:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Sandbox** elemet.
5. A **Integration with Sandbox ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. A(z) **Integration mode** területen válassza ki az összetevő működési módját: **Kaspersky Sandbox**.

7. Kattintson a **Connection settings** hivatkozásra.

   Ekkor megnyílik a Sandbox-kiszolgáló kapcsolódási beállításai ablak.

8. A **Server TLS certificate** részen kattintson az **Upload** elemre, és válassza ki a TLS-tanúsítványfájlt.

   A Kaspersky Endpoint Security csak egy TLS-tanúsítvánnyal rendelkezhet egy Sandbox-kiszolgáló esetében. Ha korábban már felvett egy TLS-tanúsítványt, akkor azt az alkalmazás visszavonja. Csak az utoljára felvett tanúsítvány lesz felhasználva.

9. Speciális kapcsolódási beállítások konfigurálása a Sandbox-kiszolgálókhoz:

   - **Timeout (msec)**. A Sandbox-kiszolgáló kapcsolódási időtúllépése. A beállított időtúllépés letelte után a Kaspersky Endpoint Security kérést küld a következő kiszolgálónak. Növelheti a kiszolgáló kapcsolódási időtúllépését, ha a kapcsolat sebessége alacsony, vagy ha a kapcsolat instabil. A kérések ajánlott időtúllépése 0.5 másodperc vagy kevesebb.

   - **Request queue**. A kérési várólista mappájának mérete. Ha több objektumot küld vizsgálatra a Sandboxban, a Kaspersky Endpoint Security egy kérés-várólistát hoz létre. Alapértelmezés szerint a kérési várólista mappamérete 100 MB-ra van korlátozva. A maximális méret elérése után a Sandbox leállítja az új kérések hozzáadását a várólistához, és elküldi a megfelelő eseményt a Kaspersky Security Centernek. A kiszolgáló konfigurációjától függően konfigurálhatja a kérési várólista mappaméretét.

10. A **Connection to Sandbox servers** részen kattintson a **Add** gombra.

11. Ezzel megnyílik egy ablak; itt adja meg a Sandbox-kiszolgáló címét (IPv4, IPv6, DNS) és portját.

    A virtuális képek telepítésével és a Sandbox-kiszolgálók konfigurálásával kapcsolatos részletekért lásd a Kaspersky Sandbox súgót.

12. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Endpoint Security ellenőrizni fogja a TLS-tanúsítványt. Ha a tanúsítvány ellenőrzése sikerül, a Kaspersky Endpoint Security feltölti a tanúsítványfájlt a számítógépre a Kaspersky Security Centerrel való következő szinkronizálás során. Ha két TLS-tanúsítvány van hozzáadva, a Kaspersky Sandbox a legújabb tanúsítványt használja a megbízható kapcsolat létrehozásához. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. A **Sandbox** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

A Kaspersky Sandbox integrációt engedélyezheti vagy letilthatja a Web Console-ban vagy helyileg a parancssorból.

A Kaspersky Endpoint Security a Kaspersky Sandbox összetevő működésével kapcsolatos információkat jelentésbe menti. A jelentés a hibákról is tartalmaz információkat. Forduljon a Terméktámogatáshoz, ha hibaüzenetet kap a következő formátumú leírással: `Error code: XXX` (például `0xa67b01f4`).

Biztonsági sérülési indikátorok vizsgálata (önálló feladat)

A *biztonsági sérülési indikátor (IOC)* egy olyan objektumra vagy tevékenységre vonatkozó adathalmaz, amely jogosulatlan hozzáférést jelez a számítógéphez (adatok veszélyeztetése). Például sok sikertelen bejelentkezési kísérlet a rendszerbe biztonsági sérülésre utalhat. Az *IOC Scan* feladat lehetővé teszi a biztonsági sérülési indikátorok (IOC) megtalálását a számítógépen, valamint biztosítja a fenyegetésre reagáló intézkedések megtételét.

A Kaspersky Endpoint Security IOC-fájlok segítségével keresi a biztonsági sérülés indikátorait. Az *IOC-fájlok* olyan fájlok, amelyek az indikátorkészleteket tartalmazzák, és amelyekkel az alkalmazás egyezést próbál találni észlelés esetén. Az IOC-fájloknak meg kell felelniük az OpenIOC szabványnak. A Kaspersky Endpoint Security automatikusan IOC-fájlokat hoz létre a Kaspersky Sandbox számára.

Az IOC Scan feladat futásmódja

Az alkalmazás önálló IOC vizsgálati feladatokat hoz létre a Kaspersky Sandbox számára. Az *Önálló IOC vizsgálati feladat* egy olyan csoportos feladat, amely automatikusan létrejön, amikor a Kaspersky Sandbox az általa észlelt fenyegetésre reagál. A Kaspersky Endpoint Security automatikusan létrehozza az IOC-fájlt. Az egyéni IOC-fájlok nem támogatottak. A feladatok a létrehozás után 30 nappal automatikusan törlődnek. Az önálló IOC vizsgálati feladatokkal kapcsolatos további részletekért lásd a Kaspersky Sandbox súgót.

IOC Scan feladatbeállítások

A Kaspersky Sandbox automatikusan létrehozhat és futtathat *IOC Scan* i feladatokat, amikor a fenyegetésekre reagál.

A beállítások csak a webkonzolon keresztül konfigurálhatók.

A Kaspersky Security Center 13.2 verzióra van szükség a Kaspersky Sandbox önálló IOC vizsgálati feladatainak működéséhez.

Az IOC Scan feladat beállításainak módosítása:

1. A Web Console fő ablakában válassza a **Tasks** lehetőséget.

   Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **IOC Scan** feladatára.

   Megnyílik a feladatok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **IOC Scan settings** szakaszt.

5. Az IOC-észlelésre vonatkozó műveletek konfigurálása:

   - **Move copy to Quarantine, delete object**. Ha ezt az opciót választja, a Kaspersky Endpoint Security törli a számítógépen talált rosszindulatú objektumot. Az objektum törlése előtt a Kaspersky Endpoint Security biztonsági másolatot készít arra az esetre, ha az objektumot később vissza kell állítani. A Kaspersky Endpoint Security a biztonsági másolatot karanténba helyezi.

   - **Run Critical Areas Scan**. Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a *Critical Areas Scan* feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.

   - **Run only when the computer is idle**. A feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárolva van vagy ha a képernyővédő be van kapcsolva. Ha megszakította a feladat végrehajtását, például a számítógép zárolásának feloldásával, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol megszakították. Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.

6. Mentse el a módosításokat.

A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Results** szakaszban. Az észlelt biztonsági sérülési indikátorokra vonatkozó információkat a feladat tulajdonságaiban tekintheti meg: **Application settings → IOC Scan results**.

Az IOC vizsgálat eredményeinek megőrzése 30 napig történik. Ezt követően a Kaspersky Endpoint Security automatikusan törli a legrégebbi bejegyzéseket.

KEA-KES migrációs útmutató a Kaspersky Sandbox számára

A Kaspersky Endpoint Security for Windows tartalmaz egy beépített ügynököt a Kaspersky Sandbox megoldáshoz. A Kaspersky Sandbox megoldással való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra. A Kaspersky Endpoint Agent minden funkcióját a Kaspersky Endpoint Security végzi.

Amikor olyan számítógépeken telepíti a Kaspersky Endpoint Security alkalmazást, amelyekre telepítve van a Kaspersky Endpoint Agent, a Kaspersky Sandbox megoldás továbbra is együttműködik a Kaspersky Endpoint Security termékkel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről. A Kaspersky Endpoint Security 11.7.0 vagy újabb verzióra történő frissítésekor a rendszer ugyanígy viselkedik.

A Kaspersky Endpoint Security nem kompatibilis a Kaspersky Endpoint Agent szolgáltatással. Ezeket az alkalmazásokat nem telepítheti ugyanarra a számítógépre.

A következő feltételeknek kell teljesülniük ahhoz, hogy a Kaspersky Endpoint Security a Kaspersky Sandbox részeként működjön:

- Kaspersky Sandbox 2.0 vagy újabb verzió.
- Kaspersky Security Center 13.2 vagy újabb verzió (beleértve a Network Agentet is). A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az Kaspersky Sandbox szolgáltatást.
- A Kaspersky Sandbox megoldást csak a Kaspersky Security Center Web Console használatával lehet felügyelni.

- Az adatátvitel a felügyeleti kiszolgálóra engedélyezett. Az adatokra a számítógépen karanténba helyezett fájlokkal kapcsolatos információk megszerzéséhez van szükség a Web Console-on keresztül.

- Létrejön a háttérkapcsolat a Kaspersky Security Center Web Console és a Felügyeleti kiszolgáló között. Ahhoz, hogy a Kaspersky Sandbox működni tudjon a Felügyeleti kiszolgálóval a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos kapcsolatot, egy *háttérkapcsolatot*.

A [KES+KEA] konfiguráció [KES+beépített ügynök] Kaspersky Sandbox megoldásba történő migrálásának lépései

1. **A Kaspersky Endpoint Security webes bővítmény frissítése**

   Az Kaspersky Sandbox összetevő a Kaspersky Endpoint Security felügyeleti bővítmény 11.7.0 vagy újabb verziójával felügyelhető.

2. **Házirendek és a feladatok áttelepítése**

   A Kaspersky Endpoint Agent beállításainak átvitele a Kaspersky Endpoint Security for Windows megoldásba. Ehhez használja a varázslót a Kaspersky Endpoint Agentből való migráláshoz a Web Console-ban.

   A szabályzat- és feladatbeállítások áttelepítése a Kaspersky Endpoint Agent szolgáltatásból a Kaspersky Endpoint Security szolgáltatásba a Web Console-on

   A Web Console fő ablakában válassza a **Operations** → **Migration from Kaspersky Endpoint Agent** lehetőséget.

   Ezzel futtatja a szabályzat- és feladatáttelepítési varázslót. Kövesse a varázsló utasításait.

1. lépés. Szabályzat áttelepítése

Az áttelepítési varázsló új szabályzatot hoz létre, amely egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent szabályzatainak beállításait. A listában válassza ki azokat a Kaspersky Endpoint Agent szabályzatokat, amelyek beállításait egyesíteni szeretné a Kaspersky Endpoint Security szabályzatával. Kattintson a Kaspersky Endpoint Agent szabályzatára, és válassza ki azt a Kaspersky Endpoint Security szabályzatot, amellyel egyesíteni szeretné a beállításokat. Győződjön meg arról, hogy a megfelelő szabályzatokat választotta, és folytassa a következő lépéssel.

2. lépés. Feladatok áttelepítése

Az áttelepítési varázsló új feladatokat hoz létre a Kaspersky Endpoint Security számára. A feladatlistában válassza ki azokat a Kaspersky Endpoint Agent feladatokat, amelyeket létre szeretné hozni a Kaspersky Endpoint Security szabályzatához. Lépjen a következő lépésre.

3. lépés. A varázsló befejezése

Lépjen ki a varázslóból. Ennek eredményeként a varázsló a következőket teszi:

- Létrehoz egy új Kaspersky Endpoint Security szabályzatot.

  A szabályzat egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent beállításait. A szabályzat neve *<Kaspersky Endpoint Security policy name> és <Kaspersky Endpoint Agent policy name>*. Az új házirend *Inactive* állapotot kap. A folytatáshoz módosítsa a Kaspersky Endpoint Agent és a Kaspersky Endpoint Security szabályzatok állapotát *Inactive* értékre, és aktiválja az új egyesített szabályzatot.

  A Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security for Windows szolgáltatásra történő áttérés után győződjön meg arról, hogy az új házirendben be van-e állítva az Adatátvitel az adminisztrációs kiszolgálóra funkció (karanténfájl-adatok és fenyegetés-fejlődési lánc adatai). Az adatátviteli paraméterek értékei nem lesznek áttelepítve a Kaspersky Endpoint Agent házirendjéből.

- Létrehozza a Kaspersky Endpoint Security új feladatait.

  Az új feladatok a Kaspersky Endpoint Agent feladatainak másolatai. Emellett a varázsló változatlanul hagyja a Kaspersky Endpoint Agent feladatait.

3 A Kaspersky Sandbox funkció licencelése

A Kaspersky Endpoint Security aktiválásához a Kaspersky Sandbox megoldás részeként külön licenc szükséges a Kaspersky Sandbox kiegészítőhöz. A kulcsot a *Add key* feladat segítségével veheti fel. Ennek eredményeképpen a rendszer két kulcsot ad hozzá az alkalmazáshoz: *Kaspersky Endpoint Security* és *Kaspersky Sandbox*.

4 A Kaspersky Endpoint Security alkalmazás telepítése/frissítése

Az alkalmazás telepítése vagy frissítése során az Kaspersky Sandbox funkciók áttelepítéséhez ajánlott a távoli telepítési feladat használata. Távoli telepítési feladat létrehozásakor a telepítőcsomag beállításaiban ki kell választania az Kaspersky Sandbox összetevőt.

Az alkalmazást a következő módszerekkel is frissítheti:

- A Kaspersky frissítési szolgáltatás használatával.
- Helyben, a Telepítővarázsló segítségével.

A Kaspersky Endpoint Security támogatja az összetevők automatikus kiválasztását az alkalmazásfrissítés során az olyan számítógép esetében, amelyre a Kaspersky Endpoint Agent alkalmazás telepítve van. Az összetevők automatikus kiválasztása az alkalmazás frissítését végző felhasználói fiók engedélyeitől függ.

Ha a Kaspersky Endpoint Security frissítése a rendszerfiók (SYSTEM) alatt található EXE- vagy MSI-fájl használatával történik, a Kaspersky Endpoint Security hozzáférést kap a Kaspersky-megoldások aktuális licenceihez. Ezért ha a számítógépen például a telepített Kaspersky Endpoint Agent mellett az Kaspersky Sandbox megoldás aktiválva van, a Kaspersky Endpoint Security telepítője automatikusan konfigurálja az összetevőket, és kiválasztja az Kaspersky Sandbox összetevőt. Ezáltal a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt. Az MSI-telepítő rendszerfiók (SYSTEM) alatti futtatása általában a Kaspersky frissítési szolgáltatása keretében történő frissítéskor vagy egy telepítőcsomag Kaspersky Security Centerrel végzett telepítésekor zajlik.

Ha a Kaspersky Endpoint Security frissítése emelt szintű jogosultsággal nem rendelkező felhasználói fiók alatt található MSI-fájl használatával történik, a Kaspersky Endpoint Security nem kap hozzáférést a Kaspersky-megoldások aktuális licenceihez. Ilyenkor a Kaspersky Endpoint Security automatikusan választja ki az összetevőket a Kaspersky Endpoint Agent konfigurációja alapján. Ezután a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt.

A Kaspersky Endpoint Security támogatja a frissítést a számítógép újraindítása nélkül. Az alkalmazásfrissítési módot a házirend tulajdonságaiban választhatja ki.

5. **Az alkalmazás működésének ellenőrzése**

   Ha az alkalmazás telepítése vagy frissítése után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

   - Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
   - Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal. Ha egy összetevőnél *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy aktiválta a beépített ügynök funkciót.
   - Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.

Kaspersky Anti Targeted Attack Platform

A Kaspersky Endpoint Security for Windows támogatja a Kaspersky Anti Targeted Attack Platform (EDR (KATA)) megoldást. A *Kaspersky Anti Targeted Attack Platform* egy megoldás, ami a kifinomult fenyegetések, például célzott támadások és speciális, állandó veszélyek (APT), valamint nagy kockázatú veszélyforrások időszerű észlelésére szolgál. A Kaspersky Anti Targeted Attack Platform három funkcionális egységet tartalmaz:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Az összes funkcionális egységet vagy az egyes funkcionális egységeket külön is megvásárolhatja. A megoldás részleteivel kapcsolatos információért lásd a Kaspersky Anti Targeted Attack Platform útmutatót. Az alkalmazás beépített ügynököket tartalmaz az EDR, NDR összetevők számára. Az alkalmazás támogatja a KATA részét képező Sandbox összetevővel való együttműködést is.

Fenyegetés-felderítési eszközök

A Kaspersky Endpoint Detection and Response a következő Threat Intelligence eszközöket használja:

- Integráció a Kaspersky Threat Intelligence Portállal, amely információkat tartalmaz és jelenít meg fájlok és webcímek megbízhatóságáról.
- Kaspersky Threats adatbázis.
- Kaspersky Security Network (a továbbiakban: KSN) felhőszolgáltatási infrastruktúra, amely hozzáférést biztosít a Kaspersky tudásbázisából származó valós idejű fájl-, webhely- és szoftver-megbízhatósági információkhoz. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban képes reagálni a fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken.

A megoldás működési elve

A Kaspersky Endpoint Security a vállalati IT-infrastruktúra egyes számítógépeire van telepítve, és folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítás alatt álló fájlokat. A számítógépen zajló eseményekkel kapcsolatos információk (telemetriai adatok) elküldésre kerülnek a Kaspersky Anti Targeted Attack Platform kiszolgálóra. Ebben az esetben a Kaspersky Endpoint Security információkat küld a Kaspersky Anti Targeted Attack Platform kiszolgálónak az alkalmazás által észlelt fenyegetésekről, valamint az ilyen fenyegetések feldolgozási eredményeiről is.

Az EDR (KATA) és NDR (KATA) integráció a Kaspersky Security Center konzolon van konfigurálva. A beépített ügynök ezután a Kaspersky Anti Targeted Attack Platform konzol segítségével kezelhető, beleértve a feladatok futtatását, a karanténba helyezett objektumok kezelését, a jelentések megtekintését és az egyéb műveleteket.

Kaspersky Endpoint Security-konfigurációk a EDR/NDR (KATA) használatához

A következő konfigurációk használhatók a EDR/NDR (KATA) megoldással való munkavégzéshez:

- **[KES+beépített ügynök]**. Ebben a konfigurációban a Kaspersky Endpoint Security a számítógép biztonságát garantáló alkalmazásként és a EDR/NDR (KATA) megoldással való munkavégzéshez is használható alkalmazásként működik. Az EDR (KATA) beépített ügynöke a Kaspersky Endpoint Security 12.1 for Windows vagy újabb verzióban érhető el. Az NDR (KATA) beépített ügynöke a Kaspersky Endpoint Security 12.7 for Windows vagy újabb verzióban érhető el.

- **[külső EPP+EDR Agent]**. Ebben a konfigurációban az IT-infrastruktúra biztonságát a harmadik féltől származó Endpoint Protection Platform (EPP) garantálja. A EDR / NDR (KATA) megoldással való interakciót a Kaspersky Endpoint Security biztosítja az Endpoint Detection and Response Agent (EDR Agent) konfigurációban. Ebben a konfigurációban az EDR Agent kompatibilis a harmadik féltől származó EPP-alkalmazásokkal. Az EDR (KATA) EDR Agent a Kaspersky Endpoint Security 12.3 for Windows vagy újabb verzióban érhető el. Az NDR (KATA) EDR Agent a Kaspersky Endpoint Security 12.7 for Windows vagy újabb verzióban érhető el.

A Kaspersky Endpoint Security korábbi verzióinak támogatása

Ha a Kaspersky Endpoint Security 11.2.0 – 11.8.0 verzióját használja a Kaspersky Anti Targeted Attack Platform (EDR) megoldással való együttműködésre, akkor az alkalmazás magában foglalja a Kaspersky Endpoint Agent szolgáltatást. A Kaspersky Endpoint Agent szolgáltatást a Kaspersky Endpoint Security szolgáltatással együtt telepítheti.

Ha a Kaspersky Endpoint Security 11.9.0 – 12.0 verzióját használja, a Kaspersky Endpoint Agentet külön kell telepítenie, mert a Kaspersky Endpoint Security 11.9.0-tól kezdve a Kaspersky Endpoint Agent terjesztőcsomag már nem része a Kaspersky Endpoint Security terjesztőkészletnek.

A beépített ügynök integrálása az EDR / NDR (KATA) megoldással

Az EDR / NDR (KATA) integrációhoz hozzá kell adnia a megfelelő összetevőt: Endpoint Detection and Response (KATA) vagy Network Detection and Response (KATA). Az EDR / NDR (KATA) integráció összetevőjét az alkalmazás telepítése vagy frissítése közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

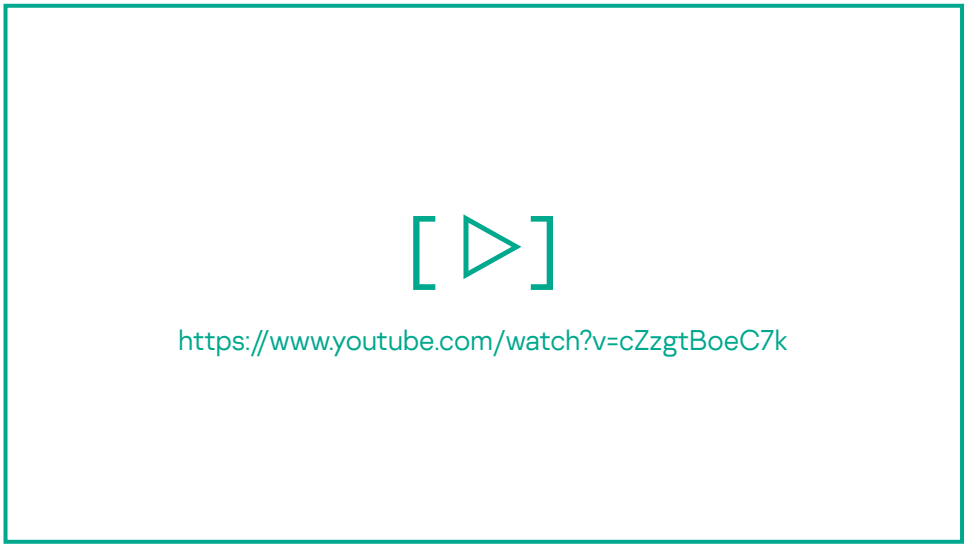
A Kaspersky Endpoint Security for Windows 12.11-es verziójától kezdődően az EDR (KATA) összetevő át lett nevezve erre: **Endpoint Detection and Response Expert (version 8.0 or later)**. Az alkalmazás ezen verziójában az összetevő kompatibilis a Kaspersky Anti Targeted Attack Platform 7.1 és korábbi verzióival, valamint a Kaspersky Endpoint Detection and Response Expert (on-premises) programmal.

Az Endpoint Detection and Response Optimum, az Endpoint Detection and Response Expert (cloud) és az Endpoint Detection and Response Expert (on-premises) összetevők nem kompatibilisek egymással.

Az EDR / NDR (KATA) használatához az alábbi feltételeknek kell teljesülniük:

- A EDR (KATA): Kaspersky Anti Targeted Attack Platform 5.0–7.1 verziók.
- A NDR (KATA): Kaspersky Anti Targeted Attack Platform 7.0 vagy újabb verzió.
- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 vagy újabb. A KATA és a Kaspersky Endpoint Security különböző verzióival való kompatibilitásáról további részleteket a Kaspersky Anti Targeted Attack Platform súgójában találsz.
- NDR (KATA): Kaspersky Endpoint Security for Windows 12.7 vagy újabb.
- Kaspersky Security Center 14.2 vagy újabb verzió. A Kaspersky Security Center korábbi verzióiban nem lehet aktiválni az EDR / NDR (KATA) integráció funkcióját.
- Az alkalmazás aktiválva van, és a funkciójára a licenc kiterjed.
- Az Endpoint Detection and Response (KATA) és a Network Detection and Response (KATA) összetevők engedélyezve vannak.
- Az EDR / NDR (KATA) működését biztosító alkalmazásösszetevők engedélyezve vannak és működőképesek. A EDR/NDR (KATA) működését a következő összetevők biztosítják:
  - Fájl védelem.
  - Web védelem.
  - Levelezés védelem.
  - Biztonsági rések kihasználásának megelőzése.
  - Viselkedésészlelés.
  - Behatolásmegelőző rendszer.

- AMSI védelem.
- Vizsgálat a háttérben.
- Kaspersky Security Network.



https://www.youtube.com/watch?v=cZzgtBoeC7k



https://www.youtube.com/watch?v=gd-rySv0ThQ

Az Endpoint Detection and Response (KATA) integrálása a következő lépéseket foglalja magában:

1. **Az Endpoint Detection and Response (KATA) és a Network Detection and Response (KATA) összetevők telepítése**

   Az EDR (KATA) és NDR (KATA) összetevőt telepítés vagy frissítés közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

   Újra kell indítania a számítógépét az alkalmazás új elemekkel történő frissítésének befejezéséhez.

2. **Az Endpoint Detection and Response (KATA) és a Network Detection and Response (KATA) aktiválása**

   Külön licenc vásárlására van szükség az EDR (KATA) és NDR (KATA) számára (például Kaspersky Endpoint Detection and Response (KATA) bővítmény).

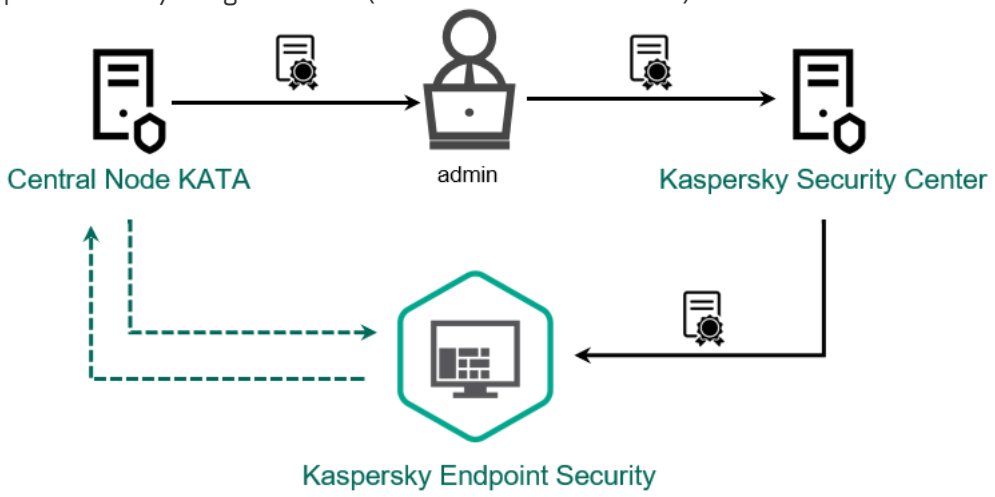
   A funkció egy külön kulcs hozzáadása után válik elérhetővé, amely az EDR (KATA) és NDR (KATA) funkciókat foglalja magában. Ennek eredményeképpen több kulcs kerül hozzáadásra a számítógépen: egy kulcs a Kaspersky Endpoint Security, valamint kulcsok a Kaspersky Endpoint Detection and Response (KATA) és a Network Detection and Response (KATA) számára.

   Az önálló EDR (KATA) és NDR (KATA) funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

Győződjön meg arról, hogy az EDR (KATA) és az NDR (KATA) funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén fut.

3 Csatlakozás a Central Node-hoz

A Kaspersky Anti Targeted Attack Platform megbízható kapcsolatot létesít a Kaspersky Endpoint Security és a Central Node összetevő között. A megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell használnia. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). Ezután hozzá kell adnia a TLS-tanúsítványt a Kaspersky Endpoint Security szolgáltatáshoz (lásd az alábbi utasításokat).



A TLS-tanúsítvány hozzáadása a Kaspersky Endpoint Security szolgáltatáshoz

Alapértelmezés szerint a Kaspersky Endpoint Security csak a Central Node TLS-tanúsítványát ellenőrzi. A kapcsolat biztonságosabbá tétele céljából ezenkívül engedélyezheti a számítógép ellenőrzését a Central Node-on (kétirányú hitelesítés). Az ellenőrzés engedélyezéséhez be kell kapcsolnia a kétirányú hitelesítést a Central Node és a Kaspersky Endpoint Security beállításaiban. A kétirányú hitelesítés használatához kriptotárolóra is szüksége lesz. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Central Node-hoz az adminisztrációs konzol (MMC) segítségével

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A szabályzat ablakban válassza a **Detection and Response** lehetőséget, majd válassza ki a konfigurálni kívánt összetevőt: **Endpoint Detection and Response Expert (on-premises)** vagy **Network Detection and Response (KATA)**.
5. Jelölje be a megfelelő jelölőnégyzetet: **Endpoint Detection and Response Expert (7.1 vagy korábbi verzió)** vagy **Network Detection and Response (KATA)**.
6. Kattintson a **Kiszolgáló kapcsolódási beállításai** lehetőségre.

7. Konfigurálja a kiszolgálói kapcsolatot:

   - **Időtúllépés (mp)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz.

   - **Kiszolgálói TLS-tanúsítvány hibája**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

   - **Kétirányú hitelesítés használata**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

8. Kattintson az **OK** gombra.

9. Central Node-kiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

   Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

10. Ha szükséges, konfigurálja a telemetriát.

11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Central Node-hoz a Web Console segítségével

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration** részt, és válassza ki a konfigurálni kívánt összetevőt: **Endpoint Detection and Response Expert (on-premises)** vagy **Network Detection and Response (KATA)**.

5. Kapcsolja be a megfelelő kapcsolót: **Endpoint Detection and Response Expert (on-premises) ENABLED** vagy **Network Detection and Response (KATA) ENABLED**.

6. Az EDR (KATA) beállításához válassza ki az **Endpoint Detection and Response Expert (version 7.1 or earlier)**lehetőséget a megoldások listájából.

7. Kattintson az **Connection settings** gombra.

8. Konfigurálja a kiszolgálói kapcsolatot:

   - **Timeout (sec)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz.

   - **Server certificate**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja).

   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

9. Kattintson az **OK** gombra.

10. Central Node-kiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

    Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

11. Ha szükséges, konfigurálja a telemetriát.

12. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

TLS-tanúsítványt helyileg is hozzáadhat a parancssor segítségével.

Ennek eredményeként a számítógép hozzá lesz adva a Kaspersky Anti Targeted Attack Platform konzolhoz. Ellenőrizheti az összetevők működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Endpoint Detection and Response Expert (version 8.0 or later)** és a **Network Detection and Response (KATA)** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

A Kaspersky Security Center konzol összetevőinek állapotát a számítógép tulajdonságainál ellenőrizheti az **Components** részen. Vegye figyelembe a következőket az összetevő állapotának ellenőrzésekor a konzolon. Ha az összetevő nincs telepítve, és a funkcióra nem vonatkozik a licence, a konzolon a **Not supported by license** állapot jelenik meg a **Not installed** helyett.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve az EDR (KATA) összetevő állapotát a Kaspersky Security Center Felügyeleti konzolon (MMC) követheti nyomon. Az összetevő aktuális állapota a számítógép tulajdonságaiban látható a következő részen: **Endpoint Sensor status** oszlop (*Running*, *Starting*, *Stopped*, *Paused*, *Failed*, *Unknown*). A Web Console nem jeleníti meg az Endpoint Sensor állapotát.

Az EDR (KATA) telemetria konfigurálása

A *Telemetria* a védett számítógépen történt események listája. A Kaspersky Endpoint Security elemzi a telemetriai adatokat, és elküldi a Kaspersky Anti Targeted Attack Platform számára a szinkronizálás során. A telemetriai események szinte folyamatosan érkeznek a kiszolgálóra. A Kaspersky Endpoint Security akkor kezdeményezi a szinkronizálást a kiszolgálóval, ha az alábbi feltételek bármelyike teljesül:

- A szinkronizálási intervallum lejárt.
- A pufferben lévő események száma meghaladja a felső határt.

Ezért alapértelmezés szerint az alkalmazás 30 másodpercenként szinkronizál, vagy amikor a puffer 1024 eseményt tartalmaz. A szinkronizálási viselkedést a Kaspersky Endpoint Security házirendjében konfigurálhatja, és kiválaszthatja a hálózati terhelésnek megfelelő optimális értékeket (lásd az alábbi utasításokat).

Ha nincs kapcsolat a Kaspersky Endpoint Security és a kiszolgáló között, az alkalmazás sorba állítja az új eseményeket. Amikor a kapcsolat helyreáll, a Kaspersky Endpoint Security megfelelő sorrendben küldi el a sorban álló eseményeket a kiszolgálónak. A kiszolgáló túlterhelésének elkerülése érdekében a Kaspersky Endpoint Security kihagyhat néhány eseményt. Ennek engedélyezéséhez optimalizálhatja az eseményátviteli beállításokat, például beállíthatja az események óránkénti maximális értékét (lásd az alábbi utasításokat).

Ha a Kaspersky Anti Targeted Attack Platformot egy másik, szintén telemetriát használó megoldással együtt használja, kikapcsolhatja a KATA (EDR) telemetriáját (lásd az alábbi utasításokat). Ez lehetővé teszi a kiszolgálói terhelés optimalizálását ezekhez a megoldásokhoz. Ha például telepítette a Managed Detection and Response megoldást és a KATA (EDR) megoldást, használhatja az MDR-telemetriát, és létrehozhat Fenyegetésekre adott válasz típusú feladatokat a KATA (EDR) megoldásban.

A telemetria konfigurálása a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A szabályzat ablakban válassza a **Detection and Response** lehetőséget, majd válassza ki a konfigurálni kívánt összetevőt: **Endpoint Detection and Response Expert (on-premises)** vagy **Network Detection and Response (KATA)**.
5. Konfigurálhatja a **Szinkronizálási kérés küldése a KATA kiszolgálójának ennyi percenként (perc)** beállítást. A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security információkat küld a módosított alkalmazásbeállításokról és feladatokról.
6. Győződjön meg arról, hogy a **Telemetriai adatok küldése a KATA számára** jelölőnégyzet be van jelölve.
7. Ha szükséges, konfigurálja a szinkronizálást a kiszolgáló beállításaival az **Adatátviteli beállítások** részen:
   - **Maximális eseményátviteli késleltetés (mp)**. Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc.
   - **Eseménycsomagok maximális száma**. Az alkalmazás akkor szinkronizál a kiszolgálóval, amikor a puffer megtelik eseményekkel. Az alapértelmezett beállítás 1024 esemény.

8. Ha szükséges, jelölje be a **Kérésszabályzás engedélyezése** jelölőnégyzetet a **Kérésszabályzás** részen.

   Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését.

9. Konfigurálja az optimalizálási beállításokat az események kiszolgálóra küldéséhez:

   - **Események maximális száma óránként**. Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni.

   - **Eseménykorlát túllépésének százalékos aránya**. Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.

10. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A telemetria konfigurálása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)** elemet.

5. Az EDR (KATA) beállításához válassza ki az **Endpoint Detection and Response Expert (version 7.1 or earlier)**lehetőséget a megoldások listájából.

6. Győződjön meg róla, hogy a **Send telemetry to KATA servers** négyzet be van jelölve az **Data transmission settings** területen.

7. Konfigurálja a **Send sync request to server every (min)** beállítást. A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security információkat küld a módosított alkalmazásbeállításokról és feladatokról.

8. Győződjön meg arról, hogy a **Send telemetry to KATA servers** négyzet be van jelölve.

9. Ha szükséges, konfigurálja a szinkronizálást a kiszolgáló beállításaival az **Data transmission settings** részen:

   - **Maximum event transmission delay (sec)**. Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc.

   - **Maximum number of event packages**. Az alkalmazás akkor szinkronizál a kiszolgálóval, amikor a puffer megtelik eseményekkel. Az alapértelmezett beállítás 1024 esemény.

10. Ha szükséges, jelölje be a **Enable request throttling** jelölőnégyzetet a **Request throttling** részen.

    Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését.

11. Konfigurálja az optimalizálási beállításokat az események kiszolgálóra küldéséhez:

    - **Maximum number of events per hour**. Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni.

    - **Percentage of event limit excess**. Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.

12. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **KATA integráció** → **Telemetriai kizárások** szakaszt.

5. Az **Adatátvitel beállításai** részen jelölje be a **Kizárások használata** jelölőnégyzetet.

6. Kattintson a **Hozzáadás** gombra, és konfigurálja a kizárásokat:

   > A kritériumokat az *AND* logikai értékkel kombinálhatja.

   - **Elérési út**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. A kizárás működéséhez meg kell adni a fájl elérési útját.

   - **Parancssor**. Az objektum futtatásához használt parancs.

   - **Leírás**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból.

     A VersionInfo erőforrás működésének további részleteiért keresse fel a Microsoft webhelyét.

   - **Eredeti fájlnév**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból.

   - **Verzió**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból.

   - **MD5**. a fájl MD5 kivonata.

- **SHA256**. a fájl SHA256 kivonata.
- **Eseménytípusok**. Ahhoz, hogy a kizárás működjön, ki kell választania legalább egy eseménytípust.

7. Mentse el a módosításokat.

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Tasks** lehetőséget.
   Megnyílik a feladatok listája.
2. Kattintson az **New task** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés A feladat típusának kiválasztása

1. Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** → **Frissítés visszaállítása** elemet.

2. lépés Az eszközök kiválasztása, amelyekhez a feladatot hozzárendeli

Válassza ki azokat a számítógépeket, amelyeken a feladatot végre kívánja hajtani. A következők közül választhat:

- Feladat hozzárendelése egy adminisztrációs csoporthoz. Ebben az esetben a feladat a korábban létrehozott adminisztrációs csoportokban található számítógépekhez lesz hozzárendelve.
- Válassza ki az Adminisztrációs szerver által a hálózaton észlelt számítógépeket– *hozzá nem rendelt eszközök*. Bizonyos eszközökbe tartozhatnak adminisztrációs csoportokban lévő, valamint hozzá nem rendelt eszközök is.
- Adja meg az eszközcímeket kézileg, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. lépés Feladatindítási ütemezés konfigurálása

Konfigurálja a feladat ütemezését, például manuálisan.

4. lépés A feladat nevének megadása

Adja meg a feladat nevét.

7. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Run the task after the wizard finishes** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

EDR (KATA)-telemetriai kizárások

A teljesítmény növelése és a Telemetria-kiszolgáló felé irányuló adatátvitel optimalizálása céljából konfigurálhatja a telemetria kizárásait. Dönthet például úgy, hogy az egyes alkalmazásokhoz nem küld hálózati kommunikációs adatokat.

Telemetriai kizárások létrehozásának menete az Adminisztrációs Konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.
4. A **Telemetriai beállítások → EDR (KATA) / NDR (KATA) telemetria** területen kattintson a **Beeállítások** gombra.
5. A megnyíló ablakban konfigurálja a telemetriai kizárásokat (lásd az alábbi táblázatot).

   Az alkalmazás a kizárási feltételeket a logikai ÉS jellel kombinálja. Szabály létrehozásához meg kell adnia egy értéket a **Teljes elérési út** mezőben, és válasszon ki legalább egy eseménytípust a **Használja a következő eseménytípusokhoz** listában.
6. Mentse el a módosításokat.

Telemetriai kizárások létrehozásának menete a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings → Telemetry Settings** elemet.
5. Válassza ki az **EDR (KATA) / NDR (KATA) telemetry** lapot.
6. A megnyíló ablakban konfigurálja a telemetriai kizárásokat (lásd az alábbi táblázatot).

   Az alkalmazás a kizárási feltételeket a logikai ÉS jellel kombinálja. Szabály létrehozásához meg kell adnia egy értéket a **Full path** mezőben, és ki kell választania legalább egy eseménytípust.
7. Mentse el a módosításokat.

Paraméter	Leírás
Kizárt folyamatok	**A küldendő telemetriai adatok méretének optimalizálása**. A Kaspersky Endpoint Security lehetővé teszi a továbbított adatok mennyiségének optimalizálását és a bizonyos kódú események kizárását a telemetriából: 102-es kód (alapvető kommunikáció) és 8-as kód (a folyamat hálózati tevékenysége) a Microsoft SMB protokollhoz, a WinRM szolgáltatás és a Hálózati ügynök klnagent.exe folyamata, valamint részletes információk a hálózati csomagok típusáról minden típusú hálózati protokoll esetében. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg. **A következő eseménytípusokhoz használja**: • **Fájlmódosítás**. • **Hálózati események**. • **Folyamat: konzolos interaktív bevitel**. • **Modul betöltve**. • **A rendszerleíró adatbázis módosult**. • **DNS-naplók**. • **Folyamat-hozzáférés**. • **Kódbeszúrás**. • **WMI lekérdezés**. • **Folyamat**. • **LDAP**. • **AMSI**.
Kizárt hálózati kommunikáció	**Szabály neve**. **Irány**. **Protokoll**. **Nyers szoftvercsatorna**. **Protokollszám**. **TLS-tanúsítvány**. **Helyi port vagy tartomány**. **Távoli port vagy tartomány**. **Helyi cím**. Annak a számítógépnek a hálózati címe, amelynél a Kaspersky Endpoint Security kizárja a telemetriát a hálózati forgalomból. **Távoli cím**. Annak a számítógépnek a hálózati címe, amelynél a Kaspersky Endpoint Security kizárja a telemetriát a hálózati forgalomból. Az IP-címeknél csak az IPv4 formátum támogatott. **Alkalmazások**. Azon alkalmazások futtatható fájljainak listája, amelyeknél a Kaspersky Endpoint Security kizárja az EDR-telemetriát a hálózati forgalomból.

Paraméter	Leírás
Kizárt fájlműveletek	**Szabály neve**. **Fájlnév vagy maszk**. Fájl vagy mappa neve vagy maszkja; a Kaspersky Endpoint Security alkalmazza a kizárási szabályt e fájl vagy mappa elérésekor. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy maszk megadásakor. **Művelet típusa**. **Előző elérési út**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.
Kizárt DNS-műveletek	**Szabály neve**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg. **DNS**: • **DNS-kiszolgáló IP-címe**. • **Lekérdezési lehetőségek**. • **Status**. • **Tartománynév**. • **Beállítástípus azonosítója**. • **Válaszadatok**.

Paraméter	Leírás
Kizárt LDAP-műveletek	**Szabály neve**. **LDAP keresési hatókör**. **Szűrő**. **Megkülönböztetett név az LDAP objektumok kereséséhez**. **Objektum attribútumai**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.
Kizárt folyamat-hozzáférési lekérdezések	**Szabály neve**. **Művelet típusa**. **Kért hozzáférés a folyamathoz**. **Híváslánc**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process**, **Parent process**, **File of the target process**, **Handle to the source process** és **Handle to the target process**. • **Teljes elérési út**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Parancssori szöveg**. A fájl futtatásához használt parancs. • **Adja meg a szabály aktiválási feltételeit és az eseménytípusokat, amelyekhez a szabályt használni szeretné**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Eredeti fájlnév**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Verzió**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Fájl ellenőrzőösszegei**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.

Paraméter	Leírás
Kizárt kódbeszúrások	**Szabály neve**. **Hozzáférési metódus**. **Hívássorozat**. **Módosított parancssor**. **Beszúrási cím**. **Beszúrási DLL neve**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.
Kizárt WMI lekérdezések	**Szabály neve**. **WMI művelet típusa**. **Távoli lekérdezés**. **A WMI parancsot végrehajtó számítógép neve**. **WMI felhasználói fiók**. **Végrehajtott WMI parancs**. **WMI névtér**. **WMI eseményfogyasztói szűrő**. **A létrehozott WMI eseményfogyasztó neve**. **A WMI eseményfogyasztó forráskódja**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.

Paraméter	Leírás
Kizárt csőműveletek	**Szabály neve**. **A cső neve**. **Művelet típusa**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.
Kizárt beállításjegyzék-módosítások	**Szabály neve**. **Művelet típusa**. **Elérési út**. **Érték neve**. **Value**. **A beállításjegyzék-fájl teljes neve**. A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja. **Process** és **Parent process**: • **Full path**. A fájl teljes elérési útja, beleértve a nevét és kiterjesztését. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. • **Command line text**. A fájl futtatásához használt parancs. • **Description**. A FileDescription paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Original file name**. Az OriginalFilename paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **Version**. A FileVersion paraméter értéke egy RT_VERSION (VersionInfo) erőforrásból. • **File checksums**. MD5 és SHA256. A fájlokat manuálisan is kiválaszthatja, és az alkalmazás automatikusan a kiválasztott fájlból fogja kitölteni a mezőket. 64 bites operációs rendszereken manuálisan kell megadnia a `C:\windows\system32` mappában található folyamat végrehajtható fájljának 64 bites verziójához tartozó paramétereket, mivel az alkalmazás a végrehajtható fájl paramétermezőit a `C:\windows\syswow64` mappában található ugyanezen végrehajtható fájl 32 bites verziójának tulajdonságaiból származó adatokkal tölti ki. Ha például kiválasztja a `C:\windows\system32\cmd.exe` lehetőséget, a bővítmény megjeleníti a `C:\windows\syswow64\cmd.exe` paramétereit. Az ilyen viselkedést az operációs rendszer sajátosságai határozzák meg.
Kizárt műveletek eszközökkel	**Szabály neve**. **Eszköztípus**. **Eszközazonosító**. **Eszköz neve**.

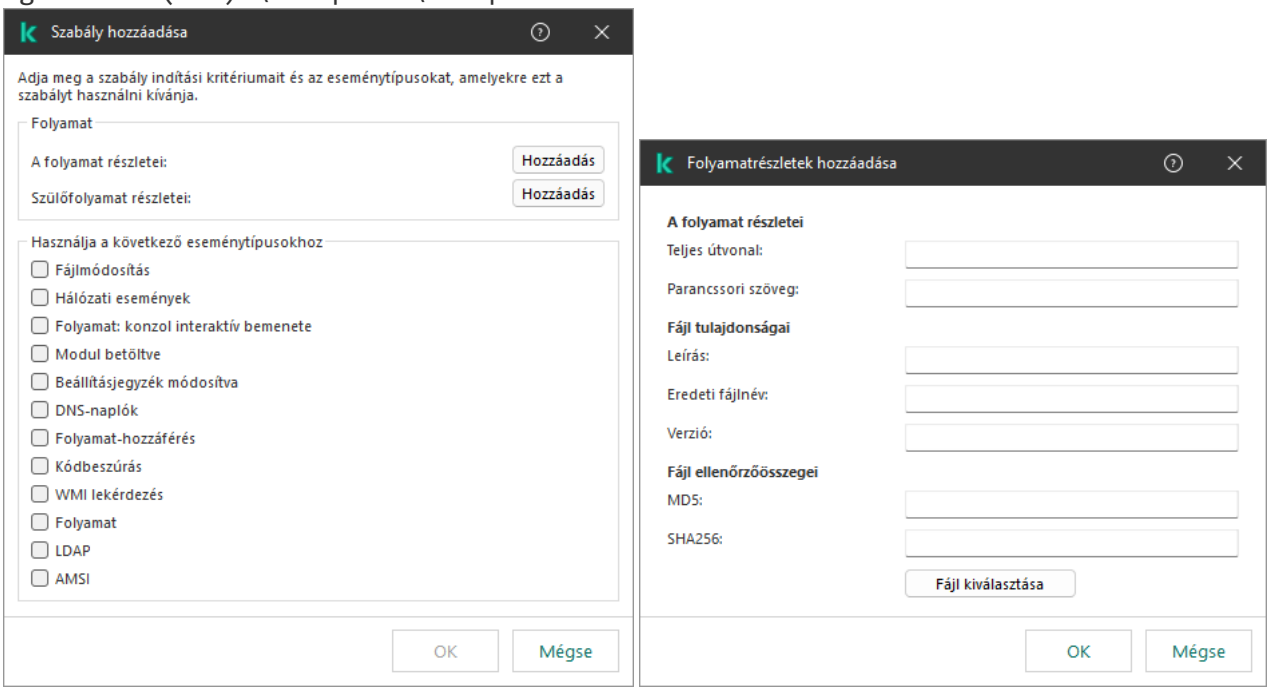
1. példa Kizárt folyamatok

Külső alkalmazások (folyamatok) eseményeinek telemetriából való kizárásához nyissa meg az EDR-telemetria kizárásai ablakot a **Kizárt folyamatok** lapon, és adja hozzá az alkalmazás futtatható fájlját.

A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja.

A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. Például:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Folyamat kizárása

1. példa Fájlmódosítás

Ha gyakran szerkeszt szkripteket a Notepad++ alkalmazásban, és ki szeretné zárni az adott szkriptek módosítási eseményeit, adja hozzá a Notepad++ futtatható fájlját a telemetriai kizárásokhoz.

Adja meg a beállításokat az alábbiak szerint:

- **Teljes elérési út**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Használja a következő eseménytípusokhoz**: Fájlmódosítás.

2. példa Hálózati események

Ha a WinSCP alkalmazást fájlkezeléshez használja egy távoli kiszolgálón, és ki szeretné zárni a hálózati eseményeket, adja hozzá a WinSCP futtatható fájlját a telemetriai kizárásokhoz.

Adja meg a beállításokat az alábbiak szerint:

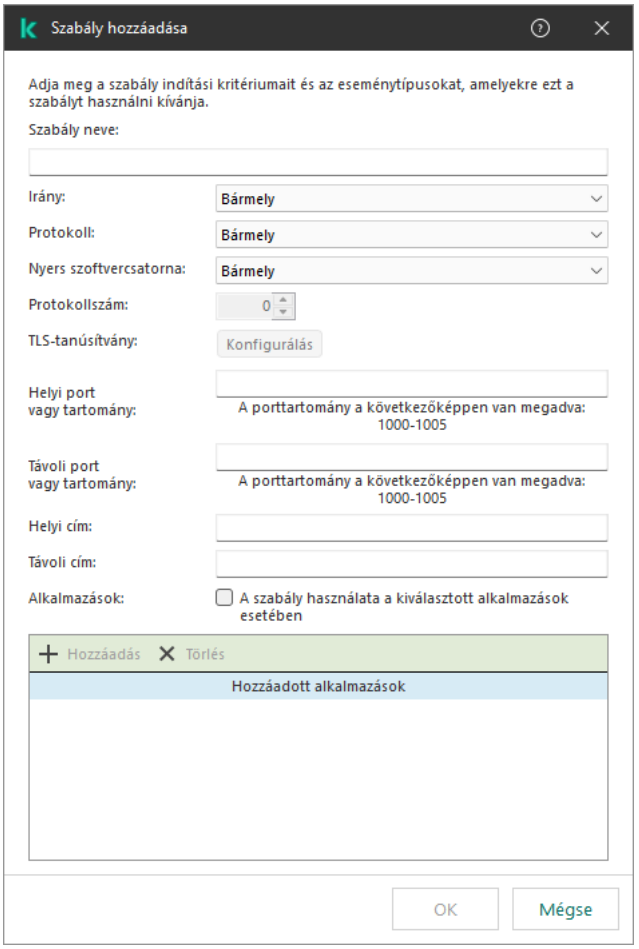
- **Teljes elérési út**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (opcionális).
- **Használja a következő eseménytípusokhoz**: Hálózati események.

2. példa Kizárt hálózati kommunikáció

A távoli szolgáltatás kapcsolódási eseményeinek telemetriából való kizárásához nyissa meg az EDR-telemetria kizárásai ablakot a **Kizárt hálózati kommunikáció** lapon, és adja meg a csatlakozási beállításokat: protokoll, port, irány, IP-cím, TLS-tanúsítvány és egyebek.

A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja.

> Nem adhat meg alhálózati címet (például 10.28.0.0/24). Az alkalmazás csak egy IP-cím megadását teszi lehetővé (például 10.28.0.105).



Hálózati kommunikáció kizárása

Ha vállalati webkiszolgálót használ, és a böngésző eseményeit szeretné kizárni, amikor ehhez a webkiszolgálóhoz csatlakozik, adja hozzá a kiszolgáló IP-címét és a böngésző futtatható fájlját a telemetriai kizárásokhoz.

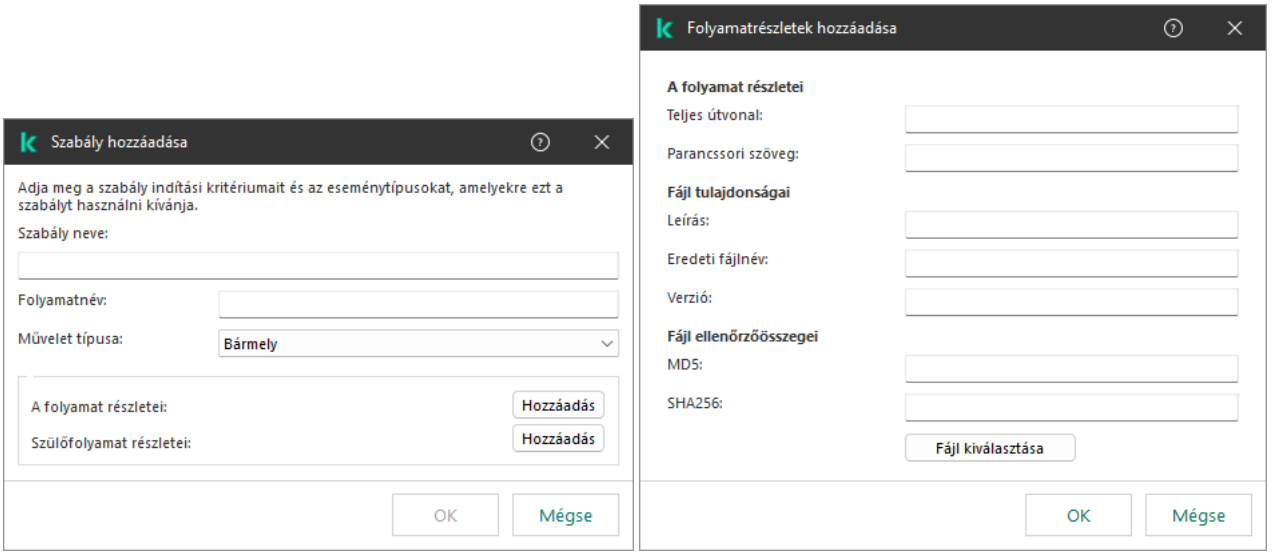
Adja meg a beállításokat az alábbiak szerint:

- **Protokoll**: TCP.
- **Távoli port vagy tartomány**: 443.
- **Távoli cím**: 10.28.0.105.
- **Alkalmazások**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

3. példa Kizárt fájlműveletek

A megbízható fájlokkal végzett műveleteket tartalmazó események telemetriából való kizárásához nyissa meg az EDR-telemetria kizárásai ablakot a **Kizárt fájlműveletek** lapon, és adja hozzá a megbízható fájlt.

A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja.



Fájlműveletek kizárása

Ha egy alkalmazás naplóba ír, és ki szeretné zárni a naplófájl módosítási eseményeit, adja hozzá a naplófájlt és az alkalmazás futtatható fájlját a telemetriából.

Adja meg a beállításokat az alábbiak szerint:

- **Fájlnév vagy maszk**: `C:\Apache24\logs\error.log`.
- **Művelet típusa**: Fájlmódosítás.
- **Teljes elérési út**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

4. példa Kizárt beállításjegyzék-módosítások

A beállításjegyzék-módosítási események telemetriából való kizárásához nyissa meg az EDR-telemetria kizárásai ablakot a **Kizárt beállításjegyzék-módosítások** lapon, és adjon hozzá egy beállításkulcsot.

A Kaspersky Endpoint Security a szabálykiváltó feltételeket a logikai AND jelekkel kombinálja.

Ha egy alkalmazás gyakran módosítja a beállításjegyzék értékeit, és szeretné kizárni ezeket a beállításjegyzék-módosítási eseményeket a telemetriából, adja hozzá a beállításkulcsot és az alkalmazás futtatható fájlját a telemetriai kizárásokhoz.

Adja meg a beállításokat az alábbiak szerint:

- **A művelet típusa**: Módosítás.
- **Elérési út**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Teljes elérési út**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

A Kaspersky Anti Targeted Attack Platform tartalmazza a Sandbox (KATA Sandbox) összetevőt. A *Sandbox* egy olyan technológia, amely lehetővé teszi a speciális fenyegetések észlelését egy számítógépen. A Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (a Sandbox-kiszolgálók). A megoldás részleteivel kapcsolatos információért lásd a Kaspersky Anti Targeted Attack Platform útmutatót.

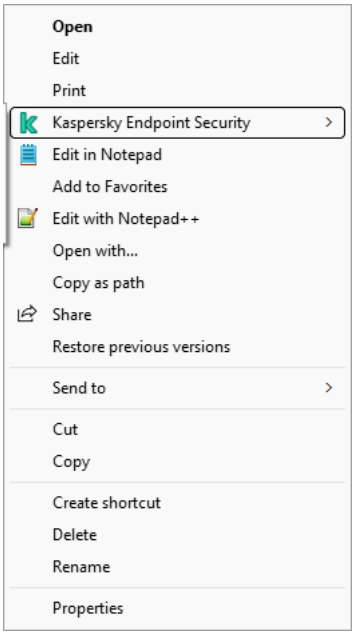
A KATA Sandbox aktiválásához olyan licenckulcsra van szükség, amely tartalmazza a KATA vagy KEDR funkciókat. A rendelkezésre álló funkciók részleteiről lásd a Kaspersky Anti Targeted Attack Platform útmutatót.

A KATA Sandbox a fájlok vizsgálatát a következő módokban teszi lehetővé:

- *Manually*. A felhasználó manuálisan küldi be a fájlt vizsgálatra a helyi menüből (**Küldés a Sandboxba**). Amikor egy fájlt elküld a Sandboxba, az alkalmazás a vírusadatbázisok segítségével is megvizsgálja a fájlt.
- *Automatikus*. Az alkalmazás automatikusan észleli az objektumokat, és vizsgálat céljából elküldi azokat a Sandboxba.

A fájl Sandboxba való küldése után az továbbra is elérhető a felhasználó számára. A Kaspersky Endpoint Security naplózza a megfelelő eseményt, és elküldi a Kaspersky Security Centernek és a Kaspersky Anti Targeted Attack Platform konzolnak. Ha a Sandbox rosszindulatú tevékenységet észlel, a Kaspersky Endpoint Security végrehajt egy fenyegetésre adott válaszműveletet automatikusan (például törli az objektumot, és elindítja a kritikus területek vizsgálatát).

A KATA Sandbox kézi üzemmódú működéséhez a Kaspersky Anti Targeted Attack Platform 7.0 vagy újabb verzióját kell telepíteni. A KATA Sandbox automatikus üzemmódú működéséhez a Kaspersky Anti Targeted Attack Platform 8.0 vagy újabb verzióját kell telepíteni.



Vizsgálat a KATA Sandboxban a helyi menüből

A beépített ügynök integrációja a KATA Sandbox megoldással

A Sandbox összetevővel való integrációhoz a KATA Sandbox összetevő hozzáadása szükséges. A Sandbox összetevőt telepítés vagy frissítés közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

A fájlok vizsgálatra való elküldéséhez engedélyeznie kell a KATA Sandbox integrációt, és hozzá kell adnia a megoldáson belül telepített Central Node-kiszolgálót. Az összetevőt csak a Kaspersky Security Center Web Console használatával lehet felügyelni. Ezt az összetevőt nem felügyelheti az Adminisztrációs Konzol (MMC) használatával.

A KATA Sandbox-szal való integráció engedélyezése vagy letiltása:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Sandbox** elemet.
5. A **Integration with Sandbox ENABLED** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

6. Válassza ki a KATA Sandbox működési módját:

   - **Manually**. A felhasználó manuálisan küldi be a fájlt vizsgálatra a helyi menüből (**Küldés a Sandboxba**).
   - **Automatically**. Az alkalmazás automatikusan észleli az objektumokat, és vizsgálat céljából elküldi azokat a Sandboxba.
   - **Combined**.

7. Kattintson a **Connection settings** hivatkozásra.

8. Central Node-kiszolgáló kapcsolódási beállításainak konfigurálása:

   - **Timeout (msec)**. Csatlakozás időtúllépése a Central Node-kiszolgálónál. A beállított időtúllépés letelte után a Kaspersky Endpoint Security kérést küld a következő kiszolgálónak. Növelheti a kiszolgáló kapcsolódási időtúllépését, ha a kapcsolat sebessége alacsony, vagy ha a kapcsolat instabil. A kérések ajánlott időtúllépése 0.5 másodperc vagy kevesebb.
   - **Request queue**. A kérési várólista mappájának mérete. Ha több objektumot küld vizsgálatra a Sandboxban, a Kaspersky Endpoint Security egy kérés-várólistát hoz létre. Alapértelmezés szerint a kérési várólista mappamérete 100 MB-ra van korlátozva. A maximális méret elérése után a Sandbox leállítja az új kérések hozzáadását a várólistához, és elküldi a megfelelő eseményt a Kaspersky Security Centernek. A kiszolgáló konfigurációjától függően konfigurálhatja a kérési várólista mappaméretét.
   - **Server TLS certificate**. Ha megbízható kapcsolatot szeretne konfigurálni a Central Node-kiszolgálóival, elő kell készítenie egy TLS-tanúsítványt. Ezután hozzá kell adnia a tanúsítványt a számítógéphez egy házirend segítségével. A tanúsítványt a Central Node-kiszolgálóhoz is hozzá kell adnia.
   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

9. A **Connection to Sandbox servers** részen kattintson a **Add** gombra.

10. Ezzel megnyílik egy ablak; itt adja meg a Central Node-kiszolgáló címét (IPv4, IPv6, DNS) és portját.

    A virtuális képek telepítésével és a Central Node-kiszolgálók konfigurálásával kapcsolatos részletekért lásd a Kaspersky Anti Targeted Attack Platform súgót.

11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Ennek eredményeként a Sandbox összetevő engedélyezve van. Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. A **Sandbox** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

A fenyegetésre adott válasz műveleteinek konfigurálása

Ha a Sandbox rosszindulatú tevékenységet észlel, a Kaspersky Endpoint Security végrehajt egy fenyegetésre adott válaszműveletet automatikusan (például törli az objektumot, és elindítja a kritikus területek vizsgálatát).

A fenyegetésre adott válasz műveleteinek konfigurálása:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Sandbox** elemet.
5. Válassza ki a vonatkozó műveletet a **Action on threat detection** területen:

   - **Move copy to Quarantine, delete object**. Ha ezt az opciót választja, a Kaspersky Endpoint Security törli a számítógépen talált rosszindulatú objektumot. Az objektum törlése előtt a Kaspersky Endpoint Security biztonsági másolatot készít arra az esetre, ha az objektumot később vissza kell állítani. A Kaspersky Endpoint Security a biztonsági másolatot karanténba helyezi.
   - **Run Critical Areas Scan**. Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a *Critical Areas Scan* feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.
   - **Create IOC Scan task**. Ha ezt az opciót választja, a Kaspersky Endpoint Security automatikusan létrehozza az *IOC Scan (autonóm IOC vizsgálati feladat)* elemet. Ehhez a feladathoz konfigurálhatja a futásmódot, a vizsgálat hatókörét és az IOC észlelési műveletet (*Move copy to Quarantine, delete object* vagy *Run Critical Areas Scan*). Az *IOC Scan* feladat beállításainak módosításához nyissa meg a feladat beállításait.
6. Ha szükséges, az *IOC vizsgálat* feladat beállításait az **IOC Scan scope** területen konfigurálhatja.

   - **Critical file areas**. Ha ezt az opciót választja, a Kaspersky Endpoint Security csak a számítógép kritikus fájlterületein végez IOC vizsgálatot: rendszermag memóriája és rendszerindítási szektorok.
   - **File areas on system drive of the computer**. Ha ez az opció van kiválasztva, a Kaspersky Endpoint Security IOC vizsgálatot végez a számítógép rendszermeghajtóján.
7. Ha szükséges, az *IOC vizsgálat* feladat beállításait az **Run IOC Scan task** területen konfigurálhatja.

   - **Manually**. A futásmód, amelyben manuálisan elindíthatja az *IOC Scan* feladatot, amikor az Önnek kényelmes.
   - **Automatically**. Olyan futtatási mód, amelyben a Kaspersky Endpoint Security egy fenyegetés észlelését követően automatikusan elindítja az *IOC Scan* szolgáltatást.
   - **Run only when the computer is idle**. A futásmód, amelyben a Kaspersky Endpoint Security futtatja az *IOC vizsgálat* feladatot, ha a képernyővédő aktív, vagy a képernyő zárolva van. Ha a felhasználó feloldja a számítógép zárolását, a Kaspersky Endpoint Security felfüggeszti a feladatot. Ez azt jelenti, hogy a feladat végrehajtása több napot is igénybe vehet.
8. Speciális feladatbeállítások konfigurálása *IOC vizsgálathoz*.
9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

KEA-KES migrációs útmutató az EDR számára (KATA)

A 12.1-es verzióval kezdődően a Kaspersky Endpoint Security for Windows már tartalmaz egy beépített ügynököt a Kaspersky Endpoint Detection and Response összetevő kezelésére a Kaspersky Anti Targeted Attack Platform megoldás részeként. Az EDR-rel (KATA) való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra. A Kaspersky Endpoint Agent minden funkcióját a Kaspersky Endpoint Security végzi. A Kaspersky Anti Targeted Attack Platform kiszolgálók terhelése változatlan marad.

Amikor olyan számítógépeken telepíti a Kaspersky Endpoint Security alkalmazást, amelyekre telepítve van a Kaspersky Endpoint Agent, a Kaspersky Anti Targeted Attack Platform (EDR) megoldás továbbra is együttműködik a Kaspersky Endpoint Security termékkel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről. A Kaspersky Endpoint Security 12.1 vagy újabb verzióra történő frissítésekor a rendszer ugyanígy viselkedik.

A Kaspersky Endpoint Security nem kompatibilis a Kaspersky Endpoint Agent szolgáltatással. Ezeket az alkalmazásokat nem telepítheti ugyanarra a számítógépre.

A következő feltételeknek kell teljesülniük ahhoz, hogy a Kaspersky Endpoint Security az Endpoint Detection and Response (KATA) részeként működjön:

- Kaspersky Anti Targeted Attack Platform 5.0 vagy újabb verzió.
- Kaspersky Security Center 14.2 vagy újabb verzió (beleértve a Network Agentet is). A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az Endpoint Detection and Response (KATA) szolgáltatást.

A [KES+KEA] konfiguráció [KES+beépített ügynök] EDR-be (KATA) történő migrálásának lépései

1. **A Kaspersky Endpoint Security felügyeleti bővítményének frissítése**

   Az EDR (KATA) összetevő a Kaspersky Endpoint Security felügyeleti bővítmény 12.1 vagy újabb verziójával felügyelhető. A Kaspersky Security Center konzol típusától függően frissítse a felügyeleti bővítményt az adminisztrációs konzolon (MMC) vagy a webes bővítményt a Web Console-on.

2. **Házirendek és a feladatok áttelepítése**

   A Kaspersky Endpoint Agent beállításainak átvitele a Kaspersky Endpoint Security for Windows megoldásba. A következők közül választhat:

   - Varázsló a Kaspersky Endpoint Agent termékről a Kaspersky Endpoint Security termékre történő áttelepítéshez. A Kaspersky Endpoint Agent termékről a Kaspersky Endpoint Security termékre történő áttelepítést segítő varázsló csak a Web Console-ban működik

     A szabályzat- és feladatbeállítások áttelepítése a Kaspersky Endpoint Agent szolgáltatásból a Kaspersky Endpoint Security szolgáltatásba a Web Console-on

     A Web Console fő ablakában válassza a **Operations → Migration from Kaspersky Endpoint Agent** lehetőséget.

     Ezzel futtatja a szabályzat- és feladatáttelepítési varázslót. Kövesse a varázsló utasításait.

1. lépés. Szabályzat áttelepítése

Az áttelepítési varázsló új szabályzatot hoz létre, amely egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent szabályzatainak beállításait. A listában válassza ki azokat a Kaspersky Endpoint Agent szabályzatokat, amelyek beállításait egyesíteni szeretné a Kaspersky Endpoint Security szabályzatával. Kattintson a Kaspersky Endpoint Agent szabályzatára, és válassza ki azt a Kaspersky Endpoint Security szabályzatot, amellyel egyesíteni szeretné a beállításokat. Győződjön meg arról, hogy a megfelelő szabályzatokat választotta, és folytassa a következő lépéssel.

2. lépés. Feladatok áttelepítése

Az áttelepítési varázsló nem támogatja az EDR (KATA) feladatokat. Átugorhatja ezt a lépést.

3. lépés. A varázsló befejezése

Lépjen ki a varázslóból. A varázsló eredményeként egy új Kaspersky Endpoint Security házirend jön létre. A szabályzat egyesíti a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent beállításait. A szabályzat neve *<Kaspersky Endpoint Security policy name> és <Kaspersky Endpoint Agent policy name>*. Az új házirend *Inactive* állapotot kap. A folytatáshoz módosítsa a Kaspersky Endpoint Agent és a Kaspersky Endpoint Security szabályzatok állapotát *Inactive* értékre, és aktiválja az új egyesített szabályzatot.

A Web Console áttelepítési varázslója kihagyja a következő házirend-beállításokat, és nem telepíti át őket:

- Beállítások módosításának tiltása **Connection settings** („zárolás”).

  Alapértelmezés szerint a beállítások módosíthatók (a „lakat” nyitva van). Ezért a beállítások nem kerülnek alkalmazásra a számítógépen. Meg kell tiltania a beállítások módosítását, és be kell zárnia a „lakatot”.

- Kriptotároló.

  Ha kétirányú hitelesítést használ a Central Node kiszolgálóihoz való csatlakozáshoz, akkor újra fel kell vennie a kriptotárolót.

Mivel az áttelepítés varázsló nem telepíti át ezeket a beállításokat, előfordulhat, hogy a számítógép Central Node-kiszolgálókhoz való csatlakoztatásakor hibák lépnek fel. A hibák kijavításához meg kell nyitnia a házirend-tulajdonságokat, és konfigurálnia kell a kapcsolat beállításait.

- A standard Házirend és feladatok kötegelt konvertálási varázslója. A Házirendek és feladatok kötegelt konvertálási varázslója csak az Adminisztrációs konzolon (MMC) érhető el. A Házirendek és feladatok kötegelt konvertálási varázslójával kapcsolatos további részletekért olvassa el a következőt: Kaspersky Security Center Súgó.

Annak érdekében, hogy a Kaspersky Endpoint Security megfelelően működjön a kiszolgálókon, ajánlatott a kiszolgáló működése szempontjából fontos fájlokat hozzáadni a megbízható zónához. SQL-kiszolgálók esetén MDF- és LDF-adatbázisfájlokat kell hozzáadnia. A Microsoft Exchange kiszolgálókhoz CHK-, EDB-, JRS-, LOG- és JSL-fájlokat kell hozzáadnia. Használhat maszkokat, pl. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon.

Az EDR telemetriai kizárásai nem kerülnek át a Kaspersky Endpoint Agent házirendből a Kaspersky Endpoint Security házirendbe. A Kaspersky Endpoint Security saját kizárási eszközökkel rendelkezik – megbízható alkalmazások. A Kaspersky Endpoint Security működése úgy van optimalizálva, hogy az egyedi EDR telemetriai kizárások hiánya ne okozzon további terhelést a számítógépen a Kaspersky Endpoint Agenthez képest. A Kaspersky Endpoint Security a telemetriát nemcsak az EDR (KATA), hanem az alkalmazásvédelmi összetevők működéséhez is használja. Ezért nincs szükség egyedi EDR telemetriai kizárások átvitelére. Ha a számítógép teljesítményének csökkenését tapasztalja, ellenőrizze az alkalmazás működését (lásd az 7. lépést: A teljesítmény ellenőrzése).

3 Az EDR (KATA) funkció licencelése

A Kaspersky Endpoint Security aktiválásához a Kaspersky Anti Targeted Attack Platform megoldás részeként külön licenc szükséges a Kaspersky Endpoint Detection and Response (KATA) kiegészítőhöz. A kulcsot a *Add key* feladat segítségével veheti fel. Ennek eredményeképpen a rendszer két kulcsot ad hozzá az alkalmazáshoz: *Kaspersky Endpoint Security* és *Kaspersky Endpoint Detection and Response (KATA)*.

A Kaspersky Endpoint Detection and Response (KATA) bővítmény licencelése korábban aktivált EDR Optimum vagy EDR Expert funkciókkal rendelkező számítógépeken a következő speciális szempontokat foglalja magában:

- Ha *kulcsfájlt* használ a Kaspersky Endpoint Security EDR Optimum vagy EDR Expert funkciókat tartalmazó licenceléshez, akkor nem adhat hozzá önálló kulcsot a Kaspersky Endpoint Detection and Response (KATA) bővítményhez. A licenceléshez áttérhet az aktiváló kód használatára, vagy kapcsolatba léphet a szolgáltatójával, hogy új kulcsfájlt kapjon a Kaspersky Endpoint Security és az EDR funkciók aktiválásához. A szolgáltató egy vagy több kulcsfájlt biztosít a licenceléshez.

- Ha *kulcsfájlt* használ a Kaspersky Endpoint Security EDR Optimum vagy EDR Expert funkciókat nem tartalmazó licenceléshez, akkor hozzáadhat egy önálló kulcsot a Kaspersky Endpoint Detection and Response (KATA) bővítményhez a kulcsfájlok újbóli kiadása nélkül.

- Ha *aktiváló kódot* használ a licenceléshez, a Kaspersky aktiválási kiszolgálója automatikusan újból kiadja a kulcsokat, és az EDR (KATA) funkciók automatikusan elérhetővé válnak. Ebben az esetben az EDR Optimum és az EDR Expert letiltásra kerül.

- A Kaspersky Endpoint Security legfeljebb két aktív kulcs hozzáadását teszi lehetővé: Kaspersky Endpoint Security-kulcs és kiegészítő típusú kulcs. Legfeljebb két tartalék kulcsot is hozzáadhat. Egy Kaspersky Endpoint Security-tartalékkulcsot és egy kiegészítő típusú tartalékkulcsot.

4 A Kaspersky Endpoint Security alkalmazás telepítése/frissítése

Az alkalmazás telepítése vagy frissítése során az EDR (KATA) funkciók áttelepítéséhez ajánlott a távoli telepítési feladat használata. Távoli telepítési feladat létrehozásakor a telepítőcsomag beállításaiban ki kell választania az EDR (KATA) összetevőt.

Az alkalmazást a következő módszerekkel is frissítheti:

- A Kaspersky frissítési szolgáltatás használatával.
- Helyben, a Telepítővarázsló segítségével.

A Kaspersky Endpoint Security támogatja az összetevők automatikus kiválasztását az alkalmazásfrissítés során az olyan számítógép esetében, amelyre a Kaspersky Endpoint Agent alkalmazás telepítve van. Az összetevők automatikus kiválasztása az alkalmazás frissítését végző felhasználói fiók engedélyeitől függ.

Ha a Kaspersky Endpoint Security frissítése a rendszerfiók (SYSTEM) alatt található EXE- vagy MSI-fájl használatával történik, a Kaspersky Endpoint Security hozzáférést kap a Kaspersky-megoldások aktuális licenceihez. Ezért ha a számítógépen telepítve van a Kaspersky Endpoint Agent és aktiválva van az EDR (KATA) megoldás, a Kaspersky Endpoint Security telepítője automatikusan konfigurálja az összetevők készletét, és kiválasztja az EDR (KATA) összetevőt. Ezáltal a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt. Az MSI-telepítő rendszerfiók (SYSTEM) alatti futtatása általában a Kaspersky frissítési szolgáltatása keretében történő frissítéskor vagy egy telepítőcsomag Kaspersky Security Centerrel végzett telepítésekor zajlik.

Ha a Kaspersky Endpoint Security frissítése emelt szintű jogosultsággal nem rendelkező felhasználói fiók alatt található MSI-fájl használatával történik, a Kaspersky Endpoint Security nem kap hozzáférést a Kaspersky-megoldások aktuális licenceihez. Ebben az esetben a Kaspersky Endpoint Security automatikusan kiválasztja az összetevőket a Kaspersky Endpoint Agent összetevőinek készlete alapján. Ezután a Kaspersky Endpoint Security a beépített ügynök használatára vált, és eltávolítja a Kaspersky Endpoint Agent ügynököt.

A Kaspersky Endpoint Security támogatja a frissítést a számítógép újraindítása nélkül. Az alkalmazásfrissítési módot a házirend tulajdonságaiban választhatja ki.

5 Az alkalmazás működésének ellenőrzése

Ha az alkalmazás telepítése vagy frissítése után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

- Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
- Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal. Ha egy összetevőnél *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy aktiválta a beépített ügynök funkciót.
- Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.

6 A Kaspersky Anti Targeted Attack Platform kiszolgálóval való kapcsolat ellenőrzése

A Kaspersky Anti Targeted Attack Platform kiszolgálóval való kapcsolat ellenőrzése. Ehhez:

1. Ellenőrizze, hogy rendelkezik-e érvényes tanúsítvánnyal.
2. Ellenőrizze a kiszolgálói kapcsolat beállításait.
3. Ellenőrizze az eseménynaplót.

   Ha létrejön a kapcsolat a kiszolgálóval, az alkalmazás elküldi a *Successful connection to the EDR Expert server* eseményt. Ha nincs sikeres kapcsolódási esemény, és nincsenek hibás kapcsolódási események, ellenőrizze az eseménynapló beállításait, és engedélyezze az eseményküldést az Endpoint Detection and Response (KATA) számára.

A kiszolgálókapcsolat állapota nem befolyásolja a számítógép állapotát a Kaspersky Security Center konzolon. Ezért, ha nincs kapcsolat a kiszolgálóval, a számítógép továbbra is rendelkezhet az *OK* állapottal. Nézze meg az eseménynaplót a kiszolgálóval való kapcsolat ellenőrzéséhez.

7 A teljesítmény ellenőrzése

Ha a számítógép teljesítménye lelassult egy alkalmazás telepítése vagy frissítése után, optimalizálhatja az adatátvitelt. Ehhez:

1. Tiltsa le az EDR (KATA) összetevőt és ellenőrizze, hogy a teljesítményromlás az EDR (KATA) miatt következett-e be.
2. Megbízható alkalmazások esetén kapcsolja ki a telemetriai adatok gyűjtését a konzol bemeneti műveleteinél (alapértelmezés szerint engedélyezve van).
3. A számítógép teljesítményét csökkentő alkalmazásokat felveheti a megbízható alkalmazások listájára.
4. Vegye fel a kapcsolatot a Kaspersky Terméktámogatással. A támogatási szakértők segítenek a telemetriai szűrés konfigurálásában a Kaspersky Anti Targeted Attack Platformon. Ez csökkenti az adatforgalom mennyiségét. Ha a számítógép teljesítményét egy bizonyos alkalmazás befolyásolja, csatolja a kéréshez az adott alkalmazás terjesztőcsomagját.

Endpoint Detection and Response Expert (on-premises)



A Kaspersky Endpoint Security for Windows támogatja az integrációt a Kaspersky Endpoint Detection and Response Expert (on-premises) megoldással. *Kaspersky Endpoint Detection and Response Expert (on-premises)* egy vállalati kiberbiztonsági megoldás, amely olyan Kaspersky-alkalmazásokat tartalmaz, amelyek segítségével a vállalatok a legtöbb típusú kiberkockázattal szemben védekezhetnek, és a legfontosabb fenyegetés-terjesztési forgatókönyveket lefedhetik. Az EDR Expert (on-premises) összetevők az Open Single Management Platformon (OSMP) vannak telepítve. Ez a platform egyetlen felületen futtat platformokon átívelő forgatókönyveket, és lehetővé teszi a Kaspersky-alkalmazások és a harmadik féltől származó alkalmazások egy átfogó biztonsági rendszerbe való integrálását.

A megoldás egyik központi eleme a *SIEM*. A SIEM nyomon követi az összes összetevőből érkező eseményeket, és a gyártó és a felhasználó által meghatározott szabályok segítségével korrelálja ezeket az eseményeket egymással. Az EDR Expert (on-premises) a vállalati infrastruktúrából kapott naplókat és telemetriát vizsgálja a támadások automatikus észlelése érdekében, és lehetővé teszi az incidensek egységes vizsgálati grafikon segítségével való kivizsgálását, amely az összes, az EDR Expert (on-premises) alkalmazásban gyűjtött eseményt egyesíti, beleértve a Kaspersky alkalmazásokból és harmadik fél információbiztonsági termékeiből származó eseményeket is.

Az összetett incidensekre való reagáláshoz az EDR Expert (on-premises) előre beállított és felhasználó által meghatározott forgatókönyveket használ. Harmadik féltől származó alkalmazásokból származó válaszakciókat és több alkalmazást is érintő válaszforgatókönyveket is használhat.

Fenyegetés-felderítési eszközök

A Kaspersky Endpoint Detection and Response a következő Threat Intelligence eszközöket használja:

- Integráció a Kaspersky Threat Intelligence Portállal, amely információkat tartalmaz és jelenít meg fájlok és webcímek megbízhatóságáról.
- Kaspersky Threats adatbázis.
- Kaspersky Security Network (a továbbiakban: KSN) felhőszolgáltatási infrastruktúra, amely hozzáférést biztosít a Kaspersky tudásbázisából származó valós idejű fájl-, webhely- és szoftver-megbízhatósági információkhoz. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban képes reagálni a fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken.

A megoldás működési elve

A Kaspersky Endpoint Security a vállalati IT-infrastruktúra egyes számítógépeire van telepítve, és folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítás alatt álló fájlokat.

Amikor normál módban telepítve van a VDI infrastruktúrában, a Kaspersky Endpoint Security támogatja az EDR Expert (on-premises) integrációját. Az alkalmazás többi funkciójának működőképessége azonban nem garantált. A VDI infrastruktúrában lévő virtuális gépek védelme érdekében a Kaspersky Endpoint Security Light Agent módban történő használatát javasoljuk.

A számítógépen zajló eseményekkel kapcsolatos információkat (telemetria) a rendszerl elküldi az EDR Expert (on-premises) kiszolgálónak. Ebben az esetben a Kaspersky Endpoint Security információkat küld a telemetriagyűjtő kiszolgálóknak az alkalmazás által észlelt fenyegetésekről, valamint az ilyen fenyegetések feldolgozási eredményeiről is.

Az EDR Expert (on-premises) integráció a Kaspersky Security Center konzolon van konfigurálva. A beépített ügynök ezután az Open Single Management Platform (OSMP) segítségével kezelhető, beleértve a feladatok futtatását, a karanténba helyezett objektumok kezelését, a jelentések megtekintését és az egyéb műveleteket.

Kaspersky Endpoint Security-konfigurációk az EDR Expert (on-premises) használatához

A következő konfigurációk használhatók az EDR Expert (on-premises) megoldással való munkavégzéshez:

- **[KES+beépített ügynök]**. Ebben a konfigurációban a Kaspersky Endpoint Security a számítógép biztonságát garantáló alkalmazásként és az EDR Expert (on-premises) megoldással való munkavégzéshez is használható alkalmazásként működik. Az EDR Expert (on-premises) beépített ügynöke a Kaspersky Endpoint Security 12.11 for Windows vagy újabb verzióban érhető el.

- **[külső EPP+EDR Agent]**. Ebben a konfigurációban az IT-infrastruktúra biztonságát a harmadik féltől származó Endpoint Protection Platform (EPP) garantálja. Az EDR Expert (on-premises) megoldással való interakciót a Kaspersky Endpoint Security biztosítja az Endpoint Detection and Response Agent (EDR Agent) konfigurációban. Ebben a konfigurációban az EDR Agent kompatibilis a harmadik féltől származó EPP-alkalmazásokkal. Az EDR Expert (on-premises) beépített ADR Agent ügynöke a Kaspersky Endpoint Security 12.11 for Windows vagy újabb verzióban érhető el.

A beépített ügynök integrálása az EDR Expert (on-premises) megoldással

A Kaspersky Endpoint Detection and Response Expert (on-premises) megoldással való integrációhoz hozzá kell adni az Endpoint Detection and Response Expert (on-premises) összetevőt, és konfigurálni kell a Kaspersky Endpoint Security alkalmazást.

Az Endpoint Detection and Response Optimum, az Endpoint Detection and Response Expert (cloud) és az Endpoint Detection and Response Expert (on-premises) összetevők nem kompatibilisek egymással.

A következő feltételeknek kell teljesülniük ahhoz, hogy az Endpoint Detection and Response Expert (on-premises) működjön:

- Az OSMP (Open Single Management Platform) telepítve van.
- Az alkalmazás aktiválva van, és a funkciójára a licenc kiterjed.
- Az Endpoint Detection and Response Expert (on-premises) összetevő be van kapcsolva.
- Az EDR Expert (on-premises) működését biztosító alkalmazásösszetevők engedélyezve vannak és működőképesek. A EDR Expert (on-premises) működését a következő összetevők biztosítják:
  - Fájl védelem.
  - Web védelem.
  - Levelezés védelem.
  - Biztonsági rések kihasználásának megelőzése.
  - Viselkedésészlelés.
  - Behatolásmegelőző rendszer.

- Kármentesítő motor.
- Adaptív Anomáliafelügyelő.

A EDR Expert (on-premises) integráció beállítása a következő lépésekből áll:

1. **Az EDR Expert (on-premises) összetevő telepítése**

   A EDR Expert (on-premises) összetevőt telepítés vagy frissítés közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

   > Újra kell indítania a számítógépét az alkalmazás új összetevővel történő frissítésének befejezéséhez.

2. **A Kaspersky Endpoint Detection and Response Expert (on-premises) aktiválása**

   Külön licenc vásárlására van szükség az EDR Expert (on-premises) számára (Kaspersky Endpoint Detection and Response Expert (on-premise) bővítmény).

   A szolgáltatás a Kaspersky Endpoint Detection and Response Expert (on-premises) külön kulcsának hozzáadását követően válik elérhetővé. Ennek eredményeképpen két kulcs kerül hozzáadásra a számítógépen: egy kulcs a Kaspersky Endpoint Security és egy másik az Endpoint Detection and Response Expert (on-premises) számára.

   Az önálló Endpoint Detection and Response Expert (on-premises) funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

   Győződjön meg arról, hogy az EDR Expert (on-premises) funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén fut.

3. **Csatlakozás a telemetriagyűjtő kiszolgálóhoz és a válaszkiszolgálóhoz**

   A Kaspersky Endpoint Detection and Response Expert (on-premises) megoldásnak megbízható kapcsolatra van szüksége a Kaspersky Endpoint Security és két kiszolgáló között:

   - A *telemetriagyűjtő kiszolgáló* egy olyan SIEM-megoldás részét képező kiszolgáló, amely a számítógépen bekövetkező eseményekre vonatkozó információkat gyűjti, normalizálja, korrelálja, elemzi és tárolja.
   - A *válaszkiszolgáló* egy olyan kiszolgáló, amely adatokat fogad és vizsgál, tanulmányozza az objektumok viselkedését, és közzéteszi az ilyen tanulmányok eredményeit.

   A megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell használnia. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). Ezután hozzá kell adnia a TLS-tanúsítványt a Kaspersky Endpoint Security szolgáltatáshoz (lásd az alábbi utasításokat).

   Alapértelmezés szerint a Kaspersky Endpoint Security csak a kiszolgálók TLS-tanúsítványát ellenőrzi. A kapcsolat biztonságosabbá tétele céljából ezenkívül engedélyezheti a számítógép ellenőrzését a kiszolgálón (kétirányú hitelesítés). Az ellenőrzés engedélyezéséhez be kell kapcsolnia a kétirányú hitelesítést a kiszolgálón és a Kaspersky Endpoint Security beállításaiban. A kétirányú hitelesítés használatához kriptotárolóra is szüksége lesz. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja).

   A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Expert (on-premises) megoldáshoz a Web Console segítségével

   1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
   2. Kattintson a Kaspersky Endpoint Security házirend nevére.

      Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)** elemet.

5. Kapcsolja be az **Endpoint Detection and Response Expert (on-premises) ENABLED** kapcsolót.

6. Az EDR Expert (on-premises) beállításához válassza ki az **Endpoint Detection and Response Expert (version 8.0 or later)**lehetőséget a megoldások listájából.

7. Konfigurálja a *telemetriagyűjtő kiszolgálók* csatlakozását:

   a. A **Connection to telemetry collection servers** részen kattintson a **Connection settings** hivatkozásra.

   b. A telemetriagyűjtő kiszolgálók csatlakozásának konfigurálása:

   - **Timeout (sec)**. A kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik kiszolgálóhoz.

   - **Server certificate**. TLS-tanúsítvány a kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja).

   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). A kiszolgáló beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

   c. Kattintson az **OK** gombra.

   d. Telemetria-gyűjtőkiszolgálók hozzáadása. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

      Több telemetriagyűjtő kiszolgáló címét is hozzáadhatja. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

   e. Ha szükséges, konfigurálja a telemetriát.

8. A *válaszkiszolgálók* kapcsolatának konfigurálása:

   a. Az **Connection to response servers** területen konfigurálhatja a **Send sync request to server every (min)** beállítást. A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security fogadja a fenyegetésre adott válasz feladatait, és elküldi a feladatok eredményeit.

   b. Kattintson a **Connection settings** hivatkozásra.

c. A válaszkiszolgálók kapcsolatának konfigurálása:

- **Timeout (sec)**. A kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik kiszolgálóhoz.
- **Server certificate**. TLS-tanúsítvány a kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja).
- **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). A kiszolgáló beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

  A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

d. Kattintson az **OK** gombra.

e. Adja hozzá a válaszkiszolgálókat. Ehhez adja meg a kiszolgáló címét (IPv4, IPv6) és a kiszolgálóhoz csatlakozó portot.

Több válaszkiszolgáló-címet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

9. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Ennek eredményeként a számítógép hozzáadódik a felügyelt eszközök listájához az Open Single Management Platformon (OSMP). Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Endpoint Detection and Response Expert (on-premises)** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

Az EDR Expert (on-premises) telemetriabeállításainak konfigurálása

A *Telemetria* a védett számítógépen történt események listája. A Kaspersky Endpoint Security elemzi a telemetriai adatokat, és elküldi azokat Kaspersky Anti Targeted Attack Platform számára a szinkronizálás során. A telemetriai események szinte folyamatosan érkeznek a kiszolgálóra. A Kaspersky Endpoint Security akkor kezdeményezi a szinkronizálást a kiszolgálóval, ha az alábbi feltételek bármelyike teljesül:

- A szinkronizálási intervallum lejárt.
- A pufferben lévő események száma meghaladja a felső határt.

Ezért alapértelmezés szerint az alkalmazás 30 másodpercenként szinkronizál, vagy amikor a puffer 1024 eseményt tartalmaz. A szinkronizálási viselkedést a Kaspersky Endpoint Security házirendjében konfigurálhatja, és kiválaszthatja a hálózati terhelésnek megfelelő optimális értékeket (lásd az alábbi utasításokat).

Ha nincs kapcsolat a Kaspersky Endpoint Security és a kiszolgáló között, az alkalmazás sorba állítja az új eseményeket. Amikor a kapcsolat helyreáll, a Kaspersky Endpoint Security megfelelő sorrendben küldi el a sorban álló eseményeket a kiszolgálónak. A kiszolgáló túlterhelésének elkerülése érdekében a Kaspersky Endpoint Security kihagyhat néhány eseményt. Ennek engedélyezéséhez optimalizálhatja az eseményátviteli beállításokat, például beállíthatja az események óránkénti maximális értékét (lásd az alábbi utasításokat).

A telemetriai beállítások konfigurálásához tegye a következőket:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)** elemet.
5. Az EDR Expert (on-premises) beállításához válassza ki az **Endpoint Detection and Response Expert (version 8.0 or later)**lehetőséget a megoldások listájából.
6. Győződjön meg róla, hogy a **Send telemetry to telemetry collection servers** négyzet be van jelölve az **Data transmission settings** területen.
7. Ha szükséges, tegyen jelölést a **Send telemetry with IOA only** jelölőnégyzetbe. A *támadásjelző (IOA)* szabály a rendszeren belüli olyan gyanús viselkedések leírását tartalmazza, amelyek célzott támadásra utalhatnak. Az alkalmazás összehasonlítja a rendszerben zajló viselkedést ezekkel a szabályokkal, és naplózza a célzott támadásra utaló eseményeket. Az alkalmazás *streameléses vizsgálati* technológiát használ, amely lehetővé teszi az ilyen események valós idejű nyomon követését.
8. Ha szükséges, konfigurálja a szinkronizálást a kiszolgáló beállításaival az **Data transmission settings** részen:

   - **Maximum event transmission delay (sec)**. Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc.
   - **Maximum number of event packages**. Az alkalmazás akkor szinkronizál a kiszolgálóval, amikor a puffer megtelik eseményekkel. Az alapértelmezett beállítás 1024 esemény.
9. Ha szükséges, törölje az **Enable request throttling** jelölőnégyzet bejelölését a **Request throttling** részen.

   Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését. Ez az opció alapértelmezés szerint be van kapcsolva.
10. Konfigurálja az optimalizálási beállításokat az események kiszolgálóra küldéséhez:

    - **Maximum number of events per hour**. Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni.
    - **Percentage of event limit excess**. Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.

11. A **Connection to response servers** területen adjon meg egy értéket a **Send sync request to server every (min)** paraméterhez.

12. A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security információkat küld a módosított alkalmazásbeállításokról és feladatokról.

13. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az EDR Expert (on-premises) telemetriai kizárásai

A teljesítmény javítása és a telemetriagyűjtő kiszolgálóra történő adatátvitel optimalizálása érdekében telemetria-kivételeket adhat hozzá. Dönthet például úgy, hogy az egyes alkalmazásokhoz nem küld hálózati kommunikációs adatokat.

Túl sok szabály használata növelheti a telemetriagyűjtő kiszolgáló terhelését és csökkentheti a számítógép teljesítményét. Javasoljuk, hogy csak a szükséges szabályokat adja hozzá.

Telemetria kizárás létrehozása a Web Console-ban és a Cloud Console-ban:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.

5. Válassza ki az **EDR Expert (on-premises) telemetry** lapot.

6. A **General exclusions** részen kattintson a **Add** gombra.

   Megnyílik a **Add exclusion rule** ablak.

7. Szükség esetén módosítsa a szabály állapotát. Alapértelmezés szerint a szabály engedélyezve van.

8. Adja meg a szabály nevét.

9. Válassza ki a szabály aktiválásakor végrehajtandó műveletet:

   - **Do not collect**. A szűrt esemény kizárásra kerül az elküldött telemetriai adatokból.

   - **Exclude IOA**. Az IOA-szabályt kiváltó esemény kizárásra kerül az elküldött telemetriai adatokból.

10. Ha a **Exclude IOA** opció van kiválasztva, adja meg a kizárásokhoz hozzáadni kívánt IOA-szabályokat:

    - **Exclude all**. Amikor a megadott feltétel teljesül, az alkalmazás kizárja a telemetriai adatokból az összes IOA-szabály alapján generált eseményt.

    - **Exclude by GUID**. Adja meg az IOA-szabály GUID azonosítóját. Több GUID-t is megadhat a(z) `,` használatával. Az IOA-szabályokkal kapcsolatos további részletekért kérjük, tekintse meg az EDR Expert (on-premises) súgóját.

11. Adja meg a szűrési feltételt:

    a. Válassza ki a szűréshez használandó mezőnevet.

    b. Válasszon ki egy operátort (lásd az alábbi táblázatot), és adja meg azt az értéket, amellyel az eseményből származó mező értékét össze kell hasonlítani.

Feltételes operátorok listája

Operátor	Leírás
<	Ha a mező értéke kisebb, mint a feltételben megadott érték, a rendszer kiszűri az eseményt.
≤	Ha a mező értéke kisebb vagy egyenlő a feltételben megadott értékkel, a rendszer kiszűri az eseményt.
=	Ha a mező értéke megegyezik a feltételben megadott értékkel, a rendszer kiszűri az eseményt.
≥	Ha a mező értéke nagyobb vagy egyenlő, mint a feltételben megadott érték, a rendszer kiszűri az eseményt.
>	Ha a mező értéke nagyobb, mint a feltételben megadott érték, a rendszer kiszűri az eseményt.
≠	Ha a mező értéke nem egyenlő a feltételben megadott értékkel, a rendszer kiszűri az eseményt.
is like	Ha a mező értéke megegyezik a feltételben megadott maszkkal, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a(z) `*` és `?` karaktereket:
is not like	Ha a mező értéke nem egyezik meg a feltételben megadott maszkkal, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a(z) `*` és `?` karaktereket:
one of	Ha a mező értéke megegyezik a feltételben megadott lista valamelyik értékével, a rendszer szűrtnek tekinti az eseményt.
none of	Ha a mező értéke nem egyezik meg a feltételben megadott lista egyik értékével sem, a rendszer szűrtnek tekinti az eseményt.
is like one of	Ha a mező értéke megegyezik a feltételben megadott maszkok egyikével, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a * és a ? karaktereket.
is not like one of	Ha a mező értéke nem egyezik a feltételben megadott maszkok egyikével sem, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a * és a ? karaktereket.
exists	Ha a feltételben megadott mező jelen van az eseményben, a rendszer kiszűri az eseményt.
not exists	Ha a feltételben megadott mező nincs jelen az eseményben, a rendszer kiszűri az eseményt.
contains	Ha a feltételben megadott érték szerepel a mező értékében, a rendszer kiszűri az eseményt.
is equal to	Ha a mező értéke megegyezik a feltételben megadott értékkel, a rendszer kiszűri az eseményt. A vizsgálat megkülönbözteti a kis- és nagybetűket.
bitwise AND	Ha a mezőérték és a feltételben megadott érték közötti bitenkénti ÉS (&) művelet eredménye 1, akkor a rendszer kiszűri az eseményt.

12. Szükség esetén összetett szűrőfeltételeket hozhat létre több szűrőfeltétel és feltételcsoport hozzáadásával. Beágyazott feltételeket és feltételcsoportokat is hozzáadhat egy feltételcsoporthoz. A következő operátorokat használhatja:

    - A(z) **AND** azt jelenti, hogy a szűrő azokat az eseményeket választja ki, amelyek megfelelnek az összes megadott feltételnek.
    - A(z) **OR** azt jelenti, hogy a szűrő azokat az eseményeket választja ki, amelyek megfelelnek a megadott feltételek valamelyikének.
    - A(z) **NOT** (az operátor használatához válassza a **Add NOT before** opciót) azt jelenti, hogy a szűrő azokat az eseményeket választja ki, amelyek nem felelnek meg a megadott feltételek egyikének sem.

    A feltételeket és az első szintű feltételcsoportokat a(z) **AND** operátorral kombináljuk.

13. Ha a számítógépén az Open Single Management Platform (OSMP) fut, akkor beolvashatja a létrehozott szűrési szabályt. A vizsgálat futtatásához kattintson a(z) **Check rule** gombra.

    A megnyíló ablakban megjelenik a létrehozott szabály által szűrt események táblázata. További részletekért kérjük, tekintse meg az EDR Expert (on-premises) súgóját.

14. Ha szükséges, az **All event types**, területen adhat hozzá telemetriai kizárásokat eseménytípus szerint.

    a. Kattintson az eseménytípus nevére.

    b. Az ablakban kattintson a **Set up manually** gombra.

    c. Szükség esetén konfigurálja a telemetriai adatok átvitelét a kiválasztott eseménytípushoz a(z) **Send event** kapcsolóval. Alapértelmezés szerint a telemetriai adatok átvitele minden eseménytípusnál engedélyezve van.

    d. A **Exclusion rules** részen kattintson a **Add** gombra.

    Megnyílik a **Add exclusion rule** ablak.

    e. Végezze el a 7–13. lépésekben leírt műveleteket minden hozzáadott szabályhoz.

15. Bizonyos eseménytípusokhoz belefoglalási szabályokat is hozzáadhat az összegyűjtött telemetriai adatok körének bővítéséhez:

    a. A **Inclusion rules** részen kattintson a **Add** gombra.

    Megnyílik a **Add inclusion rules** ablak.

    b. Adja meg a szabály nevét.

    c. A(z) **Condition** alatt adja meg a megjelenített mezők értékeit. Az elérhető mezők típusa a kiválasztott eseménytől függ.

    A kizárási szabályok elsőbbséget élveznek a belefoglalási szabályokkal szemben.

16. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az EDR Expert (on-premises) eseményszűrőinek exportálása és importálása

A kizárások listáját exportálhatja egy JSON-fájlba. Ezután módosíthatja a fájlt, például nagy számú eseményazonosító hozzáadásával. Használhatja az exportálás/importálás funkciót az eseményszűrők biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

Túl sok szabály használata növelheti a telemetriagyűjtő kiszolgáló terhelését és csökkentheti a számítógép teljesítményét. Javasoljuk, hogy csak a szükséges szabályokat adja hozzá.

Eseményszűrők exportálása és importálása az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.

5. A **Telemetriai beállítások → Telemetria EDR Expert számára (on-premises)** területen kattintson a **Beállítások** gombra.

6. Az eseményszűrők exportálása:

   a. Kattintson az **Export** gombra.

   A megnyíló ablakban adja meg a JSON-fájl nevét, amelybe exportálni szeretné az eseményszűrőket, és válassza ki a fájl mentésére kiszemelt mappát.

   b. Mentse a fájlt.

   A Kaspersky Endpoint Security exportálja az eseményszűrőket a JSON-fájlba.

7. Az eseményszűrők importálása:

   a. Kattintson az **Import** gombra.

   b. A megnyíló ablakban válassza ki azt a JSON-fájlt, amelyből importálni szeretné az eseményszűrőket.

   c. Nyissa meg a fájlt.

   Ha már léteznek eseményszűrési szabályok a számítógépen, a Kaspersky Endpoint Security lecseréli ezeket az importálás során.

8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Eseményszűrők exportálása és importálása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings → Telemetry Settings** elemet.

5. Válassza ki az **EDR Expert (on-premises) telemetry** lapot.

6. Az eseményszűrők exportálása:

   a. Kattintson az **Export** gombra.

   b. A megnyíló ablakban adja meg a JSON-fájl nevét, amelybe exportálni szeretné az eseményszűrőket, és válassza ki a fájl mentésére kiszemelt mappát.

   c. Mentse a fájlt.

   A Kaspersky Endpoint Security exportálja az eseményszűrőket a JSON-fájlba.

7. Az eseményszűrők importálása:

   a. Kattintson az **Import** gombra.

   b. A megnyíló ablakban válassza ki azt a JSON-fájlt, amelyből importálni szeretné az eseményszűrőket.

c. Válassza ki, hogyan szeretné az eseményszűrési szabályokat importálni: a meglévő szabályok hozzáadásával vagy a meglévő szabályok elvetésével és azok újakkal való helyettesítésével.

d. Nyissa meg a fájlt.

8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Eseményszűrőket is exportálhat vagy importálhat a parancssorból.

Különleges szempontok a rendszabályprofilok használatakor az EDR Expert (on-premises) és az EDR (KATA) integrációjának konfigurálásához

Ahhoz, hogy egyetlen házirend keretében bizonyos rendszergazdai csoportok számára az EDR (KATA) integrációját, mások számára pedig az EDR Expert (on-premises) integrációját állítsa be, rendszabályprofilokat kell használnia. Az EDR (KATA) integrációs beállításait a szabályzat tulajdonságaiban kell konfigurálnia, míg a kiválasztott rendszergazdai csoportokra vonatkozó EDR Expert (on-premises) integrációt a szabályzatprofil tulajdonságaiban kell beállítania.

A rendszabályprofilok használatával az EDR Expert (on-premises) rendszerrel való integráció beállításakor a következő korlátozások érvényesek:

- Ha a házirend tulajdonságaiban beállítja az EDR Expert (on-premises) integrációját, ezek a beállítások minden rendszergazdai csoportra vonatkoznak; a rendszabályprofilok integrációs beállításai nem kerülnek alkalmazásra.

- Ha rendszabályprofilokat használ az EDR Expert (on-premises) integrációjának konfigurálásához, akkor a rendszabályok kezeléséhez nem használhatja az Administration Console-t (MMC). Amikor az Administration Console-ban megnyitja a szabályzat tulajdonságait, a rendszabályprofilokban található EDR Expert (on-premises) integrációs beállításait felülírják a szabályzat beállításai, ami az összetevő hibás működéséhez vezet. Az alábbi utasításoknak megfelelően vissza kell állítania az Endpoint Detection and Response Expert (on-premises) összetevő beállításait.

- Ha rendszabályprofilokat használ az EDR Expert (on-premises) integrációjának konfigurálásához, akkor a rendszabályok kezeléséhez nem használhatja az alházirendeket.

Ha már beállított egy szabályzatot a webes beépülő modul egy korábbi verziójában, akkor vissza kell állítania az Endpoint Detection and Response Expert (on-premises) összetevő beállításait ahhoz, hogy az EDR Expert (on-premise) integrációs beállításait a rendszabályprofilokból a felügyelt eszközökre alkalmazhassa.

Az összetevő beállításainak visszaállítása:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)** elemet.

5. Állítsa át az üzemmódot az **Endpoint Detection and Response Expert (version 7.1 or earlier)** módról **Endpoint Detection and Response Expert (8.0 vagy újabb verzió) módra**.

6. Váltson vissza az **Endpoint Detection and Response Expert (version 7.1 or earlier)** módra.

7. Mentse el a módosításokat.

Endpoint Detection and Response Expert (cloud)

A Kaspersky Endpoint Security for Windows integrációja a Kaspersky Endpoint Detection and Response Expert (cloud) szolgáltatással átmenetileg nem érhető el. A funkció a tervek szerint 2026 végére lesz támogatva. Figyelje a kiadási megjegyzéseket, hogy értesüljön az alkalmazás frissítéseiről és új funkcióiról.



A Kaspersky Endpoint Security for Windows támogatja az integrációt a Kaspersky Endpoint Detection and Response Expert (cloud) megoldással. *A Kaspersky Endpoint Detection and Response Expert (cloud)* egy felhőalapú vállalati kiberbiztonsági megoldás, amely olyan Kaspersky alkalmazásokat tartalmaz, amelyek lehetővé teszik a szervezetek számára, hogy a legtöbb típusú kiberkockázattal szemben védekezzenek, és lefedik a legfontosabb fenyegetésterjedési forgatókönyveket. Az EDR Expert (cloud) összetevők az Open Single Management Platformon (OSMP) vannak telepítve. Ez a platform egyetlen felületen futtat platformokon átívelő forgatókönyveket, és lehetővé teszi a Kaspersky-alkalmazások és a harmadik féltől származó alkalmazások egy átfogó biztonsági rendszerbe való integrálását.

> A Kaspersky Endpoint Detection and Response Expert (cloud) alkalmazás integrációja az ARM alapú számítógépeken nem támogatott.

A megoldás egyik központi eleme a *SIEM*. A SIEM nyomon követi az összes összetevőből érkező eseményeket, és a gyártó és a felhasználó által meghatározott szabályok segítségével korrelálja ezeket az eseményeket egymással. Az EDR Expert (cloud) a vállalati infrastruktúrából kapott naplókat és telemetriát vizsgálja a támadások automatikus észlelése érdekében, és lehetővé teszi az incidensek egységes vizsgálati grafikon segítségével való kivizsgálását, amely az összes, az EDR Expert (cloud) alkalmazásban gyűjtött eseményt egyesíti, beleértve a Kaspersky alkalmazásokból és harmadik fél információbiztonsági termékeiből származó eseményeket is.

Az összetett incidensekre való reagáláshoz az EDR Expert (cloud) előre beállított és felhasználó által meghatározott forgatókönyveket használ. Harmadik féltől származó alkalmazásokból származó válaszakciókat és több alkalmazást is érintő válaszforgatókönyveket is használhat.

Fenyegetés-felderítési eszközök

A Kaspersky Endpoint Detection and Response a következő Threat Intelligence eszközöket használja:

- Integráció a Kaspersky Threat Intelligence Portállal, amely információkat tartalmaz és jelenít meg fájlok és webcímek megbízhatóságáról.
- Kaspersky Threats adatbázis.
- Kaspersky Security Network (a továbbiakban: KSN) felhőszolgáltatási infrastruktúra, amely hozzáférést biztosít a Kaspersky tudásbázisából származó valós idejű fájl-, webhely- és szoftver-megbízhatósági információkhoz. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban képes reagálni a fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken.

A megoldás működési elve

A Kaspersky Endpoint Security a vállalati IT-infrastruktúra egyes számítógépeire van telepítve, és folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítás alatt álló fájlokat.

A számítógépen zajló eseményekkel kapcsolatos információkat (telemetria) a rendszerl elküldi az EDR Expert (cloud) kiszolgálónak. Ebben az esetben a Kaspersky Endpoint Security információkat küld a telemetriagyűjtő kiszolgálóknak az alkalmazás által észlelt fenyegetésekről, valamint az ilyen fenyegetések feldolgozási eredményeiről is.

Az EDR Expert (cloud) integráció a Kaspersky Security Center konzolon van konfigurálva. A beépített ügynök ezután az Open Single Management Platform (OSMP) segítségével kezelhető, beleértve a feladatok futtatását, a karanténba helyezett objektumok kezelését, a jelentések megtekintését és az egyéb műveleteket.

A beépített ügynök integrálása az EDR Expert (cloud) megoldással

A Kaspersky Endpoint Detection and Response (cloud) megoldással való integráció beállításához telepítenie kell az Endpoint Detection and Response Expert (cloud) összetevőt, és konfigurálnia kell a Kaspersky Endpoint Security alkalmazást.

Az Endpoint Detection and Response Optimum, az Endpoint Detection and Response Expert (cloud) és az Endpoint Detection and Response Expert (on-premises) összetevők nem kompatibilisek egymással.

Az EDR Expert (cloud) működési feltételei

Az EDR Expert (cloud) működéséhez a következő feltételeknek kell teljesülniük:

- A Kaspersky Endpoint Detection and Response Expert (cloud) infrastruktúra elérhető az Ön régiójában. Az EDR Expert (cloud) infrastruktúra elérhetőségével kapcsolatos információkért az Ön régiójában, kérjük, lépjen kapcsolatba a Terméktámogatással.
- Az OSMP (Open Single Management Platform) telepítve van.
- A Kaspersky Endpoint Security normál módban lett telepítve.
- A Kaspersky Endpoint Security alkalmazás aktiválva van, és a funkciókra a licenc vonatkozik.
- Ön elfogadta a Kaspersky Endpoint Detection and Response Expert (cloud) adatfeldolgozási megállapodásának feltételeit.
- Az Endpoint Detection and Response Expert (cloud) összetevő engedélyezve van.
- Az EDR Expert (cloud) működését biztosító alkalmazásösszetevők engedélyezve vannak és működőképesek:
  - Fájl védelem.
  - Web védelem.
  - Levelezés védelem.
  - Biztonsági rések kihasználásának megelőzése.
  - Viselkedésészlelés.

- Behatolásmegelőző rendszer.
- Kármentesítő motor.
- Adaptív Anomáliafelügyelő.

Az EDR Expert (cloud) integrálásának lépései

Az EDR Expert (cloud) integráció beállítása a következő lépésekből áll:

1. **Az Endpoint Detection and Response Expert (cloud) összetevő telepítése**

   Kiválaszthatja az Endpoint Detection and Response Expert (cloud) összetevőt telepítés vagy frissítés közben, valamint a *Change application components* feladat használatával.

   > Újra kell indítania a számítógépét az alkalmazás új összetevővel történő frissítésének befejezéséhez.

2. **A Kaspersky Endpoint Detection and Response Expert (cloud) aktiválása**

   Külön licenc vásárlására van szükség az MDR számára (Kaspersky Endpoint Detection and Response Expert (cloud) bővítmény).

   A szolgáltatás a Kaspersky Endpoint Detection and Response Expert (cloud) külön kulcsának hozzáadását követően válik elérhetővé. Ennek eredményeképpen két kulcs kerül hozzáadásra a számítógépen: egy kulcs a Kaspersky Endpoint Security és egy másik az Endpoint Detection and Response Expert (cloud) számára.

   Az önálló Endpoint Detection and Response Expert (cloud) funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

   Győződjön meg arról, hogy az EDR Expert (cloud) funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén fut.

3. **Csatlakozás a telemetriagyűjtő kiszolgálóhoz és a válaszkiszolgálóhoz**

   A Kaspersky Endpoint Detection and Response Expert (cloud) megoldásnak megbízható kapcsolatra van szüksége a Kaspersky Endpoint Security és két kiszolgáló között:

   - A *telemetriagyűjtő kiszolgáló* egy olyan SIEM-megoldás részét képező kiszolgáló, amely a számítógépen bekövetkező eseményekre vonatkozó információkat gyűjti, normalizálja, korrelálja, elemzi és tárolja.
   - A *válaszkiszolgáló* egy olyan kiszolgáló, amely adatokat fogad és vizsgál, tanulmányozza az objektumok viselkedését, és közzéteszi az ilyen tanulmányok eredményeit.

   A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a Expert (cloud) megoldáshoz a Web Console segítségével

   1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
   2. Kattintson a Kaspersky Endpoint Security házirend nevére.

      Megnyílik a rendszabályok tulajdonságai ablak.
   3. Válassza ki az **Application settings** lapot.
   4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)** elemet.

5. Engedélyezze az összetevőt a(z) **Endpoint Detection and Response Expert (cloud) DISABLED** kapcsolóval.

6. Ha az aktuális szabályzat egy gyermekszabályzat, és a szülőszabályzat tiltja az EDR Expert (cloud) integrációs beállításainak módosítását (zárt „lakat"), akkor a beállítások öröklődését a(z) **Inheritance** részben konfigurálhatja:

   - **Inherit connection settings from the policy** (alapértelmezett érték). A kapcsolatbeállítások a szülőszabályzatból öröklődnek. A beállításokat nem fogja tudni szerkeszteni.

   - **Use custom connection settings**. A kapcsolat beállításait manuálisan is konfigurálhatja.

7. A(z) **Response server** lapon a válaszkiszolgáló automatikusan lekért teljes tartományneve (FQDN) és portszáma jelenik meg. Ha az infrastruktúrájában lévő biztonsági szabályzat nem teszi lehetővé a közvetlen csatlakozást az EDR Expert (cloud) kiszolgálókhoz, akkor TCP alagúton keresztül is beállíthat kapcsolatot:

   a. Tegyen jelölést a **Use a TCP tunnel for response** jelölőnégyzetbe.

   b. Adja meg a kiszolgáló címét (IPv4, IPv6) és a portot, amelyen keresztül az alagúthoz csatlakozni kell.

8. Szükség esetén a(z) **Send sync request to server every (min)** mezőben állítsa be a kiszolgálónak küldött szinkronizációs kérések gyakoriságát. A szinkronizálás során a Kaspersky Endpoint Security fogadja a fenyegetésre adott válasz feladatait, és elküldi a feladatok eredményeit.

9. Nyissa meg a **Telemetry collection server** lapot.

10. Állítsa be a telemetriai adatgyűjtő kiszolgáló kapcsolati beállításait:

    a. Kattintson a **Edit** hivatkozásra.

    b. A megnyíló ablakban válassza ki a listából a telemetriai adatkiszolgálót. A KUMA gyűjtő telemetriagyűjtő kiszolgálóként szolgál az EDR Expert (cloud) szolgáltatásban. További részletekért kérjük, tekintse meg a Kaspersky Unified Monitoring and Analysis Platform súgóját.

    Ha a telemetriai adatgyűjtő kiszolgálóhoz való csatlakozás során hiba lép fel, válasszon egy másik kiszolgálót. Ha nem tud csatlakozni a telemetriagyűjtő kiszolgálóhoz, kérjük, lépjen kapcsolatba a Terméktámogatással.

    c. Szükség esetén TCP-alagúton keresztül is beállíthat egy kapcsolatot a telemetriai adatgyűjtő kiszolgálóhoz, ugyanúgy, mint a válaszkiszolgáló esetében.

11. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Ennek eredményeként a számítógép hozzáadódik a felügyelt eszközök listájához az Open Single Management Platformon (OSMP). Ellenőrizheti az összetevő működési állapotát az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. Az **Endpoint Detection and Response Expert (cloud)** összetevő hozzáadódik a Kaspersky Endpoint Security összetevők listájához.

Az EDR Expert (cloud) telemetriabeállításainak konfigurálása

A *Telemetria* a védett számítógépen történt események listája. A Kaspersky Endpoint Security elemzi a telemetriai adatokat, és elküldi azokat Kaspersky Anti Targeted Attack Platform számára a szinkronizálás során. A telemetriai események szinte folyamatosan érkeznek a kiszolgálóra. A Kaspersky Endpoint Security akkor kezdeményezi a szinkronizálást a kiszolgálóval, ha az alábbi feltételek bármelyike teljesül:

- A szinkronizálási intervallum lejárt.
- A pufferben lévő események száma meghaladja a felső határt.

Ezért alapértelmezés szerint az alkalmazás 30 másodpercenként szinkronizál, vagy amikor a puffer 1024 eseményt tartalmaz. A szinkronizálási viselkedést a Kaspersky Endpoint Security házirendjében konfigurálhatja, és kiválaszthatja a hálózati terhelésnek megfelelő optimális értékeket (lásd az alábbi utasításokat).

Ha nincs kapcsolat a Kaspersky Endpoint Security és a kiszolgáló között, az alkalmazás sorba állítja az új eseményeket. Amikor a kapcsolat helyreáll, a Kaspersky Endpoint Security megfelelő sorrendben küldi el a sorban álló eseményeket a kiszolgálónak. A kiszolgáló túlterhelésének elkerülése érdekében a Kaspersky Endpoint Security kihagyhat néhány eseményt. Ennek engedélyezéséhez optimalizálhatja az eseményátviteli beállításokat, például beállíthatja az események óránkénti maximális értékét (lásd az alábbi utasításokat).

A telemetriai beállítások konfigurálásához tegye a következőket:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)** elemet.
5. A megnyíló ablakban válassza ki a(z) **Data transmission settings** lapot.
6. Győződjön meg arról, hogy a **Sending telemetry ENABLED** négyzet be van jelölve.
7. Ha szükséges, tegyen jelölést a **Send telemetry with IOA only** jelölőnégyzetbe. A *támadásjelző (IOA)* szabály a rendszeren belüli olyan gyanús viselkedések leírását tartalmazza, amelyek célzott támadásra utalhatnak. Az alkalmazás összehasonlítja a rendszerben zajló viselkedést ezekkel a szabályokkal, és naplózza a célzott támadásra utaló eseményeket. Az alkalmazás *streameléses vizsgálati* technológiát használ, amely lehetővé teszi az ilyen események valós idejű nyomon követését.
8. Szükség esetén konfigurálja a kiszolgáló szinkronizálási beállításait:

   - **Maximum event transmission delay (sec)**. Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc.
   - **Maximum number of event packages**. Az alkalmazás akkor szinkronizál a kiszolgálóval, amikor a puffer megtelik eseményekkel. Az alapértelmezett beállítás 1024 esemény.
9. Nyissa meg a **Request throttling** lapot.

10. Szükség esetén tiltsa le a kérések szabályozását a **Request throttling ENABLED** kapcsoló használatával.

    Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését. Ez az opció alapértelmezés szerint be van kapcsolva.

11. Konfigurálja az optimalizálási beállításokat az események kiszolgálóra küldéséhez:

    - **Maximum number of events per hour**. Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni.

    - **Percentage of event limit excess (%)**. Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.

12. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az EDR Expert (cloud) telemetriai kizárásai

A teljesítmény javítása és a telemetriagyűjtő kiszolgálóra történő adatátvitel optimalizálása érdekében telemetria-kivételeket adhat hozzá. Dönthet például úgy, hogy az egyes alkalmazásokhoz nem küld hálózati kommunikációs adatokat.

Túl sok szabály használata növelheti a telemetriagyűjtő kiszolgáló terhelését és csökkentheti a számítógép teljesítményét. Javasoljuk, hogy csak a szükséges szabályokat adja hozzá.

Telemetria kizárás létrehozása a Web Console-ban és a Cloud Console-ban:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.
5. Válassza ki az **EDR Expert (cloud) telemetry** lapot.
6. A **General exclusions** részen kattintson a **Add** gombra.

   Megnyílik a **Add exclusion rule** ablak.
7. Szükség esetén módosítsa a szabály állapotát. Alapértelmezés szerint a szabály engedélyezve van.
8. Adja meg a szabály nevét.

9. Válassza ki a szabály aktiválásakor végrehajtandó műveletet:

   - **Do not collect**. A szűrt esemény kizárásra kerül az elküldött telemetriai adatokból.
   - **Exclude IOA**. Az IOA-szabályt kiváltó esemény kizárásra kerül az elküldött telemetriai adatokból.

10. Ha a **Exclude IOA** opció van kiválasztva, adja meg a kizárásokhoz hozzáadni kívánt IOA-szabályokat:

    - **Exclude all**. Amikor a megadott feltétel teljesül, az alkalmazás kizárja a telemetriai adatokból az összes IOA-szabály alapján generált eseményt.
    - **Exclude by GUID**. Adja meg az IOA-szabály GUID azonosítóját. Több GUID-t is megadhat a(z) `,` használatával. Az IOA-szabályokkal kapcsolatos további részletekért lásd az EDR szakértői (cloud) súgóját.

11. Adja meg a szűrési feltételt:

    a. Válassza ki a szűréshez használandó mezőnevet.

    b. Válasszon ki egy operátort (lásd az alábbi táblázatot), és adja meg azt az értéket, amellyel az eseményből származó mező értékét össze kell hasonlítani.

Feltételes operátorok listája

Operátor	Leírás
<	Ha a mező értéke kisebb, mint a feltételben megadott érték, a rendszer kiszűri az eseményt.
≤	Ha a mező értéke kisebb vagy egyenlő a feltételben megadott értékkel, a rendszer kiszűri az eseményt.
=	Ha a mező értéke megegyezik a feltételben megadott értékkel, a rendszer kiszűri az eseményt.
≥	Ha a mező értéke nagyobb vagy egyenlő, mint a feltételben megadott érték, a rendszer kiszűri az eseményt.
>	Ha a mező értéke nagyobb, mint a feltételben megadott érték, a rendszer kiszűri az eseményt.
≠	Ha a mező értéke nem egyenlő a feltételben megadott értékkel, a rendszer kiszűri az eseményt.
is like	Ha a mező értéke megegyezik a feltételben megadott maszkkal, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a(z) `*` és `?` karaktereket:
is not like	Ha a mező értéke nem egyezik meg a feltételben megadott maszkkal, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a(z) `*` és `?` karaktereket:
one of	Ha a mező értéke megegyezik a feltételben megadott lista valamelyik értékével, a rendszer szűrtnek tekinti az eseményt.
none of	Ha a mező értéke nem egyezik meg a feltételben megadott lista egyik értékével sem, a rendszer szűrtnek tekinti az eseményt.
is like one of	Ha a mező értéke megegyezik a feltételben megadott maszkok egyikével, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a * és a ? karaktereket.
is not like one of	Ha a mező értéke nem egyezik a feltételben megadott maszkok egyikével sem, a rendszer kiszűri az eseményt. Az alkalmazás a maszk megadásakor támogatja a * és a ? karaktereket.
exists	Ha a feltételben megadott mező jelen van az eseményben, a rendszer kiszűri az eseményt.
not exists	Ha a feltételben megadott mező nincs jelen az eseményben, a rendszer kiszűri az eseményt.
contains	Ha a feltételben megadott érték szerepel a mező értékében, a rendszer kiszűri az eseményt.
is equal to	Ha a mező értéke megegyezik a feltételben megadott értékkel, a rendszer kiszűri az eseményt. A vizsgálat megkülönbözteti a kis- és nagybetűket.
bitwise AND	Ha a mezőérték és a feltételben megadott érték közötti bitenkénti ÉS (&) művelet eredménye 1, akkor a rendszer kiszűri az eseményt.

12. Szükség esetén összetett szűrőfeltételeket hozhat létre több szűrőfeltétel és feltételcsoport hozzáadásával. Beágyazott feltételeket és feltételcsoportokat is hozzáadhat egy feltételcsoporthoz. A következő operátorokat használhatja:

    - A(z) **AND** azt jelenti, hogy a szűrő azokat az eseményeket választja ki, amelyek megfelelnek az összes megadott feltételnek.
    - A(z) **OR** azt jelenti, hogy a szűrő azokat az eseményeket választja ki, amelyek megfelelnek a megadott feltételek valamelyikének.
    - A(z) **NOT** (az operátor használatához válassza a **Add NOT before** opciót) azt jelenti, hogy a szűrő azokat az eseményeket választja ki, amelyek nem felelnek meg a megadott feltételek egyikének sem.

    A feltételeket és az első szintű feltételcsoportokat a(z) **AND** operátorral kombináljuk.

13. A létrehozott szűrőszabály beolvasásához kattintson a(z) **Check rule** gombra.

    A megnyíló ablakban megjelenik a létrehozott szabály által szűrt események táblázata. További részletekért kérjük, tekintse meg az EDR Expert (cloud) súgóját.

14. Ha szükséges, az **All event types**, területen adhat hozzá telemetriai kizárásokat eseménytípus szerint.

    a. Kattintson az eseménytípus nevére.

    b. Az ablakban kattintson a **Set up manually** gombra.

    c. Szükség esetén konfigurálja a telemetriai adatok átvitelét a kiválasztott eseménytípushoz a(z) **Send event** kapcsolóval. Alapértelmezés szerint a telemetriai adatok átvitele minden eseménytípusnál engedélyezve van.

    d. A **Exclusion rules** részen kattintson a **Add** gombra.

    Megnyílik a **Add exclusion rule** ablak.

    e. Végezze el a 7–13. lépésekben leírt műveleteket minden hozzáadott szabályhoz.

15. Bizonyos eseménytípusokhoz belefoglalási szabályokat is hozzáadhat az összegyűjtött telemetriai adatok körének bővítéséhez:

    a. A **Inclusion rules** részen kattintson a **Add** gombra.

    Megnyílik a **Add inclusion rules** ablak.

    b. Adja meg a szabály nevét.

    c. A(z) **Condition** alatt adja meg a megjelenített mezők értékeit. Az elérhető mezők típusa a kiválasztott eseménytől függ.

    A kizárási szabályok elsőbbséget élveznek a belefoglalási szabályokkal szemben.

16. Ahhoz, hogy a szabályzatot alkalmazni lehessen a számítógépekre, győződjön meg arról, hogy a lakatok zárva vannak (🔒), majd mentse a módosításokat.

Az EDR Expert (cloud) eseményszűrőinek exportálása és importálása

A kizárások listáját exportálhatja egy JSON-fájlba. Ezután módosíthatja a fájlt, például nagy számú eseményazonosító hozzáadásával. Használhatja az exportálás/importálás funkciót az eseményszűrők biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

Túl sok szabály használata növelheti a telemetriagyűjtő kiszolgáló terhelését és csökkentheti a számítógép teljesítményét. Javasoljuk, hogy csak a szükséges szabályokat adja hozzá.

Eseményszűrők exportálása vagy importálása a Web Console-ban:

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.
5. Válassza ki az **EDR Expert (cloud) telemetry** lapot.
6. Az eseményszűrők exportálása:
   a. Kattintson az **Export** gombra.
   b. A megnyíló ablakban adja meg a JSON-fájl nevét, amelybe exportálni szeretné az eseményszűrőket, és válassza ki a fájl mentésére kiszemelt mappát.
   c. Mentse a fájlt.

      A Kaspersky Endpoint Security exportálja az eseményszűrőket a JSON-fájlba.
7. Az eseményszűrők importálása:
   a. Kattintson az **Import** gombra.
   b. A megnyíló ablakban válassza ki azt a JSON-fájlt, amelyből importálni szeretné az eseményszűrőket.
   c. Válassza ki, hogyan szeretné az eseményszűrési szabályokat importálni: a meglévő szabályok hozzáadásával vagy a meglévő szabályok elvetésével és azok újakkal való helyettesítésével.
   d. Nyissa meg a fájlt.

8. Ahhoz, hogy a szabályzatot alkalmazni lehessen a számítógépekre, győződjön meg arról, hogy a lakatok zárva vannak (), majd mentse a módosításokat.

    1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
    2. Kattintson a Kaspersky Endpoint Security házirend nevére.

       Megnyílik a rendszabályok tulajdonságai ablak.
    3. Válassza ki az **Application settings** lapot.
    4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.
    5. Válassza ki az **EDR Expert (cloud) telemetry** lapot.
    6. Az eseményszűrők exportálása:

        a. Kattintson az **Export** gombra.

        b. A megnyíló ablakban adja meg a JSON-fájl nevét, amelybe exportálni szeretné az eseményszűrőket, és válassza ki a fájl mentésére kiszemelt mappát.

        c. Mentse a fájlt.

           A Kaspersky Endpoint Security exportálja az eseményszűrőket a JSON-fájlba.
    7. Az eseményszűrők importálása:

        a. Kattintson az **Import** gombra.

        b. A megnyíló ablakban válassza ki azt a JSON-fájlt, amelyből importálni szeretné az eseményszűrőket.

        c. Válassza ki, hogyan szeretné az eseményszűrési szabályokat importálni: a meglévő szabályok hozzáadásával vagy a meglévő szabályok elvetésével és azok újakkal való helyettesítésével.

        d. Nyissa meg a fájlt.
    8. Ahhoz, hogy a szabályzatot alkalmazni lehessen a számítógépekre, győződjön meg arról, hogy a lakatok zárva vannak (), majd mentse a módosításokat.

Karantén kezelése

A *karantén* egy speciális helyi tároló a számítógépen. A felhasználó karanténba helyezheti azokat a fájlokat, amelyeket veszélyesnek ítél meg a számítógépen. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha az integrálva van a Kaspersky Detection and Response megoldásokkal. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a Biztonsági mentésbe helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért olvassa el a Kaspersky Sandbox súgót, a Kaspersky Endpoint Detection and Response Optimum súgót, a Kaspersky Endpoint Detection and Response Expert súgót, a Kaspersky Anti Targeted Attack Platform súgót és a Kaspersky Endpoint Detection and Response Expert (on-premises) súgót.

A Kaspersky Endpoint Security a rendszerfiókot (SYSTEM) használja a fájlok karanténba helyezéséhez.

A karanténbeállításokat csak a Kaspersky Security Center konzolban konfigurálhatja. A Kaspersky Security Center konzol segítségével karanténba helyezett objektumokat is kezelhet (visszaállítás, törlés, hozzáadás stb.). Helyileg a számítógépen csak a parancssor segítségével állíthatja vissza az objektumot.

A karantén maximális méretének konfigurálása

Alapértelmezés szerint a karantén mérete 1024 MB-ra van korlátozva. Amikor a karantén eléri a maximális méretet, a Kaspersky Endpoint Security leállítja a fájlok küldését, és létrehozza a *Nincs elegendő hely a karanténként szolgáló tárhelyen* eseményt. Annak elkerülése érdekében, hogy a karantén lemezterülete kifogyjon, beállíthat egy küszöbértéket, amelynél a Kaspersky Endpoint Security létrehozza *A karanténként szolgáló tárhely majdnem megtelt* eseményt. Nem állíthat be megőrzési időszakot a karanténba helyezett olyan fájloknál, amelyek automatikusan eltávolításra kerülnek.

Ha a Kaspersky Anti Targeted Attack Platform (EDR) megoldás van telepítve a vállalatnál, ajánlott megnövelni a Karantén méretét. YARA-vizsgálat során előfordulhat, hogy az alkalmazás nagy méretű memóriaképpel találkozik. Ha a memóriakép mérete meghaladja a karantén méretét, a YARA-vizsgálat befejeződik és hibát ad vissza, a memóriakép pedig nem kerül karanténba. Javasoljuk, hogy állítsa a karantén méretét a számítógép RAM-jával megegyezőre (például 8 Gb-ra), vagy tiltsa le a karantén méretkorlátozását.

A maximális karanténméret konfigurálásának menete az Felügyeleti konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirendek ablakában válassza az **Általános beállítások → Jelentések és tároló** lehetőséget.
4. A **Quarantine** részen adhatja meg a karantén méretét:
   - **Limit the size of Quarantine to N MB**. Ha a jelölőnégyzet be van jelölve, a karantén maximális tárhelyét a meghatározott érték korlátozza. Alapértelmezés szerint a maximális méret 1024 MB. Amikor a karantén eléri a maximális méretet, a Kaspersky Endpoint Security elküldi a *Nincs elegendő hely a karantén tárhelyen* eseményt a Kaspersky Security Centernek, és közzéteszi az eseményt a Windows Eseménynaplóban. Eközben az alkalmazás leállítja az új objektumok karanténba helyezését. A karantént kézzel kell kiürítenie.

     Ha a jelölőnégyzet nincs bejelölve, a karantén méretét a rendelkezésre álló szabad lemezterület korlátozza.
   - **Notify when the Quarantine storage reaches N percent**. A karantén küszöbértéke. Például beállíthatja a karantén küszöbértékét 50%-ra. Amikor a karantén eléri a küszöbértéket, a Kaspersky Endpoint Security elküldi a megfelelő eseményt a Kaspersky Security Centernek, és közzéteszi az eseményt a Windows Eseménynaplóban. Eközben az alkalmazás folytatja az új objektumok karanténba helyezését.

     Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem generál eseményeket a karantén küszöbértékének elérésekor.
5. Mentse el a módosításokat.

A maximális karanténméret konfigurálása a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management → Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Reports and Storage** elemet.

5. A **Quarantine** részen adhatja meg a karantén méretét:

   - **Limit the size of Quarantine**. Ha a négyzet be van jelölve, a karantén mérete a megadott értékre korlátozódik. Ha a jelölőnégyzet nincs bejelölve, a karantén méretét a rendelkezésre álló szabad lemezterület korlátozza. Erre a YARA vizsgálathoz lehet szükség, mert az alkalmazás nagy memóriakiíratási fájlokat tud menteni.

   - **Maximum size of Quarantine (MB)**. Ha a jelölőnégyzet be van jelölve, a karantén maximális tárhelyét a meghatározott érték korlátozza. Alapértelmezés szerint a maximális méret 1024 MB. Amikor a karantén eléri a maximális méretet, a Kaspersky Endpoint Security elküldi a *Nincs elegendő hely a karantén tárhelyen* eseményt a Kaspersky Security Centernek, és közzéteszi az eseményt a Windows Eseménynaplóban. Eközben az alkalmazás leállítja az új objektumok karanténba helyezését. A karantént kézzel kell kiürítenie.

     Ha a jelölőnégyzet nincs bejelölve, a karantén méretét a rendelkezésre álló szabad lemezterület korlátozza.

   - **Notify when the Quarantine storage reaches (%)**. A karantén küszöbértéke. Például beállíthatja a karantén küszöbértékét 50%-ra. Amikor a karantén eléri a küszöbértéket, a Kaspersky Endpoint Security elküldi a megfelelő eseményt a Kaspersky Security Centernek, és közzéteszi az eseményt a Windows Eseménynaplóban. Eközben az alkalmazás folytatja az új objektumok karanténba helyezését.

6. Mentse el a módosításokat.

A karanténba helyezett fájlok adatainak küldése a Kaspersky Security Centernek

A karanténba helyezett objektumokkal végzett műveletek végrehajtásához a Web Console-ban engedélyeznie kell a karanténba helyezett fájlok adatainak elküldését a Felügyeleti kiszolgálóra. Letölthet például egy fájlt a karanténból a Web Console-ban történő elemzéshez. A karanténba helyezett fájlok adatainak küldését engedélyezni kell a Kaspersky Sandbox és a Kaspersky Endpoint Detection and Response összes funkciójának működéséhez.

A karanténba helyezett fájladatok küldésének engedélyezése az Felügyeleti konzolban (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirendek ablakában válassza az **Általános beállítások** → **Jelentések és tároló** lehetőséget.

4. Az **Adatátvitel az adminisztrációs kiszolgálóra** részen kattintson a **Beállítások** gombra.

5. A megnyíló ablakban jelölje be a **Fájlok karanténba helyezése** jelölőnégyzetet.

6. Mentse el a módosításokat.

A karanténba helyezett fájladatok küldésének engedélyezése a Web Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **KSC Integration** elemet.
5. A **Data transfer to Administration Server** részen jelölje be az **About Quarantine files** jelölőnégyzetet.
6. Mentse el a módosításokat.

A művelet eredményeképpen a Kaspersky Security Center konzolján megtekintheti a számítógépen karanténba helyezett fájlok listáját. A Kaspersky Security Center konzolján kezelni is tudja a karanténba helyezett objektumokat (visszaállítás, törlés, hozzáadás stb.). A Karantén használatával kapcsolatos további tudnivalókért lásd a Kaspersky Security Center súgóját.

Fájlok visszaállítása a Karanténból

Alapértelmezés szerint a Kaspersky Endpoint Security visszaállítja a fájlokat az eredeti mappába. Ha a célmappát törölték, vagy a felhasználónak nincs hozzáférési joga ehhez a mappához, az alkalmazás a fájlt a következő mappába helyezi: `%DataRoot%\QB\Restored`. Ezután manuálisan át kell helyeznie a fájlt a célmappába.

Fájlok visszaállítása a Karanténból:

1. A Web Console fő ablakában válassza az **Operations** → **Repositories** → **Quarantine** lehetőséget.
2. Ez megnyitja a Karanténban található fájlok listáját; a listában válassza ki a visszaállítani kívánt fájlokat, majd kattintson a **Restore** gombra.

   A Kaspersky Endpoint Security visszaállítja a fájlt. Ha a célmappában már van azonos nevű fájl, az alkalmazás megszakítja a fájl visszaállítását. Az EDR Optimum és EDR Expert megoldások esetében az alkalmazás a visszaállítás után törli a fájlt. Más megoldások esetén az alkalmazások a fájl másolatát a karanténban tartják.

EDR műveletek figyelése

A Kaspersky Endpoint Security for Windows 12.9 bevezeti az EDR műveletfigyelési központot. Az *EDR műveletfigyelési központ* egy olyan konzol, amelyen megtekintheti a fenyegetésekre adott válasz előzményeit az összes Kaspersky Detection és Response megoldás esetében. Ha a vállalatnél több Detection and Response megoldás (például EDR Optimum és MDR) van telepítve, a Kaspersky Endpoint Security minden megoldásnál megjeleníti a fenyegetésekre adott válasz előzményeit. Ez lehetővé teszi a Detection and Response megoldások teljesítményének külön számítógépen történő elemzését, és e megoldások beállításainak optimalizálását.

A figyelési központ a következő információkat szolgáltatja:

- Információk a fenyegetésekre adott válasz feladatairól (például a *Folyamat megszakítása* feladat)
- A hálózatelkülönítéshez és a végrehajtás-megelőzéshezt tartozó szabályok változásai

Ha a fenyegetésekre adott válasz egy hálózati megosztáshoz való hozzáféréssel kapcsolatos hibába ütközik, az ilyen hiba nem kerül ki a fenyegetésekre adott válasz megjelenített előzményeiből.

Navigálás az EDR műveletfigyelési központhoz:

1. A Web Console fő ablakában válassza a **Asset management** → **Assets (Devices)** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.

   Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki az **Applications** lapot.
4. Kattintson az **Kaspersky Endpoint Security for Windows** gombra.

   Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** lapot.
6. Nyissa meg a **Detection and Response** → **Response history** elemet.

Ezzel megnyitja az EDR műveletfigyelési központ konzolját. A konzolon megtekintheti a fenyegetésre adott válasz feladatállapotát, a feladat időtartamát, a szabályok módosításait és a kezdeményező részleteit.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



A Kaspersky Endpoint Security for Windows támogatja a Kaspersky Unified Monitoring and Analysis Platform megoldást. A *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* egy biztonsági információ- és eseménykezelő megoldás (SIEM) a vállalatok IT-infrastruktúrájához. A KUMA lehetővé teszi a biztonsági fenyegetések észlelését, elemzését és elhárítását, mielőtt azok kárt okozhatnának.

A Kaspersky Endpoint Security a vállalati IT-infrastruktúra egyes számítógépeire van telepítve, és folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítás alatt álló fájlokat. A számítógépen zajló eseményekkel kapcsolatos információk (telemetria) elküldésre kerülnek a Kaspersky Unified Monitoring and Analysis Platform (KUMA) kiszolgálóra. A konzolon a KUMA az eseményeket jelölés nélküli listaként jeleníti meg, hasonlóan a Windows eseménynaplójához.

A Kaspersky Endpoint Security nem biztosítja az ügynökök minden funkcióját a KUMA-hoz. Az alkalmazás csak jelölés nélkül küld eseményeket a KUMA-nak. A KUMA összes funkciójának eléréséhez licencet kell vásárolnia, és a megoldást a KUMA rendszergazdai útmutatójának megfelelően kell telepítenie.

A Kaspersky Endpoint Security integrálása a KUMA-val

A KUMA használatához az alábbi feltételeknek kell teljesülniük:

- Kaspersky Security Center 14.2 vagy újabb verzió. A Kaspersky Security Center korábbi verzióiban nem lehet aktiválni a KUMA-integráció funkcióját.
- Az alkalmazás aktiválva van, és a funkciójára a licenc kiterjed.
- A KUMA-integráció összetevője engedélyezve van.

A KUMA-integráció beállítása a következő lépésekből áll:

1. **A KUMA-integráció összetevőjének telepítése**

   A KUMA-integráció összetevőjét az alkalmazás telepítése vagy frissítése közben, valamint az *Alkalmazásösszetevők módosítása* feladat használatával választhatja ki.

   Újra kell indítania a számítógépét az alkalmazás új összetevővel történő frissítésének befejezéséhez.

2. **KUMA aktiválás**

   A Kaspersky Endpoint Security alkalmazás licencén (például Kaspersky Endpoint Security for Business Standard) kívül külön licencre van szükség a Kaspersky Endpoint Security és a KUMA integrációjához (Kaspersky Endpoint Security for Windows KUMA integrációs bővítmény).

Ha az alkalmazást EDR Agent üzemmódban telepíti, licencre van szükség a Kaspersky Endpoint Security és a KUMA integrálásához, valamint szükség van a Kaspersky Anti Targeted Attack Platform (KATA) licencre vagy Kaspersky Managed Detection and Response (MDR) licencre. Nem telepítheti az EDR Agent csak a KUMA-hoz.

A funkció külön KUMA-kulcs hozzáadása után válik elérhetővé. Ennek eredményeként a számítógépen egy másik aktív kulcs jelenik meg a Kaspersky Endpoint Security és a KUMA integrációjához.

Az önálló KUMA funkció licencelése megegyezik a Kaspersky Endpoint Security licencelésével.

Győződjön meg arról, hogy az KUMA funkció szerepel a licencben, és jelenleg az alkalmazás helyi felületén működik.

3 A KUMA csatlakoztatása

A Kaspersky Endpoint Security alkalmazással rendelkező számítógép csatlakoztatása a KUMA megoldáshoz:

1. A Kaspersky Endpoint Security házirendjében vegye fel a KUMA-kiszolgáló címeit, és adja meg a kapcsolat hálózati beállításait.
2. A KUMA konzolon adjon hozzá egy adatgyűjtőt tcp vagy udp típusú csatlakozóval, és adja meg a kapcsolat alapvető hálózati beállításait. Az adatgyűjtők kezelésével kapcsolatos részletekért olvassa el a Kaspersky Unified Monitoring and Analysis Platform súgóját.

Megbízható kapcsolatot hozhat létre a Kaspersky Endpoint Security és a KUMA-kiszolgálók között. A megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell használnia. A KUMA Core kiszolgálón TLS-tanúsítványt kaphat (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában). Ezután hozzá kell adnia a TLS-tanúsítványt a Kaspersky Endpoint Security szolgáltatáshoz (lásd az alábbi utasításokat).

A kapcsolat biztonságosabbá tétele céljából ezenkívül engedélyezheti a számítógép ellenőrzését a KUMA megoldásban (kétirányú hitelesítés). Az ellenőrzés engedélyezéséhez be kell kapcsolnia a kétirányú hitelesítést a KUMA és a Kaspersky Endpoint Security beállításaiban. A kétirányú hitelesítés használatához kriptotárolóra is szüksége lesz. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A titkos kulcsot tartalmazó tanúsítványt PKCS#12 tárolóformátumban kell létrehoznia egy külső hitelesítésszolgáltatónál. Ezután hozzá kell adnia a PFX-archívumot a KUMA-konzolon és a Kaspersky Endpoint Security alkalmazásban (a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában találja).

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a KUMA megoldáshoz az adminisztrációs konzol (MMC) segítségével

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakában válassza ki a **KUMA integráció** lehetőséget.
4. Jelölje be a **KUMA integráció** jelölőnégyzetet.
5. Az **Integrációs beállítások** területen, jelölje be a **$IsKUMATelemetry ? "Windows-események továbbításának engedélyezése KUMA-kiszolgálóra" : "Windows-események továbbításának engedélyezése SIEM-kiszolgálóra"** négyzet.
6. Ha szükséges, jelölje be a **TLS titkosítás használata** négyzetet **A KUMA kiszolgálóihoz való csatlakozás beállításai** területen.

7. Konfigurálja a megbízható kapcsolatot:

   a. Kattintson **A KUMA kiszolgálóihoz való csatlakozás beállításai** elemre.

   b. Konfigurálja a kiszolgálói kapcsolatot:

   - **Időtúllépés (mp)**. A KUMA kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik KUMA-kiszolgálóhoz.
   - **Kiszolgálói TLS-tanúsítvány hibája**. TLS-tanúsítvány a KUMA-kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt a Kaspersky Unified Monitoring and Analysis Platform konzolon szerezhet be (az utasításokat lásd: Kaspersky Unified Monitoring and Analysis Platform).

     A megbízható kapcsolat létrehozásához a KUMA-konzolon a tcp-csatlakozó beállításai között a **With verification** TLS módot kell kiválasztania (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában).
   - **Kétirányú hitelesítés használata**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a KUMA közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához a KUMA-konzolon a tcp-csatlakozó beállításai között a **Custom PFX** TLS módot kell kiválasztania (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában). Ezután szereznie kell egy kriptokonténert, és be kell állítania egy jelszót a kriptokonténer védelmére. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A KUMA beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     > A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

   c. Kattintson az **OK** gombra.

8. Adja hozzá a KUMA-kiszolgálókat:

   a. Kattintson **Hozzáadás** gombra.

   Megnyílik az űrlap, ahol hozzáadhat KUMA-kiszolgálót.

   b. Válassza ki a KUMA-kiszolgálókhoz való csatlakozás protokollját: **HTTP / HTTPS**, **TCP**, **UDP**.

   Ha a **HTTP / HTTPS** protokollt választja, alapértelmezés szerint az alkalmazás HTTPS-kapcsolatot használ a KUMA-kiszolgálókhoz való kapcsolódáshoz. A HTTP használatához manuálisan kell megadnia ezt a protokollt a kiszolgáló címében (például `http://server.com`).

   c. Adja meg a kiszolgáló címét (IPv4, IPv6) és a portot a kiszolgálóhoz való csatlakozáshoz.

   d. Kattintson az **OK** gombra.

   A Kaspersky Endpoint Security a listán szereplő első KUMA-kiszolgálóhoz csatlakozik. Ha a kapcsolat sikertelen, a Kaspersky Endpoint Security a listán szereplő második KUMA-kiszolgálóhoz csatlakozik, és így tovább.

9. Ha szükséges, konfigurálja a **Maximális eseményátviteli idő (mp)** beállítást az **Adatátviteli beállítások** területen. Amikor a megadott idő lejár, a Kaspersky Endpoint Security megpróbál csatlakozni ugyanahhoz a kiszolgálóhoz, vagy a listán következő kiszolgálóhoz, ha több kiszolgáló is van. Az alapértelmezett beállítás 30 másodperc.

10. Mentse el a módosításokat.

A Kaspersky Endpoint Security alkalmazást futtató számítógép csatlakoztatása a KUMA megoldáshoz a Web Console segítségével

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Built-in Agents Configuration** → **KUMA Integration** elemet.
5. Kapcsolja be az **KUMA Integration ENABLED** kapcsolót.
6. Ha szükséges, a **Use TLS encryption** kapcsolót állítsa be állásba a **Server connection settings** területen.
7. Konfigurálja a megbízható kapcsolatot:

   a. Kattintson az **Connection settings** gombra.

   b. Konfigurálja a kiszolgálói kapcsolatot:

   - **Timeout (sec)**. A KUMA kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik KUMA-kiszolgálóhoz.
   - **Server TLS certificate**. TLS-tanúsítvány a KUMA-kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt a Kaspersky Unified Monitoring and Analysis Platform konzolon szerezhet be (az utasításokat lásd: Kaspersky Unified Monitoring and Analysis Platform).

     A megbízható kapcsolat létrehozásához a KUMA-konzolon a tcp-csatlakozó beállításai között a **With verification** TLS módot kell kiválasztania (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában).
   - **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a KUMA közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához a KUMA-konzolon a tcp-csatlakozó beállításai között a **Custom PFX** TLS módot kell kiválasztania (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában). Ezután szereznie kell egy kriptokonténert, és be kell állítania egy jelszót a kriptokonténer védelmére. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A KUMA beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.

     > A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.

   c. Kattintson az **OK** gombra.
8. Adja hozzá a KUMA-kiszolgálókat:

   a. Kattintson az **Add** gombra.

   Megnyílik az űrlap, ahol hozzáadhat KUMA-kiszolgálót.

b. Válassza ki a KUMA-kiszolgálókhoz való csatlakozás protokollját: **HTTP/HTTPS**, **TCP**, **UDP**.

Ha a **HTTP/HTTPS** protokollt választja, alapértelmezés szerint az alkalmazás HTTPS-kapcsolatot használ a KUMA-kiszolgálókhoz való kapcsolódáshoz. A HTTP használatához manuálisan kell megadnia ezt a protokollt a kiszolgáló címében (például `http://server.com`).

c. Adja meg a kiszolgáló címét (IPv4, IPv6) és a portot a kiszolgálóhoz való csatlakozáshoz.

d. Kattintson az **OK** gombra.

A Kaspersky Endpoint Security a listán szereplő első KUMA-kiszolgálóhoz csatlakozik. Ha a kapcsolat sikertelen, a Kaspersky Endpoint Security a listán szereplő második KUMA-kiszolgálóhoz csatlakozik, és így tovább.

9. Ha szükséges, konfigurálja a **Maximum delay when sending events (sec)** beállítást a **Server connection settings** részen. Amikor a megadott idő lejár, a Kaspersky Endpoint Security megpróbál csatlakozni ugyanahhoz a kiszolgálóhoz, vagy a listán következő kiszolgálóhoz, ha több kiszolgáló is van. Az alapértelmezett beállítás 30 másodperc.

10. Mentse el a módosításokat.

A KUMA-konzolon ellenőrizheti, hogy a KUMA-integráció helyesen van-e konfigurálva (a részleteket a Kaspersky Unified Monitoring and Analysis Platform súgójában találja). Ellenőrizheti az összetevő működési állapotát a Kaspersky Security Center konzolon az *Report on status of application components* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található jelentésekben is megtekintheti. A **KUMA integráció** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

4 Telemetriai adatok küldésének engedélyezése a KUMA kiszolgálóra

Alapértelmezés szerint az események KUMA kiszolgálóra való küldése le van tiltva. A KUMA megfelelő működéséhez engedélyeznie kell a telemetriai adatok küldését. Az eseményforrást a következő standard naplók közül választhatja ki: *Alkalmazás*, *Biztonság* vagy *Rendszer*.

A telemetriai adatok küldésének engedélyezése a KUMA kiszolgálóra a Felügyeleti konzolon (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A szabályzat ablakban válassza ki az **Általános beállítások → Jelentések és objektumtípusok** részt.
5. A **Telemetriai beállítások → KUMA telemetria** területen kattintson a **Beállítások** gombra.
6. Válassza ki az eseményforrásként használni kívánt eseménynaplókat: *Alkalmazás*, *Biztonság* vagy *Rendszer*.

   A standard naplók mellett megadhat harmadik féltől származó alkalmazásnaplót is.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A telemetriai adatok küldésének engedélyezése a KUMA kiszolgálóra a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management → Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.
5. Válassza ki az **KUMA telemetry** lapot.
6. Válassza ki az eseményforrásként használni kívánt eseménynaplókat: *Application*, *Security* vagy *System*.
   A standard naplók mellett megadhat harmadik féltől származó alkalmazásnaplót is.
7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A KUMA-nak küldendő szűrési események

Alapértelmezés szerint az események KUMA kiszolgálóra való küldése le van tiltva. A KUMA megfelelő működéséhez engedélyeznie kell a telemetriai adatok küldését. Az eseményforrást a következő standard naplók közül választhatja ki: *Alkalmazás*, *Biztonság* vagy *Rendszer*. A teljesítmény növelése és az adatok KUMA kiszolgálóra történő továbbításának optimalizálása céljából manuálisan hozzáadhat vagy kizárhat egyes eseményeket a telemetriából. Például kizárhatja a Sysmon eseményeket.

A KUMA-nak küldendő eseménylista létrehozása a Felügyeleti konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A szabályzat ablakban válassza ki az **Általános beállítások** → **Jelentések és objektumtípusok** részt.
5. A **Telemetriai beállítások** → **KUMA telemetria** területen kattintson a **Beállítások** gombra.
6. A megjelenő ablakban konfigurálja a KUMA-nak küldendő eseményszűrőket.
   Beállíthatja az eseményszűrést a normál *Application*, *Security*, *System* naplókhoz, vagy manuálisan is hozzáadhat egy másik naplót:
   a. Nyissa meg a napló tulajdonságait, vagy kattintson az **Hozzáadás** gombra, és adja meg a napló nevét.
   b. Válasszon ki egy eseménykülési módot:
   - **Összes esemény küldése**. Ebben a módban az alkalmazás az összes eseményt a Windows naplójából küldi el, kivéve a kizárási szabályokhoz hozzáadott eseményeket.
   - **Csak kiválasztott események küldése**. Ebben a módban az alkalmazás csak a belefoglalási szabályokban hozzáadott eseményeket küldi el.

c. Hozzon létre listákat a kizárási vagy felvételi szabályokról a vonatkozó eseménykuldési módhoz.

Szabályok hozzáadásához meg kell adnia az esemény azonosítóját a Windows eseménynaplójában. Egy szabályban több eseményazonosítót is listázhat. Több eseményazonosító megadásához használjon vesszőt (**,**).

d. Szükség esetén engedélyezze az eseménynaplózást a napló neve melletti jelölőnégyzet aktiválásával.

7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A KUMA-nak küldendő eseménylista létrehozása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.
5. Válassza ki az **KUMA telemetry** lapot.
6. A megjelenő ablakban konfigurálja a KUMA-nak küldendő eseményszűrőket.

Beállíthatja az eseményszűrést a normál *Application*, *Security*, *System* naplókhoz, vagy felvehet manuálisan egy másik naplót:

a. Nyissa meg a napló tulajdonságait, vagy kattintson a(z) **Add** gombra, és adja meg a napló nevét.

b. Válasszon ki egy eseménykuldési módot:

- **Send all events**. Ebben a módban az alkalmazás az összes eseményt a Windows naplójából küldi el, kivéve a kizárási szabályokhoz hozzáadott eseményeket.
- **Send only selected events**. Ebben a módban az alkalmazás csak a belefoglalási szabályokban hozzáadott eseményeket küldi el.

c. Hozzon létre listákat a kizárási vagy felvételi szabályokról a vonatkozó eseménykuldési módhoz.

Szabályok hozzáadásához meg kell adnia az esemény azonosítóját a Windows eseménynaplójában. Egy szabályban több eseményazonosítót is listázhat. Több eseményazonosító megadásához használjon vesszőt (**,**).

d. Szükség esetén engedélyezze az eseménynaplózást a napló neve melletti kapcsolóval.

7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

KUMA-eseményszűrők exportálása és importálása

A kizárások listáját exportálhatja egy JSON-fájlba. Ezután módosíthatja a fájlt, például nagy számú eseményazonosító hozzáadásával. Használhatja az exportálás/importálás funkciót az eseményszűrők biztonsági mentésének létrehozásához, vagy a lista egy másik kiszolgálóra való áttelepítéséhez.

Túl sok szabály használata növelheti a KUMA-kiszolgáló terhelését és csökkentheti a számítógép teljesítményét. Javasoljuk, hogy csak a szükséges szabályokat adja hozzá.

Eseményszűrők exportálása és importálása az Adminisztrációs konzolban (MMC)

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. A konzolfán válassza ki a **Policies** lehetőséget.
3. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
4. A szabályzat ablakban válassza ki az **Általános beállítások** → **Jelentések és objektumtípusok** részt.
5. A **Telemetriai beállítások** → **KUMA telemetria** területen kattintson a **Beállítások** gombra.
6. Az eseményszűrők exportálása:
   a. Válassza ki az exportálni kívánt szűrőkkel rendelkező eseménynaplókat.
   b. Kattintson a → **Hozzáadás** gombra.
   c. A megnyíló ablakban adja meg a JSON-fájl nevét, amelybe exportálni szeretné az eseményszűrőket, és válassza ki a fájl mentésére kiszemelt mappát.
   d. Mentse a fájlt.
      A Kaspersky Endpoint Security exportálja az eseményszűrőket a JSON-fájlba.
7. Az eseményszűrők importálása:
   a. Kattintson a → **Hozzáadás** gombra.
   b. A megnyíló ablakban válassza ki azt a JSON-fájlt, amelyből importálni szeretné az eseményszűrőket.
   c. Nyissa meg a fájlt.
      Ha már léteznek eseményszűrési szabályok a számítógépen, a Kaspersky Endpoint Security lecseréli ezeket az importálás során.
8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Eseményszűrők exportálása és importálása a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lapot.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Telemetry Settings** elemet.
5. Válassza ki az **KUMA telemetry** lapot.
6. Az eseményszűrők exportálása:

   a. Válassza ki az exportálni kívánt szűrőkkel rendelkező eseménynaplókat.

   b. Kattintson az → **Export** gombra.

   c. A megnyíló ablakban adja meg a JSON-fájl nevét, amelybe exportálni szeretné az eseményszűrőket, és válassza ki a fájl mentésére kiszemelt mappát.

   d. Mentse a fájlt.

   A Kaspersky Endpoint Security exportálja az eseményszűrőket a JSON-fájlba.
7. Az eseményszűrők importálása:

   a. Kattintson az → **Import** gombra.

   b. A megnyíló ablakban válassza ki azt a JSON-fájlt, amelyből importálni szeretné az eseményszűrőket.

   c. Nyissa meg a fájlt.

   Ha már léteznek eseményszűrési szabályok a számítógépen, a Kaspersky Endpoint Security lecseréli ezeket az importálás során.
8. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Eseményszűrőket is exportálhat vagy importálhat a parancssorból.

Áttérés a KSWS rendszerről KES rendszerre – áttelepítési útmutató

A 11.8.0 verzióval kezdődően a Kaspersky Endpoint Security for Windows támogatja a Kaspersky Security for Windows Server (KSWS) megoldás alapvető funkcióit. *Kaspersky Security for Windows Server* védi a Microsoft Windows operációs rendszert futtató kiszolgálókat és a hálózathoz csatlakoztatott tárolókat olyan vírusokkal és más számítógépes biztonsági fenyegetésekkel szemben, amelyeknek a kiszolgálók és a hálózathoz csatlakoztatott tárolók ki vannak téve a fájlcsere során. A megoldás működéséről részletes információt a Kaspersky Security for Windows Server súgójában talál. A Kaspersky Endpoint Security 11.8.0-tól kezdve áttérhet a Kaspersky Security for Windows Server termékről a Kaspersky Endpoint Security for Windows termékre, és ugyanazt a megoldást használhatja a munkaállomások és kiszolgálók védelmére.

Szoftverkövetelmények

Mielőtt elkezdené a KSWS rendszerről a KES rendszerre való áttelepítést, győződjön meg arról, hogy a kiszolgáló megfelel a Kaspersky Endpoint Security for Windows hardver- és szoftverkövetelményeinek. A támogatott operációsrendszer-verziók listája eltér a KES és a KSWS esetében. Például a KES nem támogatja a Windows Server 2003 rendszert futtató kiszolgálókat.

Minimális szoftverkövetelmények a KSWS rendszerről a KES rendszerre való áttelepítéskor:

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Ha a Kaspersky Security for Windows Server korábbi verziója van telepítve, javasoljuk, hogy frissítse az alkalmazást a legújabb verzióra. A Házirendek és feladatok konvertálási varázslója nem támogatja a Kaspersky Security for Windows Server korábbi verzióit.
- Kaspersky Security Center 14.2

  Ha a Kaspersky Security Center korábbi verziója van telepítve, frissítse azt a 14.2 vagy újabb verzióra. A Kaspersky Security Center ezen verziójában a Házirendek és feladatok kötegelt konvertálási varázslója lehetővé teszi a házirendek házirend helyett profilba történő áttelepítését. A Kaspersky Security Center ezen verziójában a Házirendek és feladatok kötegelt konvertálási varázslója a házirend-beállítások szélesebb körének áttelepítését is lehetővé teszi.
- Kaspersky Endpoint Agent 3.10.

  Ha a Kaspersky Endpoint Agent korábbi verziója van telepítve, javasoljuk, hogy frissítse az alkalmazást a legújabb verzióra. A Kaspersky Endpoint Security támogatja a [KSWS+KEA] konfiguráció áttelepítését a [KES+beépített ügynök] szolgáltatásba a Kaspersky Endpoint Agent 3.10-től kezdve.

Áttelepítési javaslatok

Amikor KSWS-ről KES-re vált, vegye figyelembe a következő javaslatokat:

- Tervezze meg előre a KSWS-ről a KES-re történő áttelepítés időpontját. Válasszon olyan időpontot, amikor a kiszolgálók a legkisebb terhelés mellett működnek, például hétvégén.
- Az áttelepítés után fokozatosan kapcsolja be az alkalmazásösszetevőket. Vagyis először csak a Fájl védelem összetevő engedélyezésével kezdje, majd engedélyezze a többi védelmi összetevőt, majd engedélyezze a felügyeleti összetevőket, és így tovább. Minden lépésnél meg kell győződnie arról, hogy az alkalmazás megfelelően működik, és figyelnie kell a kiszolgáló teljesítményét. A KES architektúrája eltér a KSWS-étől, ezért az operációs rendszer is eltérően viselkedhet.
- Fokozatosan hajtsa végre az áttelepítést. Először egyetlen, majd több kiszolgálóra végezze el az áttelepítést, és csak ezután hajtsa végre az áttelepítést a szervezet összes kiszolgálóján.
- Külön végezze el a különböző típusú kiszolgálók áttelepítését. Vagyis például először az adatbázis-kiszolgálókat, majd a levelezőkiszolgálókat és így tovább.
- A nagy terhelésű kiszolgálókon történő áttelepítés különleges megfontolást igényel.

Az áttelepítés lépései

A KSWS-ről a KES-re való áttelepítés félautomatikusan történik. Erre az alkalmazások eltérő architektúrái miatt van szükség. A házirend-beállítások áttelepítéséhez futtassa a Házirendek és feladatok kötegelt konvertálási varázslót (áttelepítési varázsló). A házirend-beállítások áttelepítése után manuálisan kell konfigurálnia azokat a beállításokat, amelyeket az áttelepítési varázsló nem tud automatikusan áttelepíteni (például a jelszóvédelmi beállításokat). Az áttelepítés után ajánlott ellenőrizni azt is, hogy az áttelepítési varázsló megfelelően végezte-e el az összes beállítás áttelepítését.

Végezze el az áttelepítést a KSWS-ről a KES-re a következő sorrendben:

1. **A KSWS feladatok és házirendek áttelepítése**

   A házirendek és feladatok áttelepítése után további konfigurációs lépéseket kell végrehajtania. Azt is javasoljuk, hogy győződjön meg arról, hogy a Kaspersky Endpoint Security biztosítja-e a szükséges szintű biztonságot a KSWS-ről való átállás után.

   > A Kaspersky Security for Windows Server Házirendek és feladatok kötegelt konvertálási varázslója csak az Adminisztrációs konzolon (MMC) érhető el. A házirend- és feladatbeállítások nem telepíthetők át a Web Console-ban és a Kaspersky Security Center Cloud Console-ban.

2. **Telepítse a Kaspersky Endpoint Security alkalmazást**

A Kaspersky Endpoint Security a következő módokon telepíthető:

- A KES telepítése a KSWS eltávolítása után (ajánlott).

  A kavremover segédprogram nem támogatja a KSWS-t.

- A KES telepítése a KSWS-re.

3. **A KES aktiválása egy KSWS-kulccsal**

4. **Győződjön meg arról, hogy az alkalmazás az áttelepítés után működőképes**

   A KSWS-ről a KES-re való átállás után győződjön meg arról, hogy az alkalmazás megfelelően működik. Ellenőrizze a kiszolgáló állapotát a konzolon (*OK* állapotúnak kell lennie). Győződjön meg arról, hogy az alkalmazás nem jelez hibát, valamint ellenőrizze az adminisztrációs kiszolgálóhoz való legutóbbi csatlakozás idejét, az utolsó adatbázis-frissítés időpontját és a kiszolgáló védelmi állapotát.

   Fordítson különös figyelmet a kizárási listák, a megbízható alkalmazások, a megbízható webcímek és az alkalmazásfelügyeleti szabályok áttelepítésére.

A KSWS és a KES összetevőinek megfeleltetése

A KSWS-ről a KES-re való áttéréskor az összetevőkészlet csak akkor kerül áthelyezésre, ha az alkalmazást helyileg telepíti.

A Kaspersky Security for Windows Server és a Kaspersky Endpoint Security for Windows összetevőinek megfeleltetése

Kaspersky Security for Windows Server összetevő	Kaspersky Endpoint Security for Windows összetevő
Basic functionality	Alkalmazáskernel
Log Inspection	Naplóvizsgálat
Device Control	Eszközfelügyelő
Firewall Management	*(nem támogatott)* A KSWS Tűzfal funkciókat a rendszer-szintű Tűzfal látja el. A KES-ben egy külön összetevő felel a Tűzfal funkcióért. Áttelepítést követően beállíthatja a Kaspersky Endpoint Security Tűzfal beállításait.
File Integrity Monitor	Rendszerintegritás-figyelő
Exploit Prevention	Biztonsági rések kihasználásának megelőzése
System Tray Icon	*(nem támogatott)* A felhasználói interakciót az alkalmazásfelület beállításaiban konfigurálhatja.
Integration with Kaspersky Security Center	Hálózati Ügynök Csatoló
Endpoint Agent	*(nem támogatott)* A Kaspersky Endpoint Security 11.9.0 verziójában a Kaspersky Endpoint Agent terjesztőcsomag már nem része a Kaspersky Endpoint Security terjesztőkészletének. A Kaspersky Endpoint Agent terjesztőcsomagot külön kell letöltenie.
Network Threat Protection	Hálózati védelem
Anti-Cryptor	Viselkedésészlelés
Anti-Cryptor for NetApp	*(nem támogatott)*

Kaspersky Security for Windows Server összetevő	Kaspersky Endpoint Security for Windows összetevő
Traffic Security	Web védelem Levelezés védelem Webfelügyelő
On-Demand Scan	Alkalmazáskernel
ICAP Network Storage Protection	*(nem támogatott)* A Kaspersky Endpoint Security nem támogatja a hálózati tárolóeszköz védelmi összetevőket. Ha szüksége van ezekre az összetevőkre, folytathatja a Kaspersky Security for Windows Server használatát.
RPC Network Storage Protection	*(nem támogatott)* A Kaspersky Endpoint Security nem támogatja a hálózati tárolóeszköz védelmi összetevőket. Ha szüksége van ezekre az összetevőkre, folytathatja a Kaspersky Security for Windows Server használatát.
Real-Time File Protection	Fájl védelem
Script Monitoring	*(nem támogatott)* A parancsfájlok figyelését más összetevők, például az AMSI védelem kezeli.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Alkalmazásfelügyelő
Performance counters	*(nem támogatott)*

A KSWS és a KES beállításainak megfeleltetése

A házirendek és feladatok áttelepítésekor a KES a KSWS-beállításokkal összhangban van konfigurálva. Azon alkalmazásösszetevők beállításai, amelyekkel a KSWS nem rendelkezik, alapértelmezett értékekre vannak állítva.

Application settings

Scalability, interface and scanning settings

A Kaspersky Endpoint Security for Windows nem támogatja az alkalmazásbeállításokat.

Alkalmazásbeállítások

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Scalability settings	*(nincs áttelepítés)* A Kaspersky Endpoint Security felügyeli az összes munkafolyamatot.
Show System Tray Icon	*(nincs áttelepítés)* Ügyfélszámítógépeken a Kaspersky Endpoint Security fő ablaka és a Windows értesítési területén lévő ikon érhető el alapértelmezés szerint. Az ikon helyi menüjében a felhasználó műveleteteket hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security értesítéseket is megjelenít az alkalmazásikon felett. A felhasználói interakciót az alkalmazásfelület beállításaiban konfigurálhatja.
Restore file attributes after scanning	*(nincs áttelepítés)* A Kaspersky Endpoint Security automatikusan visszaállítja a fájlattribútumokat a fájl vizsgálata után.
Limit CPU usage for scanning threads	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem korlátozza a CPU-használatot a vizsgálat során. Konfigurálhatja a feladatot, hogy akkor fusson, amikor a számítógép minimális terhelés mellett működik.

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Folder for temporary files created during scanning	*(nincs áttelepítés)* A Kaspersky Endpoint Security az ideiglenes fájlokat a `C:\Windows\Temp` mappába helyezi.
HSM system settings	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem támogatja a HSM-rendszereket.

Security and reliability

A KSWS biztonsági beállításai átkerülnek az **Általános beállítások** szakaszba, illetve az **Alkalmazásbeállítások** és **Felület** alszakaszba.

Alkalmazásbiztonsági beállítások

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Protect application processes from external threats	**Engedélyezze az Önvédelem** funkciót (**Alkalmazásbeállítások** alszakasz)
Apply password protection	*(nincs áttelepítés)* A Kaspersky Endpoint Security beépített Jelszóvédelem funkcióval (lásd **Felület** alrészt).
Perform task recovery	*(nincs áttelepítés)* A Kaspersky Endpoint Security csak a *Kártevő vizsgálata* feladatait állítja vissza automatikusan. A Kaspersky Endpoint Security egyéb feladatokat ütemezetten futtat.
Do not start scheduled scan tasks	**Ütemezett feladatok elhalasztása, amíg a számítógép akkumulátorról üzemel** (**Alkalmazásbeállítások** alszakasz)
Stop current scan tasks	*(nincs áttelepítés)* Amikor a számítógépet szünetmentes tápegység táplálja, a Kaspersky Endpoint Security nem állítja le a már futó vizsgálati feladatokat.

Connection settings

A Felügyeleti kiszolgáló interakciós beállításai átkerülnek az **Általános beállítások** szakasz **Hálózati beállítások** és **Alkalmazásbeállítások** alszakaszába.

Felügyeleti kiszolgáló interakciós beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Proxy server settings	**Proxykiszolgáló beállításai** (**Hálózati beállítások** alszakasz)
Do not use proxy server for local addresses	**Proxykiszolgáló kihagyása helyi címek esetén** (**Hálózati beállítások** alszakasz)
Proxy server authentication settings	**Proxykiszolgáló-hitelesítés használata** (**Hálózati beállítások** alszakasz) A proxykiszolgáló hitelesítési jelszó nem kerül áttelepítésre. Új szabályzat áttelepítése után a jelszavat manuálisan kell megadni.
Use Kaspersky Security Center as a proxy server when activating the application	**A Kaspersky Security Center használata proxykiszolgálóként az aktiváláshoz** (**Alkalmazásbeállítások** alszakasz)

Run local system tasks

A Kaspersky Endpoint Security figyelmen kívül hagyja a Kaspersky Security for Windows Server helyi rendszerfeladatainak futtatására vonatkozó beállításokat. A helyi KES-feladatok használatát a **Helyi feladatok**, **Feladatkezelés** részben konfigurálhatja. Ütemezést is konfigurálhat a *Kártevő vizsgálata* és *Adatbázisok és alkalmazásmodulok frissítése* feladatokhoz a feladatok tulajdonságainál.

Supplementary

Trusted zone

A KSWS megbízható zónára vonatkozó beállításai átkerülnek az **Általános beállítások** szakasz Kizárások alszakaszába.

Megbízható zóna beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Object to scan (Exclusions)	**Kizárások a vizsgálatból** (Kizárások a vizsgálatból) A KSWS és a KES által az objektumok kiválasztására használt módszerek különböznek. Áttelepítéskor a KES támogatja az egyedi fájlokként vagy a fájlhoz/mappához vezető útvonalakként meghatározott kizárásokat. Ha a KSWS-ben a kizárások előre meghatározott területként vagy szkript URL-ként vannak konfigurálva, az ilyen kizárások nem kerülnek áttelepítésre. Az áttelepítés után ezeket a kizárásokat manuálisan kell hozzáadnia. Az előre definiált területekből álló kizárásokat a *Kártevő vizsgálata* feladat beállításaiban kell konfigurálni. A parancsfájl típusú webcímekből álló kizárásokat hozzá kell adni a megbízható webcímekhez a Web védelem esetében.
Apply also to subfolders (Exclusions)	**Almappákkal együtt** (Kizárás a vizsgálatból)
Objects to detect (Exclusions)	**Az észlelt objektum típusa** (Kizárások a vizsgálatból)
Exclusion usage scope (Exclusions)	**Védelmi összetevők** (Kizárás a vizsgálatból) Ha legalább egy összetevő ki van választva a KSWS-ben, a KES a kizárásokat az összes alkalmazásösszetevőre alkalmazza.
Comment (Exclusions)	**Megjegyzés** (Kizárás a vizsgálatból)
Trusted process (Trusted process)	**Megbízható alkalmazások** A megbízható folyamat / alkalmazás kiválasztási módszerei különböznek a KSWS-ben és a KES-ben. Áttelepítéskor a KES támogatja a futtatható fájl vagy maszk elérési útjaként konfigurált megbízható alkalmazásokat. Ha a KSWS megbízható folyamatokat fájlkivonatként konfigurál, akkor az ilyen megbízható folyamatok nem kerülnek áttelepítésre. Az áttelepítés után ezeket a megbízható folyamatokat manuálisan kell hozzáadnia.
Do not check file backup operations (Trusted process)	**Ne figyelje az alkalmazástevékenységet** (Megbízható alkalmazások)

Removable drives scan

A cserélhető meghajtók vizsgálati beállításai átkerülnek a **Helyi feladatok** szakasz Cserélhető meghajtók vizsgálata alszakaszába.

Cserélhető meghajtók vizsgálatának beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Scan removable drives on connection via USB	**Cserélhető meghajtó csatlakoztatásakor végzendő művelet**
Scan removable drives if its stored data volume does not exceed (MB)	**Cserélhető meghajtó maximális mérete**

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Cserélhető meghajtó csatlakoztatásakor végzendő művelet**: • **Maximális védelem** • **Ajánlott** A KSWS biztonsági szintjei megfelelnek a KES vizsgálati módjainak az alábbiak szerint: • Maximum protection – Maximális védelem • Recommended – Ajánlott • Maximum performance – Ajánlott

User permissions for application management

A Kaspersky Endpoint Security nem támogatja a felhasználói hozzáférési engedélyek hozzárendelését az alkalmazáskezelés és az alkalmazásszolgáltatás-kezelés esetében. A felhasználók és felhasználói csoportok hozzáférési beállításait alkalmazáskezelés esetében a Kaspersky Security Centerben konfigurálhatja.

User access permissions for Kaspersky Security Service management

A Kaspersky Endpoint Security nem támogatja a felhasználói hozzáférési engedélyek hozzárendelését az alkalmazáskezelés és az alkalmazásszolgáltatás-kezelés esetében. A felhasználók és felhasználói csoportok hozzáférési beállításait alkalmazáskezelés esetében a Kaspersky Security Centerben konfigurálhatja.

Storages

A KSWS tárhelybeállításai átkerülnek az **Általános beállítások** szakasz **Jelentések és tároló** alszakaszába, illetve a **Fenyegetések elleni alapvető védelem** szakasz **Hálózati védelem** alszakaszába.

A Storage beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Backup folder	*(nincs áttelepítés)* A Kaspersky Endpoint Security a fájlok biztonsági másolatait a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappába menti.
Maximum Backup size (MB)	**A biztonsági mentés méretének korlátozása N MB** értékre (**Általános beállítások** → **Jelentések és tároló** szakasz)
Threshold value for space available (MB)	*(nincs áttelepítés)* A Kaspersky Endpoint Security naplózza *A karanténként szolgáló tárhely majdnem megtelt* eseményt az 50%-os küszöbérték elérésekor.
Target folder for restoring objects	*(nincs áttelepítés)* A Kaspersky Endpoint Security visszaállítja a fájlokat az eredeti mappába.
Quarantine folder	*(nincs áttelepítés)* A Kaspersky Endpoint Security a fájlok biztonsági másolatait a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappába menti.
Maximum Quarantine size (MB)	*(nincs áttelepítés)* A Kaspersky Endpoint Security a biztonsági mentést használja a valószínűleg fertőzött objektumok tárolására. Az áttelepítés során a Kaspersky Endpoint Security figyelmen kívül hagyja a karanténbeállításokat.
Threshold value for space available (MB)	*(nincs áttelepítés)* A Kaspersky Endpoint Security a biztonsági mentést használja a valószínűleg fertőzött objektumok tárolására. Az áttelepítés során a Kaspersky Endpoint Security figyelmen kívül hagyja a karanténbeállításokat.
Target folder for restoring objects	*(nincs áttelepítés)* A Kaspersky Endpoint Security visszaállítja a fájlokat az eredeti mappába.
Unblock automatically in N	**Támadó eszközök blokkolása N percre** (**Fenyegetések elleni alapvető védelem** → **Hálózati védelem** szakasz)

Real-time server protection

Real-Time File Protection

A KSWS valós idejű fájlvédelmi beállításai átkerülnek a **Fenyegetések elleni alapvető védelem** szakasz **Fájlvédelem** alszakaszába.

Valós idejű fájlvédelem beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Vizsgálat módja**: • **Intelligens mód** • **Végrehajtáskor** • **Hozzáféréskor** • **Hozzáféréskor és módosításkor**
Deeper analysis of launching processes	*(nincs áttelepítés)* A Kaspersky Endpoint Security csak egy elemzési módot támogat, az Optimal módot.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Heurisztikus elemzés**: • **Egyszerű vizsgálat** • **Közepes vizsgálat** • **Alapos vizsgálat**
Apply Trusted Zone	*(nincs áttelepítés)* A Kaspersky Endpoint Security minden összetevőre alkalmazza a megbízható zónát. A kizárásokat a megbízható zóna beállításaiban konfigurálhatja.
Use KSN for protection	*(nincs áttelepítés)* A Kaspersky Endpoint Security a KSN-t használja az összes alkalmazásösszetevőhöz.
Block access to network shared resources for the hosts that show malicious activity	*(nincs áttelepítés)* A Kaspersky Endpoint Security alapértelmezés szerint blokkolja a rosszindulatú tevékenységet mutató gazdagépek hozzáférését a hálózati megosztott erőforrásokhoz.
Launch critical areas scan when active infection is detected	*(nincs áttelepítés)* A Kaspersky Endpoint Security aktív fertőzés észlelésekor nem indítja el a kritikus területek vizsgálatát.
Use Kaspersky Sandbox for protection	*(nincs áttelepítés)* Alapértelmezés szerint a Kaspersky Endpoint Security elküldi az objektumokat vizsgálatra a Kaspersky Sandboxba.
Protection scope	**Védelem hatóköre**
Schedule settings	*(nincs áttelepítés)* A Kaspersky Endpoint Security a saját ütemezését használja a Fájl védelem szüneteltetésére.

KSN Usage

A Kaspersky Security Network KSWS-beállításai átkerülnek a **Fenyegetések elleni fejlett védelem** szakasz **Kaspersky Security Network** alszakaszába.

Kaspersky Security Network beállítások

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Kaspersky Security Network nyilatkozat** A Kaspersky Endpoint Security kéri a Kaspersky Security Network nyilatkozat elfogadását az alkalmazás telepítésekor, új házirend létrehozásakor, vagy a Kaspersky Security Network használatának engedélyezésekor.
Send data about scanned files	*(nincs áttelepítés)* A Kaspersky Endpoint Security automatikusan adatokat küld a vizsgált fájlokról, ha a KSN engedélyezve van.
Send data about requested URLs	*(nincs áttelepítés)* A Kaspersky Endpoint Security automatikusan adatokat küld a kért URL-ekről, ha a KSN engedélyezve van.
Send Kaspersky Security Network statistics	**Kiterjesztett KSN mód engedélyezése**
Accept the terms of the Kaspersky Managed Protection Statement	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem tartalmazza a KMP szolgáltatást.
Action to perform on KSN untrusted objects	*(nincs áttelepítés)* A fenyegetés észlelésekor végrehajtandó műveletet a Védelmi összetevő beállításaiban és a Vizsgálati feladat beállításaiban konfigurálhatja.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(nincs áttelepítés)* A nagyméretű fájlok vizsgálatára vonatkozó korlátozásokat a Védelmi összetevő beállításaiban és a Vizsgálati feladat beállításaiban konfigurálhatja.
Use Kaspersky Security Center as KSN Proxy	**Adminisztrációs kiszolgáló használata KSN-proxykiszolgálóként**
Schedule settings	*(nincs áttelepítés)* Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

Traffic Security

A KSWS adatforgalom-biztonsági beállításai átkerülnek a **Fenyegetések elleni alapvető védelem** szakasz **Web védelem** és **Levelezés védelem** alszakaszába; a **Biztonsági felügyelet** szakasz **Webfelügyelő** alszakaszába; és az **Általános beállítások** szakasz **Hálózati beállítások** alszakaszába.

A Traffic Security beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Apply URL-based rules	**Webfelügyelő** (**Webfelügyelő** alszakasz) Az URL-alapú szabályok külön szabályokba kerülnek a Kaspersky Endpoint Security alkalmazásban.
Apply certificate-based rules	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem támogatja a tanúsítvány alapú szabályokat.
Apply rules for web traffic category control	**Webfelügyelő** (**Webfelügyelő** alszakasz) A webes forgalom kategóriáinak szabályozására vonatkozó blokkolási szabályok egyetlen blokkolási szabályba kerülnek a Kaspersky Endpoint Security alkalmazásban. A Kaspersky Endpoint Security figyelmen kívül hagyja a kategóriák szabályozására vonatkozó szabályokat. Az alábbiakban találja a KSWS és a KES kategóriáinak megfeleltetését.
Allow access if the web page can not be categorized	*(nincs áttelepítés)* A Kaspersky Endpoint Security engedélyezi a hozzáférést, ha a weboldal nem kategorizálható.
Allow access to legitimate web resources that can be used to damage a protected device	*(nincs áttelepítés)* A Kaspersky Endpoint Security engedélyezi a hozzáférést olyan legitim webes erőforrásokhoz, amelyek felhasználhatók a védett eszköz károsítására.
Allow access to legitimate advertisement	*(nincs áttelepítés)* A legitim hirdetésekhez való hozzáférést a Webfelügyelő beállításaiban a *Reklámcsíkok* webes erőforrás kategóriájával kezelheti.

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(nincs áttelepítés)* A Kaspersky Endpoint Security csak a Driver Interceptor módot támogatja.
ICAP-service connection settings	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem támogatja az ICAP hálózati tárolóvédelmet.
Check safe connections through the HTTPS protocol	**Titkosított kapcsolatok vizsgálata/Mindig vizsgálja a titkosított kapcsolatokat** mód (**Hálózati beállítások** alrész)
Use TLS protocol version	*(nincs áttelepítés)* A Kaspersky Endpoint Security a következő protokollokon keresztül továbbított titkosított hálózati forgalmat vizsgálja: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Ezenkívül letilthatja az SSL 2.0 kapcsolatokat a titkosított kapcsolatok vizsgálati beállításaiban.
Do not trust web-servers with invalid certificate	**Cím** (**Hálózati beállítások** alszakasz)
Intercept ports (Interception area)	**Figyelt portok** (**Hálózati beállítások** alszakasz) A migrálás során a KES törli **A Kaspersky által javasolt alkalmazások összes portjának figyelése** és **A megadott alkalmazások figyelése minden porton** jelölőnégyzetek kijelölését.
Exclude ports (Interception area)	*(nincs áttelepítés)*
Exclude IP addresses (Interception area)	**Megbízható címek konfigurálása** (**Hálózati beállítások** alszakasz)
Exclude processes (Interception area)	**Megbízható alkalmazások konfigurálása** (**Hálózati beállítások** alszakasz) Migrálás során a KES a megbízható alkalmazás következő beállításait konfigurálja: • A **Ne vizsgálja a hálózati forgalmat** jelölőnégyzet be van jelölve. A KES nem vizsgálja a távoli IP-címek és a portok hálózati forgalmát. • A rendszer törli a megbízható alkalmazások beállításainak többi jelölőnégyzetét.
Security port	*(nincs áttelepítés)*
Use malicious URL database to scan web links	**A webcím ellenőrzése a rosszindulatú webcímek adatbázisában** (**Web védelem** alszakasz)
Use anti-phishing database to scan web pages	**A webcím ellenőrzése az adathalász webcímek adatbázisában** (**Web védelem** alszakasz)
Use KSN for protection	*(nincs áttelepítés)* A Kaspersky Endpoint Security a KSN-t használja az összes alkalmazásösszetevőhöz.
Use Trusted Zone	*(nincs áttelepítés)* A Kaspersky Endpoint Security minden összetevőre alkalmazza a megbízható zónát. A kizárásokat a megbízható zóna beállításaiban konfigurálhatja.
Use heuristic analyzer	**Heurisztikus elemzés használata** (**Web védelem** és **Levelezés védelem** alszakaszok)
Security level	*(nincs áttelepítés)* A Kaspersky Endpoint Security saját biztonsági szinttel rendelkezik a Web védelem és a Levelezés védelem összetevőkhöz. Alapértelmezés szerint a Kaspersky Endpoint Security beállítja az ajánlott biztonsági szintet.
Enable mail threat protection	**Levelezés védelem** (**Levelezés védelem** alszakasz) **Microsoft Outlook-bővítmény csatlakoztatása** **Csak bejövő üzenetek** (Védelem hatóköre) **Vizsgálat fogadáskor** (E-mail védelem)
Schedule settings	*(nincs áttelepítés)* Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

Exploit Prevention

A KSWS „Biztonsági rések kihasználásának megelőzése” beállításai átkerülnek a **Fenyegetések elleni fejlett védelem** szakasz **Biztonsági rések kihasználásának megelőzése** alszakaszba.

Exploit Prevention beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Sebezhetőség kihasználásának észlelésekor**: • **Blokkolás** • **Értesítés**
Notify about abused processes via Terminal Service	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem támogatja a terminálszolgáltatásokat.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(nincs áttelepítés)* A Kaspersky Endpoint Security folyamatosan végzi a sebezhető folyamatok kihasználásának megakadályozását.
Protected processes	**Rendszerfolyamatok memóriavédelmének engedélyezése** A Kaspersky Endpoint Security nem támogatja a védett folyamatok kiválasztását. Csak a rendszerfolyamatok memóriavédelmét engedélyezheti.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(nincs áttelepítés)* A Kaspersky Endpoint Security alkalmazza a biztonsági rések kihasználásának összes elérhető megelőzési technikáját.

Network Threat Protection

A KSWS Hálózati védelem beállításai átkerülnek a **Fenyegetések elleni alapvető védelem** szakasz **Hálózati védelem** alszakaszába.

A Hálózati védelem beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Hálózati védelem** Ha az **Pass-through** módot kiválasztották, a Hálózati védelem ki van kapcsolva. Ha az **Only inform about network attacks** vagy **Block connections when attack is detected** mód van kiválasztva, a Hálózati védelem engedélyezve van. A Kaspersky Endpoint Security mindig **Block connections when attack is detected** módban működik.
Do not stop traffic analysis when the task is not running	*(nincs áttelepítés)* A Kaspersky Endpoint Security folyamatosan elemzi a forgalmat, ha az összetevő engedélyezve van.
Do not control excluded IP addresses	**Kizárások**
Schedule settings	*(nincs áttelepítés)* Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

Script Monitoring

A Kaspersky Endpoint Security nem támogatja a Script Monitoring összetevőt. A parancsfájlok figyelését más összetevők, például az AMSI védelem kezeli.

Website categories

A Kaspersky Endpoint Security nem támogatja a Kaspersky Security for Windows Server összes kategóriáját. A Kaspersky Endpoint Securitybe a nem létező kategóriák nem kerülnek áttelepítésre. Ezért a nem támogatott kategóriájú webes erőforrás besorolási szabályai nem kerülnek áttelepítésre.

Webhelykategóriák

A Kaspersky Security for Windows Server kategóriái	A Kaspersky Endpoint Security for Windows kategóriái
Wargaming	Videojátékok
Abortion	*(nincs áttelepítés)*

A Kaspersky Security for Windows Server kategóriái	A Kaspersky Endpoint Security for Windows kategóriái
Lotteries (extended)	Szerencsejáték, lottó, sorsolás
Alcohol	Alkohol, dohány, kábítószerek
Anonymous proxy servers	Anonimizálók
Anorexia	*(nincs áttelepítés)*
Rentals for real estate	*(nincs áttelepítés)*
Audio, video and software	Szoftver, hang, videó
Banks	Bankok
Blogs	Blogok
Military	Fegyverek, robbanóanyagok, hadviselés
For children	*(nincs áttelepítés)*
Discrimination	Erőszak, intolerancia
Home and family	*(nincs áttelepítés)*
Hosting and domain services	Hálózati kommunikáció
Pets and animals	*(nincs áttelepítés)*
Law and politics	Helyi törvények által tiltott
Restricted by Roskomnadzor (RF)	Tiltva az Orosz Föderáció törvényei szerint
Restricted by Federal Law 436 (RF)	Tiltva az Orosz Föderáció törvényei szerint
Restricted by RF legislation	Tiltva az Orosz Föderáció törvényei szerint
Restricted by global legislation	Helyi törvények által tiltott
Adult dating	Csak felnőtteknek szóló tartalom
Internet services	*(nincs áttelepítés)*
Sex shops	Csak felnőtteknek szóló tartalom
Information technologies	*(nincs áttelepítés)*
Casinos, card games	Szerencsejáték, lottó, sorsolás
Books and writing	*(nincs áttelepítés)*
Computer games	Videojátékok
Health and beauty	*(nincs áttelepítés)*
Culture and society	*(nincs áttelepítés)*
LGBT	Csak felnőtteknek szóló tartalom
Lotteries	Szerencsejáték, lottó, sorsolás
Medicine	*(nincs áttelepítés)*
Fashion	*(nincs áttelepítés)*
Music	*(nincs áttelepítés)*
Drugs	Alkohol, dohány, kábítószerek
Violence	Erőszak, intolerancia
Discontent	*(nincs áttelepítés)*
Illegal drugs	Alkohol, dohány, kábítószerek
Hate and discrimination	Erőszak, intolerancia
Obscene vocabulary	Durva nyelvezet, obszcenitás
Lingerie	Csak felnőtteknek szóló tartalom
News	Hírmédia

A Kaspersky Security for Windows Server kategóriái	A Kaspersky Endpoint Security for Windows kategóriái
Nudism	Csak felnőtteknek szóló tartalom
Education	*(nincs áttelepítés)*
Online shopping	Online üzletek
All communication media	Hálózati kommunikáció
Payment by credit cards	Fizetési rendszerek
Online shopping (own payment system)	Online üzletek
Online encyclopedias	*(nincs áttelepítés)*
Online banking	Bankok
Weapons	Fegyverek, robbanóanyagok, hadviselés
Fishing and hunting	*(nincs áttelepítés)*
Payment systems	Fizetési rendszerek
Job search	Álláskeresés
Search engines	*(nincs áttelepítés)*
Police decision (JP)	Tiltva a japán hatóságok által
Trusted by KPSN	*(nincs áttelepítés)*
Untrusted by KPSN	*(nincs áttelepítés)*
Porn	Csak felnőtteknek szóló tartalom
Media hosting and streaming	Hírmédia
Web Mail	Webalapú e-mail
Traveling	*(nincs áttelepítés)*
TV and radio	Hírmédia
Teasers and ads services	Reklámcsíkok
Religion	Vallások, vallási szervezetek
Restaurants, cafe and food	*(nincs áttelepítés)*
Dating sites	Társkereső webhelyek
Sex education	Csak felnőtteknek szóló tartalom
Social networks	Közösségi hálózatok
Sport	*(nincs áttelepítés)*
Betting	Szerencsejáték, lottó, sorsolás
Suicide	Erőszak, intolerancia
Tobacco	Alkohol, dohány, kábítószerek
Torrents	Torrentek
Mentioned in Federal list of extremists (RF)	Tiltva az Orosz Föderáció törvényei szerint
File sharing	Fájlmegosztás
Pharmacy	*(nincs áttelepítés)*
Hobby and entertainment	*(nincs áttelepítés)*
Chats and forums	Csevegőprogramok, fórumok, IM
Schools and universities pages	*(nincs áttelepítés)*
Astrology and esoterica	*(nincs áttelepítés)*
Extremism and racism	Erőszak, intolerancia
E-commerce	Online üzletek

A Kaspersky Security for Windows Server kategóriái	A Kaspersky Endpoint Security for Windows kategóriái
Erotic	Csak felnőtteknek szóló tartalom
Humor	*(nincs áttelepítés)*

Local activity control

Applications Launch Control

A KSWS Alkalmazásfelügyelő beállításai átkerülnek a **Biztonsági felügyelet** szakasz **Alkalmazásfelügyelő** alszakaszába.

Az Alkalmazások indításvezérlése beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Operation mode: • **Statistics only** • **Active**	**Művelet** (Alkalmazásfelügyelő): • **Tesztszabályok**. • **Szabályok alkalmazása**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(nincs áttelepítés)* A Kaspersky Endpoint Security minden alkalommal megvizsgálja az alkalmazást, amikor megkísérel futni.
Deny the command interpreters launch with no command to execute	*(nincs áttelepítés)* A Kaspersky Endpoint Security lehetővé teszi a parancsértelmezők futtatását, ha azokat az Alkalmazásfelügyelő nem tiltja.
Rules	**Alkalmazásfelügyelői szabályok** *(korlátozásokkal támogatott)* A Kaspersky Endpoint Security 11.11.0 támogatja az Alkalmazásindítás-vezérlési szabályok migrálását. Az Alkalmazásindítás-vezérlési szabályok migrálási funkciójára bizonyos korlátozások vonatkoznak. Alapértelmezés szerint a KSWS Alkalmazásindítás-vezérlés két szabályt tartalmaz: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Ha legalább az egyik KSWS-szabály **Allow** típusú, a migrálás során a KES létrehoz egy új, **Applications with trusted root certificates** nevű engedélyezési szabályt. Vagyis a KES Alkalmazásfelügyelő egyetlen szabállyal engedélyezi a megbízható parancsfájlok, MSI-csomagok és végrehajtható fájlok futtatását. Ha mindkét forrás KSWS-szabály **Deny** típusú, a KES nem ad hozzá szabályokat a megbízható főtanúsítványokkal rendelkező alkalmazások kezeléséhez.
Apply rules to executable files	*(nincs áttelepítés)* A szabály alkalmazási hatóköre nem konfigurálható a KES Alkalmazásfelügyelő beállításaiban. A KES Alkalmazásfelügyelő minden típusú fájlra alkalmazza a szabályokat: a végrehajtható fájlokra, a parancsfájlokra és az MSI-csomagokra. Ha minden fájltípus szerepel a szabály alkalmazási hatókörében a KSWS-ben, a migrálás során a KES áthelyezi a KSWS-szabályokat. Ha egyes fájltípusok ki vannak zárva a szabály alkalmazási hatóköréből a KSWS-ben, a migrálás során a KES átviszi ugyan a KSWS-szabályokat, de a **Tesztszabályok** alkalmazásfelügyelői művelet lesz kiválasztva.
Monitor loading of DLL modules	**A DLL-modulok betöltésének figyelése (jelentősen megnöveli a rendszer terhelését)**
Apply rules to scripts and MSI packages	*(nincs áttelepítés)* A szabály alkalmazási hatóköre nem konfigurálható a KES Alkalmazásfelügyelő beállításaiban. A KES Alkalmazásfelügyelő minden típusú fájlra alkalmazza a szabályokat: a végrehajtható fájlokra, a parancsfájlokra és az MSI-csomagokra. Ha minden fájltípus szerepel a szabály alkalmazási hatókörében a KSWS-ben, a migrálás során a KES áthelyezi a KSWS-szabályokat. Ha egyes fájltípusok ki vannak zárva a szabály alkalmazási hatóköréből a KSWS-ben, a migrálás során a KES átviszi ugyan a KSWS-szabályokat, de a **Tesztszabályok** alkalmazásfelügyelői művelet lesz kiválasztva.
Deny applications untrusted by KSN	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem veszi figyelembe az alkalmazások megbízhatóságát, és az alkalmazások futtatását a szabályoknak megfelelően engedélyezi vagy tiltja.
Allow applications trusted by KSN	A migrálás során a KES új engedélyezési szabályt ad hozzá. Az **Other Software\Applications, trusted according to reputation in KSN** KL kategória van meghatározva a szabály kiváltó feltételeként.

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Users and / or user groups allowed to run applications trusted by KSN	A **Felhasználók és jogaik** egy olyan alkalmazásfelügyelői engedélyezési szabályban, amely tartalmazza a **Other Software\Applications, trusted according to reputation in KSN** KL-kategóriát.
Automatically allow software distribution via applications and packages listed	A KSWS-ben és a KES-ben máshogy működik a szoftverterjesztés felügyelete. A migrálás során a KES új engedélyezési szabályokat ad hozzá azokhoz az alkalmazásokhoz, amelyekhez engedélyezve van az automatikus szoftverterjesztés. A fájl kivonata van meghatározva a szabály kiváltó feltételeként.
Always allow software distribution via Windows Installer	A KSWS-ben és a KES-ben máshogy működik a szoftverterjesztés felügyelete. A migrálás során a KES új engedélyezési szabályokat ad hozzá azokhoz az alkalmazásokhoz, amelyekhez engedélyezve van az automatikus szoftverterjesztés (**Software distribution applications and packages allowed**). A fájl kivonata van meghatározva a szabály kiváltó feltételeként. A fióktulajdonságokban a **Megbízható frissítéstelepítők** jelölőnégyzet be van jelölve.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(nincs áttelepítés)*
Software distribution applications and packages allowed	A KSWS-ben és a KES-ben máshogy működik a szoftverterjesztés felügyelete. A migrálás során a KES új engedélyezési szabályokat ad hozzá azokhoz az alkalmazásokhoz, amelyekhez engedélyezve van az automatikus szoftverterjesztés. A fájl kivonata van meghatározva a szabály kiváltó feltételeként. A fióktulajdonságokban a **Megbízható frissítéstelepítők** jelölőnégyzet be van jelölve.
Schedule settings	*(nincs áttelepítés)* Ha ütemezés van konfigurálva az összetevőhöz a KSWS beállításaiban, az Alkalmazásfelügyelő összetevő engedélyezve van a migráláskor. Ha nincs konfigurálva ütemezés az összetevőhöz a KSWS beállításaiban, az Alkalmazásfelügyelő le van tiltva a migráláskor. Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

Device Control

A KSWS Eszközfelügyelő beállításai átkerülnek a **Biztonsági felügyelet** szakasz **Eszközfelügyelő** alszakaszába.

Az Eszközfelügyelő beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Operation mode: • **Active** • **Statistics only**	*(nincs áttelepítés)* Az Alkalmazásfelügyelő *Active* módban működik. Az eszközcsatlakozási statisztikákat a felülvizsgálat folyamatosan szolgáltatja.
Allow using all external devices when the Device Control task is not running	*(nincs áttelepítés)* Az Eszközfelügyelő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security fut.
Device Control rules	**Megbízható eszközök** Az áttelepítés során a Kaspersky Endpoint Security figyelmen kívül hagyja a letiltott KSWS szabályokat.
Schedule settings	*(nincs áttelepítés)* Kaspersky Endpoint Security saját ütemezést használ bizonyos eszköztípusokhoz való hozzáférés esetén.

Network-Attached Storages Protection

RPC Network Storage Protection

A Kaspersky Endpoint Security nem támogatja a hálózati tárolóeszköz védelmi összetevőket. Ha szüksége van ezekre az összetevőkre, folytathatja a Kaspersky Security for Windows Server használatát.

ICAP Network Storage Protection

A Kaspersky Endpoint Security nem támogatja a hálózati tárolóeszköz védelmi összetevőket. Ha szüksége van ezekre az összetevőkre, folytathatja a Kaspersky Security for Windows Server használatát.

Anti-Cryptor for NetApp

A Kaspersky Endpoint Security nem támogatja az Anti-Cryptor for NetApp szolgáltatást. Az Anti-Cryptor funkciót más alkalmazásösszetevők, például a Viselkedésészlelés biztosítják.

Network activity control

Firewall Management

A Kaspersky Endpoint Security nem támogatja az KSWS Tűzfal Kezelését. A KSWS Tűzfal funkciókat a rendszer-szintű Tűzfal látja el. Áttelepítést követően beállíthatja a Kaspersky Endpoint Security Tűzfal beállításait.

Anti-Cryptor

A hálózat Anti-Cryptor beállításai átkerülnek a **Fenyegetések elleni fejlett védelem** szakasz **Viselkedésészlelés** alszakaszába.

Anti-Cryptor beállításai

KSWS beállításai	KES beállításai
Operation mode: • **Statistics only** • **Active**	**A megosztott mappák külső titkosításának észlelése esetén**: • **Értesítés** • **Blokkolás**
Heuristic analyzer	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem használ heurisztikus elemzést a Viselkedésészleléshez.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(nincs áttelepítés)* A Kaspersky Endpoint Security megakadályozza a védett számítógép összes megosztott hálózati mappájának titkosítását.
Exclusions	*(nincs áttelepítés)* A Kaspersky Endpoint Security saját kizárásokkal rendelkezik a Viselkedésészlelés összetevőhöz. Áttelepítés után manuálisan hozzáadhat kizárásokat.
Schedule settings	*(nincs áttelepítés)* Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

System Inspection

File Integrity Monitor

A rendszer a KSWS-ből a **Biztonsági felügyelet** szakasz **Rendszerintegritás-figyelő** alszakaszába migrálja a Rendszerintegritás-figyelő beállításait.

Fájlintegritás-figyelő beállításai

KSWS beállításai	KES beállításai
Log information about file operations that appear during the monitor interruption period	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem naplózza a monitorozás megszakítási időszaka alatt végzett fájlműveletek eseményeit.
Block attempts to compromise the USN log	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem blokkolja az USN-napló feltörésére irányuló kísérleteket.
Monitoring scope	**Figyelési hatókör** → **Fájl** *(korlátozásokkal támogatott)* A rendszer nem migrálja a KES-be a letiltott monitorozási hatókörök rekordjait. A Kaspersky Endpoint Security csak engedélyezett rekordokat ad a monitorozási hatókörhöz.
Trusted users	**Megbízható felhasználók és/vagy felhasználói csoportok**
File operation markers	**Fájlműveleti jelölők**
Calculate checksum for the file if possible	**Kivonatolás**
Exclusions	**Kizárások** → **Fájl**

Log Inspection

A KSWS naplóvizsgálati beállításai átkerülnek a **Biztonsági felügyelet** szakasz **Naplóvizsgálat** alszakaszába.

Naplóvizsgálat beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Apply custom rules for log inspection	*(nincs áttelepítés)* A Kaspersky Endpoint Security alkalmazza az összes engedélyezett egyéni szabályt.
Custom rules	**Egyéni szabályok** Az előre definiált **A service was installed in the system (for Server 2003 OS)** szabály nem kerül át a KES-be.
Apply predefined rules for log inspection	*(nincs áttelepítés)* A Kaspersky Endpoint Security alkalmazza az összes engedélyezett előre definiált szabályt.
Predefined rules	**Előre definiált szabályok**
Password brute-force detection	**Találgatásos támadás észlelése**
Network logon detection	**Hálózati bejelentkezés észlelése**
Exclusions (IP addresses)	**Kizárások** (IP-címek)
Exclusions (users)	**Kizárások** (felhasználók)
Schedule settings	*(nincs áttelepítés)* Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

Logs and notifications

Task logs

A KSWS-naplók beállításai átkerülnek az **Általános beállítások** szakasz **Felület** és **Jelentések és tároló** alszakaszába.

Naplóbeállítások

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Event logging	**Értesítések** (**Felület** alszakasz)
Logs folder	*(nincs áttelepítés)* A Kaspersky Endpoint Security a jelentéseket a `C:\ProgramData\Kaspersky Lab\KES.14.1\Report` mappába menti.
Remove task logs older than N day(s)	*(nincs áttelepítés)* A KES jelentések tárolási idejét az **Általános beállítások**, **Jelentések és tároló** menüpontok alatt állíthatja be.
Remove from the audit log events N day(s)	*(nincs áttelepítés)* A Kaspersky Endpoint Security jelentések tárolására vonatkozó korlátozásokat alkalmaz minden jelentésre, beleértve a rendszernaplózási jelentéseket is.
Integration with SIEM	*(nincs áttelepítés)* A SIEM integrációt a Kaspersky Security Centerben konfigurálhatja.

Event notifications

A KSWS értesítési beállításai átkerülnek az **Általános beállítások** szakasz **Felület** alszakaszába.

Értesítési beállítások

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Notifications	**Értesítések**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem támogatja az értesítés szövegének módosítását. A Kaspersky Endpoint Security szabványos értesítéseket jelenít meg.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Csak az e-mailes értesítési beállítások kerülnek át a Kaspersky Endpoint Security szolgáltatásba – **E-mail értesítési beállítások** (**Értesítések** blokkban). A rendszergazdák értesítésének egyéb módjai nem támogatottak.
Application database is out of date	**Az „Adatbázisok nem naprakészek” értesítés küldése, ha az adatbázisok nem frissültek**
Application database is extremely out of date	**Az „Adatbázisok messze nem naprakészek” értesítés küldése, ha az adatbázisok nem frissültek**
Critical areas scan has not been performed for a long time	*(nincs áttelepítés)* A Kaspersky Endpoint Security három nap elteltével egy elmulasztott Kritikus területek vizsgálata eseményt generál.

Interaction with Administration Server

A KSWS felügyeleti kiszolgálóra vonatkozó interakciós beállításai átkerülnek az **Általános beállítások** szakasz **Jelentések és tároló** alszakaszába.

Felügyeleti kiszolgáló interakciós beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Quarantined files	**Fájlok karanténba helyezése**
Backed up files	**Fájlok biztonsági mentése**
Blocked hosts	*(nincs áttelepítés)* A Kaspersky Endpoint Security automatikusan adatokat küld a blokkolt gazdagépekről.

Tasks

Activating the application

A Kaspersky Endpoint Security nem támogatja az *Application activation* feladatot (KSWS). Létrehozhat egy *Kulcs hozzáadása* feladatot (KES), és hozzáadhat egy licenckulcsot a Telepítőcsomaghoz, vagy engedélyezheti a licenckulcsok automatikus kiosztását.

Copying Updates

A *Copying Updates* feladatbeállításai (KSWS) átkerülnek az *Adatbázisok és alkalmazásmodulok frissítése* feladatba (KES).

Frissítések másolása feladat beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Frissítésforrás**: • **Kaspersky Security Center** • **Kaspersky frissítési kiszolgálók** • **Felhasználó által megadva**
Use Kaspersky update servers if specified servers are not available	*(nincs áttelepítés)* A Kaspersky Endpoint Security lehetővé teszi több frissítési forrás kiválasztását, beleértve a Kaspersky frissítési kiszolgálóit is. Ha az első frissítési forrás nem érhető el, a Kaspersky Endpoint Security lehetővé teszi a frissítések letöltését a listában szereplő más forrásokból is.
Use proxy server settings to connect to Kaspersky update servers	*(nincs áttelepítés)* A Kaspersky Endpoint Security az összes összetevőnél a proxykiszolgálót használja. A proxykiszolgálói kapcsolatot az alkalmazás hálózati beállításaiban konfigurálhatja.
Use proxy server settings to connect to other servers	*(nincs áttelepítés)* A Kaspersky Endpoint Security az összes összetevőnél a proxykiszolgálót használja. A proxykiszolgálói kapcsolatot az alkalmazás hálózati beállításaiban konfigurálhatja.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(nincs áttelepítés)* A Kaspersky Endpoint Security egyetlen csomagként másolja az adatbázis-frissítéseket és az alkalmazásmodulok kritikus frissítéseit.
Folder for local storage of copied updates	**Frissítések másolása mappába**

Baseline File Integrity Monitor

A *Baseline File Integrity Monitor* feladatbeállításai (KSWS) átkerülnek a *Rendszerintegritás-ellenőrzés* feladatba és a házirend **Biztonsági felügyelet** szakaszának **Rendszerintegritás-figyelés** alszakaszába.

A Fájlintegritás-figyelő alapszintű feladatbeállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Hash calculation algorithm: • **MD5** • **SHA256**	*(nincs áttelepítés)* A Kaspersky Endpoint Security az SHA256 algoritmust használja az ellenőrzőösszeg kiszámításához.
Scan scope	**Figyelési hatókör** (**Rendszerintegritás-figyelés** alszakasz)

Database Update

A *Database Update* feladatbeállításai (KSWS) átkerülnek az *Adatbázisok és alkalmazásmodulok frissítése* feladatba (KES).

Adatbázis-frissítési feladat beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Frissítésforrás**: • **Kaspersky Security Center** • **Kaspersky frissítési kiszolgálók** • **Felhasználó által megadva**
Use Kaspersky update servers if specified servers are not available	*(nincs áttelepítés)* A Kaspersky Endpoint Security lehetővé teszi több frissítési forrás kiválasztását, beleértve a Kaspersky frissítési kiszolgálóit is. Ha az első frissítési forrás nem érhető el, a Kaspersky Endpoint Security lehetővé teszi a frissítések letöltését a listában szereplő más forrásokból is.
Use proxy server settings to connect to Kaspersky update servers	*(nincs áttelepítés)* A Kaspersky Endpoint Security az összes összetevőnél a proxykiszolgálót használja. A proxykiszolgálói kapcsolatot az alkalmazás hálózati beállításaiban konfigurálhatja.
Use proxy server settings to connect to other servers	*(nincs áttelepítés)* A Kaspersky Endpoint Security az összes összetevőnél a proxykiszolgálót használja. A proxykiszolgálói kapcsolatot az alkalmazás hálózati beállításaiban konfigurálhatja.
Lower the load on the disk I/O	*(nincs áttelepítés)*

Software modules updates

A *Software Modules Update* feladatbeállításai (KSWS) átkerülnek az *Adatbázisok és alkalmazásmodulok frissítése* feladatba (KES).

Szoftvermodulok frissítése feladat beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Frissítésforrás**: • **Kaspersky Security Center** • **Kaspersky frissítési kiszolgálók** • **Felhasználó által megadva**
Use Kaspersky update servers if specified servers are not available	*(nincs áttelepítés)* A Kaspersky Endpoint Security lehetővé teszi több frissítési forrás kiválasztását, beleértve a Kaspersky frissítési kiszolgálóit is. Ha az első frissítési forrás nem érhető el, a Kaspersky Endpoint Security lehetővé teszi a frissítések letöltését a listában szereplő más forrásokból is.
Use proxy server settings to connect to Kaspersky update servers	*(nincs áttelepítés)* A Kaspersky Endpoint Security az összes összetevőnél a proxykiszolgálót használja. A proxykiszolgálói kapcsolatot az alkalmazás hálózati beállításaiban konfigurálhatja.
Use proxy server settings to connect to other servers	*(nincs áttelepítés)* A Kaspersky Endpoint Security az összes összetevőnél a proxykiszolgálót használja. A proxykiszolgálói kapcsolatot az alkalmazás hálózati beállításaiban konfigurálhatja.
Copy and install critical software modules updates	**Kritikus és jóváhagyott frissítések telepítése**
Only check for critical software updates available	*(nincs áttelepítés)* A Kaspersky Endpoint Security folyamatosan ellenőrzi az alkalmazás modulok kritikus frissítéseinek elérhetőségét.
Allow operating system restart	*(nincs áttelepítés)* A Kaspersky Endpoint Security engedélyt kér a felhasználótól a számítógép újraindításához.
Receive information about available scheduled software modules updates	*(nincs áttelepítés)* A Kaspersky Endpoint Security értesítéseket jelenít meg a szoftvermodulok frissítéseiről.

Rollback of Application Database Update

Az *Rollback of Application Database Update* feladatbeállításai (KSWS) átkerülnek a *Frissítés visszaállítása* feladatba (KES). Az új *Frissítés visszaállítása* feladat (KES) rendelkezik *Manually* állapottal a feladatkezdési ütemezéshez.

On-Demand Scan

Az *On-Demand Scan* feladatbeállításai (KSWS) átkerülnek a *Rosszindulatú programok keresése* feladatba (KES).

A vírusvizsgálati feladat beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Scan scope	**Vizsgálat hatóköre**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Biztonsági szint**: • **Magas** • **Ajánlott** • **Alacsony** A biztonsági szint beállításai eltérnek a KSWS-ben és a KES-ben.
Objects to scan: • **All objects** • **Objects scanned by format** • **Objects scanned according to list of extensions specified in anti-virus database** • **Objects scanned by specified list of extensions**	**Fájltípusok**: • **Minden fájl** • **Formátum alapján vizsgált fájlok** • **Kiterjesztés alapján vizsgált fájlok** A Kaspersky Endpoint Security nem teszi lehetővé egyéni kiterjesztési listák létrehozását. A Kaspersky Endpoint Security lecseréli az **Objects scanned by specified list of extensions** értéket a **Kiterjesztés alapján vizsgált fájlok** értékre.
Subfolders	**Almappákkal együtt**
Subfiles	*(nincs áttelepítés)*
Scan disk boot sectors and MBR	*(nincs áttelepítés)*
Scan alternate NTFS streams	*(nincs áttelepítés)*
Scan only new and modified files	**Csak új és módosult fájlok vizsgálata**
Scan of compound objects: • **All archives** • **All SFX archives** • **All email databases** • **All packed objects** • **All plain email** • **All embedded OLE objects**	**Összetett fájlok vizsgálata**: • **Archívumok vizsgálata**. • **Jelszóvédett archívumok vizsgálata**. • **Terjesztési csomagok vizsgálata**. • **E-mail formátumú fájlok vizsgálata**. • **Microsoft Office formátumú fájlok vizsgálata**.
Action to perform on infected and other objects: • **Disinfect** • **Disinfect. Remove if disinfection fails** • **Remove** • **Perform recommended action** • **Notify only**	**Művelet fenyegetés észlelésekor**: • **Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. • **Vírusmentesítés, értesítés, ha a vírusmentesítés nem sikerül**. • **Tájékoztatás**.
Action to perform on probably infected objects: • **Quarantine** • **Remove** • **Perform recommended action** • **Notify only**	*(nincs áttelepítés)* A Kaspersky Endpoint Security végrehajtja a műveletet, ha a rendszer fenyegetést észlel.
Perform actions depending on the type of object detected	*(nincs áttelepítés)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(nincs áttelepítés)*
Exclude files	*(nincs áttelepítés)* A Kaspersky Endpoint Security minden összetevőre alkalmazza a megbízható zónát. A kizárásokat a megbízható zóna beállításaiban konfigurálhatja.
Do not detect	*(nincs áttelepítés)*

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Stop scanning if it takes longer than N sec	**Fájlok kihagyása, ha a vizsgálat több mint: N mp**
Do not scan compound objects larger than N MB	**Ne csomagoljon ki nagy összetett fájlokat**
Use iSwift technology	**iSwift Technológia**
Use iChecker technology	**iChecker Technológia**
Action on the offline files: • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(nincs áttelepítés)* A Kaspersky Endpoint Security a kapcsolat nélküli fájlokat teljes egészében megvizsgálja.

Application Integrity Check

Az *Application Integrity Control* feladatbeállítások (KSWS) átkerülnek az *Alkalmazás integritás-ellenőrzése* feladatba (KES).

Rule Generator for Applications Launch Control

A Kaspersky Endpoint Security nem támogatja a *Applications Launch Control Generator* feladat. Szabályokat generálni az Alkalmazásfelügyelő beállításaiban tud.

Rule Generator for Device Control

A Kaspersky Endpoint Security nem támogatja a *Rule Generator for Device Control* feladat. Hozzáférési szabályokat generálhat Device Control beállításaiban.

A KSWS-összetevők áttelepítése

A helyi telepítést megelőzően a Kaspersky Endpoint Security ellenőrzi a számítógépen megtalálható Kaspersky alkalmazásokat. Ha a Kaspersky Security for Windows Server telepítve van a számítógépen, a KES észleli a telepített KSWS-összetevőket, és ugyanazokat az összetevőket választja ki a telepítéshez.

A KSWS-ben nem található KES összetevők telepítése a következőképpen történik:

- Az AMSI védelem, a Behatolásmegelőző rendszer és a Kármentesítő motor alapértelmezett beállításokkal települ.
- A BadUSB védelem, az Adaptív Anomáliafelügyelő, az Adattitkosítás és a Detection and Response összetevőket a rendszer mellőzi.

Távoli telepítés esetén a KES alkalmazás figyelmen kívül hagyja a telepített KSWS-összetevők készletét. A telepítő telepíti a telepítőcsomag tulajdonságaiban kiválasztott összetevőket. A Kaspersky Endpoint Security telepítése, valamint a házirendek és feladatok áttelepítése után a KES beállításai a KSWS beállításainak megfelelően kerülnek konfigurálásra.

A KSWS feladatok és házirendek áttelepítése

A KSWS szabályzat- és feladatbeállításait a következő módokon telepítheti át:

- A Házirendek és feladatok kötegelt átalakítása varázsló (a továbbiakban úgy is, mint Áttelepítési varázsló) használata.

  > A KSWS áttelepítési varázsló csak a felügyeleti konzolon (MMC) elérhető. A házirend- és feladatbeállítások nem telepíthetők át a Web Console-ban és a Cloud Console-ban.

  A kötegelt átalakítási varázsló eltérően működik a Kaspersky Security Center különböző verzióiban. Ajánlott frissíteni a megoldást a 14.2 vagy újabb verzióra. A Kaspersky Security Center ezen verziójában a Házirendek és feladatok kötegelt konvertálási varázslója lehetővé teszi a házirendek házirend helyett profilba történő áttelepítését. A Kaspersky Security Center ezen verziójában a Házirendek és feladatok kötegelt konvertálási varázslója a házirend-beállítások szélesebb körének áttelepítését is lehetővé teszi.

- A Kaspersky Endpoint Security for Windows új házirend varázslójának használata.

  Az új házirend varázsló lehetővé teszi KES-házirend létrehozását egy KSWS-házirend alapján.

A KSWS házirend-áttelepítési eljárásai eltérnek az Áttelepítési varázsló és az Új házirend varázsló használatakor.

Házirend és feladatok kötegelt konvertálási varázslója

Az áttelepítési varázsló a KES házirend-beállításai helyett a KSWS házirend-beállításait telepíti át a házirendprofilba. A *házirendprofil* olyan házirend-beállítások összessége, amely akkor aktiválódik a számítógépen, ha a számítógép megfelel a konfigurált aktiválási szabályoknak. Az `UpgradedFromKSWS` eszközcímke ki van választva a házirendprofil aktiválási feltételeként. A Kaspersky Security Center automatikusan hozzáadja az `UpgradedFromKSWS` címkét minden olyan számítógéphez, amelynél a távoli telepítési feladattal telepíti a KES-t a KSWS-re. Ha más telepítési módot választott, a címkét manuálisan is hozzárendelheti az eszközökhöz.

Címke hozzáadása eszközhöz:

1. Hozzon létre egy új címkét a kiszolgálókhoz — `UpgradedFromKSWS`.

   Az eszközcímkék létrehozásával kapcsolatos további tudnivalókért lásd a Kaspersky Security Center súgóját.

2. Hozzon létre egy új adminisztrációs csoportot a Kaspersky Security Center konzolon, és adjon hozzá kiszolgálókat, amelyekhez hozzá szeretné rendelni a címkét.

   A kijelölő eszközzel csoportosíthatja a kiszolgálókat. A kijelölések használatával kapcsolatos további tudnivalókért lásd a Kaspersky Security Center súgóját.

3. Válassza ki az adminisztrációs csoport összes kiszolgálóját a Kaspersky Security Center konzolon, nyissa meg a kiválasztott kiszolgálók tulajdonságait, és rendelje hozzá a címkét.

Ha több KSWS-házirendet helyez át, minden házirend egy átfogó házirenden belüli profillá alakul. Ha a KSWS-házirend már tartalmaz profilokat, akkor ezek a profilok is profilként lesznek áttelepítve. Ennek eredményeként egyetlen házirendet kap, amely az összes KSWS-házirendnek megfelelő profilokat tartalmaz.

A Házirendek és feladatok kötegelt átalakítása varázsló használata a KSWS-házirendek beállításainak áttelepítéséhez

1. A Felügyeleti konzolon válassza a Felügyeleti kiszolgáló lehetőséget, és kattintson a jobb gombbal a helyi menü megnyitásához.
2. Válassza az **All tasks** → **Policies and tasks batch conversion wizard** lehetőséget.

A Házirendek és feladatok kötegelt átalakítása varázsló elindul. Kövesse a varázsló utasításait.

1. lépés: Válassza ki azt az alkalmazást, amelyhez házirendeket és feladatokat kell konvertálnia

Ennél a lépésnél a Kaspersky Endpoint Security for Windows lehetőséget kell választania. Lépjen a következő lépésre.

2. lépés: Házirendek átalakítása

Az áttelepítési varázsló KSWS-házirendprofilokat hoz létre egy KES-házirendben. Válassza ki a házirendprofilokká átalakítani kívánt Kaspersky Security for Windows Server-házirendeket. Lépjen a következő lépésre.

Az áttelepítési varázsló ezután elkezdi a házirendek átalakítását. Az új házirendprofilok neve megegyezik az eredeti KSWS-házirendekkel.

3. lépés. A házirend-áttelepítési jelentés

Az áttelepítési varázsló házirend-áttelepítési jelentést hoz létre. A házirend-áttelepítési jelentés tartalmazza a házirendek átalakításának dátumát és időpontját, az eredeti KSWS-házirend nevét, a céloldali KES-házirend nevét és az új házirendprofil nevét.

4. lépés: Feladatok átalakítása

Az áttelepítési varázsló új feladatokat hoz létre a Kaspersky Endpoint Security for Windows számára. A feladatlistából válassza ki azokat a KSWS-feladatokat, amelyeket létre szeretne hozni a Kaspersky Endpoint Security termékhez. Az új feladatok neve *<KSWS-feladatnév> (átalakítva)* lesz. Lépjen a következő lépésre.

5. lépés. A varázsló befejezése

Lépjen ki a varázslóból. Ennek eredményeként a varázsló a következőket teszi:

- Új házirendprofilok kerülnek hozzáadásra a Kaspersky Endpoint Security házirendhez.

  A házirend tartalmazza a profilokat a Kaspersky Security for Windows Server beállításaival. Az új házirend *Active* állapotot kap. A varázsló változatlanul meghagyja a KSWS házirendeket.

- Létrehozza a Kaspersky Endpoint Security új feladatait.

  Az új feladatok a KSWS-feladatok másolatai. A varázsló változatlanul meghagyja a KSWS feladatokat.

A KSWS-beállításokkal rendelkező új házirendprofil neve *UpgradedFromKSWS – <A Kaspersky Security for Windows Server-házirend neve>* lesz. A profil tulajdonságainál az áttelepítési varázsló automatikusan kiválasztja az `UpgradedFromKSWS` eszközcímkét aktiválási feltételként. Így a házirendprofil beállításai automatikusan érvényesülnek a kiszolgálókon.

Varázsló házirend létrehozásához KSWS-házirend alapján

Amikor egy KES-házirendet KSWS-házirend alapján hoznak létre, a varázsló ennek megfelelően áthelyezi a beállításokat az új házirendbe. Vagyis egy KES-házirend egy KSWS-házirendnek felel meg. A varázsló nem alakítja át a házirendet profillá.

Az Új házirend varázsló használata a KSWS házirend-beállítások áttelepítéséhez

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol **Managed devices** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. Válassza ki a munkaterületen a **Policies** lapot.
4. Kattintson az **New policy** gombra.

   Elindul a Rendszabályvarázsló.
5. Kövesse a Rendszabályvarázsló utasításait.

1. lépés: A csoportházirend létrehozására szolgáló alkalmazás kiválasztása

Válassza ki a **Kaspersky Endpoint Security for Windows (14.1)** alkalmazást.

2. lépés: A csoportházirend elnevezése

Adjon meg egy nevet a csoportházirendnek, például *Az iroda házirendje*.

Tegyen jelölést a **Use policy settings for an earlier version of the application** jelölőnégyzetbe. Kattintson a **Browse** gombra, és válassza ki a KSWS-házirendet.

3. lépés. Részvétel a Kaspersky Security Networkben

Olvassa el és fogadja el a Kaspersky Security Network (KSN) nyilatkozatának feltételeit.

4. lépés: Az alkalmazás használati módjának kiválasztása számítógépeken

Válassza a **Normál mód a gazdagépek védelmére** opciót. A Kaspersky Endpoint Security közös házirendet biztosít minden alkalmazási módhoz és operációs rendszer típushoz.

Javasoljuk, hogy a különböző üzemmódokhoz és operációsrendszer-típusokhoz különböző házirendeket használjon.

5. lépés Importálási beállítások

Ez a lépés akkor érhető el, ha a szabályzat manuális konfigurációját választotta a 4. lépésben.

A Kaspersky Endpoint Security beállításai alapján szabályzatot hozhat létre egy CFG konfigurációs fájlból. Alkalmazás konfigurációs fájljának importálásakor nem minden szabályzati beállítás érhető el a varázsló számára. Például hiányoznak a szabályzati profilok az alkalmazás beállításaiból. Ha az összes beállítást és profilt át szeretné vinni a szabályzatba, importálhat egy másik szabályzatot egy KLP-fájlból.

Konfigurációs fájlok importálásakor a Kaspersky Endpoint Security nem továbbítja a kriptokonténer jelszavait. Ha a kiszolgálókhoz való csatlakozáskor kétirányú hitelesítést használ, akkor a kriptokonténer jelszavait újra meg kell adnia.

6–10. lépés. Szabályzati beállításainak konfigurálása

Ez a lépés akkor érhető el, ha a szabályzat manuális konfigurációját választotta a 4. lépésben.

Kövesse a szabályzati beállítások kezelésének lépéseit.

11. lépés. A megbízható zóna konfigurálása

Konfigurálja a megbízható zónát. Előre definiált vizsgálati kizárásokat és megbízható alkalmazásokat adhat hozzá. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon. Az előre definiált vizsgálati kizárások és a megbízható alkalmazások szintén segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Light Agent üzemmódban Citrix és VMware virtuális környezetekben.

12. lépés. A szabályzat állapotának kiválasztása

- **Active**. A következő szinkronizáció után a rendszabály aktív rendszabályként lesz használva a számítógépen.

  Az aktív rendszabály beállításai az ügyfélszámítógépekre vannak mentve a szinkronizáció alatt. Nem tud egyszerre több rendszabályt alkalmazni egy számítógépen, ezért egy csoportban csak egy rendszabály lehet aktív.

- **Inactive**. Biztonsági mentési rendszabály. Szükség esetén az inaktív rendszabály átváltható aktív állapotra.

  Korlátlan számú inaktív rendszabályt hozhat létre. Az inaktív rendszabály nincs hatással a hálózatban a számítógépen lévő alkalmazásbeállításokra. Az inaktív rendszabályok vészhelyzetek esetére készültek, például vírustámadásra. Ha a flash meghajtókon keresztül érkezik támadás, akkor aktiválhat egy rendszabályt, ami blokkolja a flash meghajtókhoz való hozzáférést. Ebben az esetben az aktív rendszabály inaktív lesz.

- **Out-of-office**. A rendszabály akkor lesz aktív, ha a számítógép elhagyja a szervezet hálózatának területét.

Lépjen ki a varázslóból.

Házirendek és feladatok további konfigurálása az áttelepítés után

A KSWS és a KES különböző összetevőkészletekkel és házirend-beállításokkal rendelkezik, ezért az áttelepítés után ellenőriznie kell, hogy a házirend-beállítások megfelelnek-e a vállalati biztonsági követelményeknek.

Ellenőrizze a következő alapvető házirend-beállításokat:

- Jelszóvédelem. A KSWS jelszóvédelmi beállításai nem kerülnek áttelepítésre. A Kaspersky Endpoint Security beépített Jelszóvédelem funkcióval rendelkezik. Ha szükséges, kapcsolja be a Jelszóvédelem funkciót, és állítson be jelszót.

- Megbízható zóna. A KSWS és a KES által az objektumok kiválasztására használt módszerek különböznek. Áttelepítéskor a KES támogatja az egyedi fájlokként vagy a fájlhoz/mappához vezető útvonalakként meghatározott kizárásokat. Ha a KSWS-ben a kizárások előre meghatározott területként vagy szkript URL-ként vannak konfigurálva, az ilyen kizárások nem kerülnek áttelepítésre. Az áttelepítés után ezeket a kizárásokat manuálisan kell hozzáadnia.

Annak érdekében, hogy a Kaspersky Endpoint Security megfelelően működjön a kiszolgálókon, ajánlatott a kiszolgáló működése szempontjából fontos fájlokat hozzáadni a megbízható zónához. SQL-kiszolgálók esetén MDF- és LDF-adatbázisfájlokat kell hozzáadnia. A Microsoft Exchange kiszolgálókhoz CHK-, EDB-, JRS-, LOG- és JSL-fájlokat kell hozzáadnia. Használhat maszkokat, pl. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon.

- Tűzfal. A KSWS Tűzfal funkciókat a rendszer-szintű Tűzfal látja el. A KES-ben egy külön összetevő felel a Tűzfal funkcióért. Áttelepítést követően beállíthatja a Kaspersky Endpoint Security Tűzfal beállításait.
- Kaspersky Security Network. A Kaspersky Endpoint Security nem támogatja a KSN konfigurálását az egyes összetevők esetében. A Kaspersky Endpoint Security a KSN-t használja az összes alkalmazásösszetevőhöz. A KSN használatához el kell fogadnia a Kaspersky Security Network nyilatkozat új feltételeit.
- Webfelügyelő. A webes forgalom kategóriáinak szabályozására vonatkozó blokkolási szabályok egyetlen blokkolási szabályba kerülnek a Kaspersky Endpoint Security alkalmazásban. A Kaspersky Endpoint Security figyelmen kívül hagyja a kategóriák szabályozására vonatkozó szabályokat. A Kaspersky Endpoint Security nem támogatja a Kaspersky Security for Windows Server összes kategóriáját. A Kaspersky Endpoint Securitybe a nem létező kategóriák nem kerülnek áttelepítésre. Ezért a nem támogatott kategóriájú webes erőforrás besorolási szabályai nem kerülnek áttelepítésre. Ha szükséges, adja hozzá a Webfelügyelő szabályait.
- Proxykiszolgáló. A proxykiszolgáló csatlakoztatási jelszava nem kerül áttelepítésre. Adja meg a proxykiszolgáló manuális csatlakoztatásához használandó jelszót.
- Az egyes összetevők ütemezése. A Kaspersky Endpoint Security nem támogatja ütemezések konfigurálását az egyes összetevők esetében. Az összetevők mindig be vannak kapcsolva, amikor a Kaspersky Endpoint Security működik.
- Összetevőkészlet. A Kaspersky Endpoint Security elérhető funkciói az operációs rendszer típusától, a munkaállomástól és a kiszolgálótól függenek. Például a titkosítási eszközök közül csak a BitLocker meghajtótitkosítás érhető el a kiszolgálókon.
- attribútum. A attribútum állapota nem kerül áttelepítésre. A attribútum az alapértelmezett értéket kapja. Alapértelmezés szerint az új házirendben szinte minden beállítás esetében tiltott a beállítások módosítása az alárendelt házirendekben és a helyi alkalmazásfelületen. Az attribútum a értékkel rendelkezik a **Managed Detection and Response (Industrial CyberSecurity)** szakaszban és a **Felhasználói támogatás** beállításcsoportban (**Felület** szakasz) található házirend-beállítások esetében. Szükség esetén konfigurálhatja a beállítások öröklését a fölérendelt házirendből.
- Munkavégzés az aktív fenyegetésekkel. A Fejlett vírusmentesítés másként működik munkaállomásokon és kiszolgálókon. A fejlett vírusmentesítést konfigurálhatja a *Kártevő vizsgálata* feladat beállításaiban és az alkalmazásbeállításokban.
- Az alkalmazás frissítése. A fontosabb frissítések és javítások újraindítás nélküli telepítéséhez módosítania kell az alkalmazás frissítési módját. Alapértelmezés szerint Az alkalmazás frissítéseinek telepítése újraindítás nélkül funkció le van tiltva.

- Kaspersky Endpoint Agent. A Kaspersky Endpoint Security a Managed Detection and Response megoldásokhoz készült beépített ügynökkel rendelkezik. Ha szükséges, helyezze át a Kaspersky Endpoint Agent házirendbeállításait a Kaspersky Endpoint Security házirendjébe.

- *Adatbázisok és alkalmazásmodulok frissítése* feladatok. Győződjön meg arról, hogy az *Adatbázisok és alkalmazásmodulok frissítése* feladat beállításai megfelelően lettek áttelepítve. A KSWS három feladata helyett a KES egyetlen KES-feladatot használ. Optimalizálhatja az *Adatbázisok és alkalmazásmodulok frissítése* feladatokat, és eltávolíthatja a felesleges feladatokat.

- Egyéb feladatok. Az Alkalmazásfelügyelő, az Eszközfelügyelő és a Fájlintegritás-figyelő összetevők eltérően működnek a KSWS-ben és a KES-ben. A KES nem használja a *Baseline File Integrity Monitor*, *Applications Launch Control Generator* és *Rule Generator for Device Control* feladatokat. Ezért e feladatok áttelepítése nem történik meg. Az áttelepítés után konfigurálhatja a Fájlintegritás-figyelő, az Alkalmazásfelügyelő és az Eszközfelügyelő összetevőket.

A KSWS megbízható zóna áttelepítése

A *megbízható zóna* olyan, a rendszergazda által beállított objektumok és alkalmazások listája, melyeket a Kaspersky Endpoint Security aktív módban nem figyel. A megbízható zónaobjektumokat a KSWS-ből a KES-be a *Házirendek és feladatok kötegelt átalakítása varázslóval* vagy a *KSWS-házirenden alapuló, új KES-házirend létrehozására szolgáló varázslóval* lehet áttelepíteni. A KSWS és a KES különböző összetevőkészletekkel és funkciókkal rendelkezik, ezért az áttelepítés után ellenőriznie kell, hogy a kizárások megfelelnek-e a vállalati biztonsági követelményeknek. A megbízható zónához tartozó kizárások hozzáadásának módszerei is eltérőek a KES és a KSWS esetében. Az áttelepítési varázsló nem rendelkezik az összes KSWS-kizárás áttelepítéséhez szükséges eszközökkel. Ez azt jelenti, hogy az áttelepítés után kézzel kell hozzáadni néhány KSWS-kizárást.

Annak érdekében, hogy a Kaspersky Endpoint Security megfelelően működjön a kiszolgálókon, ajánlatott a kiszolgáló működése szempontjából fontos fájlokat hozzáadni a megbízható zónához. SQL-kiszolgálók esetén MDF- és LDF-adatbázisfájlokat kell hozzáadnia. A Microsoft Exchange kiszolgálókhoz CHK-, EDB-, JRS-, LOG- és JSL-fájlokat kell hozzáadnia. Használhat maszkokat, pl. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon.

A KES és a KSWS megbízható zónák létrehozásának módszerei.

KSWS		KES
Object to scan		
• Predefined scope	*(nincs áttelepítés)*	
• Disk, folder or network location	→	**Fájl vagy mappa**
• File	→	**Fájl vagy mappa**
• Script file or web address	*(nincs áttelepítés)*	
Detected object	→	**Észlelt objektum típusa**
Trusted processes	→	**Megbízható alkalmazások**

A vizsgált objektumok áttelepítése

Azok a KSWS-kizárások, amelyek tulajdonságaiban a **Object to scan** módszer van kiválasztva, bizonyos korlátozásokkal átkerülnek azokba a KES-kizárásokba, amelyek tulajdonságaiban a **Fájl vagy mappa** módszer van kiválasztva. A kizárás áttelepítése az objektum kiválasztási módszerétől függ:

- Predefined scope – *nincs áttelepítés*.

  Az áttelepítés után ezeket a kizárásokat manuálisan kell hozzáadnia. Az előre definiált területekből álló kizárásokat a *Kártevő vizsgálata* feladat beállításaiban kell konfigurálni.

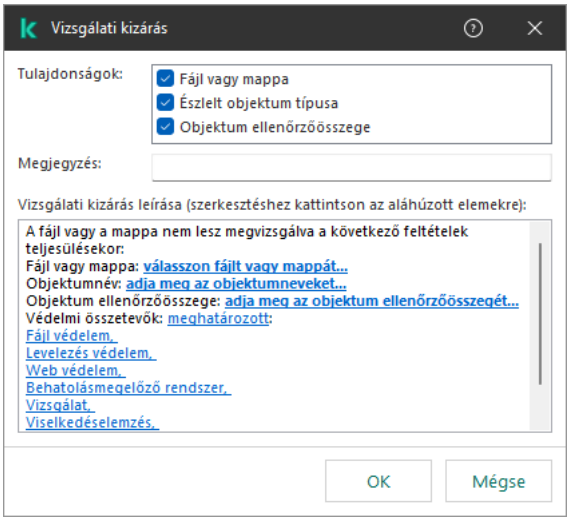
- Disk, folder or network location – olyan KES-kizárásokba való áttelepítés, amelyeknél a tulajdonságok között a „Fájl vagy mappa” módszer van kiválasztva.

- File – olyan KES-kizárásokba való áttelepítés, amelyeknél a tulajdonságok között a „Fájl vagy mappa” módszer van kiválasztva.

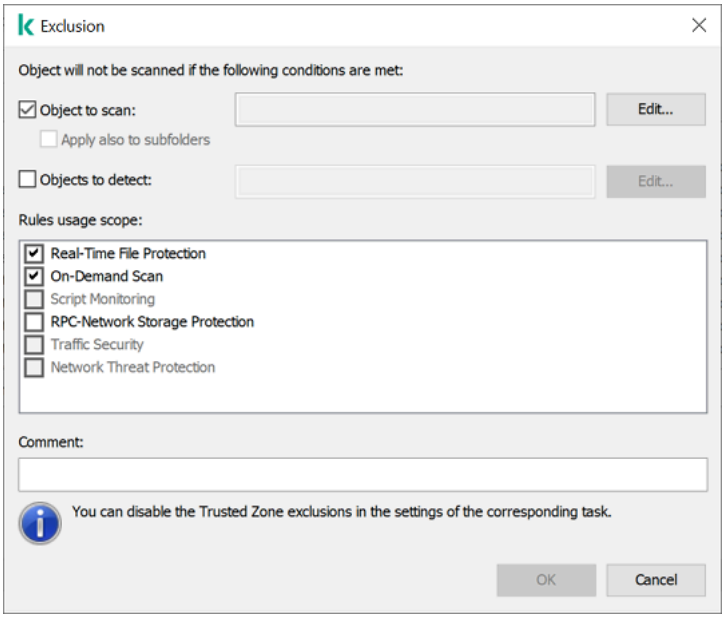
- Script file or web address – *nincs áttelepítés*.

  Az áttelepítés után ezeket a kizárásokat manuálisan kell hozzáadnia. A parancsfájl típusú webcímekből álló kizárásokat hozzá kell adni a megbízható webcímekhez a Web védelem esetében.

Ha a vizsgálandó objektumnál be van jelölve az **Apply also to subfolders** jelölőnégyzet, akkor ez a beállítás átkerül a KES-kizárásokba (az **Almappákkal együtt** jelölőnégyzet).



KES kizárási beállítások



KSWS kizárási beállítások

Észlelt objektumok áttelepítése

Azok a KSWS-kizárások, amelyek tulajdonságaiban a **Detected object** módszer van kiválasztva, bizonyos korlátozásokkal átkerülnek azokba a KES-kizárásokba, amelyek tulajdonságaiban az **Észlelhető objektum típusa** módszer van kiválasztva. Az észlelt objektum neve a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például `Email-Worm`, `Rootkit` vagy `RemoteAdmin`). A Kaspersky Endpoint Security támogatja a kérdőjellel (`?`, bármely egyetlen karakterrel megegyező) és a csillaggal (`*`, bármely karaktersorozattal megegyező) maszkokat.

A kizárás alkalmazási körének áthelyezése

A kizárás alkalmazási köre azon összetevők összessége, amelyekre a kizárás vonatkozik. A KES és a KSWS különböző összetevőkészletekkel rendelkezik, így az áttelepítési varázsló nem tudja áttelepíteni a kizárás alkalmazási körét. Ezért ha legalább egy összetevő ki van választva a KSWS alkalmazási körében, a KES a kizárást az összes alkalmazásösszetevőre alkalmazza.

A KSWS alkalmazási körét a megbízható zóna beállításaiban és a KSWS védelmi összetevők beállításaiban is konfigurálhatja. Ehhez bejelölheti vagy törölheti a **Apply Trusted Zone** jelölőnégyzetet a házirend megfelelő szakaszában. A KES védelmi összetevőinek beállításai nem tartalmaznak ilyen jelölőnégyzetet. Ez azt jelenti, hogy az egyes összetevők beállításaiban a megbízható zóna állapota az áttelepítéskor elvész. Az áttelepítés befejezése után jelölje ki a KES-házirend megbízható zóna beállításaiban azokat az összetevőket, amelyekre a kizárás vonatkozik.

Megjegyzések áttelepítése

A KSWS megbízható zónából származó megjegyzések módosítás nélkül átkerülnek a KES kizárási megjegyzéseibe.

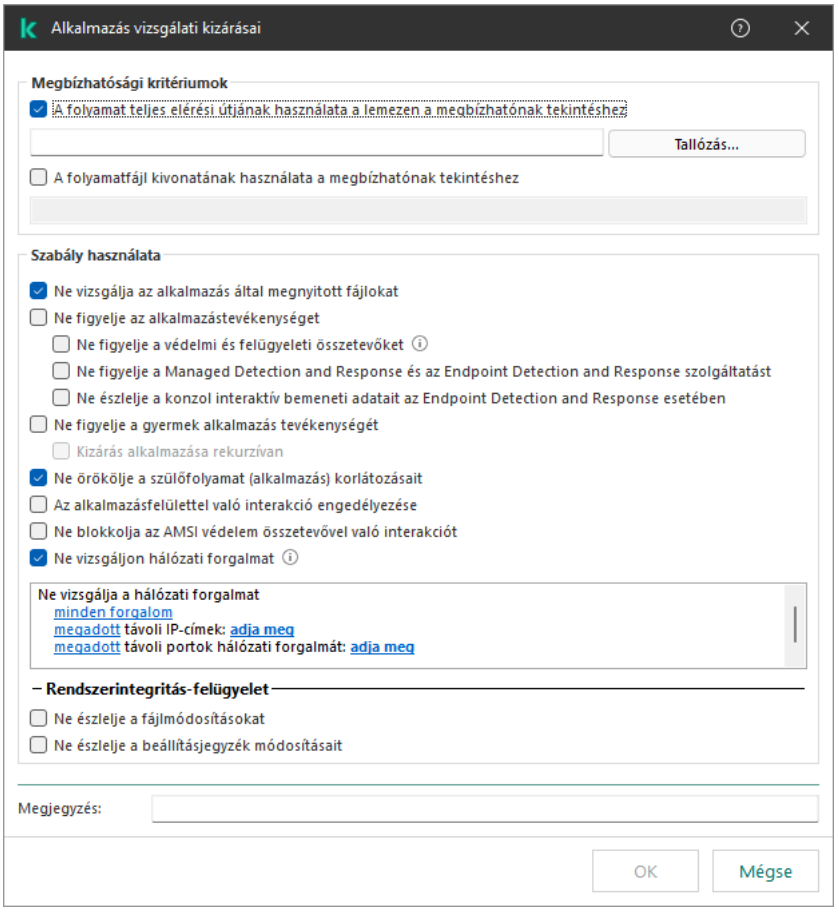
Megbízható folyamatok áttelepítése

A KSWS megbízható folyamatok bizonyos korlátozásokkal átkerülnek a KES megbízható folyamatokba. A megbízható folyamatok áttelepítése az objektum kiválasztási módszerétől függ:

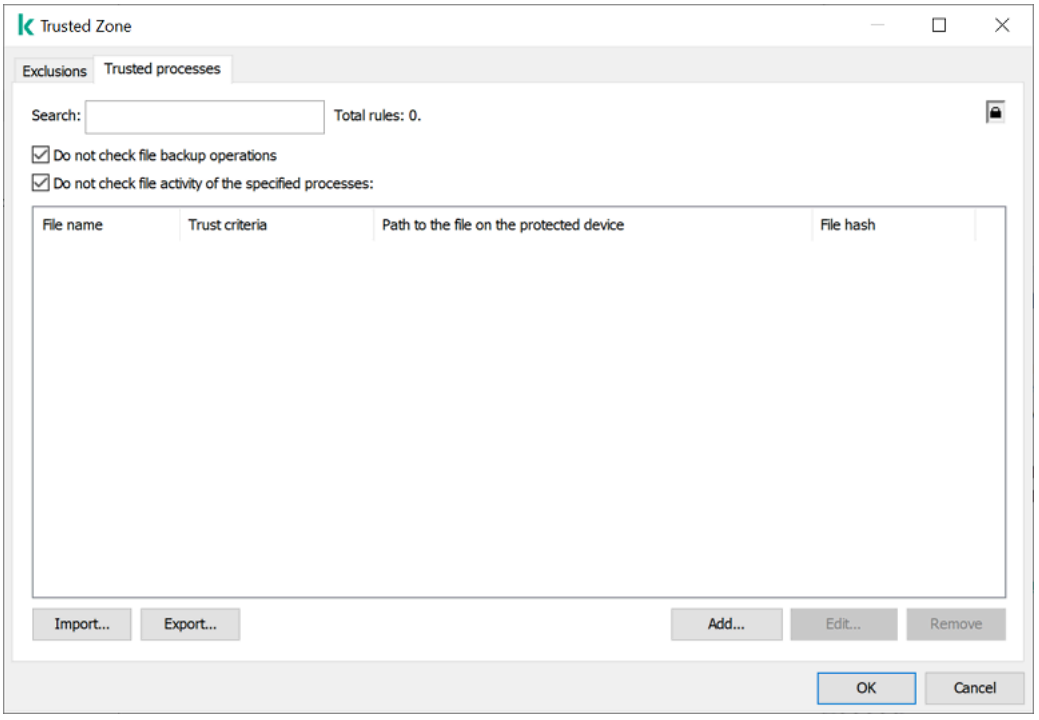
- Path to the file on the protected device – a KES megbízható alkalmazásaiba való áttelepítés.
- File hash – *nincs áttelepítés*.

Ha a KSWS megbízható folyamatokat fájlkivonatként konfigurál, akkor az ilyen megbízható folyamatok nem kerülnek áttelepítésre. Az áttelepítés után ezeket a megbízható folyamatokat manuálisan kell hozzáadnia.

Ha a **Do not check file backup operations** jelölőnégyzet be van jelölve a megbízható folyamatok beállításaiban, ez a beállítás átkerül a KES megbízható alkalmazásokba (a **Ne ellenőrizze az alkalmazások tevékenységét** jelölőnégyzet).



KES megbízható alkalmazás beállításai



KSWS megbízható folyamat beállításai

A KSWS Alkalmazások indításvezérlése szabályainak áttelepítése

A KSWS Alkalmazások indításvezérlése alapértelmezés szerint blokkoláson alapul. Ez azt jelenti, hogy az Alkalmazások indításvezérlése automatikusan blokkol minden olyan alkalmazást, amely a szabályokban engedélyezett alkalmazásként nincs megadva. Ezért a KES Alkalmazásfelügyelő migrációs varázslója automatikusan beállítja az **Engedélyezési lista** vezérlési módot, amely megfelel az alapértelmezés szerinti blokkolás elvének.

A szabályokat a KSWS-ből a KES-be a *Házirendek és feladatok kötegelt átalakítása varázslóval* vagy a *KSWS-házirenden alapuló, új KES-házirend létrehozására szolgáló varázslóval* lehet áttelepíteni.

Az Alkalmazások indításvezérlése üzemmód áttelepítése

A KSWS Alkalmazások indításvezérlése mód áttelepítése a KES Alkalmazásfelügyelőbe a következőképpen történik:

- **Statistics only → Szabályok tesztelése**;
- **Active → Szabályok alkalmazása**.

A KSWS Alkalmazások indításvezérlése előre megadott szabályainak áttelepítése

Alapértelmezés szerint a KSWS Alkalmazásindítás-vezérlés két szabályt tartalmaz:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Az előre megadott szabályok lehetővé teszik megbízható főtanúsítvánnyal aláírt *parancsfájlok*, *MSI-csomagok* és *futtatható fájlok* futtatását. Ha legalább az egyik előre definiált KSWS-szabály **Allow** típusú, a migrációs varázsló létrehoz egy új, **Applications with trusted root certificates** nevű engedélyezési szabályt. Vagyis a KES Alkalmazásfelügyelő egyetlen szabállyal engedélyezi a megbízható parancsfájlok, MSI-csomagok és végrehajtható fájlok futtatását.

Ha mindkét KSWS előre megadott szabály **Deny** típusú, a KES figyelmen kívül hagyja az előre megadott szabályokat.

A KSWS Alkalmazások indításvezérlése egyéni szabályainak áttelepítése

A KSWS Alkalmazások indításvezérlése szabályai a következő feltételeknek megfelelően szabályozzák a fájlok végrehajtását:

- aláírás digitális tanúsítvánnyal;
- SHA256 kivonat;
- fájl elérési útja.

A szabályok létrehozása a KSWS-ben és a KES-ben eltérő módon történik, ezért a migrációs varázsló olyan *alkalmazáskategóriákat* hoz létre, amelyek a KSWS szabályainak feltételeit és kizárásait tartalmazzák, és ezeket az alkalmazáskategóriákat hozzáadja a KES szabályaihoz. A varázsló a **Tanúsítvány**, a **Mappa elérési útja** és a **Fájlkivonat** feltételeket használja az alkalmazáskategóriákban. Új alkalmazáskategóriák érhetők el a Kaspersky Security Center felügyeleti konzol **Application management** → **Application categories** részén.

A migrációs varázsló a KSWS szabályokat típus és felhasználó szerint csoportosítja. Ezután a varázsló létrehozza a KSWS szabályok feltételeit és kizárásait tartalmazó alkalmazáskategóriákat, és hozzáadja az alkalmazáskategóriákat az új KES-szabályokhoz. A varázsló a KSWS szabályok nevét a KES szabályok **Leírás** mezőjében adja meg.

A KSWS Alkalmazások indításvezérlése speciális beállításainak áttelepítése

A KSWS Alkalmazások indításvezérlése és a KES Alkalmazásfelügyelő működési elve eltérő, így a migrációs varázsló a beállítások egy részhalmazát telepítheti át.

Az Alkalmazások indításvezérlése beállításai

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Repeat action taken for the first file launch on all the subsequent launches for this file	*(nincs áttelepítés)* A Kaspersky Endpoint Security minden alkalommal megvizsgálja az alkalmazást, amikor megkísérel futni.
Deny the command interpreters launch with no command to execute	*(nincs áttelepítés)* A Kaspersky Endpoint Security lehetővé teszi a parancsértelmezők futtatását, ha azokat az Alkalmazásfelügyelő nem tiltja.
Apply rules to executable files	*(nincs áttelepítés)* A szabály alkalmazási hatóköre nem konfigurálható a KES Alkalmazásfelügyelő beállításaiban. A KES Alkalmazásfelügyelő minden típusú fájlra alkalmazza a szabályokat: a végrehajtható fájlokra, a parancsfájlokra és az MSI-csomagokra. Ha minden fájltípus szerepel a szabály alkalmazási hatókörében a KSWS-ben, a migrálás során a KES áthelyezi a KSWS-szabályokat. Ha egyes fájltípusok ki vannak zárva a szabály alkalmazási hatóköréből a KSWS-ben, a migrálás során a KES átviszi ugyan a KSWS-szabályokat, de a **Tesztszabályok** alkalmazásfelügyelői művelet lesz kiválasztva.
Monitor loading of DLL modules	**A DLL-modulok betöltésének figyelése (jelentősen megnöveli a rendszer terhelését)**
Apply rules to scripts and MSI packages	*(nincs áttelepítés)* A szabály alkalmazási hatóköre nem konfigurálható a KES Alkalmazásfelügyelő beállításaiban. A KES Alkalmazásfelügyelő minden típusú fájlra alkalmazza a szabályokat: a végrehajtható fájlokra, a parancsfájlokra és az MSI-csomagokra. Ha minden fájltípus szerepel a szabály alkalmazási hatókörében a KSWS-ben, a migrálás során a KES áthelyezi a KSWS-szabályokat. Ha egyes fájltípusok ki vannak zárva a szabály alkalmazási hatóköréből a KSWS-ben, a migrálás során a KES átviszi ugyan a KSWS-szabályokat, de a **Tesztszabályok** alkalmazásfelügyelői művelet lesz kiválasztva.

A Kaspersky Security for Windows Server beállításai	A Kaspersky Endpoint Security for Windows beállításai
Deny applications untrusted by KSN	*(nincs áttelepítés)* A Kaspersky Endpoint Security nem veszi figyelembe az alkalmazások megbízhatóságát, és az alkalmazások futtatását a szabályoknak megfelelően engedélyezi vagy tiltja.
Allow applications trusted by KSN	A migrálás során a KES új engedélyezési szabályt ad hozzá. Az **Other Software\Applications, trusted according to reputation in KSN** KL kategória van meghatározva a szabály kiváltó feltételeként.
Users and / or user groups allowed to run applications trusted by KSN	A **Felhasználók és jogaik** egy olyan alkalmazásfelügyelői engedélyezési szabályban, amely tartalmazza a **Other Software\Applications, trusted according to reputation in KSN** KL-kategóriát.
Automatically allow software distribution via applications and packages listed	A KSWS-ben és a KES-ben máshogy működik a szoftverterjesztés felügyelete. A migrálás során a KES új engedélyezési szabályokat ad hozzá azokhoz az alkalmazásokhoz, amelyekhez engedélyezve van az automatikus szoftverterjesztés. A fájl kivonata van meghatározva a szabály kiváltó feltételeként.
Always allow software distribution via Windows Installer	A KSWS-ben és a KES-ben máshogy működik a szoftverterjesztés felügyelete. A migrálás során a KES új engedélyezési szabályokat ad hozzá azokhoz az alkalmazásokhoz, amelyekhez engedélyezve van az automatikus szoftverterjesztés (**Software distribution applications and packages allowed**). A fájl kivonata van meghatározva a szabály kiváltó feltételeként. A fióktulajdonságokban a **Megbízható frissítéstelepítők** jelölőnégyzet be van jelölve.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(nincs áttelepítés)*
Software distribution applications and packages allowed	A KSWS-ben és a KES-ben máshogy működik a szoftverterjesztés felügyelete. A migrálás során a KES új engedélyezési szabályokat ad hozzá azokhoz az alkalmazásokhoz, amelyekhez engedélyezve van az automatikus szoftverterjesztés. A fájl kivonata van meghatározva a szabály kiváltó feltételeként. A fióktulajdonságokban a **Megbízható frissítéstelepítők** jelölőnégyzet be van jelölve.
Schedule settings	*(nincs áttelepítés)* Ha ütemezés van konfigurálva az összetevőhöz a KSWS beállításaiban, az Alkalmazásfelügyelő összetevő engedélyezve van a migráláskor. Ha nincs konfigurálva ütemezés az összetevőhöz a KSWS beállításaiban, az Alkalmazásfelügyelő le van tiltva a migráláskor. Az összetevőhöz nem lehet külön ütemezést konfigurálni. Az összetevő mindig be van kapcsolva, amikor a Kaspersky Endpoint Security működik.

A KES telepítése a KSWS helyett

A Kaspersky Endpoint Security a következő módokon telepíthető:

- A KES telepítése a KSWS eltávolítása után (ajánlott).
- A KES telepítése a KSWS-re.

A Kaspersky Security for Windows Server eltávolítása

Az alkalmazás eltávolítása történhet távolról az *Uninstall application remotely* feladat segítségével vagy helyileg a kiszolgálón. Előfordulhat, hogy a KSWS eltávolítása után újra kell indítania a kiszolgálót. Ha a Kaspersky Endpoint Security-t újraindítás nélkül szeretné telepíteni, akkor győződjön meg arról, hogy a Kaspersky Security for Windows Server teljesen eltávolításra került. Ha az alkalmazást nem távolítja el teljesen, a Kaspersky Endpoint Security telepítése a kiszolgáló hibás működését okozhatja. Győződjön meg arról, hogy az alkalmazást teljesen eltávolította, ha a kavremover segédprogramot használta. A kavremover segédprogram nem támogatja a KSWS-t.

Ha a jelszóvédelem engedélyezve van a KSWS-hez való hozzáférés korlátozása céljából, adja meg az eltávolítási jelszót a KES telepítőcsomag beállításaiban.

A KSWS eltávolítása után telepítse a Kaspersky Endpoint Security for Windows terméket bármely rendelkezésre álló módszerrel.

Telepítse a Kaspersky Endpoint Security alkalmazást

Amikor távolról telepíti a KES-t, a telepítőcsomag tulajdonságaiban kiválasztott összetevők települnek a kiszolgálón. Javasoljuk, hogy a telepítőcsomag tulajdonságaiban válassza ki az alapértelmezett összetevőket. Az újraindítás nem szükséges, ha a KES-t a KSWS-re telepíti.

A helyi telepítést megelőzően a Kaspersky Endpoint Security ellenőrzi a számítógépen megtalálható Kaspersky alkalmazásokat. Ha a Kaspersky Security for Windows Server telepítve van a számítógépen, a KES észleli a telepített KSWS-összetevőket, és ugyanazokat az összetevőket választja ki a telepítéshez. Az újraindítás nem szükséges, ha a KES-t a KSWS-re telepíti.

Ha a KES telepítése a KSWS-re nem sikerült, visszagörgetheti a telepítést. A telepítés visszagörgetése után ajánlott újraindítani a kiszolgálót, és újra próbálkozni.

A Kaspersky Endpoint Security for Windows telepítésekor a KSWS-beállítások és -feladatok nem lesznek áttelepítve. A beállítások és feladatok áttelepítéséhez futtassa a Házirendek és feladatok kötegelt átalakítása varázslót.

A telepített összetevők listáját az alkalmazásfelület **Biztonság** részén ellenőrizheti a `status` paranccsal vagy a Kaspersky Security Center-konzolon, a számítógép tulajdonságainál. Az összetevők készletét a telepítés után az *Alkalmazásösszetevők módosítása* feladattal módosíthatja.

A [KSWS+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra

A Kaspersky Endpoint Security for Windows EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA és MDR használati támogatásának részeként egy beépített ügynök került be az alkalmazásba. Az ezekkel a megoldásokkal való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra.

A KSWS-ről a KES-re való áttéréskor az EDR (KATA), az EDR Optimum, az EDR Expert, a Kaspersky Sandbox, a KUMA és az MDR megoldás továbbra is együttműködik a Kaspersky Endpoint Security beépülő ügynökeivel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről.

A [KSWS+KEA] konfiguráció [KES+beépített ügynök] konfigurációra történő áttelepítése a következő lépéseket foglalja magában:

1. **Áttérés a KSWS-ről a KES-re**

   A KSWS-ről a KES-re való áttérés a Kaspersky Endpoint Security termék Kaspersky Security for Windows Server helyére való telepítését foglalja magában.

   A rendszergazdák általában engedélyezik a Jelszóvédelmet, hogy korlátozzák a KSWS és KEA megoldáshoz való hozzáférést. A Kaspersky Security Center Linux 15.1 verziótól kezdve megadhatja az alkalmazás eltávolítási jelszavát az *Install application remotely* feladat beállításaiban. A feladat csak egy eltávolítási jelszó megadását teszi lehetővé. Ez azt jelenti, hogy ha ugyanaz a jelszó van megadva a KSWS és a KEA alkalmazáshoz, akkor a KSWS és a KEA alkalmazások sikeresen eltávolításra kerülnek. Ha a jelszavak különböznek, az egyik alkalmazás eltávolítása hozzáférési hibával sikertelen. A migrálás befejezéséhez le kell tiltania a Jelszóvédelmet azon alkalmazások esetében, amelyek jelszavát nem tudta megadni az *Install application remotely* feladat beállításaiban.

   Az áttérés végrehajtásához ki kell választania a Kaspersky Endpoint Security részét képező Detection and Response megoldások támogatásához szükséges összetevőket. Az alkalmazás telepítése után a Kaspersky Endpoint Security átvált a beépített ügynök használatára, és eltávolítja a Kaspersky Endpoint Agent megoldást.

2. **A házirend és a feladatok áttelepítése**

   A [KSWS+KEA] házirendek és feladatok [KES+beépített ügynök] konfigurációra történő áttelepítése a következő lépéseket foglalja magában:

   1. A házirendek és feladatok áttelepítése a KSWS-ről a KES-re a Házirendek és feladatok kötegelt átalakítása varázsló segítségével (csak az Adminisztrációs konzolon (MMC) érhető el).

      Ennek eredményeként egy *UpgradedFromKSWS <a Kaspersky Security for Windows Server házirend neve>* nevű házirendprofil kerül be a KES házirendjébe. Továbbá új KES feladatok jönnek létre *<KSWS feladatnév> (átalakítva)* néven.

   2. Házirendek és feladatok áttelepítése a KEA-ból a KES-be a Kaspersky Endpoint Agent áttelepítési varázslójával (csak a Web Console-on és a Cloud Console-on érhető el).

      Ennek eredményeként egy új szabályzat jön létre *<a Kaspersky Endpoint Security házirend neve> és <a Kaspersky Endpoint Agent házirend neve>* névvel. Új feladatok és KES feladatok is jönnek létre.

3. **Licencelési funkcionalitás**

   Ha egy közös Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security licencet használ a Kaspersky Endpoint Security for Windows és a Kaspersky Endpoint Agent aktiválásához, az EDR Optimum funkció automatikusan aktiválódik az alkalmazás 11.7.0 verzióra történő frissítése után. Semmi mást nem kell tennie.

   Ha önálló Kaspersky Endpoint Detection and Response Optimum bővítményi licencet használ az EDR Optimum funkció aktiválásához, akkor győződjön meg arról, hogy az EDR Optimum bővítményi kulcsot hozzáadta a Kaspersky Security Center tárolójához, és engedélyezte az automatikus licenckulcs-szolgáltatói funkciót. Az alkalmazás 11.7.0 verzióra történő frissítése után az EDR Optimum funkció automatikusan aktiválódik.

   Ha Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security licencet használ a Kaspersky Endpoint Agent aktiválásához, és egy másik licencet a Kaspersky Endpoint Security for Windows aktiválásához, akkor a Kaspersky Endpoint Security for Windows kulcsot a közös Kaspersky Endpoint Detection and Response Optimum vagy Kaspersky Optimum Security kulcsra kell cserélnie. A kulcsot a *Add key* feladat segítségével cserélheti ki.

   A Kaspersky Sandbox funkciót nem kell aktiválnia. A Kaspersky Sandbox funkció a Kaspersky Endpoint Security for Windows frissítése és aktiválása után azonnal elérhetővé válik.

   Csak a Kaspersky Anti Targeted Attack Platform licence használható a Kaspersky Endpoint Security aktiválására a Kaspersky Anti Targeted Attack Platform megoldás részeként. Az alkalmazás 12.1 verzióra történő frissítése után az EDR (KATA) funkció automatikusan aktiválódik. Semmi mást nem kell tennie.

4. **A Kaspersky Endpoint Detection and Response Optimum és a Kaspersky Sandbox állapotának ellenőrzése**

   Ha a frissítés után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

   - Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
   - Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal.
   - Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.

   Győződjön meg arról, hogy az EDR Optimum funkció aktiválva van az *Report on status of application components* segítségével. Ha egy összetevőnél a *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy az EDR Optimum automatikus licenckulcs-szolgáltatói funkciója be van kapcsolva.

Győződjön meg arról, hogy a Kaspersky Security for Windows Server sikeresen eltávolításra került

Győződjön meg arról, hogy a Kaspersky Security for Windows Server teljesen eltávolításra került:

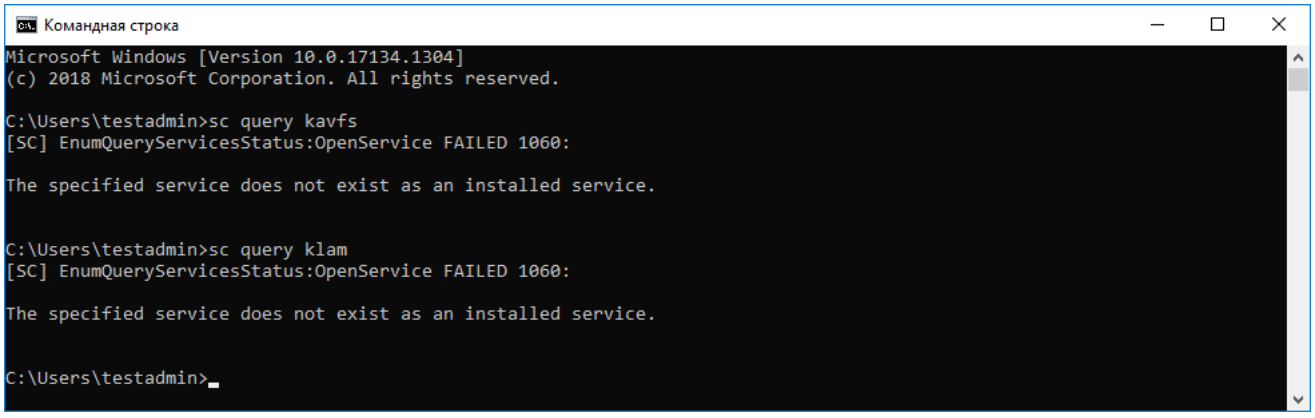
- A `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` mappa nem létezik.
- A következő szolgáltatások nincsenek jelen:
  - Kaspersky Security Service (KAVFS)
  - Kaspersky Security Management szolgáltatás (KAVFSGT)

- Kaspersky Security Exploit Prevention szolgáltatás (KAVFSSLP)
- Kaspersky Security Script Checker szolgáltatás (KAVFSSCS)

A futó szolgáltatásokat a Feladatkezelőben vagy az `sc query` parancs megadásával ellenőrizheti (lásd az alábbi ábrát).

- A következő illesztőprogramok nincsenek jelen:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

  A telepített illesztőprogramokat a `C:\Windows\System32\drivers` mappában vagy az `sc query` parancs megadásával ellenőrizheti. Ha egy szolgáltatás vagy illesztőprogram hiányzik, a következő választ kapja:



Győződjön meg arról, hogy a Kaspersky Security for Windows Server szolgáltatásait és illesztőprogramjait sikeresen eltávolította

Ha az alkalmazás- vagy illesztőprogram-fájlok a kiszolgálón maradnak, törölje manuálisan a megfelelő fájlokat. Ha a Kaspersky Security for Windows Server szolgáltatások továbbra is futnak a kiszolgálón, állítsa le (`sc stop`) és törölje (`sc delete`) a szolgáltatásokat manuálisan. A klam.sys illesztőprogram leállításához használja az `fltmc unload klam` parancsot.

A KES aktiválása egy KSWS-kulccsal

Az alkalmazás telepítése után aktiválhatja a Kaspersky Endpoint Security for Windows (KES) szolgáltatást a Kaspersky Security for Windows Server (KSWS) licenckulcs használatával. Az áttelepítés utáni aktiválási folyamat a KSWS aktiválási módszerétől függ (lásd az alábbi táblázatot).

A Kaspersky Endpoint Security nem támogatja a *Kaspersky Security for Storage licencet*. Ehhez a licenchez a Kaspersky Security for Windows Server használatára van szükség.

A KES termék KSWS-kulccsal való aktiválásához csak az aktiváló kódot használhatja. Ha kulcsfájlt használ az alkalmazás aktiválásához, forduljon az Ügyfélszolgálathoz egy Kaspersky Endpoint Security-kulcsfájlért.

A Kaspersky Endpoint Security for Windows aktiválása Kaspersky Security for Windows Server kulccsal

A Kaspersky Security for Windows Server aktiválási módja	A kulcs áttelepítése a Kaspersky Endpoint Security for Windows termékbe.
A KSWS licenckulcs automatikus terjesztése a számítógépek között.	Ha az automatikus kulcsterjesztés engedélyezve van a KSWS licenckulcs tulajdonságaiban, a KES automatikusan aktiválódik a KSWS kulccsal.
A KSWS kulcsot egy feladat adja hozzá.	Ha a KSWS a feladattal van aktiválva, a rendszer törli a KSWS licenckulcsát a KSWS-ből az áttelepítés során. Újra aktiválnia kell az alkalmazást. Például hozzáadhat egy licenckulcsot a Kaspersky Endpoint Security for Windows telepítőcsomaghoz.
A KSWS kulcs helyileg hozzáadásra kerül az alkalmazás felületén.	Ha a KSWS helyileg az Alkalmazásaktiválási varázsló segítségével aktiválódik, a rendszer törli a KSWS licenckulcsot a KSWS-ből az áttelepítés során. Újra aktiválnia kell az alkalmazást. Például hozzáadhat egy licenckulcsot a Kaspersky Endpoint Security for Windows telepítőcsomaghoz.
A KSWS kulcs hozzáadásra került a telepítőcsomaghoz.	Ha a KSWS a telepítőcsomagban található kulccsal aktiválódik, a rendszer törli a KSWS licenckulcsot a KSWS-ből az áttelepítés során. Újra aktiválnia kell az alkalmazást. Például hozzáadhat egy licenckulcsot a Kaspersky Endpoint Security for Windows telepítőcsomaghoz.
Fizetős virtuálisgép-lemezkép (Amazon Machine Image – AMI) az Amazon Web Services (AWS) szolgáltatásban.	Ha a Kaspersky Security Centert fizetős virtuálisgép-lemezképként (Amazon Machine Image – AMI) vásárolta meg az Amazon Web Services (AWS) szolgáltatásban, akkor nincs szükség a KES aktiválására. Ebben az esetben a Kaspersky Security Center az alkalmazáshoz már hozzáadott AWS-előfizetést használja.
Előre gyártott, ingyenes Kaspersky Security Center-lemezkép saját licenccel (saját licenc használata – BYOL modell).	Ha felhőkörnyezetben saját licenccel rendelkező ingyenes Kaspersky Security Center-lemezképet használ (saját licenc használata – BYOL modell), akkor az alkalmazást bármely rendelkezésre álló módszerrel aktiválnia kell. Szüksége lesz egy Kaspersky Hybrid Cloud Security licencre.

Speciális szempontok nagy terhelésű kiszolgálókon történő áttelepítéskor

A nagy terhelésű kiszolgálókon fontos a teljesítmény figyelése és a hibák elkerülése. A Kaspersky Endpoint Security for Windows rendszerre való áttérés után javasoljuk, hogy ideiglenesen tiltsa le azokat az alkalmazásösszetevőket, amelyek jelentős kiszolgálóerőforrást használnak a többi összetevőhöz képest. Miután megbizonyosodott arról, hogy a kiszolgáló a szokásos módon működik, újra bekapcsolhatja az alkalmazásösszetevőket.

A nagy terhelésű kiszolgálók áttelepítését a következőképpen javasoljuk:

1. Hozzon létre egy Kaspersky Endpoint Security házirendet alapértelmezett beállításokkal.

   Az alapértelmezett beállítások tekinthetők optimálisnak. A Kaspersky szakértői ezeket a beállításokat ajánlják. Az alapértelmezett beállítások biztosítják az ajánlott védelmi szintet és az optimális erőforrás-felhasználást.

2. A házirend-beállításokban kapcsolja ki a következő összetevőket: Hálózati védelem, Viselkedésészlelés, Biztonsági rések kihasználásának megelőzése, Kármentesítő motor, Alkalmazásfelügyelő.

   Ha a cég rendelkezik a Kaspersky Managed Detection and Response (MDR) megoldással, töltse fel a BLOB konfigurációs fájlt a Kaspersky Endpoint Security házirendjébe.

3. Távolítsa el a Kaspersky Security for Windows Server terméket a kiszolgálóról.

4. Telepítse a Kaspersky Endpoint Security for Windows rendszert az alapértelmezett összetevőkészlettel.

   Ha a cég rendelkezik Detection and Response megoldásokkal, válassza ki a megfelelő összetevőket a telepítőcsomag tulajdonságaiban.

5. Ellenőrizze az alkalmazás beállításait:

   - Az alkalmazás aktiválása a KSWS licenckulccsal történik.
   - Az új házirend alkalmazása megtörténik. A korábban kiválasztott összetevők le vannak tiltva.

6. Győződjön meg arról, hogy a kiszolgáló működik. Győződjön meg arról, hogy a Kaspersky Endpoint Security for Windows nem használja a kiszolgáló erőforrásainak több mint 1%-át.

7. Ha szükséges, hozzon létre vizsgálati kizárásokat, adjon hozzá megbízható alkalmazásokat, hozza létre a megbízható webcímek listáját.

8. Kapcsolja be a Viselkedésészlelés, a Biztonsági rések kihasználásának megelőzése és a Kármentesítő motor összetevőket. Győződjön meg arról, hogy a Kaspersky Endpoint Security for Windows nem használja a kiszolgáló erőforrásainak több mint 1%-át.

9. Kapcsolja be a Hálózati védelem összetevőt. Győződjön meg arról, hogy a Kaspersky Endpoint Security for Windows nem használja a kiszolgáló erőforrásainak több mint 2%-át.

10. Kapcsolja be az Alkalmazásfelügyelő összetevőt a szabálytesztelési módban.

11. Győződjön meg arról, hogy az Alkalmazásfelügyelő működik. Ha szükséges, adjon hozzá új alkalmazásfelügyeleti szabályokat, és kapcsolja ki a szabálytesztelési módot, miután meggyőződött arról, hogy az Alkalmazásfelügyelő működik.

A KSWS-ről a KES-re való átállás után győződjön meg arról, hogy az alkalmazás megfelelően működik. Ellenőrizze a kiszolgáló állapotát a konzolon (*OK* állapotúnak kell lennie). Győződjön meg arról, hogy az alkalmazás nem jelez hibát, valamint ellenőrizze az adminisztrációs kiszolgálóhoz való legutóbbi csatlakozás idejét, az utolsó adatbázis-frissítés időpontját és a kiszolgáló védelmi állapotát.

Az alkalmazás kezelése egy kiszolgálón Server Core mode üzemmódban

A Server Core mode üzemmódban lévő kiszolgáló nem rendelkezik grafikus felhasználói felülettel. Ezért az alkalmazást csak távolról, a Kaspersky Security Center konzolról vagy helyileg, a parancssorból kezelheti.

Az alkalmazás kezelése a Kaspersky Security Center konzollal

Az alkalmazás Kaspersky Security Center konzollal való telepítése nem különbözik a szokásos módon történő telepítéstől. Telepítőcsomag létrehozásakor licenckulcs hozzáadásával aktiválhatja az alkalmazást. Használhatja a Kaspersky Endpoint Security for Windows vagy a Kaspersky Security for Windows Server kulcsát.

A Server Core mode üzemmódban lévő kiszolgálón a következő alkalmazásösszetevők nem érhetők el: Web védelem, Levelezés védelem, Webfelügyelő, BadUSB védelem, Fájl szintű titkosítás (FLE), Kaspersky lemeztitkosítás (FDE).

Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját. Az alkalmazás nem jeleníthet meg olyan ablakot, amely a kiszolgáló újraindítására utasítja a felhasználót. A kiszolgáló újraindításának szükségességéről a Kaspersky Security Center konzolon lévő jelentésekből tájékozódhat.

Az alkalmazás Server Core mode üzemmódban lévő kiszolgálókon történő kezelése nem különbözik a számítógép kezelésétől. Az alkalmazás konfigurálásához házirendeket és feladatokat használhat.

Az alkalmazás Server Core mode üzemmódban lévő kiszolgálókon történő kezelése a következő speciális szempontokat foglalja magában:

- A Server Core mode üzemmódban lévő kiszolgáló nem rendelkezik grafikus felhasználói felülettel, ezért a Kaspersky Endpoint Security nem jelenít meg figyelmeztetést a felhasználónak, hogy fejlett vírusmentesítés szükséges. A fenyegetések vírusmentesítéséhez engedélyeznie kell a fejlett vírusmentesítő technológiát az alkalmazásbeállításokban, és engedélyeznie kell az azonnali fejlett vírusmentesítést a *Kártevő vizsgálata* feladat beállításaiban. Ezután el kell indítania a *Kártevő vizsgálata* feladatot.

- A BitLocker meghajtótitkosítás csak a Trusted Platform Module (TPM) használatakor érhető el. PIN-kód/jelszó nem használható titkosításhoz, mert az alkalmazás nem tudja megjeleníteni a jelszót kérő ablakot az indítás előtti hitelesítéshez. Ha az operációs rendszerben engedélyezve van a Federal Information Processing szabványú kompatibilitási mód, a meghajtó titkosításának megkezdése előtt csatlakoztasson egy cserélhető meghajtót a titkosítási kulcs mentéséhez.

Az alkalmazás kezelése a parancssorból

Ha nem tud grafikus felhasználói felületet használni, a Kaspersky Endpoint Security alkalmazást a parancssorból vezérelheti.

Az alkalmazás Server Core mode üzemmódban lévő kiszolgálóra történő telepítéséhez futtassa a következő parancsot:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Az alkalmazás aktiválásához futtassa a következő parancsot:

```
avp.com license /add <activation code or key file>
```

Az alkalmazásprofil állapotának ellenőrzéséhez futtassa a következő parancsot:

```
avp.com status
```

Az alkalmazásfelügyeleti parancsok listájának megtekintéséhez futtassa a következő parancsot:

```
avp.com help
```

A [KSWS+KEA] konfigurációról migrálás a [KES+beépített ügynök] konfigurációra

Amikor a Kaspersky Security for Windows Server (KSWS) rendszerről a Kaspersky Endpoint Security (KES) rendszerre tér át, a következő ajánlások alapján konfigurálhatja a kiszolgáló védelmét, és optimalizálhatja a teljesítményt. Itt egy példát fogunk ismertetni az áttérésre egyetlen szervezet esetében.

A szervezet infrastruktúrája

A cég az alábbi termékeket telepítette:

- Kaspersky Security Center 14.2

  Az adminisztrátor a Kaspersky megoldásait az adminisztrációs konzol (MMC) segítségével kezeli. A Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) is telepítve van

  A Kaspersky Security Centerben három felügyeleti csoport jön létre, amelyek a szervezet kiszolgálóit tartalmazzák: két felügyeleti csoport az SQL-kiszolgálókhoz és egy felügyeleti csoport a Microsoft Exchange-kiszolgálókhoz. Minden felügyeleti csoportot a saját szabályzata kezel. A *Database Update* és az *On-demand scan* feladatok a szervezet összes kiszolgálójához létrehozásra kerülnek.

  A KSWS aktiváló kulcs a Kaspersky Security Centerhez van hozzáadva. Az automatikus kulcsszolgáltatás engedélyezve van.

- A Kaspersky Security for Windows Server 11.0.1 és a Kaspersky Endpoint Agent 3.11 SQL-kiszolgálói telepítve vannak. Az SQL-kiszolgálókat két fürtbe vannak egyesítve.

  A KSWS az *SQL_Policy(1)* és az *SQL_Policy(2)* házirend felügyelete alatt áll. *Database Update*, *On-demand scan* feladatok is jönnek létre.

- Microsoft Exchange-kiszolgáló, amelyen telepítve van a Kaspersky Security for Windows Server 11.0.1 és a Kaspersky Endpoint Agent 3.11.

  A KSWS az *Exchange_Policy* házirend felügyelete alatt áll. *Database Update*, *On-demand scan* feladatok is jönnek létre.

Az áttelepítés megtervezése

Az áttelepítés a következő lépésekből áll:

1. A KSWS-feladatok és -házirendek áttelepítése a Házirendek és feladatok kötegelt átalakítása varázslóval.
2. A Kaspersky Endpoint Agent-házirend áttelepítése a Házirendek és feladatok kötegelt átalakítása varázslóval.
3. Címkék használata házirendprofilok aktiválásához az új házirend tulajdonságaiban.
4. A KES telepítése a KSWS helyett.
5. Az EDR Optimum aktiválása.
6. A KES működésének megerősítése.

Az áttelepítési forgatókönyv kezdetben az SQL-kiszolgálók fürtjének egyikén kerül végrehajtásra. Majd az áttelepítési forgatókönyvet a másik SQL-kiszolgálófürtön hajtjuk végre. Ezután az áttelepítési forgatókönyv a Microsoft Exchange-kiszolgálón kerül végrehajtásra.

A KSWS-feladatok és -házirendek áttelepítése a Házirendek és feladatok kötegelt átalakítása varázslóval

A KSWS-feladatok áttelepítéséhez a Házirendek és feladatok kötegelt átalakítása varázslót (áttelepítési varázsló) használhatja. Ennek eredményeként az *SQL_Policy(1)*, *SQL_Policy(2)* és *Exchange_Policy* házirendek helyett egyetlen házirendet fog kapni három profillal az SQL és a Microsoft Exchange kiszolgálók számára. A KSWS-beállításokkal rendelkező új házirendprofil neve *UpgradedFromKSWS – <A Kaspersky Security for Windows Server-házirend neve>* lesz. A profil tulajdonságainál az áttelepítési varázsló automatikusan kiválasztja az `UpgradedFromKSWS` eszközcímkét aktiválási feltételként. Így a házirendprofil beállításai automatikusan érvényesülnek a kiszolgálókon.

A Kaspersky Endpoint Agent-házirend áttelepítése a Házirendek és feladatok kötegelt átalakítása varázslóval

A Kaspersky Endpoint Agent-házirend áttelepítéséhez a Házirendek és feladatok kötegelt átalakítása varázslót használhatja. A Kaspersky Endpoint Agent Házirendek és feladatok kötegelt átalakítása varázslója csak a Web Console-on érhető el.

Címkék használata házirendprofilok aktiválásához az új házirend tulajdonságaiban

Válassza ki a korábban hozzárendelt eszközcímkét profilaktiválási feltételként. Nyissa meg a házirend tulajdonságait, és válassza ki a *General rules for policy profile activation* lehetőséget profilaktiválási feltételként.

A KES telepítése a KSWS helyett

A KES telepítése előtt le kell tiltania a jelszavas védelmet a KSWS-házirend tulajdonságaiban.

A KES telepítése a következő lépésekből áll:

1. Készítse elő a telepítőcsomagot. A telepítőcsomag tulajdonságai között válassza ki a Kaspersky Endpoint Security for Windows 12.0 terjesztőkészletet, és válassza ki az alapértelmezett összetevőkészletet.

2. Hozzon létre egy *Install application remotely* feladatot az SQL-kiszolgáló felügyeleti csoportjainak egyikéhez.

3. A feladat tulajdonságaiban válassza ki a telepítőcsomagot és a licenckulcs fájlját.

4. Várja meg, amíg a feladat sikeresen befejeződik.

5. Ismételje meg a KES telepítését a fennmaradó felügyeleti csoportokhoz.

A Kaspersky Security Center automatikusan hozzáadja az `UpgradedFromKSWS` címkét a konzolon lévő számítógépnevekhez, miután a KES telepítése befejeződött.

A KES telepítésének ellenőrzéséhez használhatja a *Report on protection deployment* szolgáltatást. Az eszköz állapotát is ellenőrizheti. Az alkalmazás aktiválásának megerősítéséhez használja a *Report on usage of license keys* szolgáltatást.

Az EDR Optimum aktiválása

Az EDR Optimum funkciót egy önálló Kaspersky Endpoint Detection and Response Optimum bővítménylicenc használatával aktiválhatja. Meg kell erősítenie, hogy az EDR Optimum kulcs hozzá van-e adva a Kaspersky Security Center adattárához, illetve az automatikus licenckulcs-elosztási funkció engedélyezve van-e.

Az EDR Optimum aktiválásának ellenőrzéséhez használhatja a *Report on status of application components* szolgáltatást.

A KES működésének megerősítése

Annak megerősítéséhez, hogy a KES működik, ellenőrizheti, hogy az nem jelez-e hibát. Az eszközállapotnak *OK* állapotúnak kell lennie. A frissítési és a kártevővizsgálati feladatok sikeresen befejeződtek.

Light Agent üzemmód a virtuális gépek védelmére

A 12.8-as verziótól kezdve a Kaspersky Endpoint Security for Windows a Kaspersky Security for Virtualization Light Agent részeként is használható. A *Kaspersky Security for Virtualization Light Agent* egy olyan integrált megoldás, amely átfogó védelmet nyújt a virtuális gépek számára különféle típusú információbiztonsági fenyegetések, hálózati támadások és adathalász támadások ellen. A megoldás használatához az alkalmazást Light Agent üzemmódban kell telepítenie.

A Kaspersky Endpoint Security telepítése Light Agent üzemmódban Arm-alapú virtuális gépekre nem támogatott.

A Kaspersky Endpoint Security a 6.2-es verziótól kezdődően a Kaspersky Security for Virtualization Light Agent részeként használható Light Agent üzemmódban.

A Light Agent indításakor kapcsolatot létesít és tart fenn a virtuális gép SVM szolgáltatásával (Secure Virtual Machine). Egy védelmi kiszolgáló van telepítve az SVM-en. A *Védelmi kiszolgáló* a Kaspersky Security for Virtualization Light Agent megoldás összetevője, amely megvizsgálja a fájlokat vírusok és más kártevők szempontjából, frissíti a vírusadatbázisokat, és kezeli a licenckulcsokat. A Light Agent a vizsgálandó fájlokat vagy fájlrészleteket az SVM-be küldi. A vizsgálati eredmények minden olyan virtuális gépen elérhetők, amelyre telepítve van a Light Agent (a SharedCache technológia). Ez a technológia növeli a megoldás hatékonyságát, és gyorsabb reagálást tesz lehetővé a fenyegetésekre.

A vállalat infrastruktúrája számos virtuális gépet tartalmazhat, amelyeken Light Agent és számos SVM van telepítve. Az integrációs kiszolgáló kezeli a virtuális gépek és az SVM-ek közötti interakciót. *Integrációs kiszolgáló* – a Kaspersky Security for Virtualization Light Agent megoldás összetevője, amely létrehozza az elérhető SVM-ek listáját, és továbbítja ezeket az adatokat a Light Agenteknek, részt vesz az SVM-ek Light Agentek általi felderítésében, védi a Light Agentek és az SVM-ek közötti kapcsolatot, és egyéb funkciókat lát el.

Különleges szempontok a Light Agent üzemmódhoz

A Kaspersky Endpoint Security Standard és Light Agent üzemmódban is felügyelhető a Kaspersky Endpoint Security házirendek és feladatok segítségével. Light Agent üzemmódban az alkalmazás egyes összetevői és funkciói nem érhetők el.

Adatbázisok és alkalmazás-szoftvermodulok frissítése

A Kaspersky Endpoint Security Light Agent üzemmódban speciális kártevő-adatbázisokat használ, amelyekre az alkalmazásnak szüksége van, amikor a Kaspersky Security for Virtualization Light Agent megoldás részeként üzemel. A Kaspersky Endpoint Security az adatbázisokat és az alkalmazásmodul-frissítéseket a védelmi kiszolgálóról szerzi be.

A védett virtuális gépeken lévő adatbázisok és modulok frissítése a speciális *Adatbázisok és alkalmazásmodulok frissítése* feladattal történik, amelyben az SVM-en egy mappa van megadva a frissítés forrásaként. A Light Agent automatikusan futtatja az *Adatbázisok és alkalmazásmodulok frissítése* feladatot. Nem választhat másik frissítésforrást, nem konfigurálhatja a feladatütemezést, és nem távolíthatja el a feladatot.

A kártevőadatbázis legújabb frissítésének visszagörgetését is a védelmi kiszolgáló végzi. Az adatbázisok és alkalmazásmodulok frissítésének visszagörgetése után az SVM-en egy speciális helyi *Adatbázisok és alkalmazásmodulok frissítése* feladat indul el a védett virtuális gépen. Ezzel a feladattal a Light Agent visszatér a kártevő-adatbázisok korábbi csoportjának használatához.

A Kaspersky Endpoint Security Light Agent üzemmódban nem támogatja a *Frissítés visszaállítása* feladatot.

A Light Agent aktiválása

Az alkalmazás aktiválásához licenckulcsot kell hozzáadnia ahhoz az SVM-hez, amelyhez a Light Agent csatlakozik. Az alkalmazást nem kell külön aktiválni.

Egyéb különleges szempontok a Light Agent üzemmódhoz

- A házirend alkalmazáshoz való létrehozásakor javasoljuk, hogy a Light Agent üzemmódot válassza. Ebben az üzemmódban az új házirendvarázsló az SVM-kapcsolat konfigurálását kéri. Ezekre a beállításokra van szükség ahhoz, hogy az alkalmazás Light Agent üzemmódban működjön.
- Nem telepítheti az Adattitkosítás összetevőit és az Adaptív Anomáliafelügyelőt Light Agent üzemmódban. Az összetevők készlete a vendég operációs rendszer típusától is függ: munkaállomás vagy kiszolgáló.
- A Light Agent nem támogatja az integrációt a Kaspersky Endpoint Detection and Response Expert és a Kaspersky Endpoint Detection and Response Expert (cloud) megoldásokkal.
- A Light Agentet a felügyeleti konzolon (MMC) és a Kaspersky Security Center Web Console-on kezelheti. A Light Agent kezelésére nincs mód a Kaspersky Security Center Cloud Console-ban.
- Az alkalmazásösszetevők módosítása a VDI virtuális gépeken nem támogatott.
- A Kaspersky Endpoint Security egy KSN proxykiszolgálón keresztül kommunikál a KSN-kiszolgálókkal. A KSN-nel való közvetlen kommunikáció nem támogatott.
- A Kaspersky Security Network felhő módja nem támogatott.
- Az alkalmazás proxykiszolgálói használata az Integration Server (VIIS), a Protection Server (SVM) és a KSN kiszolgálókhoz való csatlakozáskor nem támogatott.

A virtuális gép előzetes konfigurálása

A Kaspersky Endpoint Security telepíthető virtuális platform technológiát használó virtuális gépre. A Kaspersky Endpoint Security VMware, Microsoft Hyper-V, Citrix virtuális platformokat támogatja. A telepítés előtt el kell végeznie a virtuális gépek előzetes konfigurációját.

Kompatibilitás a Citrix App Layering technológiával

Ha a Full User Layer szolgáltatást kívánja használni az ideiglenes virtuális gépek állapotának mentésére, akkor a virtuálisgép-sablonra történő telepítés előtt a következőket kell tennie:

1. Hozza létre a C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt fájlt, és adja hozzá a következő kizárásokat:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. Az operációs rendszer beállításjegyzékében, a HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr kulcsban hozzon létre egy új DWORD értéket MiniFilterBypass néven, és állítsa 1-re.

3. Az operációs rendszer beállításjegyzékében, a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd kulcsban hozzon létre egy új MULTI_SZ értéket ExcludeKey néven, és állítsa \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab értékre.

4. Indítsa újra a virtuális gépet.

A Citrix App Layering-et használó infrastruktúrában lévő virtuális gépekre történő telepítéshez a következőket kell tennie:

1. Telepítse a Kaspersky Security Center felügyeleti ügynököt és a Kaspersky Endpoint Security for Windows alkalmazást a virtuálisgép-sablonra az alkalmazásrétegen.

2. Hozzon létre egy több rétegből álló virtuálisgép-lemezképet.

3. Telepítse a létrehozott lemezképet a Citrix App Layering megoldást támogató hipervizorokra.

4. Állítsa be az ideiglenes virtuális gépek létrehozását a létrehozott lemezképből.

A víruskereső szoftverek Citrix App Layering melletti telepítésével kapcsolatos részletekért tekintse meg a Citrix App Layering dokumentációját.

Kompatibilitás a Citrix Provisioning (Citrix Provisioning Services) technológiával

Annak biztosítása, hogy az alkalmazás kompatibilis legyen a Citrix Provisioning technológiával (Citrix Provisioning Services):

- Ha a Citrix Provisioning Target Device szoftver telepítve van a virtuális gépen, akkor azt el kell távolítani a Kaspersky Endpoint Security alkalmazás telepítése előtt (részletekért kérjük, látogasson el a Citrix műszaki támogatási weboldalára). Az alkalmazás telepítése után újra kell telepítenie a Citrix Provisioning Target Device alkalmazást.

- Amikor az alkalmazást a Telepítővarázslóval vagy távolról a Kaspersky Security Center segítségével telepíti, be kell jelölnie a **Biztosítsa a Citrix PVS szolgáltatásokkal való kompatibilitást** jelölőnégyzetet.

Kompatibilitás a Omnissa App Volumes technológiával

A virtuálisgép-sablonra történő telepítés előtt létre kell hoznia a %SVAgent%\Config\Custom\snapvol.cfg fájlt, és hozzá kell adnia a következő kizárásokat:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

A részleteiért olvassa el a Omnissa dokumentációt.

A Light Agent telepítése

A Kaspersky Endpoint Security telepítése Light Agent üzemmódban Arm-alapú virtuális gépekre nem támogatott.

Az alkalmazás telepítése Light Agent üzemmódban ugyanaz, mint Normál üzemmódban. Mielőtt telepítené a Light Agentet egy virtuális gépre, meg kell győződnie arról, hogy a Kaspersky Security Center Network Agent telepítve van. A *Network Agent* végzi el az Adminisztrációs szerver és a virtuális gép közötti interakciót.

A Light Agent az alábbi módok egyikén telepíthető virtuális gépre:

- Távolról a Kaspersky Security Centeren keresztül.
- Helyileg a Telepítővarázsló segítségével.
- Helyileg a parancssor segítségével.

A Light Agent telepítéséhez ki kell választania a megfelelő konfigurációt telepítőcsomag beállításaiban vagy a Telepítővarázslóban.

Amikor a Light Agentet kiszolgálóra telepíti, a speciális védelmi összetevők (Viselkedésészlelés, Biztonsági rések kihasználásának megelőzése, Kármentesítő motor) nem szerepelnek az alkalmazás alapértelmezett konfigurációjában. Az alkalmazás alapértelmezett beállításai biztosítják az ajánlott védelmi szintet és a kiszolgálói erőforrások optimális felhasználását. Amikor a Light Agentet munkaállomásra telepíti, a speciális védelmi összetevők az alkalmazás alapértelmezett konfigurációjában szerepelnek.

A Light Agent telepítésekor javasoljuk, hogy az adott virtuális környezethez válasszon előre meghatározott kizárásokat és megbízható alkalmazásokat. Az előre definiált vizsgálati kizárások és a megbízható alkalmazások segítenek az alkalmazás gyors beállításában és a virtuális környezettel kapcsolatos kompatibilitási problémák elkerülésében. A telepítés után a házirendben az előre meghatározott vizsgálati kizárásokat és megbízható alkalmazásokat is konfigurálhatja.

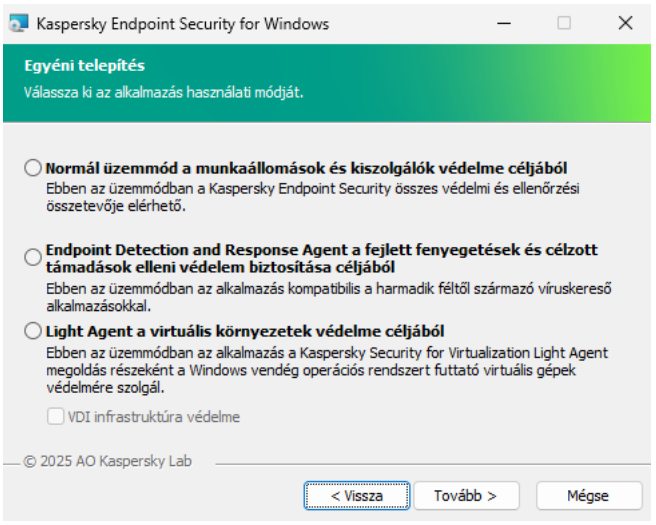
Amikor a Light Agentet állandó virtuális gépekre telepíti, előfordulhat, hogy módosítania kell az Sensor ID generálási algoritmusát. A Sensor ID a Kaspersky Anti Targeted Attack Platform megoldásban azon számítógépek azonosítására szolgál, amelyek telemetriai adatokat küldenek a kiszolgálónak. Egyedi Sensor ID létrehozásához állítsa be a következőt: `EnableUniqueSensorID=1` az alkalmazás parancssorból való telepítésekor.

A Light Agent telepítése a Telepítővarázsló segítségével

1. Másolja a terjesztőkészlet mappáját a virtuális gépre.
2. Futtassa a setup_kes.exe fájlt.

   A Telepítővarázsló elindul.

A Kaspersky Endpoint Security konfigurációja



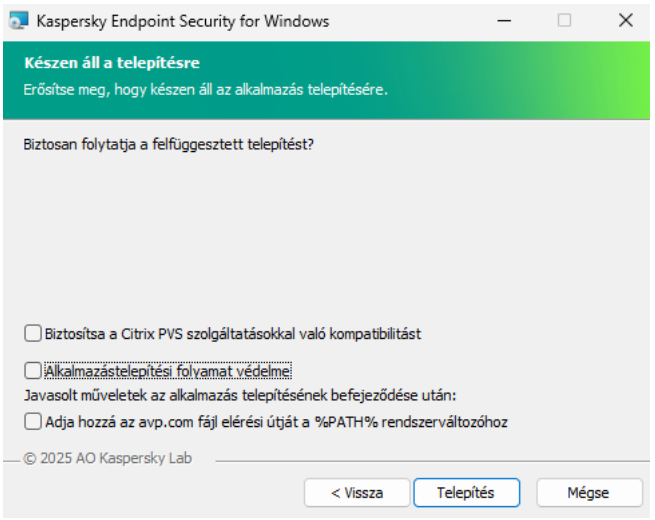
Az alkalmazás konfigurációjának kiválasztása

Válassza ki a **Light Agent a virtuális környezetek védelme céljából** konfigurációt. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **VDI infrastruktúra védelme** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.

Kaspersky Endpoint Security összetevők

Válassza ki a telepíteni kívánt összetevőket (lásd az alábbi ábrát). Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket. Ehhez futtatnia kell a Telepítővarázslót, és ki kell választania az elérhető összetevőket.

Speciális beállítások



Alkalmazás telepítési beállításai

Alkalmazástelepítési folyamat védelme. A telepítési védelembe tartozik a terjesztőcsomagok rosszindulatú alkalmazásokkal való kicserélése elleni védelem, a Kaspersky Endpoint Security telepítési mappái elérésének blokkolása, valamint az alkalmazáskulcsokat tartalmazó beállításjegyzék-rész elérésének blokkolása. Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni.

A Citrix PVS kompatibilitás biztosítása. Engedélyezheti a Citrix Provisioning Services támogatását, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre telepítse.

Adja hozzá az avp.com fájl elérési útját a %PATH% rendszerváltozóhoz. A parancssori felület kényelmes használata érdekében hozzáadhatja a telepítés elérési útvonalát a %PATH% változóhoz.

A Light Agent telepítése a parancssor használatával

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security terjesztőcsomagja telepítve van.
3. Futtassa a következő parancsot:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   vagy

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   A `VDI` opcióval engedélyezi a VDI (Virtual Desktop Infrastructure) védelmi módot. A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját. Alapértelmezés szerint a VDI védelmi mód le van tiltva.

Ennek eredményeként a Light Agent az alapértelmezett összetevőkészlettel lesz telepítve a virtuális gépen. Az összetevőkészletet szerkesztheti és speciális beállításokat adhat meg a setup.ini fájl segítségével. A telepítési beállításokat a parancssorban is megadhatja.

A Light Agent telepítése az adminisztrációs konzol (MMC) használatával

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki a konzolfán az **Advanced** → **Remote installation** → **Installation packages** mappát.

   Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.
3. Nyissa meg a Kaspersky Endpoint Security for Windows telepítőcsomag tulajdonságait.

   Ha szükséges, hozzon létre egy új telepítőcsomagot.
4. Nyissa meg a **Settings** szakaszt.
5. Válassza ki a **Light Agent a virtuális környezetek védelme céljából** konfigurációt. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **VDI infrastruktúra védelme** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.
6. Válassza ki a telepíteni kívánt összetevőket.

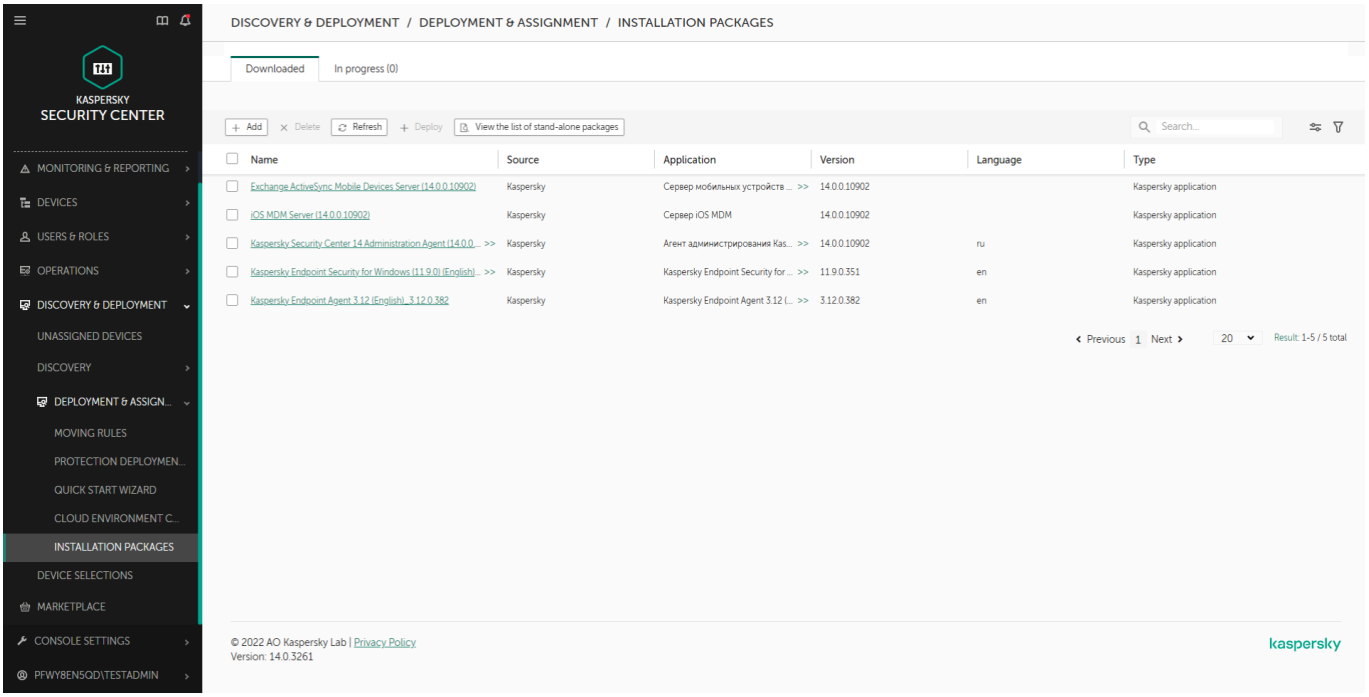
   Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket.
7. Konfigurálja a megbízható zónát. Válasszon ki előre meghatározott vizsgálati kizárásokat és megbízható alkalmazásokat ahhoz a virtuális környezethez, amelyben az alkalmazást telepíti.

   Az előre definiált vizsgálati kizárások és a megbízható alkalmazások segítenek az alkalmazás gyors beállításában és a virtuális környezettel kapcsolatos kompatibilitási problémák elkerülésében.
8. Mentse el a módosításokat.
9. Hozzon létre egy távoli telepítési feladatot. A feladat tulajdonságaiban válassza ki a létrehozott telepítőcsomagot.

A Light Agent telepítése a Web Console segítségével

1. A Web Console fő ablakában válassza az **Discovery & deployment** → **Deployment & assignment** → **Installation packages** lehetőséget.

Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.



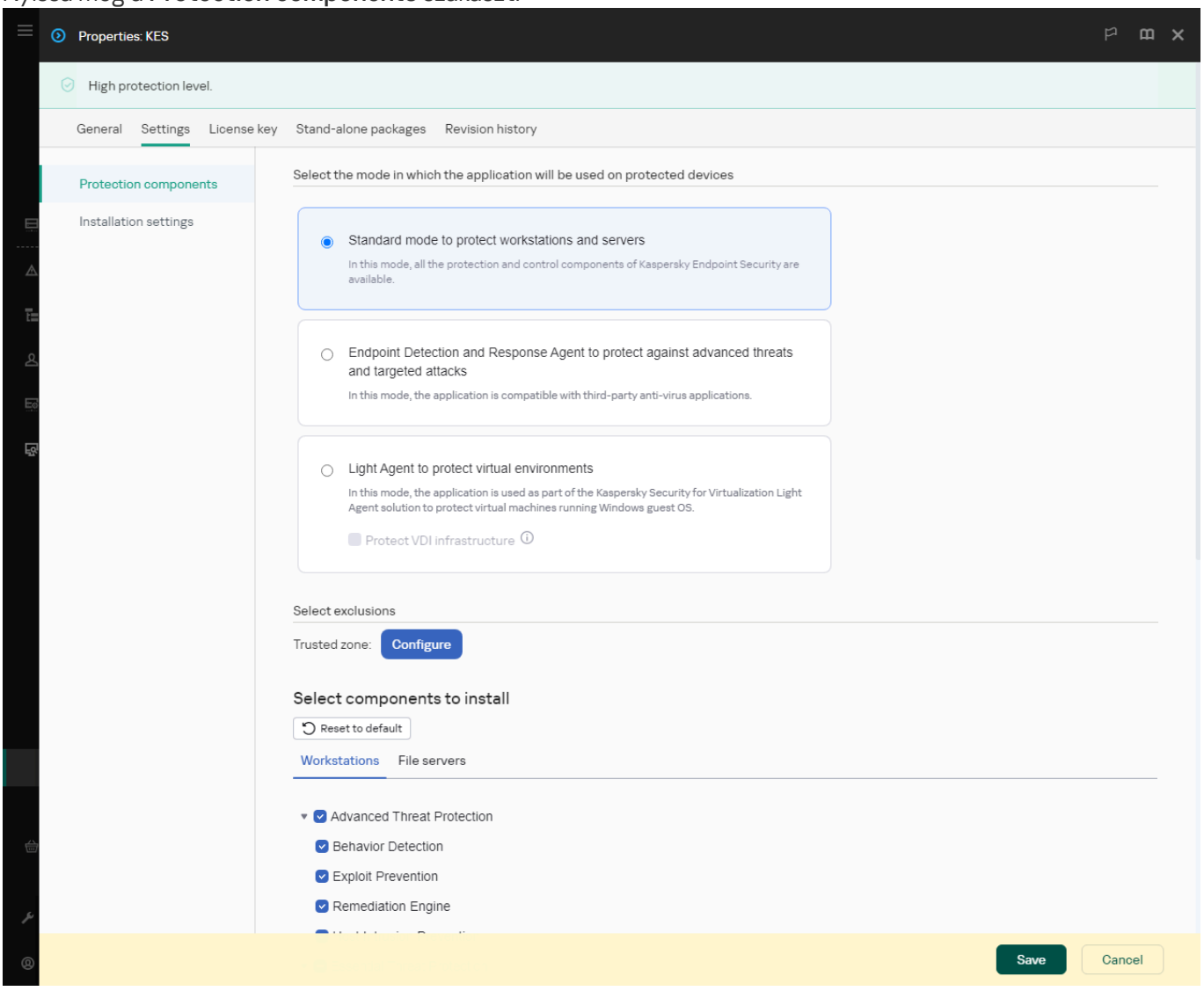
A telepítőcsomagok listája

2. Nyissa meg a Kaspersky Endpoint Security for Windows telepítőcsomag tulajdonságait.

   Ha szükséges, hozzon létre egy új telepítőcsomagot.

3. Válassza ki az **Settings** lapot.

4. Nyissa meg a **Protection components** szakaszt.



A telepítőcsomagban található összetevők

5. Válassza a **Light Agent to protect virtual environments** konfigurációt. Ez a konfiguráció a Kaspersky Security for Virtualization Light Agent megoldás részeként használt alkalmazáshoz készült. A Light Agentet minden egyes olyan virtuális gépen telepíteni kell, amelyet a megoldás segítségével védeni kell. Ebben a konfigurációban nem használhatja az adattitkosítási összetevőket vagy az Adaptív Anomáliafelügyelőt. Ha a Light Agentet olyan virtuálisgép-sablonra telepíti, amelyet *nem perzisztens virtuális gépek* létrehozására használ, jelölje be a **Protect VDI infrastructure** jelölőnégyzetet (a VDI jelentése: Virtual Desktop Infrastructure). A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ebben az üzemmódban a Light Agent elutasítja a virtuális gép újraindítását igénylő alkalmazásfrissítéseket. Újraindítást igénylő alkalmazásfrissítések fogadásakor a Light Agent eseményt generál arról, hogy frissíteni kell a védett virtuális gépek sablonját.

6. Válassza ki a telepíteni kívánt összetevőket.

   Az alkalmazás telepítése után lehetősége van kezelni az elérhető alkalmazásösszetevőket.

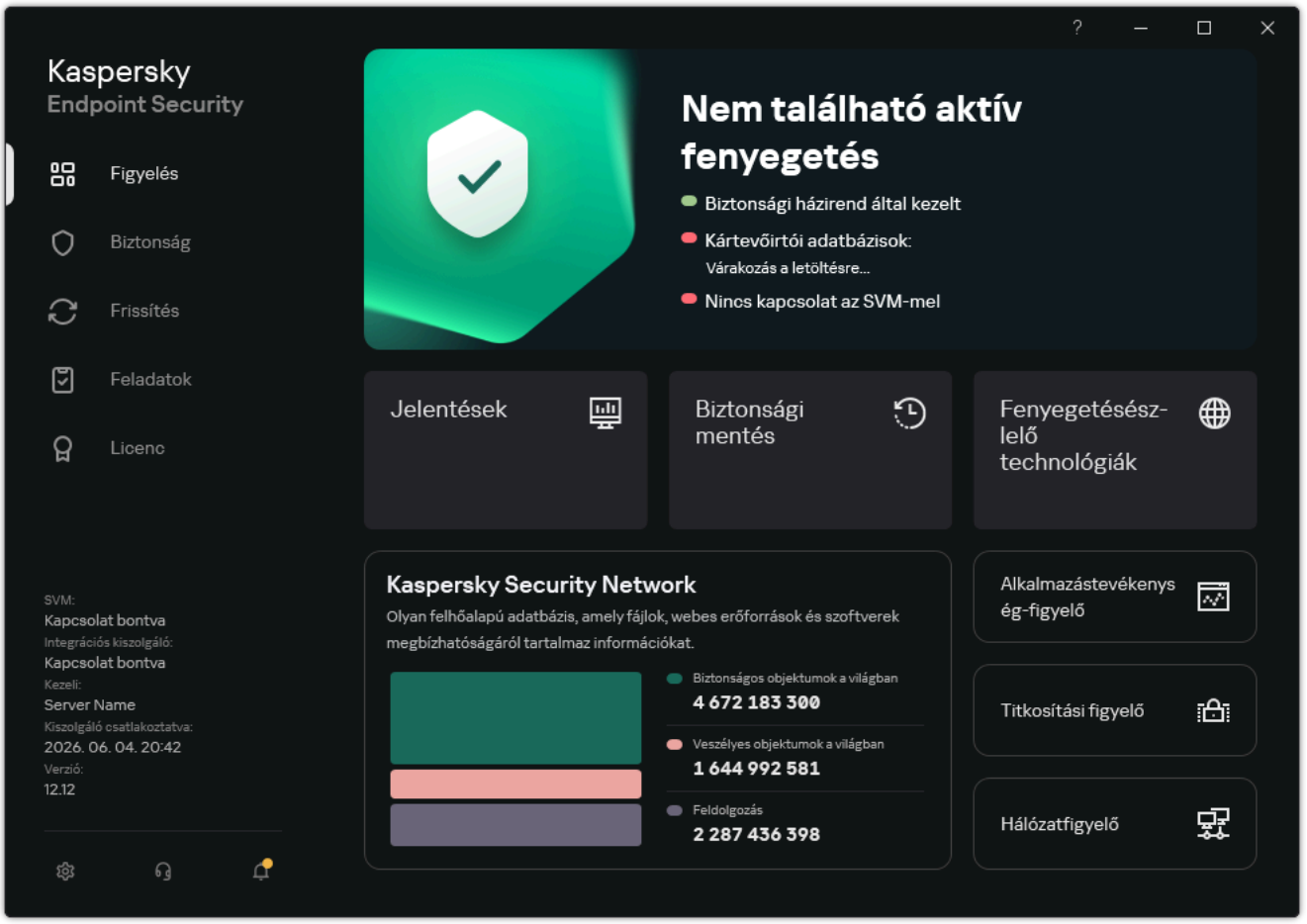
7. Konfigurálja a megbízható zónát. Válasszon ki előre meghatározott vizsgálati kizárásokat és megbízható alkalmazásokat ahhoz a virtuális környezethez, amelyben az alkalmazást telepíti.

   Az előre definiált vizsgálati kizárások és a megbízható alkalmazások segítenek az alkalmazás gyors beállításában és a virtuális környezettel kapcsolatos kompatibilitási problémák elkerülésében.

8. Mentse el a módosításokat.

9. Hozzon létre egy távoli telepítési feladatot. A feladat tulajdonságaiban válassza ki a létrehozott telepítőcsomagot.

Ennek eredményeként a Light Agent telepítésre kerül a virtuális gépen. Használhatja az alkalmazás felületét, és az alkalmazás ikonja megjelenik az értesítési területen . Most konfigurálnia kell a Light Agent csatlakozását az SVM-hez.



A Light Agent főablaka

A Light Agent csatlakoztatása az SVM-hez

A Kaspersky Security for Virtualization Light Agent megoldásához folyamatos kommunikációra van szükség a Light Agent és az SVM között. Erre a Light Agent által küldött fájlok vírusok és más kártevők szempontjából történő vizsgálatához van szükség. SVM-kapcsolat nélkül a Light Agent nem tud fájlokat küldeni vizsgálatra. Ha a kapcsolat öt percnél hosszabb ideig nem jön létre, a vizsgálat hibával fejeződik be.

A Light Agent SVM-hez való csatlakoztatása a következő lépésekből áll:

1. A Light Agent lekéri az elérhető SVM-ek listáját.

2. A Light Agent meghatározza az optimális csatlakozáshoz elérhető védelmi kiszolgálót (SVM) az SVM kiválasztási algoritmus szerint.

3. A Light Agent ellenőrzi a további SVM-kapcsolatbeállításokat: címkék, kapcsolatvédelmi állapot, a licenc hatálya alá tartozó alkalmazásfunkciók.

4. A Light Agent csatlakoztatása az SVM-hez.

Információkat kaphat a Light Agent SVM-hez való csatlakozásának állapotáról a Kaspersky Endpoint Security alkalmazásban vagy alkalmazás-paranccsal. Az alkalmazás eseményt generál, amikor a Light Agent SVM-kapcsolata megszakad vagy létrejön, és elküldi ezeket a Kaspersky Security Centernek. Ha Integrációs kiszolgálót használ az SVM-felderítéshez, az Integrációs kiszolgáló konzoljában információkat kaphat az SVM állapotáról és a csatlakoztatott Light Agentek számáról. Az SVM állapotfigyelés részletei: Kaspersky Security for Virtualization Light Agent súgó.

SVM-felderítés

Kiválaszthatja az SVM felderítési módszerek egyikét a Light Agent számára:

- Az Integrációs kiszolgáló (VIIS) használata.

  Az *Integrációs kiszolgáló* a megoldás azon összetevője, amely lehetővé teszi a Kaspersky Security for Virtualization Light Agent és a virtuális infrastruktúra közötti együttműködést, és létrehozza a csatlakozásra rendelkezésre álló SVM-ek listáját. A Light Agent kapcsolatot létesít az Integrációs kiszolgálóval, és lekéri az SVM címlistát.

  Az Integrációs kiszolgáló elsősorban nagy virtuális infrastruktúrákban bizonyul igazán hasznosnak, mivel automatikusan elosztja a terhelést az SVM-ek között, információkat gyűjt a rendelkezésre álló SVM-ekről, elemzi ezeket az adatokat, majd a Light Agenteknek megadja azoknak a védelmi kiszolgálóknak (SVM-eknek) a listáját, amelyekhez a csatlakozás a legoptimálisabb.

  Ahhoz, hogy a Light Agent hozzáférjen az SVM-ek listájához, csak az Integrációs kiszolgáló címét kell megadnia.

- Az SVM címlista használata.

  Ha meg kell adnia olyan egyedi SVM-eket, amelyekhez a Light Agentnek csatlakoznia kell, manuálisan készíthet listát.

  Fel kell sorolnia azon elérhető SVM-ek címeit, amelyekhez a Light Agent csatlakozhat.

Az SVM-felderítés konfigurálása a Light Agent által a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza ki a **Light Agent üzemmód** → **SVM-felderítési beállítások** lehetőséget.

4. Válasszon ki egy SVM-felderítési módszert.

   - **Az Integrációs kiszolgáló használata**. Adja meg az Integrációs kiszolgáló kapcsolódási beállításait. Adja meg annak az eszköznek az IPv4 formátumú IP-címét vagy teljes tartománynevét (FQDN), amelyre az Integrációs kiszolgáló telepítve van.

   - **SVM-címek egyéni listájának használata**. Hozzon létre egy listát azokról az SVM-ekről, amelyekhez a Light Agent csatlakozhat. Adja meg az IPv4 formátumú IP-címet vagy az SVM teljes tartománynevét (FQDN). Minden listaelemet új sorba kell beírni, vagy az előző elemtől pontosvesszővel (`;`) kell elválasztani.

     Az SVM-címek listájában csak olyan teljes tartományneveket (FQDN) adjon meg, amelyeknek egyetlen IP-cím felel meg. Több IP-címnek megfelelő, teljes tartománynév használata hibás megoldáshoz vezethet.

5. Mentse el a módosításokat.

Az SVM-felderítés konfigurálása a Light Agent segítségével a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **Light Agent Mode** → **SVM discovery settings** elemet.

5. Válasszon ki egy SVM-felderítési módszert.

   - **Use Integration Server**. Adja meg az Integrációs kiszolgáló kapcsolódási beállításait. Adja meg annak az eszköznek az IPv4 formátumú IP-címét vagy teljes tartománynevét (FQDN), amelyre az Integrációs kiszolgáló telepítve van.

   - **Use a custom list of SVM addresses**. Hozzon létre egy listát azokról az SVM-ekről, amelyekhez a Light Agent csatlakozhat. Adja meg az IPv4 formátumú IP-címet vagy az SVM teljes tartománynevét (FQDN). Minden listaelemet új sorba kell beírni, vagy az előző elemtől pontosvesszővel (`;`) kell elválasztani.

     Az SVM-címek listájában csak olyan teljes tartományneveket (FQDN) adjon meg, amelyeknek egyetlen IP-cím felel meg. Több IP-címnek megfelelő, teljes tartománynév használata hibás megoldáshoz vezethet.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az SVM-felderítés konfigurálása a Light Agent segítségével az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazás beállításai ablakban a **Light Agent üzemmód** részen kattintson az **SVM felderítési beállítások** csempére.

3. Válasszon ki egy SVM-felderítési módszert.

   - **Az Integrációs kiszolgáló használata**. Adja meg az Integrációs kiszolgáló kapcsolódási beállításait. Adja meg annak az eszköznek az IPv4 formátumú IP-címét vagy teljes tartománynevét (FQDN), amelyre az Integrációs kiszolgáló telepítve van.

   - **SVM-címek egyéni listájának használata**. Hozzon létre egy listát azokról az SVM-ekről, amelyekhez a Light Agent csatlakozhat. Adja meg az IPv4 formátumú IP-címet vagy az SVM teljes tartománynevét (FQDN). Minden listaelemet új sorba kell beírni, vagy az előző elemtől pontosvesszővel (`;`) kell elválasztani.

     Az SVM-címek listájában csak olyan teljes tartományneveket (FQDN) adjon meg, amelyeknek egyetlen IP-cím felel meg. Több IP-címnek megfelelő, teljes tartománynév használata hibás megoldáshoz vezethet.

4. Mentse el a módosításokat.

Az SVM kiválasztási algoritmus konfigurálása a Light Agenthez

A szervezet infrastruktúrájában több telepített SVM is lehet, amelyekhez a Light Agentek csatlakozhatnak. A hálózat terhelésének és a virtuális infrastruktúra erőforrásainak egyensúlyba hozásához el kell osztania a Light Agenteket az SVM-ek között.

A Light Agentek a következő SVM kiválasztási algoritmusokat alkalmazhatják a csatlakozáshoz:

Standard algoritmus (alapértelmezett)

Ha ezt az algoritmust alkalmazza, a telepítés és az indítás után a virtuális gépen lévő Light Agent úgy dönt, hogy egy a Light Agent szempontjából *helyi* SVM-hez csatlakozik.

Az, hogy egy SVM helyinek minősül-e egy Light Agent számára, a virtuális infrastruktúra típusától függ:

- A Basis Dynamix Enterprise-on alapuló virtuális infrastruktúrában azon SVM tekinthető egy Light Agent számára helyi SVM-nek, amely ugyanazon a csomóponton van telepítve, mint a Light Agentet tartalmazó virtuális gép.

- A Microsoft Hyper-V, a XenServer, a VMware vSphere, a KVM, a Proxmox VE, a Basis, a HUAWEI FusionSphere, a Nutanix Acropolis, az ALT Virtualization Server, az Astra Linux, a Numa vServer vagy a Basis Dynamix Standard alapú virtuális infrastruktúrában a Light Agent számára helyi SVM-nek az a SVM minősül, amely ugyanazon a hipervizoron van telepítve, mint a Light Agentet futtató virtuális gép.

- Az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában az Integrációs kiszolgáló konfigurációs fájljának (appsettings.json) `HypervisorSpecificSettings:Openstack` szakaszában található `StandardAlgorithmSvmLocality` paraméterrel lehet megadni, hogy az SVM helyét hogyan kell meghatározni a Light Agenthez viszonyítva. Az Integrációs kiszolgáló verziójától függően a fájl az alábbi elérési útvonalak egyikén található:

  - /var/opt/kaspersky/viis/common/ a Linux-alapú Integrációs kiszolgáló esetében

  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ a Windows-alapú Integrációs kiszolgáló esetében

A `StandardAlgorithmSvmLocality` paraméter a következő értékeket veheti fel:

- `ServerGroup` – ha ez az érték van kiválasztva, akkor az SVM-et a Light Agenthez tartozóként kezeljük, amennyiben ugyanabban a kiszolgálócsoportban található, mint az a virtuális gép, amelyre a Light Agent telepítve van. Ez az érték alapértelmezés szerint használatos.

- `Project` – ha ez az érték van kiválasztva, akkor az SVM a Light Agenthez tartozó helyi elemnek minősül, amennyiben ugyanazon OpenStack-projekt keretében kerül telepítésre, mint a Light Agentet futtató virtuális gép.

- `AvailabilityZone` – ha ez az érték van kiválasztva, akkor az SVM-et a Light Agenthez tartozóként kezeljük, amennyiben ugyanabban a rendelkezésre állási zónában található, mint az a virtuális gép, amelyre a Light Agent telepítve van.

Ha nem állnak rendelkezésre helyi SVM-ek a csatlakozáshoz, a Light Agent a legkevesebb csatlakoztatott Light Agenttel rendelkező SVM-et választja ki, függetlenül a virtuális infrastruktúrán lévő SVM-útvonaltól.

Az alkalmazás nem állapítja meg, hogy az SVM a Light Agenthez képest helyi-e, amennyiben az SVM-en futó védelmi kiszolgáló esetében a nagy infrastruktúra-védelmi mód engedélyezve van. Ebben az esetben ajánlott a kiterjesztett SVM-kiválasztási algoritmust használni, és az SVM-felismerési módszerként az integrációs kiszolgálót választani.

Kiterjesztett algoritmus

Ha ezt az algoritmust alkalmazza, a következő SVM-kiválasztási beállításokat adhatja meg:

- szükséges-e figyelembe venni vagy figyelmen kívül hagyni az SVM-ek helyét az infrastruktúrában az összekapcsolásra szánt SVM-ek kiválasztásakor

- ha figyelembe vesszük az SVM helyét, akkor a Light Agenthez viszonyított SVM helyzetének meghatározására szolgáló módszer

Ha a Light Agentek figyelmen kívül hagyják az SVM-ek helyét az infrastruktúrában, akkor bármelyik elérhető SVM-hez képesek lesznek csatlakozni.

Ha a Light Agenteknek figyelembe kell venniük az SVM-ek helyét az infrastruktúrában, akkor ki kell választania azt a típusú SVM-elérési utat, amelyet a Light Agenthez viszonyított SVM-hely meghatározásakor kell figyelembe venni. Az, hogy egy SVM helyinek minősül-e a Light Agent számára, a virtuális infrastruktúra típusától függ.

A Basis Dynamix Enterprise-on alapuló virtuális infrastruktúrában egy SVM a következő esetek bármelyikében a Light Agenthez tartozó helyi elemnek tekinthető:

- Az SVM ugyanazon a csomóponton van telepítve, mint a Light Agenttel felszerelt virtuális gép.

- Az SVM ugyanabban a zónában van telepítve, mint a Light Agenttel felszerelt virtuális gép.

- Az SVM ugyanabban az adatközpontban van telepítve, mint a Light Agenttel felszerelt virtuális gép.

A Microsoft Hyper-V, a XenServer, a VMware vSphere, a KVM, a Proxmox VE, a Basis, a HUAWEI FusionSphere, a Nutanix Acropolis, az ALT Virtualization Server, az Astra Linux, a Numa vServer vagy a Basis Dynamix Standard alapú virtuális infrastruktúrában egy SVM a következő esetek bármelyikében tekinthető a Light Agenthez tartozó helyi elemnek:

- Az SVM ugyanazon a hipervizoron van telepítve, mint a Light Agenttel felszerelt virtuális gép.
- Az SVM ugyanazon a hipervizor-klaszteren van telepítve, mint a Light Agenttel felszerelt virtuális gép.
- Az SVM ugyanabban az adatközpontban van telepítve, mint a Light Agenttel felszerelt virtuális gép.

Az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában egy SVM a következő esetek bármelyikében tekinthető a Light Agenthez tartozó helyi elemnek:

- Az SVM ugyanabban a kiszolgálócsoportban található, mint a Light Agenttel felszerelt virtuális gép.
- Az SVM ugyanabban az OpenStack-projektben van telepítve, mint a Light Agenttel felszerelt virtuális gép.
- Az SVM ugyanabban a rendelkezésre állási zónában található, mint a Light Agenttel felszerelt virtuális gép.

Ha a Light Agentek az infrastruktúrában található SVM-ek elhelyezkedését is figyelembe veszik annak eldöntésekor, hogy melyik SVM-hez csatlakozzanak, akkor csak a helyi SVM-ekhez tudnak csatlakozni.

Például, ha hipervizor fürtöt ad meg SVM elérési úttípusként, akkor az ezen a hipervizor fürtön telepített összes SVM-et a Light Agent helyi elemnek tekinti, és a Light Agent csak az egyik ilyen SVM-hez tud csatlakozni. Ha azon a fürtön, ahol a Light Agent fut, nincs elérhető SVM, amelyhez csatlakozhatna, a Light Agent nem csatlakozik SVM-hez.

Az SVM-ek kiválasztásakor a Light Agentek figyelembe veszik a csatlakozó Light Agentek számát is, hogy biztosítsák a Light Agentek egyenletes elosztását a csatlakozásra rendelkezésre álló SVM-ek között.

Ha a Light Agent a kiterjesztett SVM-kiválasztási algoritmust használja és az SVM-felderítési módszer SVM-címlista, valamint a nagy infrastruktúravédelmi mód engedélyezett az SVM-en, akkor a Light Agent csak akkor csatlakozhat ehhez az SVM-hez, ha az SVM-elérési út figyelmen kívül hagyható.

Az SVM csatlakozási algoritmusok mellett lehetőség van a Light Agentek és SVM-ek összekapcsolásának szabályozására címkék segítségével.

A Light Agent SVM kiválasztási algoritmusának konfigurálása a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki a **Light Agent üzemmód → SVM kiválasztási algoritmus** lehetőséget.
4. Válassza ki az algoritmust:
   - **A standard SVM kiválasztási algoritmus használata**. A Light Agent kiválasztja az ugyanabban a hipervizorban telepített SVM-eket.
   - **A kiterjesztett SVM kiválasztási algoritmus használata**. A Light Agent kiválasztja a kiválasztott SVM útvonaltípusban telepített SVM-eket (alapértelmezés szerint **Hipervizor**).

5. Ha szükséges, válassza ki az SVM elérési utat a kiterjesztett SVM kiválasztási algoritmushoz:

- **Hipervizor**. A Light Agent egy adott feltételnek megfelelő SVM-et választ ki a csatlakozáshoz (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanazon a hipervizoron vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (olyan virtuális infrastruktúrában, amely Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer vagy Basis Dynamix Standard alapú).

  - Az SVM ugyanabban a kiszolgálócsoportban található, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanazon a csomóponton található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

  Ha azon a hipervizoron vagy abban a kiszolgálói csoportban, ahol a Light Agenttel rendelkező virtuális gép található, nincs elérhető SVM, amelyhez csatlakozni lehetne, a Light Agent nem csatlakozik az SVM-hez.

- **Fürt**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanabban a hipervizor fürtön vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer vagy Basis Dynamix Standard alapú virtuális infrastruktúrában).

  - Az SVM-ek ugyanazon OpenStack-projekt keretében kerülnek telepítésre, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanabban a zónában található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

  Ha azon a hipervizor fürtön vagy abban az OpenStack-projektben, ahol a Light Agenttel rendelkező virtuális gép található, nincs elérhető SVM, amelyhez csatlakozni lehetne, a Light Agent nem csatlakozik az SVM-hez.

- **Adatközpont**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanabban az adatközpontban vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (egy olyan virtuális infrastruktúrában, amely a Microsoft Hyper-V, a XenServer, a VMware vSphere, a KVM, a Proxmox VE, a Basis, a HUAWEI FusionSphere, a Nutanix Acropolis, az ALT Virtualization Server, az Astra Linux, a Numa vServer vagy a Basis Dynamix Standard platformon alapul).

  - Az SVM-ek ugyanabban a rendelkezésre állási zónában találhatók, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanabban az adatközpontban található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

Ha nem áll rendelkezésre SVM a csatlakozáshoz ugyanabban az adatközpontban vagy elérhetőségi zónában, ahol a Light Agentet tartalmazó virtuális gép található, a Light Agent nem csatlakozik az SVM-hez.

- **Kihagyás**. A Light Agent figyelmen kívül hagyja az SVM elérési utat a védelmi kiszolgálóhoz való csatlakozáskor. A Light Agentek egyéb feltételeket is figyelembe vesznek: címkék, az SVM-hez csatlakoztatott Light Agentek száma stb.

6. Mentse el a módosításokat.

Az SVM kiválasztási algoritmus konfigurálása a Light Agenthez a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Light Agent Mode** → **SVM selection algorithm** elemet.
5. Válassza ki az algoritmust:

   - **Use the standard SVM selection algorithm**. A Light Agent kiválasztja az ugyanabban a hipervizorban telepített SVM-eket.
   - **Use the extended SVM selection algorithm**. A Light Agent kiválasztja a kiválasztott SVM útvonaltípusban telepített SVM-eket (alapértelmezés szerint **Hypervisor**).
6. Ha szükséges, válassza ki az SVM elérési utat a kiterjesztett SVM kiválasztási algoritmushoz:

   - **Hypervisor**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

     - Az SVM-ek ugyanazon a hipervizoron vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (olyan virtuális infrastruktúrában, amely Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer vagy Basis Dynamix Standard alapú).
     - Az SVM ugyanabban a kiszolgálócsoportban található, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).
     - Az SVM ugyanazon a csomóponton található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

   Ha azon a hipervizoron vagy abban a kiszolgálói csoportban, ahol a Light Agenttel rendelkező virtuális gép található, nincs elérhető SVM, amelyhez csatlakozni lehetne, a Light Agent nem csatlakozik az SVM-hez.

- **Cluster**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanabban a hipervizor fürtön vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer vagy Basis Dynamix Standard alapú virtuális infrastruktúrában).

  - Az SVM-ek ugyanazon OpenStack-projekt keretében kerülnek telepítésre, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanabban a zónában található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

  Ha azon a hipervizor fürtön vagy abban az OpenStack-projektben, ahol a Light Agenttel rendelkező virtuális gép található, nincs elérhető SVM, amelyhez csatlakozni lehetne, a Light Agent nem csatlakozik az SVM-hez.

- **Data center**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanabban az adatközpontban vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (egy olyan virtuális infrastruktúrában, amely a Microsoft Hyper-V, a XenServer, a VMware vSphere, a KVM, a Proxmox VE, a Basis, a HUAWEI FusionSphere, a Nutanix Acropolis, az ALT Virtualization Server, az Astra Linux, a Numa vServer vagy a Basis Dynamix Standard platformon alapul).

  - Az SVM-ek ugyanabban a rendelkezésre állási zónában találhatók, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanabban az adatközpontban található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

  Ha nem áll rendelkezésre SVM a csatlakozáshoz ugyanabban az adatközpontban vagy elérhetőségi zónában, ahol a Light Agentet tartalmazó virtuális gép található, a Light Agent nem csatlakozik az SVM-hez.

- **Ignore**. A Light Agent figyelmen kívül hagyja az SVM elérési utat a védelmi kiszolgálóhoz való csatlakozáskor. A Light Agentek egyéb feltételeket is figyelembe vesznek: címkék, az SVM-hez csatlakoztatott Light Agentek száma stb.

7. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

Az SVM kiválasztási algoritmus konfigurálása a Light Agenthez az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazás beállításai ablakban a **Light Agent üzemmód** részen kattintson az **SVM felderítési beállítások** csempére.

3. Válassza ki az algoritmust:

   - **A standard SVM kiválasztási algoritmus használata**. A Light Agent kiválasztja az ugyanabban a hipervizorban telepített SVM-eket.

   - **A kiterjesztett SVM kiválasztási algoritmus használata**. A Light Agent kiválasztja a kiválasztott SVM útvonaltípusban telepített SVM-eket (alapértelmezés szerint **Hipervizor**).

4. Ha szükséges, válassza ki az SVM elérési utat a kiterjesztett SVM kiválasztási algoritmushoz:

- **Hipervizor**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanazon a hipervizoron vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (olyan virtuális infrastruktúrában, amely Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer vagy Basis Dynamix Standard alapú).

  - Az SVM ugyanabban a kiszolgálócsoportban található, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanazon a csomóponton található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

  Ha azon a hipervizoron vagy abban a kiszolgálói csoportban, ahol a Light Agenttel rendelkező virtuális gép található, nincs elérhető SVM, amelyhez csatlakozni lehetne, a Light Agent nem csatlakozik az SVM-hez.

- **Fürt**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanabban a hipervizor fürtön vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer vagy Basis Dynamix Standard alapú virtuális infrastruktúrában).

  - Az SVM-ek ugyanazon OpenStack-projekt keretében kerülnek telepítésre, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanabban a zónában található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

  Ha azon a hipervizor fürtön vagy abban az OpenStack-projektben, ahol a Light Agenttel rendelkező virtuális gép található, nincs elérhető SVM, amelyhez csatlakozni lehetne, a Light Agent nem csatlakozik az SVM-hez.

- **Adatközpont**. A Light Agent kiválaszt egy olyan SVM-et a csatlakozáshoz, amely megfelel a kritériumoknak (a virtuális infrastruktúra típusától függően):

  - Az SVM-ek ugyanabban az adatközpontban vannak telepítve, mint a Light Agenttel felszerelt virtuális gép (egy olyan virtuális infrastruktúrában, amely a Microsoft Hyper-V, a XenServer, a VMware vSphere, a KVM, a Proxmox VE, a Basis, a HUAWEI FusionSphere, a Nutanix Acropolis, az ALT Virtualization Server, az Astra Linux, a Numa vServer vagy a Basis Dynamix Standard platformon alapul).

  - Az SVM-ek ugyanabban a rendelkezésre állási zónában találhatók, mint a Light Agenttel felszerelt virtuális gép (az OpenStack vagy a VK Private Cloud platformon futó virtuális infrastruktúrában).

  - Az SVM ugyanabban az adatközpontban található, mint a Light Agenttel felszerelt virtuális gép (a Basis Dynamix Enterprise virtuális infrastruktúrában).

Ha nem áll rendelkezésre SVM a csatlakozáshoz ugyanabban az adatközpontban vagy elérhetőségi zónában, ahol a Light Agentet tartalmazó virtuális gép található, a Light Agent nem csatlakozik az SVM-hez.

- **Kihagyás**. A Light Agent figyelmen kívül hagyja az SVM elérési utat a védelmi kiszolgálóhoz való csatlakozáskor. A Light Agentek egyéb feltételeket is figyelembe vesznek: címkék, az SVM-hez csatlakoztatott Light Agentek száma stb.

5. Mentse el a módosításokat.

A Light Agentek SVM-ekhez való kapcsolatainak elosztása (címkék)

Egy SVM-hez több Light Agent csatlakozhat. A Light Agent kapcsolatok terheléselosztásához megadhat egy külön listát az SVM-ekről. Ha Integrációs kiszolgálót használ az SVM-felderítéshez, használhat *címkéket* a Light Agent és az SVM-ek közötti kapcsolatok terheléselosztásához. Ez azt jelenti, hogy egy Light Agent esetében hozzárendelheti az SVM-ek listáját egy címke alapú csatlakozáshoz. Vagyis hozzá kell rendelnie egy címkét a Light Agenthez, és meg kell adnia ezt a címkét az SVM beállításaiban. A címkék SVM-beállításokban történő megadásával kapcsolatos részletek: Kaspersky Security for Virtualization Light Agent súgó.

Példa: A Kaspersky Endpoint Detection and Response Optimum megoldás telepítve van az infrastruktúrában a kijelölt virtuálisgép-állomásokon. Ebben az esetben hozzárendelheti az `[EDROptimum]` címkét a Light Agenthez, hogy az az EDR Optimum (EDR Optimum kiegészítő) licenckulcsot tartalmazó SVM-ekhez csatlakozzon. Ennek eredményeként használhatja az EDR Optimum funkciót a virtuális gépen a Light Agent segítségével. Ha a Light Agentet EDR Optimum licenckulcs nélkül csatlakoztatja egy SVM-hez, a Kaspersky Endpoint Detection and Response Optimum funkció nem érhető el.

SVM csatlakozási címke hozzárendelése egy Light Agenthez a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A házirend ablakban válassza ki a **Light Agent üzemmód** → **SVM csatlakozási címke** lehetőséget.
4. Jelölje be a **Csatlakozási címke használata** jelölőnégyzetet, és adjon meg egy SVM csatlakozási címkét.

   A címkékhez legfeljebb 255 karakter hosszúságú karakterláncot adhat meg. Bármilyen karaktert használhat, kivéve a `;` karaktert.
5. Mentse el a módosításokat.

SVM csatlakozási címke hozzárendelése egy Light Agenthez a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Light Agent Mode** → **SVM connection tag** elemet.

5. Jelölje be a **Use connection tag** jelölőnégyzetet, és adjon meg egy SVM csatlakozási címkét.

   A címkékhez legfeljebb 255 karakter hosszúságú karakterláncot adhat meg. Bármilyen karaktert használhat, kivéve a `;` karaktert.

6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

SVM csatlakozási címke hozzárendelése egy Light Agenthez az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.

2. Az alkalmazás beállításai ablakban a **Light Agent üzemmód** részen kattintson az **SVM csatlakozási címke** csempére.

3. Jelölje be a **Csatlakozási címke használata** jelölőnégyzetet, és adjon meg egy SVM csatlakozási címkét.

   A címkékhez legfeljebb 255 karakter hosszúságú karakterláncot adhat meg. Bármilyen karaktert használhat, kivéve a `;` karaktert.

4. Mentse el a módosításokat.

A Light Agent és az SVM közötti kapcsolat védelme

Beállíthatja a Light Agentek és a védelmi kiszolgáló közötti kapcsolat titkosítását. Ehhez engedélyeznie kell a Light Agent és a védelmi kiszolgáló közötti adatcsatorna titkosítását az SVM védelmi kiszolgálójának beállításaiban és a Light Agent beállításaiban.

Az a Light Agent, amelynél a kapcsolatvédelem engedélyezve van, csak olyan SVM-ekhez csatlakozhat, amelyeknél engedélyezve van a Light Agent és a védelmi kiszolgáló közötti adatcsatorna titkosítása. Az a Light Agent, amelynél a kapcsolatvédelem le van tiltva, csak olyan SVM-ekhez csatlakozhat, amelyeknél a csatornatitkosítás le van tiltva, vagy a védelmi kiszolgáló és a Light Agent közötti nem biztonságos kapcsolat engedélyezett.

A kapcsolatvédelem védelmi kiszolgálón történő konfigurálásával kapcsolatos részletek: Kaspersky Security for Virtualization Light Agent súgó.

A kapcsolat titkosítással történő védelme ronthatja a Kaspersky Security for Virtualization Light Agent teljesítményét.

A kapcsolatvédelem konfigurálása Light Agentben a felügyeleti konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A házirend ablakban válassza ki a **Light Agent üzemmód** → **Kapcsolatvédelem** lehetőséget.

4. Jelölje be a **Light Agent és a Védelmi kiszolgáló közötti adatcsatorna titkosítása** jelölőnégyzetet.

5. Mentse el a módosításokat.

A kapcsolatvédelem konfigurálása Light Agentben a Web Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **Light Agent Mode** → **Connection protection** elemet.
5. Tegyen jelölést a **Encrypt data channel between Light Agent and the Protection Server** jelölőnégyzetbe.
6. A szabályzat számítógépekre való alkalmazásához zárja le a lakat ikonokat, és mentse a módosításokat.

A kapcsolatvédelem konfigurálása Light Agentben az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az alkalmazás beállításai ablakban a **Light Agent üzemmód** részen kattintson a **Kapcsolatvédelem** csempére.
3. Jelölje be a **Light Agent és a Védelmi kiszolgáló közötti adatcsatorna titkosítása** jelölőnégyzetet.
4. Mentse el a módosításokat.

A Light Agent aktiválása

Ha a Kaspersky Endpoint Security alkalmazást Light Agent üzemmódban használja a virtuális környezetek védelmére, nem kell külön aktiválnia az alkalmazást. Az alkalmazás aktiválásához egy licenckulcsot kell hozzáadni az SVM-hez. A Kaspersky Security Center konzol speciális feladatának segítségével licenckulcsot adhat hozzá az SVM-hez. A Light Agent felületen nem kezelheti a licenckulcsokat, azonban megtekintheti a licencinformációkat (lásd az alábbi ábrát). A Light Agent licencelési információit a parancssorban is megtekintheti (lásd az alábbi utasításokat). A Light Agent ezeket az információkat az SVM-től kapja. A megoldás aktiválásával és a licenckulcsok kezelésével kapcsolatos részletek: Kaspersky Security for Virtualization Light Agent súgó.

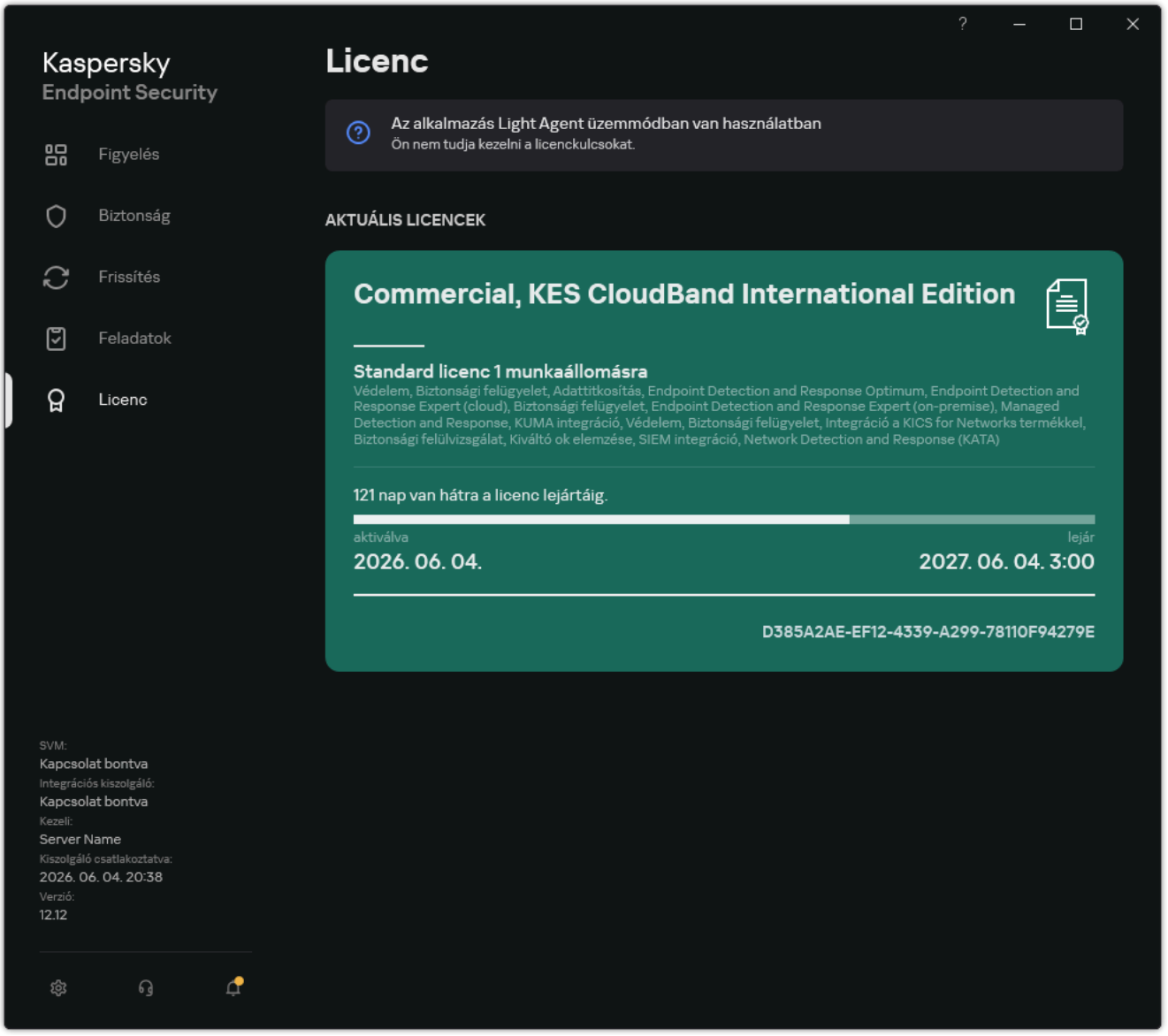
A Light Agent licencelési információinak megtekintése:

1. Futtassa az értelmező parancssort (cmd) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

3. Futtassa a következő parancsot:

```
avp.com LICENSE /CHECK
```

Ennek eredményeként a Kaspersky Endpoint Security megjeleníti a licencinformációkat: annak az SVM-nek a címét, amelyhez a Light Agent csatlakozik, a napok számát a licenc lejáratáig és az egyéb információkat. Ha bármilyen problémába ütközik a Light Agent aktiválása során, tekintse meg a Terméktámogatási tudásbázist.



Licenckezelés ablak

A KSVLA Light Agentről KES Light Agentre való áttelepítés útmutatója

A Kaspersky Security for Virtualization 5.2 Light Agent tartalmazza a Light Agent for Windows 5.2 összetevőt (a továbbiakban „KSVLA Light Agent"). A Kaspersky Security for Virtualization Light Agent 6.2-ben a Kaspersky Endpoint Security Light Agent üzemmódban használható Light Agent összetevőként. A megoldás 6.2 verzióra történő frissítéséhez a KSVLA Light Agent 5.2 verzióról át kell térnie a Kaspersky Endpoint Security Light Agent üzemmódra (a továbbiakban „KES Light Agent"). A Kaspersky Security for Virtualization Light Agent megoldás verziófrissítésével kapcsolatos részletekért lásd a Kaspersky Security for Virtualization Light Agent súgóját.

Szoftverkövetelmények

Mielőtt elkezdené a KSVLA Light Agentről a KES Light Agentre való áttelepítést, győződjön meg arról, hogy a virtuális gép megfelel-e a Kaspersky Endpoint Security for Windows hardver- és szoftverkövetelményeinek. A támogatott operációsrendszer-verziók listája eltér a KES és a KSWS esetében. Például a KES nem támogatja a Windows Server 2003 rendszert futtató kiszolgálókat.

A KSVLA Light Agentről a KES Light Agentre való átállás minimális szoftverkövetelményei:

- Kaspersky Endpoint Security for Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (beleértve a védelmi és az integrációs kiszolgáló összetevőit).
- Kaspersky Security Center 14.2

  Ha a Kaspersky Security Center korábbi verziója van telepítve, frissítse azt a 14.2 vagy újabb verzióra. A Kaspersky Security Center ezen verziójában a Házirendek és feladatok kötegelt konvertálási varázslója lehetővé teszi a házirendek házirend helyett profilba történő áttelepítését. A Kaspersky Security Center ezen verziójában a Házirendek és feladatok kötegelt konvertálási varázslója a házirend-beállítások szélesebb körének áttelepítését is lehetővé teszi.

Az áttelepítés lépései

A KSVLA Light Agentről KES Light Agentre való átállás félig automatikusan történik. Erre az alkalmazások eltérő architektúrái miatt van szükség.

A KSVLA Light Agentről a KES Light Agentre a következő sorrendben térhet át:

1. **A KSVLA Light Agent-feladatok és -házirendek áttelepítése**

   A házirend-beállítások áttelepítéséhez futtassa a Házirendek és feladatok kötegelt konvertálási varázslót (áttelepítési varázsló). A házirend-beállítások áttelepítése után manuálisan kell konfigurálnia azokat a beállításokat, amelyeket az áttelepítési varázsló nem tud automatikusan áttelepíteni (például adatbázis-frissítési beállításokat). Az áttelepítés után ajánlott ellenőrizni azt is, hogy az áttelepítési varázsló megfelelően végezte-e el az összes beállítás áttelepítését.

   Ha a Jelszóvédelem engedélyezve van a KSVLA Light Agenthez való hozzáférés korlátozásához, a KES Light Agent telepítése előtt le kell tiltania a Jelszóvédelmet a KSVLA Light Agent házirendjében. Nem adhatja meg az eltávolítási jelszót a KES Light Agent telepítőcsomag beállításaiban. Miután befejezte a KES Light Agent KSVLA Light Agent fölé való telepítését, engedélyeznie kell a jelszavas védelmet a KES házirendjében.

2. **A Kaspersky Endpoint Security Light Agent üzemmód telepítése**

   A KES Light Agent telepítése a következő módokon történhet:

   - A KES Light Agent telepítése a KSVLA Light Agent eltávolítása után (ajánlott)
   - A KES Light Agent telepítése a KSVLA Light Agent fölé

3 Győződjön meg arról, hogy az alkalmazás az áttelepítés után működőképes

A KSVLA Light Agentről a KES Light Agentre való átállás után győződjön meg arról, hogy az alkalmazás megfelelően működik-e. Aktiválja a konvertált házirendet. Ellenőrizze a virtuális gép állapotát a Kaspersky Security Center-konzolon (*OK* állapotúnak kell lennie). Győződjön meg arról, hogy az alkalmazás nem jelent hibát, valamint ellenőrizze az SVM-hez való utolsó kapcsolódás idejét és a virtuális gép védelmi állapotát is. Nem kell aktiválnia a Light Agentet, mert a licenckulcs hozzá van adva az SVM-hez.

A KES Light Agent telepítése a KSVLA Light Agent helyett

A KES Light Agent a következő módokon telepíthető:

- A KES Light Agent telepítése a KSVLA Light Agent eltávolítása után (ajánlott)
- A KES Light Agent telepítése a KSVLA Light Agent fölé

A KSVLA Light Agent eltávolítása

Az alkalmazást távolról is eltávolíthatja a *Install application remotely* feladatot használva – helyileg a virtuális gépen vagy a virtuálisgép-sablonban. A KSVLA Light Agent eltávolítása után újból előfordulhat, hogy újra kell indítania a virtuális gépet.

A KSVLA Light Agent eltávolítása után telepítse a KES Light Agentet egy arra alkalmas módszerrel.

Telepítse a Kaspersky Endpoint Security alkalmazást

Ha a Jelszóvédelem engedélyezve van a KSVLA Light Agenthez való hozzáférés korlátozásához, a KES Light Agent telepítése előtt le kell tiltania a Jelszóvédelmet a KSVLA Light Agent házirendjében. Nem adhatja meg az eltávolítási jelszót a KES Light Agent telepítőcsomag beállításaiban. Miután befejezte a KES Light Agent KSVLA Light Agentre való telepítését, engedélyeznie kell a jelszavas védelmet a KES házirendjében.

A Kaspersky Endpoint Security telepítésekor ki kell választania a **Light Agent a virtuális környezetek védelme céljából** módot. A KES Light Agent virtuális gépen való telepítése előtt a telepítő a KSVLA Light Agentet inkompatibilis szoftverként észleli, és eltávolítja azt. A KSVLA Light Agent konfigurációjának áttelepítése nem támogatott. Ez azt jelenti, hogy a KES Light Agent telepítésekor a telepítendő összetevők körét a telepítőcsomag vagy a telepítővarázsló kiválasztott beállításai határozzák meg. A KSVLA Light Agent eltávolítása után újra kell indítania a virtuális gépet.

A KSVLA Light Agent beállításai és feladatai nem települnek át a KES Light Agent telepítésekor. A beállítások és feladatok áttelepítéséhez futtassa a Házirendek és feladatok kötegelt átalakítása varázslót.

A telepített összetevők listáját az alkalmazásfelület **Biztonság** részén ellenőrizheti a `status` paranccsal vagy a Kaspersky Security Center-konzolon, a számítógép tulajdonságainál. Az összetevők készletét a telepítés után az *Alkalmazásösszetevők módosítása* feladattal módosíthatja.

A KSVLA Light Agent és a KES Light Agent összetevőinek megfeleltetése

A KSVLA Light Agent és a KES Light Agent összetevőkészlete gyakorlatilag megegyezik. A KES Light Agent több beállítással rendelkezik, mint a KSVLA Light Agent. Az áttelepítés után az új beállítások alapértelmezett értékkel rendelkeznek.

A KSVLA Light Agent és a KES Light Agent összetevőinek megfeleltetése

Light Agent 5.2	KES Light Agent
Scan kernel	Alkalmazáskernel
File Anti-Virus	Fájl védelem
Mail Anti-Virus	Levelezés védelem
Web Anti-Virus	Web védelem
Firewall	Tűzfal
Network Attack Blocker	Hálózati védelem
Application Privilege Control	Behatolásmegelőző rendszer
Applications Launch Control	Alkalmazásfelügyelő
Web Control	Webfelügyelő
Device Control	Eszközfelügyelő
System Watcher	A Kaspersky Endpoint Security alkalmazásban ez az összetevő a következő összetevőkre oszlik: • Biztonsági rések kihasználásának megelőzése • Viselkedésészlelés • Kármentesítő motor
System Integrity Monitoring	Rendszerintegritás-figyelő
Integration with Kaspersky Endpoint Agent	*(nem támogatott)* A Kaspersky Endpoint Security for Windows 11.9.0-tól kezdődően a Kaspersky Endpoint Agent terjesztőcsomag már nem része a terjesztőkészletnek.
AMSI Protection	AMSI védelem

A KSVLA Light Agent-feladatok és -házirendek áttelepítése

A KSVLA Light Agent házirendek és feladatok beállításait a Házirendek és feladatok kötegelt konvertálási varázsló (a továbbiakban: „áttelepítési varázsló") segítségével migrálhatja.

A KSVLA Light Agent áttelepítési varázsló csak a felügyeleti konzolon (MMC) érhető el. A házirend- és feladatbeállítások nem telepíthetők át a Web Console-ban és a Cloud Console-ban.

A házirendek és feladatok áttelepítésével kapcsolatban a következő különleges megfontolások merülnek fel:

- Az új házirend neve *<Házirend> (átalakítva)*.
- Az új házirend *Inactive policy* állapotot kap.
- A beállítások módosításának tilalma (a „lakat") nem kerül áttelepítésre. A Migrációs varázsló állítja be az alapértelmezett értékeket.

- A házirendprofilok nem lesznek áttelepítve. A házirendprofilokat manuálisan kell hozzáadnia.

- Továbbfejlesztett megbízható zónakezelés. A KSVLA Light Agentben csak akkor adhat hozzá előre meghatározott kizárásokat, ha már létrehozott házirendet. Ezt követően a házirend beállításaiban konfigurálhatja a korábban hozzáadott előre meghatározott kizárásokat, vagy manuálisan is hozzáadhat kizárásokat. Nem adhat hozzá előre meghatározott kizárásokat a házirend beállításaiban. A KES Light Agentben előre definiált kizárások állnak rendelkezésre mind a házirend létrehozása során, mind a létrehozott házirend beállításaiban. A telepítőcsomagban elérhető előre meghatározott kizárásokat is használhatja.

- A Kaspersky Endpoint Security alkalmazás felhasználói felületének konfigurációja átkerült a telepítőből a házirendbe. Ha például el kell rejtenie az alkalmazás felhasználói felületét, módosítsa a házirend beállításait.

- A jogosultságalapú hozzáférés-vezérlés (RBAC) konfigurálására szolgáló funkciók a Kaspersky Endpoint Security és a KSVLA Light Agent esetében eltérőek. A működési területek felhasználói hozzáférési jogosultságait teljesen manuálisan kell beállítania.

A Házirendek és feladatok kötegelt átalakítása varázsló használata a KSVLA Light Agent-házirendek beállításainak áttelepítéséhez

1. A Felügyeleti konzolon válassza a Felügyeleti kiszolgáló lehetőséget, és kattintson a jobb gombbal a helyi menü megnyitásához.

2. Válassza az **All tasks** → **Policies and tasks batch conversion wizard** lehetőséget.

A Házirendek és feladatok kötegelt átalakítása varázsló elindul. Kövesse a varázsló utasításait.

1. lépés: Válassza ki azt az alkalmazást, amelyhez házirendeket és feladatokat kell konvertálnia

Ennél a lépésnél a Kaspersky Endpoint Security for Windows lehetőséget kell választania. Lépjen a következő lépésre.

2. lépés: Házirendek átalakítása

Válassza ki a konvertálni kívánt Kaspersky Security for Virtualization 5.2 Light Agent for Windows házirendet. Lépjen a következő lépésre.

Az áttelepítési varázsló ezután elkezdi a házirendek átalakítását. Az átalakítás során az Áttelepítési varázsló felkéri a KSN nyilatkozat feltételeinek elfogadására. Az új házirend neve *<Házirend> (átalakítva)*.

3. lépés: Feladatok átalakítása

Az áttelepítési varázsló új feladatokat hoz létre a Kaspersky Endpoint Security for Windows számára. A feladatlistából válassza ki azokat a KSVLA Light Agent-feladatokat, amelyeket létre szeretne hozni a Kaspersky Endpoint Security termékhez. Az új feladatok neve *<Feladatnév> (átalakítva)* lesz. Lépjen a következő lépésre.

4. lépés. A varázsló befejezése

Lépjen ki a varázslóból.

Egy házirend áttelepítése után meg kell nyitnia a házirend tulajdonságait, ellenőriznie kell a beállításait, és mentenie kell a házirendet. Ha nem végzi el ezeket a lépéseket, a KES Light Agent figyelmen kívül hagyhatja az átalakított szabályzatot.

Fordítson különös figyelmet a Light Agent SVM csatlakozási beállítások, a kizárási listák, a megbízható alkalmazások, a megbízható webcímek és az alkalmazásfelügyeleti szabályok áttelepítésére.

A [KSVLA Light Agent+KEA] konfiguráció áttelepítése a [KES Light Agent+beépített ügynök] konfigurációra

A Kaspersky Endpoint Security for Windows EDR (KATA), EDR Optimum és Kaspersky Sandbox használati támogatásának részeként egy beépített ügynök került be az alkalmazásba. Az ezekkel a megoldásokkal való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra.

A KSVLA Light Agentről a KES Light Agentre való áttéréskor az EDR (KATA), az EDR Optimum és a Kaspersky Sandbox megoldás továbbra is együttműködik a Kaspersky Endpoint Security termékkel. Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről.

Mielőtt áttérne a KSVLA Light Agentről a KES Light Agentre, frissítenie kell a Kaspersky Security for Virtualization összes összetevőjét a 6.2-es verzióra, beleértve a védelmi és az integrációs kiszolgálót is. A Kaspersky Security for Virtualization Light Agent megoldás verziófrissítésével kapcsolatos részletekért lásd a Kaspersky Security for Virtualization Light Agent súgóját.

A [KSVLA Light Agent+KEA] konfiguráció [KES Light Agent+beépített ügynök] konfigurációra történő áttelepítése a következő lépéseket foglalja magában:

1. **A házirend és a feladatok áttelepítése**

   A [KSVLA Light Agent+KEA] házirendek és feladatok [KES Light Agent+beépített ügynök] konfigurációra történő áttelepítése a következő lépéseket foglalja magában:

   1. A házirendek és feladatok áttelepítése a KSVLA Light Agentről a KES Light Agentre a Házirendek és feladatok kötegelt átalakítása varázsló segítségével (csak az Adminisztrációs konzolon (MMC) érhető el).

      Ennek eredményeként egy új házirend jön létre a *<Házirend> (átváltva)* néven. Továbbá új KES-feladatok jönnek létre *<Feladatnév> (átalakítva)* néven.

   2. Házirendek és feladatok áttelepítése a KEA-ból a KES-be a Kaspersky Endpoint Agent áttelepítési varázslójával (csak a Web Console-on és a Cloud Console-on érhető el).

      Ennek eredményeként egy új szabályzat jön létre *<a Kaspersky Endpoint Security házirend neve> és <a Kaspersky Endpoint Agent házirend neve>* névvel. Új feladatok és KES feladatok is jönnek létre.

2 A KSVLA Light Agentről KES Light Agentre való áttelepítés útmutatója

A KSVLA Light Agentről a KES Light Agentre való áttérés magában foglalja a KSVLA Light Agent helyett a KES Light Agent telepítését.

A rendszergazdák általában engedélyezik a Jelszóvédelmet, hogy korlátozzák a KSVLA Light Agent és KEA megoldáshoz való hozzáférést. A KEA eltávolítási jelszót csak a *Install application remotely* feladat beállításaiban adhatja meg. Az áttelepítéshez ki kell kapcsolnia a KSVLA Light Agent jelszavas védelmét.

Az áttérés végrehajtásához ki kell választania a Kaspersky Endpoint Security részét képező Detection and Response megoldások támogatásához szükséges összetevőket. Az alkalmazás telepítése után a Kaspersky Endpoint Security átvált a beépített ügynök használatára, és eltávolítja a Kaspersky Endpoint Agent megoldást.

3 Licencelési funkcionalitás

Ha az alkalmazást Light Agent üzemmódban használja, nem kell külön aktiválnia az alkalmazást. Az alkalmazás aktiválásához egy licenckulcsot kell hozzáadni az SVM-hez. Ezenkívül hozzá kell adnia a licenckulcsot a kiegészítő funkciók (például az EDR Optimum) SVM-hez való aktiválásához. Vagyis az áttelepítés részeként a funkciók engedélyezése automatikusan megtörténik.

4 A Kaspersky Endpoint Detection and Response Optimum és a Kaspersky Sandbox állapotának ellenőrzése

Ha a frissítés után a Kaspersky Security Center konzolon a számítógép állapota *Critical*:

- Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 vagy újabb verziójú hálózati ügynök.
- Ellenőrizheti a beépített ügynök működési állapotát az *Report on status of application components* megtekintésével. Ha egy összetevő állapota *Not installed*, telepítse az összetevőt az *Change application components* feladattal.
- Ügyeljen arra, hogy elfogadja a Kaspersky Security Network nyilatkozatot a Kaspersky Endpoint Security for Windows új házirendjében.
- Győződjön meg arról, hogy az EDR Optimum funkció aktiválva van az *Report on status of application components* segítségével. Ha egy összetevőnél a *Nem vonatkozik rá licenc* állapot van érvényben, győződjön meg arról, hogy az EDR Optimum automatikus licenckulcs-szolgáltatói funkciója be van kapcsolva.
- Ellenőrizze a virtuális gép és az SVM közti kapcsolat állapotát. Információkat kaphat a Light Agent SVM-hez való csatlakozásának állapotáról a Kaspersky Endpoint Security alkalmazásban vagy alkalmazás-paranccsal.

Az alkalmazás kezelése a parancssorból

Kezelheti a Kaspersky Endpoint Security alkalmazást a parancssorból. Megtekintheti az alkalmazáskezeléshez tartozó parancsok listáját, ha futtatja a `avp.com HELP` parancsot. A megadott parancs szintaxisának elolvasásához adja meg a `avp.com HELP <command>` parancsot.

A parancs speciális karaktereit escape-karakterrel kell megjelölni. A `&`, `|`, `(`, `)`, `<`, `>`, `^` karakter escape-karakterrel való megjelöléséhez használja a `^` karaktert (például a `&` karakter használatához írja be ezt: `^&`). A `%` karakter escape-karakterrel való megjelöléséhez ezt írja be: `%%`.

A `1` érték alternatívái a `yes`, `on`, `enable`, `enabled` és `true` értékek. A `0` érték alternatívái a `no`, `off`, `disable`, `disabled` és `false` értékek.

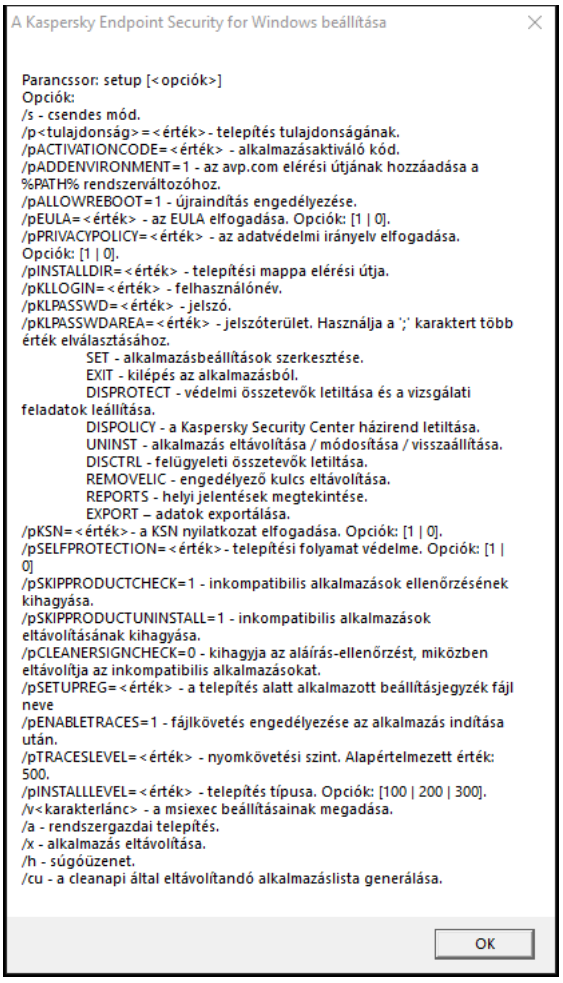
Setup. Az alkalmazás telepítése

A Kaspersky Endpoint Security telepíthető a parancssorból, a következő módon egyikében:

- Interaktív módban az Alkalmazástelepítő varázslóval.
- Csendes módban. Miután a telepítés csendes üzemmódban indult, az Ön részvétele a telepítési folyamatban nem szükséges (csendes telepítés). Az alkalmazás csendes módban történő telepítéséhez használja a `/s` és `/qn` kulcsokat.

  Mielőtt csendes módban telepítené az alkalmazást, nyissa meg és olvassa el a Végfelhasználói Licencszerződést és az Adatvédelmi szabályzat szövegét. A Végfelhasználói Licencszerződés és az Adatvédelmi szabályzat szövege a Kaspersky Endpoint Security terjesztőkészletben található. Csak akkor folytathatja az alkalmazás telepítését, ha elolvasta és elfogadta a Végfelhasználói Licencszerződés rendeleteit és fejezeteit, valamint megértette és beleegyezik az adatai feldolgozásába és továbbításába (köztük harmadik félnek számító országokba), melyek az Adatvédelmi szabályzatnak megfelelően történnek, továbbá akkor, ha alaposan elolvasta és megértette az Adatvédelmi szabályzatot. Ha nem fogadja el a Végfelhasználói Licencszerződés és az Adatvédelmi szabályzat rendeleteit és feltételeit, akkor ne telepítse vagy használja a Kaspersky Endpoint Security alkalmazást.

Megtekintheti az alkalmazás telepítéséhez tartozó parancsok listáját, ha futtatja a(z) `/h` parancsot. Ha segítségre van szüksége a telepítés parancs szintaxisával kapcsolatban, írja be a `setup_kes.exe /h` parancsot. Ennek eredményeképpen a telepítő megjelenít egy ablakot a parancsbeállítások leírásával (lásd a lenti ábrát).



A telepítési parancsbeállítások leírása

Az alkalmazás telepítéséhez vagy az alkalmazás korábbi verziójára való frissítéshez:

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security terjesztőcsomagja telepítve van.
3. Futtassa a következő parancsot:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

vagy

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

Ennek eredményeként az alkalmazás telepítve lesz a számítógépre. A `status` paranccsal ellenőrizheti az alkalmazásbeállításokat, illetve hogy az alkalmazás telepítve van-e.

`EULA=1`	A Végfelhasználói licencszerződés feltételeinek elfogadása. A Licencszerződés szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. A Végfelhasználói licencszerződés feltételeit az alkalmazás telepítéséhez, illetve verziójának frissítéséhez kötelező elfogadni.
`PRIVACYPOLICY=1`	Az Adatvédelmi szabályzat elfogadása. Az Adatvédelmi szabályzat szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. Az alkalmazás telepítéséhez, vagy a verziója frissítéséhez el kell fogadnia az Adatvédelmi szabályzatot.
`KSN`	A Kaspersky Security Network (KSN) való részvétel elfogadása vagy elutasítása. Ha nincs megadott érték a paraméterhez, a Kaspersky Endpoint Security kérni fogja, hogy erősítse meg a KSN-ben való részvételének hozzájárulását vagy elutasítását, amikor a Kaspersky Endpoint Security először elindul. Választható értékek: • `1` – a KSN-ben való részvétel elfogadása. • `0` – a KSN-ben való részvétel elutasítása (alapértelmezett érték). A Kaspersky Endpoint Security terjesztőcsomag a with Kaspersky Security Networkkel való használatra van optimalizálva. Ha úgy döntött, hogy nem vesz részt a Kaspersky Security Networkben, a telepítés befejezését követően azonnal frissítenie kell a Kaspersky Endpoint Security rendszert.
`CONFIGPATH=<path to the configuration file>`	Az alkalmazás telepítése előre megadott beállításokkal. Ehhez fel kell töltenie egy fájlt, ami megszabja a Kaspersky Endpoint Security beállításait. Létrehozhat egy konfigurációs fájlt az alkalmazás helyi felületén.
`ALLOWREBOOT=1`	A számítógép automatikus újraindítása, ha szükséges az alkalmazás telepítése vagy frissítése után. Ha nincs érték megadva ehhez a paraméterhez, blokkolva lesz a számítógép automatikus újraindítása. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.
`SKIPPRODUCTCHECK=1`	A telepített szoftverek ellenőrzésének letiltása. A kompatibilitási problémákat okozó szoftverek listája a terjesztési csomagban található incompatible.txt fájlban érhető el. Ha nincs megadva érték a paraméterhez, és a listán szereplő szoftver észlelhető, a Kaspersky Endpoint Security telepítése leáll.
`SKIPPRODUCTUNINSTALL=1`	Az incompatible.txt listán szereplő, észlelt szoftverek automatikus eltávolításának letiltása. Ha nincs megadva érték a paraméterhez, a Kaspersky Endpoint Security megpróbálja eltávolítani a kompatibilitási problémákat okozó szoftvert. A Kaspersky Endpoint Security msiexec telepítőprogrammal történő telepítésekor nem engedélyezhető a szoftverek automatikus eltávolítása. A kompatibilitási problémákat okozó szoftverek automatikus eltávolításához használja a setup_kes.exe fájlt.
`CLEANERSIGNCHECK=0|1`	Az incompatible.txt listán szereplő, észlelt szoftverfájlok digitális aláírásának ellenőrzése. A szoftver eltávolításához a Kaspersky Endpoint Security futtatja a szoftvertelepítő fájlt. Ha a telepítőfájl nem rendelkezik digitális aláírással, a Kaspersky Endpoint Security nem tekinti a fájlt megbízhatónak, és leállítja a szoftver eltávolítását, hogy elkerülje a potenciálisan rosszindulatú kód futtatását. Ha az alkalmazás nem tudja ellenőrizni az észlelt szoftverfájl digitális aláírását, a Kaspersky Endpoint Security telepítése hibával leáll. Az alapértelmezett érték a szoftvertelepítési módtól függően eltérő: • `0` azt jelenti, hogy a digitális aláírás ellenőrzése le van tiltva (alapértelmezett érték, ha a Kaspersky Security Centeren keresztül telepíti). • `1` azt jelenti, hogy a digitális aláírás ellenőrzése engedélyezve van (alapértelmezett érték, ha az alkalmazást helyileg telepíti).
`STANDALONEMODE=1`	Az alkalmazás telepítése az Endpoint Detection and Response Agent (EDR Agent) konfigurációban a Kaspersky Endpoint Detection and Response (KATA) megoldással vagy a Kaspersky Endpoint Detection and Response Expert (on-premises) megoldással való integrációhoz. Erre a konfigurációra akkor van szükség, ha a Kaspersky Endpoint Detection and Response osztály megoldás mellett egy külső Endpoint Protection Platform (EPP) is telepítve van a vállalatnál. Ezáltal a Kaspersky Endpoint Security az Endpoint Detection and Response Agent konfigurációjában kompatibilis a harmadik féltől származó EPP alkalmazásokkal.
`KLLOGIN`	Állítsa be a felhasználónevet a Kaspersky Endpoint Security funkcióinak és beállításainak eléréséhez (a Jelszóvédelem összetevő). A felhasználónevet a `KLPASSWD` és a `KLPASSWDAREA` paraméterekkel együtt kell megadni. Alapértelmezetten a KLAdmin felhasználónév van használva.

KLPASSWD	A Kaspersky Endpoint Security funkcióihoz és beállításaihoz való hozzáférés jelszavának megadása (a jelszót a KLLOGIN és a KLPASSWDAREA paraméterekkel együtt kell megadni). Ha a KLLOGIN paraméternél jelszót megadott, de felhasználónevet nem, alapértelmezés szerint a rendszer a KLAdmin felhasználónevet használja.
KLPASSWDAREA	A Kaspersky Endpoint Security-hez való hozzáférési jelszó hatókörének megadása. Ha a felhasználó megpróbál végrehajtani egy olyan tevékenységet, ami beletartozik ebbe a hatókörbe, a Kaspersky Endpoint Security kérni fogja a felhasználó fiókjának bejelentkezési adatait (KLLOGIN és KLPASSWD paraméterek). Használja a ; karaktert több érték megadásához. Választható értékek: • SET – az alkalmazásbeállítások módosítása. • EXIT – kilépés az alkalmazásból. • DISPROTECT – védelem összetevőinek letiltása és a vizsgálati feladatok leállítása. • DISPOLICY – a Kaspersky Security Center rendszabályának letiltása. • UNINST – az alkalmazás eltávolítása a számítógépről. • DISCTRL – a felügyeleti összetevők kikapcsolása. • REMOVELIC – a kulcs eltávolítása. • REPORTS – a jelentések megtekintése. • EXPORT – alkalmazásbeállítások exportálása. Például: KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. A KLAdmin felhasználói fióknak joga van végrehajtani bármilyen olyan tevékenységet, ami jelszóvédett. Ezért a KLAdmin fiók jelszótartományának konfigurálása nem lehetséges. Ha a KLAdmin fiók jelszótartományát megpróbálja konfigurálni, az alkalmazás letiltja a megadott műveleteket a „"Mindenki" csoport számára.
PROTECTOSSERVICES	Az operációs rendszer szolgáltatásainak védelme. Az operációs rendszer szolgáltatásainak védelme megakadályozza, hogy harmadik féltől származó alkalmazások beavatkozzanak az operációs rendszer szolgáltatásainak működésébe. Ilyen szolgáltatások közé tartozik például az alkalmazás automatikus indítási szolgáltatása. • Az 1 azt jelenti, hogy az operációs rendszer szolgáltatásainak védelme engedélyezve van (alapértelmezett érték). • A 0 azt jelenti, hogy az operációs rendszer szolgáltatásainak védelme le van tiltva.
ENABLETRACES	Az alkalmazások nyomkövetésének engedélyezése vagy kikapcsolása. Indulása után a Kaspersky Endpoint Security elmenti a nyomkövetési fájlokat a %ProgramData%\Kaspersky Lab\KES.14.1\Traces mappába. Választható értékek: • 1 – a nyomkövetés engedélyezve van. • 0 – a nyomkövetés ki van kapcsolva (alapértelmezett érték).
TRACESLEVEL	A nyomkövetések részleteinek szintje. Választható értékek: • 100 (kritikus). Csak a súlyos hibákról szóló üzenetek. • 200 (magas). Minden hibáról szóló üzenet, köztük a súlyos hibáké. • 300 (diagnosztika). Üzenetek a hibákról, valamint a figyelmeztetésekről. • 400 (fontos). Minden hibaüzenet, figyelmeztetés és további információ. • 500 (normális). Üzenetek a hibákról és figyelmeztetésekről, valamint részletes információ az alkalmazás normál módban történő működéséről (alapértelmezett). • 600 (alacsony). Minden üzenet.
ENABLEAZURESUPPORT	Az Azure WVD-kompatibilitási mód engedélyezése vagy letiltása. Választható értékek: • 1 – az Azure WVD-kompatibilitási mód engedélyezve van. • 0 – az Azure WVD-kompatibilitási mód le van tiltva (alapértelmezett érték). Ez a funkció biztosítja az Azure virtuális gép állapotának megfelelő megjelenítését a Kaspersky Anti Targeted Attack Platform konzolon. A számítógép teljesítményének figyelése céljából a Kaspersky Endpoint Security telemetriai adatokat küld a KATA-kiszolgálóknak. A telemetria tartalmazza a számítógép azonosítóját (Sensor ID). Az Azure WVD-kompatibilitási mód lehetővé teszi állandó egyedi (Sensor ID) hozzárendelését ezekhez a virtuális gépekhez. Ha a kompatibilitási mód ki van kapcsolva, az Azure-beli virtuális gépek működése miatt az (Sensor ID). a számítógép újraindítása után megváltozhat. Ez azt eredményezheti, hogy a virtuális gépek duplikátumai jelennek meg a konzolon.
AMPPL	Engedélyezi vagy kikapcsolja a Kaspersky Endpoint Security folyamatok védelmét az AM-PPL technológiával (Antimalware Protected Process Light). Az AM-PPL technológia részleteiért lásd a Microsoft weboldalt. Az AM-PPL technológia a Windows 10 1703-as (RS2) vagy újabb verziói, valamint a Windows Server 2019 operációs rendszerek számára érhető el. Választható értékek: • 1 – a Kaspersky Endpoint Security folyamatok AM-PPL technológiával történő védelme engedélyezve van. • 0 – a Kaspersky Endpoint Security folyamatok AM-PPL technológiával történő védelme ki van kapcsolva.

`UPGRADEMODE`	Alkalmazásfrissítési mód: • A `Seamless` azt jelenti, hogy az alkalmazás frissítése a számítógép újraindításával történik (alapértelmezett érték). • A `Force` azt jelenti, hogy az alkalmazást újraindítás nélkül frissítjük. Az alkalmazást a 11.10.0 verzióval kezdődően újraindítás nélkül frissítheti. Az alkalmazás korábbi verziójának frissítéséhez újra kell indítania a számítógépet. A javításokat a 11.11.0 verzióval kezdődően újraindítás nélkül is telepítheti. Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Tehát az alkalmazás frissítési módja az alkalmazás beállításaiban lesz megadva. Ezt a paramétert az alkalmazás beállításaiban vagy a házirendben módosíthatja. A már telepített alkalmazás frissítésekor a parancssori paraméter prioritása alacsonyabb, mint az alkalmazásbeállításokban vagy a setup.ini fájlban megadott paraméteré. Például ha a `Force` frissítési mód van megadva a parancssorban, és a `Seamless` mód van megadva az alkalmazásbeállításokban, a frissítés a számítógép újraindításával fog települni (`Seamless`).
`RESTAPI`	Alkalmazás kezelése a REST API felületen keresztül. Ahhoz, hogy az alkalmazást kezelni tudja a REST API felületen keresztül, meg kell adnia a felhasználónevet (`RESTAPI_User` paraméter). Választható értékek: • `1` – a REST API felületen keresztül történő kezelés engedélyezve van. • `0` – a REST API felületen keresztül történő kezelés blokkolva van (alapértelmezett érték). Ahhoz, hogy a REST API felületen keresztül tudjon alkalmazásokat kezelni, engedélyezni kell az adminisztrációs rendszerek használatával történő kezelést. Ehhez állítsa be az `AdminKitConnector=1` paramétert. Ha a REST API felületen keresztül kezeli az alkalmazást, akkor nem lehet az alkalmazást a Kaspersky adminisztrációs rendszereinek használatával kezelni.
`RESTAPI_User`	Az alkalmazás REST API felületen keresztül történő kezeléséhez használt Windows tartományfiók felhasználóneve. A REST API felületen keresztül történő alkalmazáskezelés csak ennek a felhasználónak lehetséges. Adja meg a felhasználónevet a következő formátumban: `<DOMAIN>\<UserName>` (például `RESTAPI_User=COMPANY\Administrator`). A REST API-val történő munkálatokhoz csak egy felhasználót választhat ki. Egy felhasználónév megadása szükséges ahhoz, hogy az alkalmazást a REST API felületen keresztül kezelhesse.
`RESTAPI_Port`	Az alkalmazás REST API felületen keresztül történő kezeléséhez használt port. A 6782 az alapértelmezett port. Győződjön meg arról, hogy a port szabad.
`RESTAPI_Certificate`	Tanúsítvány a kérések azonosítására (pl. `RESTAPI_Certificate=C:\cert.pem`). A Kaspersky Endpoint Security és a REST kliens közötti biztonságos interakció megköveteli a kérésazonosítás konfigurálását. Ehhez telepítenie kell egy tanúsítványt, majd alá kell írnia az egyes kérések adattartalmát.
`ADMINKITCONNECTOR`	Alkalmazáskezelés adminisztrációs rendszerek használatával. Adminisztrációs rendszerek, többek között a Kaspersky Security Center. A Kaspersky adminisztrációs rendszerek mellett harmadik féltől származó megoldásokat is használhat. A Kaspersky Endpoint Security API-t biztosít ebből a célból. Választható értékek: • `1` – az adminisztrációs rendszerekkel történő alkalmazáskezelés engedélyezve van (alapértelmezett érték). • `0` – az alkalmazáskezelés csak a helyi felületen keresztül van engedélyezve.
`EnableUniqueSensorID`	Egyedi számítógép-azonosító (Sensor ID) létrehozása az alkalmazás telepítése vagy frissítése során. A Sensor ID a Kaspersky Anti Targeted Attack Platform megoldásban azon számítógépek azonosítására szolgál, amelyek telemetriai adatokat küldenek a kiszolgálónak. A Sensor ID létrehozásakor az alkalmazás olyan algoritmust használ, amely figyelembe veszi a számítógép konfigurációját, például az alaplap sorozatszámát. Egyes esetekben, például amikor az alkalmazást virtuális környezetben használja, a Sensor ID duplikálódhat. Emiatt a Kaspersky Anti Targeted Attack Platform nem tudja azonosítani azt a számítógépet, amelyről a telemetriai adatokat küldték. Egyedi Sensor ID létrehozásához be kell állítania a `EnableUniqueSensorID=1` paramétert. Emiatt az alkalmazás egy másik algoritmust használ majd a Sensor ID létrehozásához, amely a számítógépre vonatkozó egyéb adatokat is figyelembe vesz. Ez egyedi Sensor ID-t biztosít. Alapértelmezés szerint a paraméter nincs beállítva. Az alkalmazás a következő esetekben örökli a Sensor ID-t: • az alkalmazás verziójának frissítése; • a [KES+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra. Az alkalmazás javításának részeként a telepítő megkísérli örökölni az Sensor ID értékét. Ha az Sensor ID nem állítható vissza, az alkalmazás új Sensor ID jön létre.
`SKIPKB5007186CHECK=1`	A KB5007186 jelű telepített operációsrendszer-frissítés ellenőrzésének letiltása. Az alkalmazás telepítése előtt a telepítő ellenőrzi az operációs rendszer telepített frissítéseit. A KB5007186 jelű frissítés szerepel az operációs rendszer azon frissítéseinek listáján, amelyek problémákat okozhatnak az alkalmazás számára. Részletes információkért tekintse meg a Terméktámogatási tudásbázist. Ezért a telepítő megszakítja a telepítést, ha ezt a frissítést észleli. A telepítés folytatásához állítsa be a `SKIPKB5007186CHECK=1` beállítást.

Példa

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

A Kaspersky Endpoint Security telepítése után a próbalicenc aktiválódik, kivéve, ha a setup.ini fájlban aktiváló kódot adott meg. A próbalicenc általában rövid ideig érvényes. A próbalicenc lejárata után a Kaspersky Endpoint Security minden funkciója letiltásra kerül. Az alkalmazás használatának folytatásához egy kereskedelmi licenccel kell aktiválnia az alkalmazást, amit az Alkalmazásaktiváló varázsló helyen vagy egy speciális paranccsal tehet meg.

Ha az alkalmazás telepítését vagy verziójának frissítését csendes módban végzi, az alábbi fájlok használata támogatott:

- setup.ini – az alkalmazástelepítés általános beállításai.

  Ahhoz, hogy alkalmazza a beállításokat a setup.ini fájlból, helyezze ezt a fájlt a Kaspersky Endpoint Security terjesztőcsomagot tartalmazó mappába.

- install.cfg – a Kaspersky Endpoint Security művelet beállításai

  A(z) install.cfg konfigurációs fájlból származó beállítások alkalmazásához, meg kell adnia a fájl elérési útját a következő alkalmazástelepítési parancsban: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – beállításkulcsok.

  A setup.reg fájl beállításkulcsai csak akkor lesznek a beállításjegyzékbe írva, ha a `setup.reg` értéke a `SetupReg` paraméterre van állítva a setup.ini fájlban. A(z) setup.reg fájlt a Kaspersky szakemberei hozzák létre. Ennek a fájlnak a tartalmát nem javasolt módosítani. Ahhoz, hogy alkalmazza a beállításokat a setup.reg fájlból, helyezze ezt a fájlt a Kaspersky Endpoint Security terjesztőcsomagot tartalmazó mappába. Elhelyezheti a setup.reg fájlt másik mappába is. Ha így tesz, meg kell adnia a fájl elérési útját a következő alkalmazástelepítési parancsban: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Az alkalmazás eltávolítása

A Kaspersky Endpoint Security eltávolítható a parancssorból, a következő módon egyikében:

- Interaktív módban az Alkalmazástelepítő varázslóval.

- Csendes módban. Az eltávolítás csendes módban való elindítását követően a felhasználónak nem szükséges beavatkoznia az eltávolítási folyamatba (beavatkozás nélküli eltávolítás). Az alkalmazás csendes módban történő eltávolításához használja a `/s` és `/qn` kulcsokat.

Ahhoz, hogy csendes módban távolítsa el az alkalmazást:

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.

2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security terjesztőcsomagja telepítve van.

3. Futtassa a következő parancsot:

- Ha az eltávolítási folyamat nem rendelkezik jelszavas védelemmel:

  ```
  setup_kes.exe /s /x
  ```

  vagy

  ```
  msiexec.exe /x <GUID> /qn
  ```

  A `<GUID>` az alkalmazás egyedi azonosítója. Az alkalmazás GUID-ját a Terméktámogatás tudásbázisában vagy a következő parancs segítségével lehet megkeresni:

  ```
  wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
  ```

- Ha az eltávolítási folyamat rendelkezik jelszavas védelemmel:

  ```
  setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
  ```

  vagy

  ```
  msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
  ```

Használhatja a `SAVEQB` paramétert is az alkalmazás által vizsgált és a Biztonsági mentés mappába helyezett fájlok mentéséhez. A fájlok biztonsági másolatai a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappában vannak tárolva. Alapértelmezés szerint a fájlok biztonsági mentése le van tiltva (`SAVEQB=0`).

Példa

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Az alkalmazás visszaállítása

A helyreállítás során az alkalmazás ellenőrzi és helyreállítja az alkalmazás telepítési folyamatának részeként létrehozott összes sérült alkalmazásmodul és beállításkulcs integritását.

A Kaspersky Endpoint Security visszaállítható a parancssorból a következő módok egyikében:

- Interaktív módban az Alkalmazástelepítő varázslóval.
- Csendes módban. Miután a helyreállítás csendes üzemmódban indult, a helyreállítási folyamatban való részvételre nincs szükség.

Ha a Kaspersky Endpoint Security telepítője helyreállítási módban fut, és az alkalmazásnak nincs szüksége helyreállításra, a telepítő nem végez módosításokat.

Ha a Kaspersky Endpoint Security telepítője helyreállítási módban fut, és az alkalmazás nincs telepítve, a telepítő elindítja a telepítési folyamatot.

Az alkalmazás csendes üzemmódban történő helyreállítása:

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security terjesztőcsomagja telepítve van.
3. Futtassa a következő parancsot:
   - Ha a helyreállítási folyamat nem jelszóvédett:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     A `<GUID>` az alkalmazás egyedi azonosítója. Az alkalmazás GUID-ját a Terméktámogatás tudásbázisában vagy a következő parancs segítségével lehet megkeresni:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Ha a helyreállítási folyamat jelszóvédett:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Példa

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

AVP parancsok

A Kaspersky Endpoint Security alkalmazás kezeléséhez a parancssorból.

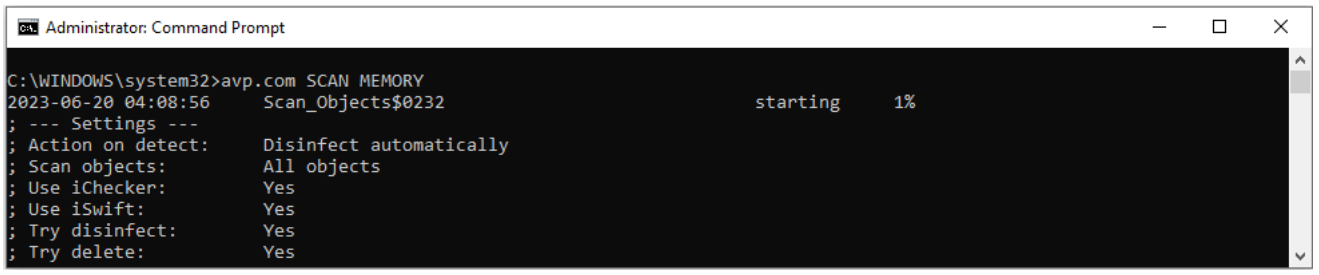
1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

   Az alkalmazás telepítése során a futtatható fájl elérési útját hozzáadhatja a %PATH% rendszerváltozóhoz.

3. A parancs végrehajtásához használja a következő sablont:

```
avp.com <command> [options]
```

Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot (lásd az alábbi ábrát).



Az alkalmazás kezelése a parancssorból

SCAN. Kártevő vizsgálata

A *Kártevő vizsgálata* feladat futtatása.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Vizsgálat hatóköre	
`<files to scan>`	Egy üres hellyel elválasztott lista a fájlokról és mappákról. A hosszú elérési útvonalakat idézőjelbe kell tenni. A rövid elérési útvonalakat (MS-DOS formátum) nem kell idézőjelbe tenni. Például: • `"C:\Program Files (x86)\Example Folder"` – hosszú elérési útvonal. • `C:\PROGRA~2\EXAMPL~1` – rövid elérési útvonal.
`/ALL`	Futtassa a *Kártevő vizsgálata* feladatot. A Kaspersky Endpoint Security az alábbi objektumokat vizsgálja: • Kernelmemória • Az operációs rendszer indulásakor betöltött objektumok • Rendszerindító szektorok • Az operációs rendszer biztonsági mentése • Minden merevlemez és cserélhető meghajtó A Kaspersky Endpoint Security for Windows 12.12-ben az e-mailek nem tartoznak az alkalmazás vizsgálati hatókörébe. A bejövő és kimenő e-mail-üzenetek vizsgálatát a Levelezésvédelem összetevő végzi. Ha az adminisztrációs bővítmény korábbi verzióját használja, az alkalmazás kizárja az e-maileket a vizsgálatból, még akkor is, ha a házirend tartalmazza azokat.
`/MEMORY`	A kernelmemória vizsgálata
`/STARTUP`	Az operációs rendszer indulásakor betöltött objektumok vizsgálata

`/REMDRIVES`	A cserélhető meghajtók vizsgálata.
`/FIXDRIVES`	A merevlemezek vizsgálata.
`/NETDRIVES`	A hálózati meghajtók vizsgálata.
`/QUARANTINE`	A Kaspersky Endpoint Security biztonsági mentésben lévő fájlok vizsgálata.
`/@:<file list.lst>`	Egy listán lévő fájlok és mappák vizsgálata. A listában lévő minden fájlnak új sorban kell lennie. A hosszú elérési útvonalakat idézőjelbe kell tenni. A rövid elérési útvonalakat (MS-DOS formátum) nem kell idézőjelbe tenni. Például: • `"C:\Program Files (x86)\Example Folder"` – hosszú elérési útvonal. • `C:\PROGRA~2\EXAMPL~1` – rövid elérési útvonal.

Művelet fenyegetés észlelésekor	
`/i0`	**Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.
`/i1`	**Vírusmentesítés, értesítés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.
`/i2`	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt. Alapértelmezésben ez a művelet van kiválasztva.
`/i3`	**Törlés, ha a vírusmentesítés nem sikerül**. Az összetett fájlok törlése is (például archívumok), ha a fertőzött fájlt nem lehet vírusmentesíteni vagy törölni.
`/i4`	**Törlés**. Az összetett fájlok törlése is (például archívumok), ha a fertőzött fájlt nem lehet törölni.

Fájltípusok	
`/fe`	**Kiterjesztés alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.
`/fi`	**Formátum alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejlécet a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres.
`/fa`	**Minden fájl**. Ha ez a beállítás van kiválasztva, az alkalmazás kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül). Ez az alapértelmezett beállítás.

Kizárás a vizsgálatból	
`-e:a`	A RAR, ARJ, ZIP, CAB, LHA, JAR, és ICE archívumok ki vannak zárva a vizsgálat hatóköréből.
`-e:<file mask>`	A fájlmaszkkal egyező fájlok ki vannak zárva a vizsgálat hatóköréből. Például: • A `*.exe` maszk tartalmazza az exe kiterjesztésű fájlok elérési útvonalait. • A `example*` maszk tartalmazza a EXAMPLE nevű fájlok elérési útvonalát.
`-e:<seconds>`	A fájlok, amelyek vizsgálati ideje meghaladja a megadott időkorlátot (másodperc), ki vannak zárva a vizsgálat hatóköréből.
`-es:<megabytes>`	A fájlok, amelyek mérete meghaladja a megadott korlátot (megabájt), ki vannak zárva a vizsgálat hatóköréből.

Események mentése jelentésfájl módba (csak a Vizsgálat, Frissítő és Visszaállítás profilok esetében)	
`/R:<report file>`	Csak kritikus események mentése a jelentésfájlba.
`/RA:<report file>`	Minden esemény mentése a jelentésfájlba.

Vizsgálati technológiák	
`/iChecker=on|off`	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).
`/iSwift=on|off`	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.

Speciális beállítások	
`/C:<file with scan settings>`	Fájl a *Kártevő vizsgálata* feladatbeállításokkal. A fájlt manuálisan kell létrehozni, és TXT formátumban kell elmenteni. A fájl a következő tartalommal rendelkezhet: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Példa

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Adatbázisok és alkalmazás-szoftvermodulok frissítése

Az *Adatbázisok és alkalmazásmodulok frissítése* feladat futtatása.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

A parancs szintaxisa

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Frissítési feladat beállításai	
`local`	Az alkalmazás telepítése után automatikusan létrehozott *Adatbázisok és alkalmazásmodulok frissítése* feladat kezdete. Az *Adatbázisok és alkalmazásmodulok frissítése* feladat beállításait a helyi alkalmazásfelületen vagy a Kaspersky Security Center konzolján módosíthatja. Ha ez a beállítás nincs konfigurálva, a Kaspersky Endpoint Security elindítja az *Adatbázisok és alkalmazásmodulok frissítése* feladatot az alapértelmezett beállításokkal vagy a parancsban megadott beállításokkal. Konfigurálhatja az *Adatbázisok és alkalmazásmodulok frissítése* feladat beállításait a következők szerint: • `UPDATE` – az *Adatbázisok és alkalmazásmodulok frissítése* feladat alapértelmezett beállításokkal történő elindítása: a frissítésforrás a Kaspersky frissítési szerverei, a fiók a System, valamint más alapértelmezett beállítások is érvényesek. • `UPDATE local` – az *Adatbázisok és alkalmazásmodulok frissítése* feladat indítása a telepítés után automatikusan létrehozott beállításaival (előre definiált feladat). • `UPDATE <update settings>` – az *Adatbázisok és alkalmazásmodulok frissítése* feladat indítása manuálisan konfigurált beállításokkal (lásd alább).

Frissítésforrás	
`"<update source>"`	A HTTP vagy az FTP szerver címe, valamint a frissítési csomaggal megosztott mappáé. Csak egy frissítésforrást adhat meg. Ha a frissítésforrás nincs megadva, a Kaspersky Endpoint Security az alapértelmezett forrást: a Kaspersky frissítési kiszolgálóit – használja.

Események mentése jelentésfájl módba (csak a Vizsgálat, Frissítő és Visszaállítás profilok esetében)	
`/R:<report file>`	Csak kritikus események mentése a jelentésfájlba.
`/RA:<report file>`	Minden esemény mentése a jelentésfájlba.

Speciális beállítások	
`/C:<file with update settings>`	Fájl az *Adatbázisok és alkalmazásmodulok frissítése* feladat beállításaival. A fájlt manuálisan kell létrehozni, és TXT formátumban kell elmenteni. A fájl a következő tartalommal rendelkezhet: `["<update source>"] [/R[A]:<report file>]`.

Példa

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Utolsó frissítés visszagörgetése

A legutóbbi vírusadatbázis-frissítés visszagörgetése. Ennek köszönhetően szükség esetén az adatbázisokat és az alkalmazásmodulokat vissza lehet görgetni korábbi verziójára, például akkor, ha az új adatbázisverzió érvénytelen aláírást tartalmaz, ami miatt a Kaspersky Endpoint Security egy biztonságos alkalmazást blokkol.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

A parancs szintaxisa

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Események mentése jelentésfájl módba (csak a Vizsgálat, Frissítő és Visszaállítás profilok esetében)	
`/R:<report file>`	Csak kritikus események mentése a jelentésfájlba.
`/RA:<report file>`	Minden esemény mentése a jelentésfájlba.

Példa

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Nyomkövetés

A nyomkövetési fájlok a számítógépen vannak tárolva az alkalmazás használata során, az alkalmazás eltávolításakor pedig véglegesen törlődnek. A nyomkövetési fájlok, kivéve a Hitelesítési ügynökben lévő nyomkövetési fájlokat, a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappában vannak tárolva. A nyomkövetés alapértelmezetten ki van kapcsolva.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Nyomkövetési szint	
`<tracing level>`	A nyomkövetések részleteinek szintje. Választható értékek: • `100` (kritikus). Csak a súlyos hibákról szóló üzenetek. • `200` (magas). Minden hibáról szóló üzenet, köztük a súlyos hibáké. • `300` (diagnosztika). Üzenetek a hibákról, valamint a figyelmeztetésekről. • `400` (fontos). Minden hibaüzenet, figyelmeztetés és további információ. • `500` (normális). Üzenetek a hibákról és figyelmeztetésekről, valamint részletes információ az alkalmazás normál módban történő működéséről (alapértelmezett). • `600` (alacsony). Minden üzenet.

Speciális beállítások	
`all`	Parancs futtatása a `file` and `mem` paraméterekkel.
`file`	Egy nyomkövetési fájl mentése (nincs méretkorlát).
`rot`	Nyomkövetés mentése egy korlátozott méretű, megadott számú fájlkészletbe, és a régi fájlok felülírása, amikor elérte a maximális méretet.
`mem`	Nyomkövetés mentése memóriakiíratási fájlokba.

Példa

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Profil indítása

Profil indítása (például adatbázis-frissítés indítása vagy egy védelmi összetevő engedélyezése esetén).

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com START <profile> [/R[A]:<report file>]
```

Profil	
`<profile>`	Profilnév. A *Profil* egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. Megtekintheti az elérhető profilok listáját, ha futtatja a `HELP START` parancsot.

Események mentése jelentésfájl módba (csak a Vizsgálat, Frissítő és Visszaállítás profilok esetében)	
`/R:<report file>`	Csak kritikus események mentése a jelentésfájlba.
`/RA:<report file>`	Minden esemény mentése a jelentésfájlba.

Példa

```
avp.com START Scan_Objects
```

STOP. Profil leállítása

A profil végrehajtásának leállítása (például a Cserélhető meghajtók vizsgálatának leállítása vagy egy védelmi összetevő letiltása esetén).

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Védelmi összetevők letiltása** és a **Felügyeleti összetevők letiltása** jogosultságokkal.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Profilnév. A *Profil* egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. Megtekintheti az elérhető profilok listáját, ha futtatja a `HELP STOP` parancsot.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

STATUS. Profilállapot

Állapotinformációk megjelenítése az alkalmazásprofiloknál (például `running` or `completed`). Megtekintheti az elérhető profilok listáját, ha futtatja a `HELP STATUS` parancsot.

A Kaspersky Endpoint Security a szolgáltatásprofilok állapotáról szóló információkat is megjeleníti. A szolgáltatásprofilok állapotáról szóló információk akkor lehetnek szükségesek, amikor kapcsolatba lép a Kaspersky Terméktámogatással.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com STATUS [<profile>]
```

Ha profil nélkül adja meg a parancsot, a Kaspersky Endpoint Security az összes profil állapotát megjeleníti az alkalmazásban.

STATISTICS. Profilműveleti statisztikák

Statisztikák megtekintése egy alkalmazásprofilról (például a vizsgálat időtartama vagy az észlelt fenyegetések száma). Megtekintheti az elérhető profilok listáját, ha futtatja a `HELP STATISTICS` parancsot.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com STATISTICS <profile>
```

RESTORE. Fájlok visszaállítása a Biztonsági mentésből

Fájl visszaállítása biztonsági mentésből az eredeti mappába. Ha a megadott elérési útvonalon már létezik azonos nevű fájl, az alkalmazás megerősítést kér a fájl cseréjéhez. A visszaállított fájl úgy lesz másolva, hogy megtartja az eredeti nevét.

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Visszaállítás a Biztonsági mentésből** jogosultsággal.

A *Biztonsági mentés* tárolja az olyan fájlok másolatait, amelyek törölve vagy módosítva lettek a vírusmentesítés során. A *biztonsági másolat* egy másolt fájl, mely a fájl vírusmentesítése vagy törlése előtt lett létrehozva. A fájlok biztonsági másolatai különleges formátumban vannak tárolva, és nem jelentenek fenyegetést.

A fájlok biztonsági másolatai a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappában vannak tárolva.

A Rendszergazda csoportban lévő felhasználók számára elérhető ez a mappa. A felhasználó, akinek a fiókjáról telepítve lett a Kaspersky Endpoint Security, korlátozott hozzáféréssel rendelkezik ehhez a mappához.

A Kaspersky Endpoint Security nem biztosít lehetőséget a fájlok biztonsági másolatához való felhasználói hozzáférések beállítására.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Speciális beállítások	
`/REPLACE`	Meglévő fájl felülírása.
`<file name>`	A visszaállítani kívánt fájl neve.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Alkalmazásbeállítások exportálása

A Kaspersky Endpoint Security beállításainak exportálása egy fájlba. Ha a parancs csak annak a fájlnak a nevét tartalmazza, amelybe a beállításokat exportálni szeretné, az alkalmazás a következőképpen helyezi el a fájlt:

- Ha az avp.com elérési útvonalát hozzáadjuk a %PATH% rendszerváltozóhoz, az alkalmazás a `C:\Windows\SysWOW64` mappába helyezi a fájlt.
- Ha a parancsot az alkalmazás telepítési mappájából futtatja, az exportálás sikertelen lesz, mivel az alkalmazás önvédelme megakadályozza egy új fájl létrehozását az alkalmazás mappájában. Az alkalmazásbeállítások fájlba történő exportálásához adja meg a fájl elérési útját.

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Beállítások exportálása** engedéllyel.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Profilnév. A *Profil* egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. Megtekintheti az elérhető profilok listáját, ha futtatja a `HELP EXPORT` parancsot.

Fájl az exportáláshoz	
`<file name>`	A fájl neve, ahová az alkalmazásbeállítások exportálva lesznek. A fájl elérési útját is megadhatja. A Kaspersky Endpoint Security beállításokat exportálhatja egy DAT vagy CFG konfigurációs fájlba, egy TXT szöveges fájlba vagy egy XML dokumentumba.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Alkalmazásbeállítások importálása

A Kaspersky Endpoint Security beállításainak importálása az `EXPORT` paranccsal létrehozott fájlból.

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Alkalmazásbeállítások konfigurálása** jogosultsággal.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Importálni kívánt fájl	
`<file name>`	A fájl neve, ahonnan az alkalmazásbeállítások importálva lesznek. A Kaspersky Endpoint Security beállításokat importálhatja egy DAT vagy CFG konfigurációs fájlba, egy TXT szöveges fájlba vagy egy XML dokumentumba.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Kulcsfájl alkalmazása

A Kaspersky Endpoint Security aktiválása kulcsfájl használatával. Ha az alkalmazás már aktiválva van, a kulcs hozzáadása tartalék kulcsként történik.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

A parancs szintaxisa

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Kulcsfájl	
`<file name>`	Kulcsfájl neve.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatok. Ezeket a bejelentkezési adatokat csak akkor kell megadni, ha a Jelszóvédelem engedélyezve van.

Példa

```
avp.com ADDKEY file.key
```

LICENSE. Licencelés

A Kaspersky Endpoint Security, EDR Optimum vagy EDR Expert licenckulcsainak kezelése (Kaspersky Endpoint Detection and Response bővítmény).

A parancs végrehajtásához és a licenckulcs eltávolításához a Jelszóvédelmet engedélyezni kell. A felhasználónak engedélyeznie kell a **Kulcs eltávolítása** jogosultságot.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

A parancs szintaxisa

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Művelet	
`/ADD <file name>`	A Kaspersky Endpoint Security aktiválása kulcsfájl használatával. Ha az alkalmazás már aktiválva van, a kulcs hozzáadása tartalék kulcsként történik.
`/ADD <activation code>`	A Kaspersky Endpoint Security aktiválása az aktiváló kód segítségével. Ha az alkalmazás már aktiválva van, a kulcs hozzáadása tartalék kulcsként történik.
`/REFRESH`	A Kaspersky Endpoint Security licenc állapotának frissítése. Ennek eredményeként az alkalmazás naprakész licencállapot információkat kap a Kaspersky aktiválási kiszolgálóitól.
`/REFRESH <license ID>`	Frissítse a licencek állapotát a licencazonosítóval. Ezzel a paranccsal frissítheti az EDR-bővítmény, az MDR-bővítmény, a KUMA-bővítmény és más licencek állapotát. A licencazonosítót a licenctanúsítványból szerezheti be. Ennek eredményeként az alkalmazás naprakész licencállapot információkat kap a Kaspersky aktiválási kiszolgálóitól.
`/CHECK`	A licencinformáció lekérése. A Kaspersky Endpoint Security megjeleníti az összes hozzáadott licenckulcsra vonatkozó információkat, beleértve a tartalékkulcsokat, az EDR kiegészítő, az MDR kiegészítő, a KUMA kiegészítő kulcsait és az egyéb kulcsokat. A Kaspersky Endpoint Security a következő licencinformációkat jeleníti meg: • licenc neve; • licenc azonosítója; • a védelmi kiszolgáló (SVM) címe, amelyhez a virtuális gép csatlakozik, és amelyre az alkalmazás Light Agent üzemmódban telepítve van; • licenc típusa: próba, kereskedelmi, béta, előfizetés; • az alkalmazás aktiválásának dátuma és időpontja; • a licenc lejáratának dátuma és időpontja; • a licenc lejártáig hátralévő napok száma.
`/CHECK <license ID>`	Licencadatok lekérdezése azonosító alapján. Ezzel a paranccsal licencinformációkat kérhet le. A licencazonosítót a licenctanúsítványból szerezheti be.
`/DEL /login=<user name> /password=<password>`	A licenckulcs eltávolítása az alkalmazásból. A rendszer a tartalék kulcsot is eltávolítja.
`/DEL <license ID> /login=<user name> /password=<password>`	Kulcs törlése a licencazonosítóval. Ezzel a paranccsal törölhet egy kulcsot az EDR-bővítményből, MDR-bővítményből, KUMA-bővítményből vagy más licencekből. A licencazonosítót a licenctanúsítványból szerezheti be.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Példa

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Licenc vásárlása

A Kaspersky webhely megnyitása a licenc megvásárlásához vagy megújításához.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

PBATESTRESET. A lemez ellenőrzési eredményeinek visszaállítása a lemez titkosítása előtt

Visszaállítja a Teljes lemeztitkosítás (FDE) kompatibilitási ellenőrzésének eredményeit, a Kaspersky lemeztitkosítás és a BitLocker meghajtótitkosítás technológiák esetében is.

A Teljes lemeztitkosítás futtatása előtt az alkalmazás végrehajt egy adott számú ellenőrzést, hogy hitelesítse, hogy a számítógép titkosítható-e. Ha a számítógép nem támogatja a Teljes lemeztitkosítást, a Kaspersky Endpoint Security naplózni fogja az inkompatibilitás információit. A legközelebbi alkalommal, amikor titkosítani próbál majd, az alkalmazás nem hajtja végre ezt az ellenőrzést, és figyelmeztetni fogja, hogy a titkosítás nem végezhető el. Ha változott a számítógép hardverkonfigurációja, az alkalmazás által naplózott korábbi kompatibilitásellenőrzés eredményeit vissza kell állítani, hogy újra ellenőrizze a rendszer merevlemezének kompatibilitását a Kaspersky lemeztitkosítás és a BitLocker meghajtótitkosítási technológiákkal.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

EXIT. Kilépés az alkalmazásból

Kilépés a Kaspersky Endpoint Security alkalmazásból. Az alkalmazás kitöltődik a számítógép RAM-jából.

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Kilépés az alkalmazásból** jogosultsággal.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Szabályzat letiltása

A Kaspersky Security Center szabályzat letiltása a számítógépen. Minden Kaspersky Endpoint Security beállítás elérhető a konfiguráció számára, köztük azok is, amelyeken zárt lakat van a szabályzatban ( ).

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell **A Kaspersky Security Center házirendjének letiltása** jogosultsággal.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Szabályzat engedélyezése

A Kaspersky Security Center szabályzat engedélyezése a számítógépen. Az alkalmazásbeállítások a szabályzat alapján lesznek konfigurálva.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

DISABLE. Védelem kikapcsolása

A Fájl védelem letiltása egy lejárt Kaspersky Endpoint Security licenccel rendelkező számítógépen. Ezt a parancsot nem lehet olyan számítógépen futtatni, amelyen megtalálható az alkalmazás, ami nincs aktiválva, vagy amin érvényes a licenc.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

SPYWARE. Spyware észlelés

Kémprogram-észlelés kezelése. Alapértelmezés szerint a spyware-észlelés engedélyezve van.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com SPYWARE on|off
```

KSN. Váltás a KSN / KPSN között

A Kaspersky megoldás kiválasztása a fájlok vagy webhelyek megbízhatóságának meghatározásához. A Kaspersky Endpoint Security a következő infrastrukturális megoldásokat támogatja a Kaspersky megbízhatósági adatbázisaival való együttműködéshez:

- A *Kaspersky Security Network (KSN)* a legtöbb Kaspersky-alkalmazás által használt megoldás. A KSN-résztvevők információkat kapnak a Kaspersky-től, és elküldik a Kaspersky számára a felhasználó számítógépén észlelt objektumokat, hogy a Kaspersky is elemezze azokat, és belevegye a megbízhatósági és statisztikai adatbázisába.

- A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről. A KPSN vállalati felhasználóknak ajánlott, akik a következő okokból nem tudnak részt venni a Kaspersky Security Networkben:

  - A helyi munkaállomások nem csatlakoznak az internethez.

  - Az adatok vállalati LAN-hálózaton vagy az országon kívüli továbbítását tiltja a törvény vagy a vállalat biztonsági rendszabálya.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

> Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

A parancs szintaxisa

```
avp.com KSN /global | /private <file name>
```

Kaspersky Security Network konfigurációs fájl	
`<file name>`	A Kaspersky Private Security Network beállításait tartalmazó konfigurációs fájl neve. Ez a fájl PKCS7 vagy PEM kiterjesztéssel rendelkezik.

Példa

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Példa

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. A kiszolgálói kapcsolatvédelmem letiltása

Azon *Felügyeleti kiszolgálói kapcsolatvédelem* feladat futtatása, amely eltávolítja a számítógépnek a Felügyeleti kiszolgálóval való kapcsolatához tartozó jelszót. Ily módon a feladat letiltja a felügyeleti kiszolgálói kapcsolatvédelmet.

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Jelszó	
`/password=<password>`	A KLAdmin felhasználói fiók jelszava vagy a *Felügyeleti kiszolgálói kapcsolatvédelem* feladat jelszava. Ha a paraméter nincs megadva, a Kaspersky Endpoint Security a következő sorban jelszó megadására kéri fel.

KESCLI parancsok

A KESCLI parancsokkal információt kaphat a számítógép védelmének állapotáról az OPSWAT összetevő használata esetén, valamint a parancsok lehetővé teszik a szokásos feladatok, például a *Kártevők vizsgálata* és az *Adatbázisok és alkalmazásmodulok frissítése* feladat végrehajtását.

A KESCLI parancsok listáját a `kescli --help` paranccsal vagy a rövidített `kescli -h` paranccsal tekintheti meg.

A Kaspersky Endpoint Security alkalmazás kezeléséhez a parancssorból.

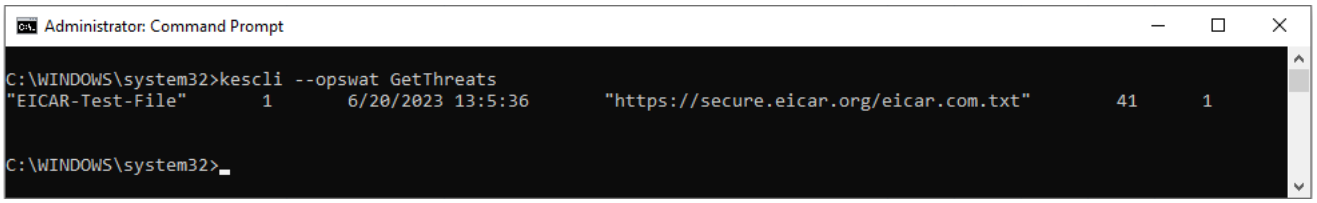
1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

   Az alkalmazás telepítése során a futtatható fájl elérési útját hozzáadhatja a %PATH% rendszerváltozóhoz.

3. A parancs végrehajtásához használja a következő sablont:

```
kescli <parancs> [options]
```

Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot (lásd az alábbi ábrát).



Az alkalmazás kezelése a parancssorból

Scan. Kártevő vizsgálata

A *Kártevő vizsgálata* (Teljes vizsgálat) feladat futtatása.

A feladat futtatásához a rendszergazdának engedélyeznie kell a helyi feladatok használatát a házirendben.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

A `GetScanState` paranccsal ellenőrizheti a *Kártevő vizsgálata* feladat befejezési állapotát, valamint a `GetLastScanTime` paranccsal megtekintheti a vizsgálat legutóbbi befejezésének dátumát és időpontját.

Vizsgálat hatóköre	
`<scan scope>`	`;` karakterrel elválasztott lista a fájlokról és mappákról. Például: `"C:\Program Files (x86)\Example Folder"`.

Művelet fenyegetés észlelésekor	
`0`	**Tájékoztatás**. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.
`1`	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt. Alapértelmezésben ez a művelet van kiválasztva.

Példa

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Vizsgálat befejezési állapota

Információ megjelenítése a *Kártevő vizsgálata* (*Teljes vizsgálat*) feladat állapotáról:

- `1` – a vizsgálat folyamatban van.
- `0` – a vizsgálat nem fut.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat GetScanState
```

GetLastScanTime. A vizsgálat befejezési időpontjának meghatározása

Információ megjelenítése az utolsó *Kártevő vizsgálata* (*Teljes vizsgálat*) feladat befejezési dátumáról és időpontjáról.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat GetLastScanTime
```

GetThreats. Az észlelt fenyegetésekre vonatkozó adatok beszerzése

Az észlelt fenyegetések listájának megjelenítése (*Report on threats*). Ez a jelentés tartalmazza a jelentés elkészítését megelőző 30 nap során észlelt fenyegetések és vírusaktivitás információit.

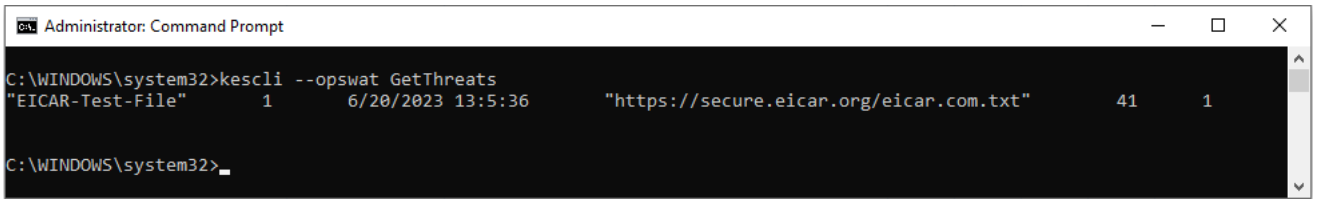
A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat GetThreats
```

A parancs végrehajtásakor a Kaspersky Endpoint Security a következő formátumban küld választ:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



Az alkalmazás kezelése a parancssorból

Objektumtípus	
0	Nem ismert (Unknown).
1	Vírusok (Virware).
2	Trójai programok (Trojware).
3	Rosszindulatú programok (Malware).
4	Reklámprogramok (Adware).
5	Automata tárcsázó programok (Pornware).
6	Olyan alkalmazások, amelyeket egy számítógépes bűnöző felhasználhat a felhasználó számítógépének vagy adatainak károsítására (Riskware).
7	Csomagolt objektumok, amelyek tömörítési metódusa felhasználható károkozásra képes kód védelmére (Packed).
20	Ismeretlen objektumok (Xfiles).
21	Ismert alkalmazások (Software).
22	Rejtett fájlok (Hidden).
23	Figyelmet igénylő alkalmazások (Pupware).
24	Rendellenes viselkedés (Anomaly).
30	Nem meghatározott (Undetect).
40	Reklámcsíkok (Banner).
50	Hálózati támadás (Attack).
51	Beállításjegyzékhez való hozzáférés (Registry).
52	Gyanús tevékenység (Suspicion).
60	Biztonsági rések (Vulnerability).
70	Phishing (Phishing).
80	Nem kívánt e-mail-melléklet (Attachment).
90	Kaspersky Security Network által észlelt rosszindulatú program (Urgent).
100	Ismeretlen hivatkozás (Suspic URL).
110	Egyéb rosszindulatú program (Behavioral).

Művelet fenyegetés észlelésekor	
0	Nem ismert (unknown).
1	A fenyegetés javítva (ok).
2	Az objektum fertőzött volt, és nem lett vírusmentesítve (infected).
5	Az objektum archívumban van, és nem lett vírusmentesítve (archive).
9	Az objektum vírusmentesítve (disinfected).

10	Az objektum nem lett vírusmentesítve (`not disinfected`).
11	Az objektum törölve (`deleted`).
13	Létrejött az objektum biztonsági másolata (`backupped`).
15	Az objektum áthelyezve a biztonsági mentésbe (`quarantined`).
23	Az objektum törölve lett a számítógép újraindításakor (`delete on reboot`).
25	Az objektum vírusmentesítve lett a számítógép újraindításakor (`disinfect on reboot`).
29	A felhasználó áthelyezte az objektumot a biztonsági mentésbe (`added by user`).
30	Az objektum hozzá lett adva a kizárásokhoz (`added to exclude`).
31	Az objektum áthelyezve a biztonsági mentésbe a számítógép újraindításakor (`quarantine on reboot`).
36	Téves riasztás (`false alarm`).
38	A folyamat le lett állítva (`terminated`).
40	Az objektum nem lett észlelve (`not found`).
41	Nem lehet feloldani a fenyegetést (`untreatable`).
42	Az objektum vissza lett állítva (`rolled back`).
43	Az objektum fenyegetési tevékenység eredményeként jött létre (`produced by threat`).
44	Az objektum vissza lett állítva a számítógép újraindításakor (`roll back on reboot`).
0xffffffff	Az objektum nem lett feldolgozva (`discarded`).

Fenyegetés veszélyszintje	
`0`	Ismeretlen
`1`	Magas
`2`	Közepes vizsgálat
`4`	Alacsony
`8`	Információ (legfeljebb *Alacsony*)

UpdateDefinitions. Adatbázisok és alkalmazás-szoftvermodulok frissítése

Az *Adatbázisok és alkalmazásmodulok frissítése* feladat futtatása. A Kaspersky Endpoint Security az alapértelmezett forrást használja: Kaspersky frissítési kiszolgálók.

A feladat futtatásához a rendszergazdának engedélyeznie kell a helyi feladatok használatát a házirendben.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

Ez a parancs nem futtatható, ha az alkalmazás Light Agent üzemmódban van telepítve.

A parancs szintaxisa

```
kescli --opswat UpdateDefinitions
```

A `GetDefinitionsetState` parancs segítségével megtekintheti az aktuális vírusirtó adatbázisok kiadásának dátumát és idejét.

GetDefinitionState. Az adatbázisok legutóbbi frissítési dátumának és időpontjának meghatározása

Információ megjelenítése a használatban lévő vírusadatbázisok legutóbbi frissítésének dátumáról és időpontjáról.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat GetDefinitionState
```

EnableRTP. Védelem engedélyezése

A Kaspersky Endpoint Security védelmi összetevők engedélyezése a számítógépen: Fájl védelem, Web védelem, Levelezés védelem, Hálózati védelem, Behatolásmegelőző rendszer.

> A védelmi összetevők engedélyezéséhez a rendszergazdának meg kell győződnie arról, hogy a vonatkozó házirend-beállítások módosíthatók (attribútumok nyitottak).

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat EnableRTP
```

Ennek eredményeként a védelmi összetevők akkor is engedélyezve vannak, ha Ön megtiltotta az alkalmazás beállításainak módosítását a Jelszóvédelemmel.

A `GetRealTimeProtectionState` paranccsal ellenőrizheti a Fájl védelem működési állapotát.

GetRealTimeProtectionState. Fájl védelem állapota

Információ megjelenítése a Fájl védelem összetevő állapotáról:

- `1` – az összetevő engedélyezve van.
- `0` – az összetevő le van tiltva.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Lemeztitkosítás állapota

Információ megjelenítése a lemez titkosítási állapotáról:

- Az `1` azt jelenti, hogy a lemezt a Kaspersky vagy a BitLocker lemeztitkosítási technológia védi.
- A `0` azt jelenti, hogy a lemez nincs titkosítva.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --opswat GetEncryptionState
```

Version. Az alkalmazás verziójának azonosítása

A Kaspersky Endpoint Security for Windows verziójának megjelenítése.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található.

A parancs szintaxisa

```
kescli --Version
```

Használhatja a rövidített `-v` parancsot is.

Detection and Response felügyeleti parancsok

A parancssor segítségével kezelheti a Detection and Response megoldások beépített funkcióit (például Kaspersky Sandbox vagy Kaspersky Endpoint Detection and Response Optimum). Kezelheti a Detection and Response megoldásokat, ha a Kaspersky Security Center konzol használatával történő felügyelet nem lehetséges. Megtekintheti az alkalmazáskezeléshez tartozó parancsok listáját, ha futtatja a `HELP` parancsot. A megadott parancs szintaxisának elolvasásához adja meg a `HELP <command>` parancsot.

A Detection and Response megoldások beépített funkcióinak kezelése parancssor használatával:

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.
3. A parancs végrehajtásához használja a következő sablont:

   ```
   avp.com <command> [options]
   ```

   Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot.

SANDBOX. A Sandbox kezelése

A Sandbox összetevő felügyeletéhez tartozó parancsok:

- A Sandbox összetevő engedélyezése vagy letiltása.

  A Sandbox-összetevők interakciót biztosítanak a Kaspersky Sandbox megoldással és a KATA Sandbox összetevővel, amely a Kaspersky Anti Targeted Attack Platform része.

- A Kaspersky Sandbox összetevő konfigurálása:

  - A számítógép csatlakoztatása a Sandbox-kiszolgálókhoz.

    A kiszolgálók a Microsoft Windows operációs rendszerek telepített virtuális képeit használják a vizsgálandó objektumok futtatására. Megadhat egy IP-címet (IPv4 vagy IPv6) vagy egy teljes tartománynevet. A virtuális lemezképek telepítésével és a Sandbox-kiszolgálók konfigurálásával kapcsolatos részletekért tekintse meg a Kaspersky Sandbox súgót és Kaspersky Anti Targeted Attack Platform súgót.

  - A kiszolgáló kapcsolódási időtúllépésének konfigurálása.

    Időtúllépés történt a Sandbox-kiszolgáló (Kaspersky Sandbox esetén) vagy a Central Node-kiszolgáló (KATA esetén) csatlakoztatásakor. A beállított időtúllépés letelte után a Kaspersky Endpoint Security kérést küld a következő kiszolgálónak. Növelheti a kiszolgáló kapcsolódási időtúllépését, ha a kapcsolat sebessége alacsony, vagy ha a kapcsolat instabil. A kérések ajánlott időtúllépése 0.5 másodperc vagy kevesebb.

  - Megbízható kapcsolat beállítása a számítógép és a kiszolgálók között.

    A Sandbox-kiszolgálóval (Kaspersky Sandbox esetén) vagy a Central Node-kiszolgálóval (KATA esetén) való megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell készítenie. Ezután hozzá kell adnia a tanúsítványt a számítógéphez egy házirend segítségével. A tanúsítványt a Sandbox-kiszolgálóhoz (Kaspersky Sandbox esetén) vagy a Central Node-kiszolgálóhoz (KATA esetén) is hozzá kell adnia.

  - Az integrációs mód konfigurálása.

    Olyan megoldást kell választania, amelynek a Sandbox – azaz a Kaspersky Sandbox vagy a KATA Sandbox – része. A *Kaspersky Sandbox* a Kaspersky önálló Detection and Response megoldása. A *KATA Sandbox* a Kaspersky Anti Targeted Attack Platform megoldás egyik összetevője. A KATA Sandboxba integrálva az összetevő a következő módokban működhet:

    - **Manually**. A felhasználó manuálisan küldi be a fájlt vizsgálatra a helyi menüből (**Küldés a Sandboxba**).
    - **Automatically**. Az alkalmazás automatikusan észleli az objektumokat, és vizsgálat céljából elküldi azokat a Sandboxba.
    - **Combined**.

- Az összetevő aktuális beállításainak megjelenítése.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Művelet	
`stop`	A Sandbox összetevő letiltása.
`start`	A Sandbox összetevő engedélyezése.

`set`	A Sandbox összetevő konfigurálása. Az alábbi beállításokat konfigurálhatja:
	• Sandbox-kiszolgálók hozzáadása (`--servers`)
	• TLS-tanúsítvány hozzáadása (`--pinned-certificate`)
	• Kriptotároló hozzáadása (`--client-certificate`)
	• Adjon meg egy jelszót a kriptokonténerhez (`--client-certificate-password`);
	• A kiszolgáló kapcsolódási időtúllépésének beállítása (`--timeout`)
	• Válasszon ki egy integrációs módot (`--mode`):
	  • `KSB` – integráció a Kaspersky Sandbox szolgáltatással;
	  • `KATAManual` – manuális integráció a KATA Sandbox szolgáltatással;
	  • `KATAAuto` – automatikus integráció a KATA Sandbox szolgáltatással;
	  • `KATAFull` – kombinált integráció a KATA Sandbox szolgáltatással.

`show`	Az összetevő aktuális beállításainak megjelenítése. A következő választ kapja:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION. A végrehajtás megakadályozásának kezelése

A Végrehajtás megakadályozása összetevő letiltása vagy az összetevő aktuális beállításainak megjelenítése, beleértve a végrehajtás megelőzésének szabályai listáját.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com prevention disable
```

```
avp.com prevention /show
```

A `prevention /show` parancs végrehajtása után a következő választ kapja:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

A parancs visszatérési értékei:

- A `-1` azt jelenti, hogy a parancsot nem támogatja a számítógépre telepített alkalmazás verziója.
- A `0` azt jelenti, hogy a parancs sikeresen végre lett hajtva.
- Az `1` azt jelenti, hogy egy kötelező argumentum nem lett átadva a parancsnak.
- A `2` azt jelenti, hogy általános hiba történt.
- A `4` azt jelenti, hogy szintaktikai hiba történt.
- `9` – helytelen működés (például az összetevő letiltására tett kísérlet, amikor az már le van tiltva).

ISOLATION. A hálózatelkülönítés kezelése

A számítógép hálózatelkülönítésének letiltása vagy az összetevő aktuális beállításainak megjelenítése. Az összetevők beállításai tartalmazzák a kizárásokhoz hozzáadott hálózati kapcsolatok listáját is.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

A `stat` parancs futtatásának eredményeként a következő választ kapja: `Network isolation on|off`.

RESTORE. Fájlok visszaállítása a Karanténból

Fájl visszaállítása a karanténból az eredeti mappába. A *karantén* egy speciális helyi tároló a számítógépen. A felhasználó karanténba helyezheti azokat a fájlokat, amelyeket veszélyesnek ítél meg a számítógépen. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha az integrálva van a Kaspersky Detection and Response megoldásokkal. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a Biztonsági mentésbe helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért olvassa el a Kaspersky Sandbox súgót, a Kaspersky Endpoint Detection and Response Optimum súgót, a Kaspersky Endpoint Detection and Response Expert súgót, a Kaspersky Anti Targeted Attack Platform súgót és a Kaspersky Endpoint Detection and Response Expert (on-premises) súgót.

A parancs végrehajtásához engedélyezni kell a Jelszóvédelmet. A felhasználónak rendelkeznie kell a **Visszaállítás a Biztonsági mentésből** jogosultsággal.

Az objektum karanténba helyezése a rendszerfiókban (SYSTEM) történik.

A fájlok visszaállítása a karanténból a következő speciális szempontokat foglalja magában:

- Ha a célmappát törölték, vagy a felhasználónak nincs hozzáférési joga ehhez a mappához, az alkalmazás a fájlt a következő mappába helyezi: `%DataRoot%\QB\Restored`. Ezután manuálisan át kell helyeznie a fájlt a célmappába.
- Az alkalmazás a visszaállítandó fájl nevében megkülönbözteti a kis- és nagybetűket. Ha a fájlnév megadásakor nem veszi figyelembe a kis- és nagybetűt, az alkalmazás nem állítja vissza a fájlt.
- Ha a célmappában már van azonos nevű fájl, az alkalmazás megszakítja a fájl visszaállítását.
- Ha a KATA (EDR) megoldást használja, az alkalmazás a fájl helyreállítása után a Karanténba menti a fájl egy másolatát. A Karantént manuálisan kell kiürítenie. Az EDR Optimum és EDR Expert megoldások esetében az alkalmazás a visszaállítás után törli a fájlt.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Speciális beállítások	
`/REPLACE`	Meglévő fájl felülírása.
`<file name>`	A visszaállítani kívánt fájl neve.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

A parancs visszatérési értékei:

- A `-1` azt jelenti, hogy a parancsot nem támogatja a számítógépre telepített alkalmazás verziója.
- A `0` azt jelenti, hogy a parancs sikeresen végre lett hajtva.
- Az `1` azt jelenti, hogy egy kötelező argumentum nem lett átadva a parancsnak.
- A `2` azt jelenti, hogy általános hiba történt.
- A `4` azt jelenti, hogy szintaktikai hiba történt.

IOCSCAN. Biztonsági sérülési indikátorok (IOC) vizsgálata

Futtassa az *IOC Scan* feladatot. A *biztonsági sérülési indikátor (IOC)* egy olyan objektumra vagy tevékenységre vonatkozó adathalmaz, amely jogosulatlan hozzáférést jelez a számítógéphez (adatok veszélyeztetése). Például sok sikertelen bejelentkezési kísérlet a rendszerbe biztonsági sérülésre utalhat. Az *IOC Scan* feladat lehetővé teszi a biztonsági sérülési indikátorok (IOC) megtalálását a számítógépen, valamint biztosítja a fenyegetésre reagáló intézkedések megtételét.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

Az IOC-vizsgálat az IOC-fájlokban leírt fertőzöttségi mutatókkal való 128 egyezés után megszakad. Erre az IOC vizsgálat feladat jelentésben szereplő bejegyzések számának korlátozása céljából van szükség, hogy a rendszer megkönnyítse a jelentés elemzését, és hogy megóvja a jelentést a túlcsordulástól a pontatlanul megfogalmazott fertőzöttségi mutatók miatt, amelyek rengeteg találatot generálhatnak.

A parancs szintaxisa

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC-fájlok	
`<full path to the IOC file>`	A vizsgálathoz használni kívánt IOC-fájl teljes elérési útja. Több IOC-fájlt is megadhat szóközökkel elválasztva. Az IOC-fájl teljes elérési útját a `/path` argumentum nélkül kell megadni. Például `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	A vizsgálathoz használni kívánt IOC-fájlokat tartalmazó mappa elérési útja. Az *IOC-fájlok* olyan fájlok, amelyek az indikátorkészleteket tartalmazzák, és amelyekkel az alkalmazás egyezést próbál találni észlelés esetén. Az IOC-fájloknak meg kell felelniük az OpenIOC szabványnak. Például `C:\Users\Admin\Desktop\IOC`

Adattípus az IOC vizsgálathoz	
`/process=on|off`	Folyamatadatok elemzése az IOC vizsgálat során (ProcessItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security a vizsgálat során nem elemzi a számítógépen futó folyamatokat. Ha az IOC-fájl tartalmazza a ProcessItem IOC-dokumentumának IOC-feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a folyamatadatokat, ha a ProcessItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/hint=<full path to the executable file of the process|full path to the file>`	Fájlok adatainak elemzése az IOC vizsgálat során (ProcessItem és FileItem kifejezés). Egy fájlt az alábbi módokon választhat ki: • `<full path to the executable file of the process>` – ProcessItem kifejezés; • `<full path to the file>` – FileItem kifejezés.
`/registry=on|off`	Windows rendszerleíró adatbázis adatainak elemzése az IOC vizsgálat során (RegistryItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja a Windows rendszerleíró adatbázisát. Ha az IOC-fájl tartalmazza a RegistryItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a Windows rendszerleíró adatbázisát, ha a RegistryItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban. A RegistryItem adattípus esetén a Kaspersky Endpoint Security átvizsgálja a beállításkulcsok készletét.
`/dnsentry=on|off`	A helyi DNS-gyorsítótárban lévő rekordok adatainak elemzése az IOC vizsgálat során (DnsEntryItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja a helyi DNS-gyorsítótárat. Ha az IOC-fájl tartalmazza a DnsEntryItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a helyi DNS-gyorsítótárat, ha a DnsEntryItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/arpentry=on|off`	Az ARP-tábla rekordadatainak elemzése az IOC vizsgálat során (ArpEntryItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja az ARP-táblát. Ha az IOC-fájl tartalmazza a ArpEntryItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi az ARP-táblát, ha az ArpEntryItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/ports=on|off`	A figyelésre megnyitott portok adatainak elemzése az IOC vizsgálat során (PortItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja az eszközön lévő aktív kapcsolatok tábláját. Ha az IOC-fájl tartalmazza a PortItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi az aktív kapcsolatok tábláját, ha a PortItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/services=on|off`	Az eszközre telepített szolgáltatások adatainak elemzése az IOC vizsgálat során (ServiceItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja az eszközre telepített szolgáltatások adatait. Ha az IOC-fájl tartalmazza a ServiceItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a szolgáltatásadatokat, ha a ServiceItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/system=on|off`	Környezeti adatok elemzése az IOC vizsgálat során (SystemInfoItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem elemzi a környezeti adatokat. Ha az IOC-fájl tartalmazza a SystemInfoItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a környezeti adatokat, ha a SystemInfoItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.

`/users=on|off`	Felhasználói adatok elemzése az IOC vizsgálat során (UserItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem elemzi a rendszerben létrehozott felhasználók adatait. Ha az IOC-fájl tartalmazza a UserItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a rendszerben létrehozott felhasználók adatait, ha a UserItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/volumes=on|off`	Kötetadatok elemzése az IOC vizsgálat során (VolumeItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja az eszközön lévő kötetek adatait. Ha az IOC-fájl tartalmazza a VolumeItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a kötetadatokat, ha a VolumeItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/eventlog=on|off`	A Windows Eseménynapló rekordadatainak elemzése az IOC vizsgálat során (EventLogItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem vizsgálja a Windows Eseménynapló rekordjait. Ha az IOC-fájl tartalmazza a EventLogItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a Windows Eseménynaplót, ha az EventLogItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/datetime=<event publication date>`	Figyelembe veszi az esemény Windows Eseménynaplóban történő közzétételének dátumát, amikor meghatározza a megfelelő IOC-dokumentumhoz tartozó IOC vizsgálat hatókörét. Az IOC vizsgálat végrehajtásakor a Kaspersky Endpoint Security megvizsgálja a Windows Eseménynaplóban közzétett bejegyzéseket a megadott időpont és dátum, valamint a feladat futtatásának pillanata között. A Kaspersky Endpoint Security lehetővé teszi az esemény közzétételi dátumának megadását az argumentum értékeként. A vizsgálat csak a Windows Eseménynapló olyan eseményeire vonatkozik, amelyeket a megadott dátum és a vizsgálat futtatása között tettek közzé. Ha az argumentum nincs megadva, a Kaspersky Endpoint Security minden közzétételi dátumú eseményt megvizsgál. A `TaskSettings::BaseSettings::EventLogItem::datetime` beállítás nem szerkeszthető. A beállítás csak akkor használható, ha az EventLogItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/channel=<list of channels>`	Azon csatorna (napló) nevek listája, amelyek esetében IOC vizsgálatot szeretne végezni. Ha az argumentum meg van adva, a Kaspersky Endpoint Security megvizsgálja a megadott naplókban közzétett rekordokat. Az IOC-dokumentumnak rendelkeznie kell a leírt EventLogItem kifejezéssel. A napló neve karakterláncként van meghatározva a napló tulajdonságaiban (Full Name paraméter) vagy az eseménytulajdonságokban (`<Channel></Channel>` paraméter az esemény xml-sémájában) a megadott napló (csatorna) nevének megfelelően. Több csatornát is megadhat szóközökkel elválasztva. Ha az argumentum nincs megadva, a Kaspersky Endpoint Security megvizsgálja az `Application`, `System`, `Security` csatornák rekordjait.
`/files=on|off`	Fájladatok elemzése az IOC vizsgálat során (FileItem kifejezés). Ha az argumentum értéke `off`, a Kaspersky Endpoint Security nem elemzi a fájladatokat. Ha az IOC-fájl tartalmazza a FileItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve). Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a fájladatokat, ha a FileItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.
`/drives=<all|system|critical|custom>`	Az IOC vizsgálat hatókörének beállítása a FileItem IOC-dokumentumadatainak elemzésekor. A következő értékeket állíthatja be a vizsgálat hatóköréhez: • `<all>` az összes rendelkezésre álló fájl hatóköréhez. • `<system>` azokban a mappákban található fájlokhoz, amelyekben az operációs rendszer telepítve van. • `<critical>` felhasználói és rendszermappákban található ideiglenes fájlokhoz. • `<custom>` a felhasználó által meghatározott hatókörű fájlokhoz (`/scope=<list of folders to scan>`). Ha az argumentum nincs megadva, a vizsgálat a kritikus területeken történik.
`/excludes=<list of exclusions>`	Kizárás hatókörének beállítása a FileItem IOC-dokumentumadatainak elemzésekor. Több elérési utat is megadhat szóközökkel elválasztva.
`/scope=<list of folders to scan>`	Felhasználó által definiált IOC vizsgálati hatókör a FileItem IOC-dokumentumadatainak elemzésekor (`/drives=custom`). Több elérési utat is megadhat szóközökkel elválasztva.

`/retro /<number of days>`	A *Visszamenőleges IOC vizsgálat* az *IOC Scan* egyik módja, amelyben a Kaspersky Endpoint Security egy bizonyos időszak adatai alapján a sérülésekre utaló jelek után kutat. Ez az üzemmód arra szolgál, hogy a védett számítógép telemetriai adatai – például a hálózati tevékenység, a folyamatok, a fájlok és egyéb telemetriai adatok – alapján felderítse a biztonsági incidensekre utaló jeleket. 1 és 14 nap közötti időtartamot állíthat be. Alapértelmezés szerint az alkalmazás egy napig szűri ki a sérülési indikátorokat.
`/network=on|off`	Hálózati adatok elemzése (NetworkItem kifejezés).
`/url=on|off`	A böngészőnaplókban lévő adatok elemzése (UrlHistoryItem kifejezés). A Visszamenőleges IOC vizsgálat a következő böngészők naplófájljait elemzi: Google Chrome, Mozilla Firefox, Microsoft Edge (79-es vagy újabb verzió).
`/email`	Levél objektumok elemzése (EmailItem kifejezés).
`/route`	Útválasztási és továbbítási táblázatok elemzése (RouteEntryItem kifejezés).

A parancs visszatérési értékei:

- A `-1` azt jelenti, hogy a parancsot nem támogatja a számítógépre telepített alkalmazás verziója.
- A `0` azt jelenti, hogy a parancs sikeresen végre lett hajtva.
- Az `1` azt jelenti, hogy egy kötelező argumentum nem lett átadva a parancsnak.
- A `2` azt jelenti, hogy általános hiba történt.
- A `4` azt jelenti, hogy szintaktikai hiba történt.

Ha a parancs végrehajtása sikeres volt (a visszaadott érték `0`), és a Kaspersky Endpoint Security közben biztonsági sérülési indikátorokat észlelt, akkor a következő feladateredmény-adatokat küldi vissza a parancssorba:

`Uuid`	Az IOC-fájl azonosítója az IOC-fájlszerkezet fejlécéből (a `<ioc id="">` címke)
`Name`	Az IOC-fájl leírása az IOC-fájlszerkezet fejlécéből (a `<description></description>` címke)
`Matched Indicator Items`	Az összes egyező indikátorelem azonosítóinak listája.
`Matched objects`	Minden olyan IOC-dokumentum adatai, amelyek esetében egyezés volt.

MDRLICENSE. MDR aktiválás

A BLOB konfigurációs fájl hozzáadása a Managed Detection and Response aktiválásához. A BLOB fájl tartalmazza az ügyfélazonosítót és a Kaspersky Managed Detection and Response licencére vonatkozó információkat. A BLOB fájl az MDR konfigurációs fájl ZIP-archívumában található. A ZIP-archívumot a Kaspersky Managed Detection and Response konzoljában szerezheti be. A BLOB fájlról részletes információt a Kaspersky Managed Detection and Response súgójában találhat.

A BLOB fájlokkal végzett műveletekhez rendszergazdai jogosultságra van szükség. A Managed Detection and Response házirendben lévő beállításainak is rendelkezésre kell állniuk szerkesztésre ().

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Művelet	
`/ADD <file name>`	Alkalmazza a BLOB konfigurációs fájlt a Kaspersky Managed Detection and Response integrálásához (P7 fájlformátum). Csak egy BLOB fájlt alkalmazhat. Ha egy BLOB fájlt már hozzáadott a számítógéphez, akkor a fájl kicserélődik.
`/DEL`	Törölje a BLOB konfigurációs fájlt.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Példa

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integráció az EDR (KATA) megoldással

Az Endpoint Detection and Response összetevő (KATA) kezeléséhez szükséges parancsok:

- Az EDR (KATA) összetevő engedélyezése vagy letiltása.

  Az EDR összetevő (KATA) együttműködést biztosít a Kaspersky Anti Targeted Attack Platform megoldással.

- A Kaspersky Anti Targeted Attack Platform kiszolgálókkal való kapcsolat konfigurálása.

- Az összetevő aktuális beállításainak megjelenítése.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
```

```
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Művelet	
stop	Letilthatja az EDR (KATA) összetevőt.
start	Engedélyezheti az EDR (KATA) összetevőt.
set	Konfigurálhatja az EDR (KATA) összetevőt. Az alábbi beállításokat konfigurálhatja: • A Central Node-kiszolgálók hozzáadása (`servers=<server address>:<port>`) • TLS-tanúsítvány hozzáadása (`server-certificate=<path to the TLS certificate>`) • Beállíthatja a Central Node-kiszolgáló kapcsolódási időtúllépését `/timeout=<Central Node server connection timeout (s)>`) • Beállíthatja a Central Node-kiszolgálóval való szinkronizálás időtartamát `/sync-period=<Central Node server synchronization period (min)>`)
show	Az összetevő aktuális beállításainak megjelenítése.

KUMA. Integráció az KUMA-rel

A beépített KUMA-ügynök kezelési parancsai:

- A KUMA-integráció engedélyezése vagy letiltása.

  A beépített KUMA-ügynök együttműködést tesz lehetővé a Kaspersky Unified Monitoring and Analysis Platform megoldással.

- A Kaspersky Unified Monitoring and Analysis Platform kiszolgálóihoz való kapcsolat konfigurálása.

- Az összetevő aktuális beállításainak megjelenítése.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Művelet	
stop	Tiltsa le a KUMA-integrációt.
start	Engedélyezze a KUMA-integrációt.

`set`	Konfigurálja a beépített KUMA-ügynököt. Az alábbi beállításokat konfigurálhatja: • Adja hozzá a KUMA-kiszolgálókat (`/servers=<protocol>://<server address>:<port>`) Az alkalmazás a következő kiszolgálókapcsolati protokollokat támogatja: `tcp`, `udp`, `http`, `https`. • TLS-tanúsítvány hozzáadása (`/server-certificate=<path to the TLS certificate>`) • A kiszolgáló kapcsolódási időtúllépésének beállítása (`/timeout=<KUMA server connection timeout (s)>`) • Kriptotároló hozzáadása (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Az esemény átviteli késleltetésének konfigurálása (`/maximum-data-transfer-time=<maximum events transmission delay (sec)>`)
`show`	Az összetevő aktuális beállításainak megjelenítése.

Hitelesítés	
`/login=<user name> /password=<password>`	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. YARA-vizsgálat futtatása

A *YARA-vizsgálati* feladat futtatása. Az alkalmazás YARA-szabályadatbázisok segítségével vizsgálja a fájlokat és objektumokat a vállalati IT-infrastruktúra elleni célzott támadásokra utaló jelzéseket keresve. A *YARA-szabályok* olyan célzott támadások és a vállalati IT-infrastruktúrába történő behatolások jellemzőinek leírásai, amelyeket a Kaspersky Endpoint Security az objektumok vizsgálatához használ.

A YARA-vizsgálat futtatásához elő kell készítenie a szabályokat leíró YARA-fájlokat. A YARA-fájlok létrehozásakor vegye figyelembe a következő követelményeket:

- A Kaspersky Endpoint Security támogatja a .YARA és .YAR kiterjesztésű YARA-fájlokat, amelyek a biztonsági incidensek jelzőinek leírására szolgáló YARA 4.2.3 nyílt szabványt követik.
- A feladathoz csak YARA-szabályokat tartalmazó fájlok adhatók meg. A *YARA-vizsgálat futtatása* feladat nem támogat más szabálytípusokat.
- Ha a Kaspersky Endpoint Security által nem támogatott YARA-fájlokat adott hozzá, vagy a szabályok szintaktikai hibákat tartalmaznak, a feladat a megfelelő hibaüzenettel megszakad.
- Az egy feladatban használt összes YARA-fájl azonosítójának egyedinek kell lennie. Ha ugyanolyan azonosítóval rendelkező YARA-fájlok vannak, az befolyásolhatja a feladatvégrehajtás eredményeit.
- A YARA-vizsgálat a YARA-szabályokban leírt indikátorokkal való 128 egyezés után megszakad. Erre a YARA vizsgálati jelentésben szereplő bejegyzések számának korlátozása céljából van szükség, hogy a rendszer megkönnyítse a jelentés elemzését, és hogy megóvja a jelentést a túlcsordulástól a pontatlanul megfogalmazott YARA-szabályok miatt, amelyek rengeteg találatot generálhatnak.

A Kaspersky YARA-fájlonként egy szabály létrehozását javasolja. Ez olvashatóbbá teszi a vizsgálat eredményeit.

A YARA-vizsgálat sok időt vehet igénybe. A meghajtó méretétől, a feladatok beállításaitól és a lemezen lévő objektumok számától függően a YARA-vizsgálat néhány perctől több óráig tarthat. Az alkalmazás nem jelenít meg állapotjelzőt. A YARA-vizsgálatot nem lehet leállítani vagy megszakítani. Javasoljuk, hogy várjon, amíg a YARA-vizsgálat eredményei elérhetők lesznek.

A parancs szintaxisa

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA-fájlok	
`<full path to the YARA file>`	A vizsgálathoz használni kívánt YARA-fájl teljes elérési útja. Több YARA-fájl elérési útját is megadhatja, szóközökkel elválasztva. Kötelező argumentum, ha a `/path=<path to the folder with YARA files>` érték nincs megadva. Példa: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	A vizsgálathoz használni kívánt YARA-fájlokat tartalmazó mappa teljes elérési útja. Kötelező argumentum, ha a `<full path to the YARA file>` érték nincs megadva. Példa: `/path=C:\Users\Admin\Desktop\YARA`

Speciális beállítások	
`/fastScan=<on|off>`	Gyors YARA-vizsgálat. Az alkalmazás minden objektumnál naplózza az észlelt indikátor egy előfordulását. Az alkalmazás az észlelt indikátorok ismétlődéseit elrejti a naplóban. A Gyors YARA-vizsgálat lehetővé teszi a nagyméretű fájlok gyorsabb vizsgálatát. Ha ez a beállítás nincs megadva, az alkalmazás szabványos YARA-vizsgálatot hajt végre. Ebben a módban az alkalmazás az észlelt indikátorok ismétlődéseit naplózza.
`/maxRules=<maximum number of scan rules>`	Az egyedi, kiváltott szabályok számának felső határa, amelynek elérése esetén az alkalmazás leállítja a YARA-vizsgálatot. Ha ennek a beállításnak az értéke nincs megadva, vagy ha `0` van megadva, az alkalmazás a YARA-vizsgálatot korlátozások nélkül végzi el.
`/timeOut=<stop scan after the specified time in seconds>`	Ennyi ideig tarthat egy YARA-vizsgálat (másodpercekben). Ha ez az idő lejár, az alkalmazás leállítja a YARA-vizsgálatot. Ha ennek a beállításnak az értéke nincs megadva, vagy ha `0` van megadva, az alkalmazás a YARA-vizsgálatot korlátozások nélkül végzi el.
`/recursive=<on|off>`	Ez az argumentum indítja el a mappán belüli almappák rekurzív vizsgálatát a `/scanFolders` egyéni vizsgálatban.
`/scanFolders=<list of folders to be scanned>`	Ez az argumentum indítja el a megadott mappák listáján lévő fájlok YARA-vizsgálatát. Több értéket is megadhat szóközökkel elválasztva. A Kaspersky Endpoint Security támogatja a `*` és `?` karaktereket egy mappaútvonal-maszk megadásakor. Ha ez a beállítás nincs megadva, az alkalmazás YARA-vizsgálatot végez az összes helyi lemezen, kivéve a hálózati megosztásokat, a felhőmeghajtókat és a cserélhető adathordozókat.
`/scanMemory=<on|off>`	Vizsgálja meg az összes futó folyamat memóriáját.
`/scanProcess=<process name>`	Memória vizsgálata csak a megadott folyamatoknál. Adja meg a folyamatok végrehajtható fájljainak teljes elérési útját szóközzel elválasztva. Használhatja a `*` és `?` karaktereket a maszk megadásához.
`/maxSize=<file size in bytes>`	Fájlméret korlátozása a YARA-vizsgálatnál. Az alkalmazás kihagyja a nagyobb fájlokat.

`/includes=<list of objects to be scanned>>`	A vizsgálat hatókörének szerkesztése. Több értéket is megadhat szóközökkel elválasztva. A következő értékek állnak rendelkezésre: • Fájlnév • Fájlkiterjesztés A vizsgálat hatókörét a `/scanFolders` paraméterrel kell megadni. Példa: `/scanFolders C:\*.* /includes=*.exe *.dll` – az alkalmazás átvizsgálja a C: meghajtón található összes .EXE és .DLL kiterjesztésű fájlt.
`/excludes=<list of objects to be scanned>`	Fájlok kizárása a YARA-vizsgálatból. Több értéket is megadhat szóközökkel elválasztva. A következő értékek állnak rendelkezésre: • A fájl elérési útja • A fájl elérési útjának maszkja A kizárásokat a `/scanFolders` paraméterrel kell megadni. Példa: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – az alkalmazás kihagyja a readme.txt fájlt, a C:\trusted mappában található összes fájlt, valamint a C: meghajtó gyökérmappájában található összes .XML kiterjesztésű fájlt.
`/scanAutoruns=<on|off>`	Az automatikus futtatási pontok YARA-vizsgálata.
`/excludeAutoruns=<list of autorun point areas to skip>`	Az automatikus futtatási pont objektumainak kizárása a vizsgálati hatókörből. Adja meg a folyamatok végrehajtható fájljainak teljes elérési útját szóközzel elválasztva. Használhatja a `*` és `?` karaktereket a maszk megadásához.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Ha megadja egy mappa elérési útját, az alkalmazás a vizsgálati eredményeket a megadott helyre menti, egy yara_<számítógép neve>_<vizsgálat befejezésének ideje>.txt nevű fájlba. Ha megadja egy adott TXT-fájl elérési útját, az alkalmazás a vizsgálati eredményeket abba a fájlba menti. Például: `/logFolder=C:\test` or `/logFolder=C:\test\abc.txt`. A vizsgálati eredmények a parancssorba kerülnek, függetlenül attól, hogy megadta-e a `/logFolder` opciót.

A parancs visszatérési értékei:

- A `-1` azt jelenti, hogy a parancsot nem támogatja a számítógépre telepített alkalmazás verziója.
- A `0` azt jelenti, hogy a parancs sikeresen végre lett hajtva.
- Az `1` azt jelenti, hogy egy kötelező argumentum nem lett átadva a parancsnak.
- A `2` azt jelenti, hogy általános hiba történt.
- A `4` azt jelenti, hogy szintaktikai hiba történt.
- Az `5` azt jelenti, hogy egy vagy több, a paraméterben megadott YARA-szabályokkal rendelkező fájl nem található.

Ha a parancs végrehajtása sikeres volt (a visszaadott érték `0`), és a Kaspersky Endpoint Security közben biztonsági sérülési indikátorokat észlelt, akkor a következő feladateredmény-adatokat küldi vissza a parancssorba:

`Started at <time>` `Finished at <time>`	A vizsgálat kezdési és befejezési ideje.
`Host name: <computer name>`	Annak a számítógépnek a neve, amelyen az objektumot észleltük.
`Result: <error>`	A feladat végrehajtása közben bekövetkezett hiba hibakódja. Ha nincs hiba, az alkalmazás `0x00000000` kimenetet jelenít meg.
`Comment: <comment text>`	A feladat végrehajtása közben bekövetkezett hiba leírása. Például: `Operation timeout`.
`Object Name:` vagy `Process:` (a folyamatmemória vizsgálatakor)	Az objektum vagy folyamat neve, amelynél a YARA-szabály aktiválódott.

`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Annak az objektumnak a kivonatai, amelynél a YARA-szabály aktiválódott.
`Rule Name`	Az aktivált YARA-szabály neve.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	A YARA szabályban megadott metaadatok.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Az objektumon belül olyan egyezések találhatók, amelyek megfelelnek a YARA-szabály feltételeinek:
	• Az a hely a folyamatmemóriában vagy a fájlban, ahol egyezés található (`Offset`).
	• Az egyező karakterlánc neve a YARA-szabályban (`String name`).
	• Az egyező karakterlánc a folyamatmemóriában vagy a fájlban (`String data`).

TELEMETRIAI SZŰRŐK. A KUMA-nak küldendő szűrési események

Alapértelmezés szerint az események KUMA kiszolgálóra való küldése le van tiltva. A KUMA megfelelő működéséhez engedélyeznie kell a telemetriai adatok küldését. Az eseményforrást a következő standard naplók közül választhatja ki: *Alkalmazás*, *Biztonság* vagy *Rendszer*. A teljesítmény növelése és az adatok KUMA kiszolgálóra történő továbbításának optimalizálása céljából manuálisan hozzáadhat vagy kizárhat egyes eseményeket a telemetriából. Például kizárhatja a Sysmon eseményeket.

A kizárások listáját exportálhatja a parancssorból egy JSON-fájlba.

Ha a parancs csak annak a fájlnak a nevét tartalmazza, amelybe a beállításokat exportálni szeretné, az alkalmazás a következőképpen helyezi el a fájlt:

- Ha az avp.com elérési útvonalát hozzáadjuk a %PATH% rendszerváltozóhoz, az alkalmazás a `C:\Windows\SysWOW64` mappába helyezi a fájlt.

- Ha a parancsot az alkalmazás telepítési mappájából futtatja, az exportálás sikertelen lesz, mivel az alkalmazás önvédelme megakadályozza egy új fájl létrehozását az alkalmazás mappájában. Az alkalmazásbeállítások fájlba történő exportálásához adja meg a fájl elérési útját.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Művelet	
`export`	A KUMA-nak küldendő eseményszűrők exportálása.
`import`	A KUMA-nak küldendő eseményszűrők importálása. Ha már léteznek eseményszűrési szabályok a számítógépen, a Kaspersky Endpoint Security lecseréli ezeket az importálás során.

Fájl exportálásra vagy importálásra	
`<file name>`	A KUMA-nak küldendő eseményszűrőket tartalmazó fájl neve. A fájl elérési útját is megadhatja. A KUMA-nak küldendő szűrőket JSON-fájlba exportálhatja.

Light Agent felügyeleti parancsok

Az alkalmazást Light Agent üzemmódban is kezelheti a parancssorból a virtuális környezetek védelme céljából. Kezelheti az alkalmazást Light Agent üzemmódban, ha a Kaspersky Security Center konzol használatával történő felügyelet nem lehetséges. Megtekintheti az alkalmazáskezeléshez tartozó parancsok listáját, ha futtatja a `HELP` parancsot. A megadott parancs szintaxisának elolvasásához adja meg a `HELP <command>` parancsot.

Az alkalmazás kezelése Light Agent üzemmódban a parancssorból:

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.
3. A parancs végrehajtásához használja a következő sablont:

   ```
   avp.com <command> [options]
   ```

   Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot.

A Light Agent üzemmódban telepített alkalmazás támogatja a Normál üzemmódban telepített alkalmazás szinte összes AVP-parancsát. Light Agent üzemmódban a vírusadatbázis frissítési feladatai és a licenckulcs felügyeleti feladatai korlátozottak.

KSVLAINFO. A Light Agent üzemmód meghatározása

A Light Agent üzemmód meghatározása.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com KSVLAINFO
```

A parancs a következő információkat küldi a konzolnak:

- Light Agent üzemmód a virtuális környezetek védelmére: engedélyezve vagy letiltva.

  Ha a Light Agent üzemmód engedélyezve van, az alkalmazás a Kaspersky Security for Virtualization Light Agent megoldás részeként használható.

- VDI védelmi mód: engedélyezve vagy letiltva.

  A VDI védelmi mód segít optimalizálni a Kaspersky Endpoint Security teljesítményét a nem perzisztens virtuális gépeken. Ha a VDI-védelmi mód engedélyezve van, a védett virtuális gép újraindítását igénylő frissítések nem települnek a nem perzisztens virtuális gépekre. Az újraindítást igénylő frissítések fogadásakor a nem perzisztens virtuális gépre telepített Light Agent üzenetet küld a Kaspersky Security Center számára, amelyben tájékoztatja, hogy a védett virtuális gép sablonját frissíteni kell.

- A védett virtuális gép típusa: perzisztens vagy nem perzisztens.

- A védett virtuális gép szerepe a virtuális infrastruktúrában: kiszolgáló vagy munkaállomás.

- Azonosító: UUID.

VIISINFO. A Light Agent és az Integrációs kiszolgáló közötti kapcsolat állapota

A Light Agent és az Integrációs kiszolgáló közötti kapcsolatra vonatkozó információk megtekintése.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com VIISINFO
```

A parancs a következő információkat küldi a konzolnak:

- Az Integrációs kiszolgáló címe és portja, amelyhez a Light Agent csatlakozik.

- Az Integrációs kiszolgáló kapcsolatának állapota.

- A Light Agent és az Integrációs kiszolgáló közötti utolsó kapcsolat dátuma és időpontja.

SVMINFO. A Light Agent és a Védelmi kiszolgáló közötti kapcsolat állapota

A Light Agent védelmi kiszolgálóhoz való csatlakozásával kapcsolatos információk megtekintése.

A parancs futtatásához lépjen abba a mappába, ahol a Kaspersky Endpoint Security futtatható fájl található. A futtatható fájl elérési útját a %PATH% rendszerváltozóhoz is hozzáadhatja, és futtathatja a parancsot anélkül, hogy az alkalmazás mappájába navigálna.

A parancs szintaxisa

```
avp.com SVMINFO
```

A parancs a következő információkat küldi a konzolnak:

- Az SVM címe, amelyhez a Light Agent csatlakozik, és az SVM helye a virtuális infrastruktúrában a Light Agenthez képest: helyi vagy nem helyi.
- A Light Agent által használt SVM-felderítési módszer: Integrációs kiszolgáló vagy az SVM-címek egyéni listájának használata.
- SVM címlista, ha SVM címlista van kiválasztva SVM-felderítési módszerként.
- Címke a Light Agent és az SVM közötti csatlakoztatáshoz.
- SVM kiválasztási algoritmus: standard vagy kiterjesztett. Ha a kiterjesztett SVM kiválasztási algoritmust használja, az SVM útvonaltípusa a virtuális infrastruktúrában is megjelenik.
- A Light Agent és a védelmi kiszolgáló közötti kapcsolat védelmi állapota.

Hibakódok

Hibák akkor léphetnek fel, amikor az alkalmazást a parancssorok keresztül kezeljük. Hiba esetén a Kaspersky Endpoint Security hibaüzenetet jelenít meg, például: `Error: Cannot start task 'EntAppControl'`. A Kaspersky Endpoint Security egy kód formájában további információkat is megjelenít, például: `error=8947906D` (lásd az alábbi táblázatot).

Hibakódok

Hibakód	Leírás
`09479001`	A kulcs már használatban van
`0947901D`	A licenc lejárt. Az adatbázis-frissítések nem érhetők el
`89479002`	Nem található kulcs
`89479003`	A digitális aláírás hiányzik vagy sérült
`89479004`	Az adatok sérültek
`89479005`	A kulcsfájl sérült
`89479006`	A licenc lejárt
`89479007`	A kulcsfájl nincs megadva
`89479008`	Érvénytelen kulcsfájl
`89479009`	Nem sikerült elmenteni az adatot
`8947900A`	Nem lehet olvasni az adatot
`8947900B`	I/O hiba
`8947900C`	Nem található adatbázis
`8947900E`	A licenckönyvtár nem tölthető be
`8947900F`	Az adatbázisok fertőzöttek vagy manuálisan lettek frissítve
`89479010`	Az adatbázisok fertőzöttek
`89479011`	Nem lehet érvénytelen kulcsfájllal hozzáadni tartalék kulcsot
`89479012`	Rendszerhiba
`89479013`	A kulcsok tiltólistája sérült
`89479014`	A fájl aláírása nem egyezik meg a Kaspersky digitális aláírásával

Hibakód	Leírás
89479015	Próbalicenchez tartozó kulcs nem használható kereskedelmi licenc kulcsaként
89479016	Bétatesztelésre vonatkozó licenc szükséges az alkalmazás bétaverziójának használatához
89479017	A kulcsfájl nem kompatibilis ezzel az alkalmazással. A Kaspersky Endpoint Security for Windows nem aktiválható egy másik alkalmazás kulcsfájljával. Ellenőrizze a telepített alkalmazást
89479018	A Kaspersky blokkolta a licenckulcsot
89479019	Az alkalmazás már használva volt próbalicenccel. Nem lehet újra hozzáadni kulcsot a próbalicenchez
8947901A	A kulcsfájl sérült
8947901B	A digitális aláírás hiányzik, sérült, vagy nem egyezik meg a Kaspersky digitális aláírásával
8947901C	Nem lehet kulcsot hozzáadni, ha a megfelelő nem kereskedelmi licenc lejárt
8947901E	A kulcsfájl létrehozási vagy használati dátuma érvénytelen. Ellenőrizze a rendszerdátumot
8947901F	Nem lehet próbalicenchez hozzáadni kulcsot: a próbalicenc egy más kulcsa már aktív
89479020	A kulcsok tiltólistája sérült vagy hiányzik
89479021	A frissítés leírása hiányzik vagy fertőzött
89479022	A kulcs nem alkalmas ehhez az alkalmazáshoz
89479023	Nem lehet érvénytelen kulcsfájllal hozzáadni tartalék kulcsot
89479025	Hiba a kérés küldésekor az aktiváló kiszolgálóra. Lehetséges okok: internetkapcsolati hiba vagy az aktivációs kiszolgáló átmeneti problémája. Próbálja meg aktiválni az alkalmazást később (1–2 óra múlva) az aktiváló kóddal. Ha ez a hiba ismét előfordul, lépjen kapcsolatba az internetszolgáltatójával
89479026	A kérés helytelen aktiváló kódot tartalmaz
89479027	Nem lehet lekérni a válasz állapotát
89479028	Hiba az ideiglenes fájl mentése közben
89479029	Helytelen aktiváló kódot írt be, vagy érvénytelen rendszerdátumot állított be a számítógépen. Ellenőrizze a rendszerdátumot a számítógépen
8947902A	A kulcs nem kompatibilis ezzel az alkalmazással, vagy a licenc lejárt
8947902B	Nem sikerült letölteni a kulcsfájlt. Helytelen aktiváló kód lett megadva
8947902C	Az aktivációs kiszolgáló a 400-as hibakódot küldte vissza
8947902D	Az aktivációs kiszolgáló a 401-as hibakódot küldte vissza
8947902E	Az aktivációs kiszolgáló a 403-as hibakódot küldte vissza
8947902F	A szükséges erőforrás nem érhető el az aktiválási kiszolgálón. Az aktivációs kiszolgáló a 404-as hibakódot küldte vissza. Ellenőrizze internetkapcsolatának beállításait
89479030	Az aktivációs kiszolgáló a 405-as hibakódot küldte vissza
89479031	Az aktivációs kiszolgáló a 406-as hibakódot küldte vissza
89479032	Proxyhitelesítésre van szükség. Ellenőrizze a hálózat beállításait
89479033	Kérés időtúllépése
89479034	Az aktivációs kiszolgáló a 409-as hibakódot küldte vissza
89479035	A szükséges erőforrás nem érhető el az aktiválási kiszolgálón. Az aktivációs kiszolgáló a 410-as hibakódot küldte vissza. Ellenőrizze internetkapcsolatának beállításait
89479036	Az aktivációs kiszolgáló a 411-as hibakódot küldte vissza
89479037	Az aktivációs kiszolgáló a 412-as hibakódot küldte vissza
89479038	Az aktivációs kiszolgáló a 413-as hibakódot küldte vissza
89479039	Az aktivációs kiszolgáló a 414-as hibakódot küldte vissza
8947903A	Az aktivációs kiszolgáló a 415-as hibakódot küldte vissza
8947903C	Belső kiszolgálóhiba

Hibakód	Leírás
8947903D	A funkció nincs támogatva
8947903E	Érvénytelen átjárói válasz. Ellenőrizze a hálózat beállításait
8947903F	Az erőforrás ideiglenesen nem érhető el
89479040	Az átjárói válasz időkorlátja lejárt. Ellenőrizze a hálózat beállításait
89479041	A protokollt nem támogatja a kiszolgáló
89479043	Ismeretlen HTTP-hiba
89479044	Érvénytelen forrásazonosító
89479046	Érvénytelen URL
89479047	Érvénytelen célmappa
89479048	Nem sikerült lefoglalni a memóriát
89479049	Hiba történt a paraméterek ANSI-karakterlánccá való átalakítása során (URL, mappa, ügynök)
8947904A	Hiba történt a munkaszál létrehozásakor
8947904B	A munkaszál már fut
8947904C	A munkaszál nem fut
8947904D	A kulcsfájl nem található az aktiváló kiszolgálón
8947904E	A kulcs blokkolva van
8947904F	Belső hiba az aktiváló kiszolgálón
89479050	Nincs elég adat az aktivációs kérelemben
89479053	A hozzáadott kulcsnak megfelelő licenc már lejárt
89479054	A számítógépen beállított rendszerdátum érvénytelen. Ellenőrizze a rendszerdátum értékét
89479055	A próbalicenc lejárt
89479056	Az alkalmazás aktiválási periódusa lejárt
89479057	Az alkalmazás aktiválási korlátja az adott kód esetében túllépve
89479058	Az aktiválási eljárás rendszerhibával fejeződött be
89479059	Próbalicenchez tartozó kulcs nem használható kereskedelmi licenc kulcsaként
8947905C	Aktiváló kód szükséges
89479062	Nem lehet csatlakozni az aktivációs kiszolgálóhoz
89479064	Az aktivációs kiszolgáló nem érhető el. Ellenőrizze az internetkapcsolata beállításait, majd próbálja újra az aktiválást
89479065	A licenc lejárt
89479066	Nem lehet lejárt kulccsal lecserélni az aktivációs kulcsot
89479067	Nem lehet hozzáadni tartalék kulcsot, ha a megfelelő licenc a jelenlegi licenc előtt lejár
89479068	A frissített előfizetési kulcs hiányzik
8947906A	Érvénytelen aktiváló kód
8947906B	A kulcs már aktív
8947906C	Az aktív és a tartalék kulcs licenctípusa nem egyezik
8947906D	Az összetevőt nem támogatja a licenc
8947906E	Előfizetési kulcsot nem lehet tartalék kulcsként hozzáadni
89479213	Átviteli réteg generikus hiba
89479214	Nem sikerült csatlakozni az aktivációs kiszolgálóhoz
89479215	Érvénytelen formátumú webcím

Hibakód	Leírás
89479216	Nem sikerült konvertálni a proxykiszolgáló címét
89479217	Nem sikerült átalakítani a kiszolgáló címét. Ellenőrizze az internetkapcsolat beállításait
89479218	A kiszolgálóhoz a kapcsolódási kísérlet sikertelen
89479219	Hozzáférés távolról megtagadva
8947921A	Művelet időtúllépése
8947921B	Hiba a HTTP-kérelem küldésekor
8947921C	SSL-kapcsolati hiba
8947921D	A művelet visszahívás miatt megszakítva
8947921E	Túl sok átirányítás
8947921F	A címzett ellenőrzése sikertelen
89479220	Üres válasz a kiszolgálótól
89479221	Hiba az adatok küldésekor
89479222	Hiba az adatok fogadásakor
89479223	SSL-tanúsítvánnyal kapcsolatos probléma
89479224	SSL-titkosítással kapcsolatos probléma
89479225	SSL-tanúsítványközponttal kapcsolatos probléma
89479226	A hálózati csomag tartalma érvénytelen
89479227	Fiókhozzáférés megtagadva
89479228	Érvénytelen SSL-tanúsítvány fájl
89479229	Nem zárható le az SSL-kapcsolat
8947922A	Ismétlődő hiba
8947922B	Érvénytelen fájl megvont tanúsítványokkal
8947922C	SSL-tanúsítvány kérelem hiba
89479401	Ismeretlen kiszolgáló hiba
89479402	Belső kiszolgálóhiba
89479403	Nincs elérhető kulcs a megadott aktiváló kódhoz
89479404	Az aktív kulcs blokkolva van
89479405	Az aktiválási kérés szükséges paraméterei hiányoznak
89479406	Érvénytelen ügyfélszám vagy jelszó
89479407	Érvénytelen aktiváló kód
89479408	Az aktiváló kód nem kompatibilis ezzel az alkalmazással. A Kaspersky Endpoint Security for Windows nem aktiválható egy másik alkalmazás aktiváló kódjával. Ellenőrizze a telepített alkalmazást
89479409	Aktiváló kód szükséges
8947940B	Az aktiválási periódus lejárt
8947940C	A kódhoz járó aktivációk száma túllépve
8947940D	A kérelemazonosító érvénytelen formátuma
8947940E	Az aktiváló kód már használatban van
8947940F	Nem sikerült az aktiváló kód megújítása
89479410	Az aktiváló kód érvénytelen ehhez a régióhoz
89479411	Az aktiváló kód nem használható az alkalmazásnak ezzel a honosított változatával

Hibakód	Leírás
89479412	Az aktiváló kód az alkalmazás új verziójához készült. Szerezzen be egy másik aktiváló kódot az alkalmazás telepített verziójának aktiválásához
89479413	Az aktiváló kiszolgáló 643-as hibát adott vissza
89479414	Az aktiváló kiszolgáló 644-as hibát adott vissza
89479415	Az aktiváló kiszolgáló 645-as hibát adott vissza
89479416	Az aktiváló kiszolgáló 646-as hibát adott vissza
89479417	1.0 verziójú aktiváló kiszolgáló szükséges
89479418	Az aktiváló kód formátuma nem megfelelő
89479419	A számítógép órája nincs szinkronizálva az aktiváló kiszolgáló órájával
8947941A	Rossz alkalmazásverzió
8947941B	Az előfizetés lejárt
8947941C	Az aktiválások száma túllépve
8947941D	Érvénytelen jegyaláírás
8947941E	További adat szükséges
8947941F	Adatok ellenőrzése sikertelen
89479420	Az előfizetés inaktív
89479421	Az aktivációs kiszolgáló karbantartás alatt áll
89479501	Váratlan hiba
89479502	Érvénytelen átadott paraméter. Például üres az aktiváló kiszolgáló címeinek listája
89479503	Érvénytelen aktiváló kód (érvénytelen ellenőrzőösszeg)
89479504	Érvénytelen felhasználói azonosító
89479505	Érvénytelen felhasználói jelszó
89479506	Az aktivációs kiszolgáló érvénytelen válasza
89479507	Aktiválási kérelem megszakítva
89479509	Az aktiváló kiszolgáló üres továbbítási listát küldött vissza

Melléklet. Alkalmazásprofilok

A *Profil* egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. A profilokkal kezelhető az alkalmazás a parancssorból. A profilok használatával végrehajthatja a `START`, `STOP`, `STATUS`, `STATISTICS` és `EXPORT` parancsokat. A profilok használatával alkalmazásbeállításokat tud megadni (például, `STOP DeviceControl`), vagy feladatokat tud futtatni (például, `START Scan_My_Computer`).

A következő profilok állnak rendelkezésre:

- `AdaptiveAnomaliesControl` – Adaptív Anomáliafelügyelő
- `AMSI` – AMSI védelem
- `AntiCryptor`
- `BehaviorDetection` – Viselkedéselemzés

- `DeviceControl` – Eszközfelügyelő
- `EntAppControl` – Alkalmazásfelügyelő
- `File_Monitoring` vagy `FM` – Fájl védelem
- `Firewall` vagy `FW` – Tűzfal
- `HIPS` – Behatolásmegelőző rendszer
- `IDS` – Hálózati védelem
- `IntegrityCheck` – Integritásellenőrző
- `LogInspector` – Naplóvizsgálat
- `Mail_Monitoring` or `EM` – Levelezés védelem
- `Rollback` – Frissítés visszagörgetése (a profil nem alkalmazható, ha az alkalmazás telepítve van Light Agent üzemmódban)
- `Scan_ContextScan` – Vizsgálat a helyi menüből
- `Scan_IdleScan` – Vizsgálat a háttérben
- `Scan_Memory` – Kernelmemória-vizsgálat
- `Scan_My_Computer` – Teljes vizsgálat
- `Scan_Objects` – Egyéni vizsgálat
- `Scan_Qscan` – Olyan objektumok vizsgálata, amelyek az operációs rendszer indításakor voltak betöltve
- `Scan_Removable_Drive` – Cserélhető meghajtók vizsgálata
- `Scan_Startup` vagy `STARTUP` – Kritikus területek vizsgálata
- `Updater` – Frissítés (a profil nem alkalmazható, ha az alkalmazás telepítve van Light Agent üzemmódban)
- `Web_Monitoring` or `WM` – Webes védelem
- `WebControl` – Webfelügyelő

A Kaspersky Endpoint Security a szolgáltatásprofilokat is támogatja. A szolgáltatásprofilok akkor lehetnek szükségesek, amikor kapcsolatba lép a Kaspersky Terméktámogatással.

Az alkalmazás kezelése a REST API-n keresztül

A Kaspersky Endpoint Security segítségével alkalmazásbeállításokat adhat meg, vizsgálatot futtathat, frissítheti az antivírus adatbázisokat, valamint harmadik féltől származó megoldásokkal egyéb feladatokat hajthat végre. A Kaspersky Endpoint Security API-t biztosít ebből a célból. A Kaspersky Endpoint Security REST API HTTP-n működik, és kérelmi/válaszadási módszerekből áll. Más szóval, a Kaspersky Endpoint Security kezelhető harmadik féltől származó megoldáson keresztül is, nem pedig a helyi alkalmazásfelületen vagy a Kaspersky Security Center Adminisztrációs konzolon.

A REST API használatának elindításához a REST API támogatásával kell telepíteni a Kaspersky Endpoint Security alkalmazást. A REST klienst és a Kaspersky Endpoint Security alkalmazást ugyanarra a számítógépre kell telepíteni.

A Kaspersky Endpoint Security és a REST kliens közötti biztonságos interakció garantálásához:

- Állítsa be a REST kliens védelmét az illetéktelen hozzáférés ellen a REST kliens fejlesztőjének ajánlásai szerint. Állítsa be a REST kliens írás elleni mappavédelmét a tulajdonosi hozzáférés-szabályozási lista (DACL) segítségével.

- A REST kliens futtatásához használjon egy külön fiókot rendszergazdai jogokkal. Tagadja meg a rendszerbe való interaktív bejelentkezést ennél a fióknál.

Az alkalmazás kezelhető REST API-n keresztül a http://127.0.0.1 vagy http://localhost címeken. Nem lehet távolról kezelni a Kaspersky Endpoint Security alkalmazást REST API-n keresztül.

NYISSA MEG A REST API DOKUMENTUMOT

Az alkalmazás telepítése a REST API-val

A REST API felülettel történő alkalmazáskezeléshez telepítenie kell a Kaspersky Endpoint Security alkalmazást, a REST API támogatásával. Ha a Kaspersky Endpoint Security alkalmazást a REST API-n keresztül kezel, akkor nem tudja kezelni az alkalmazást a Kaspersky Security Center használatával.

Az alkalmazás REST API támogatással való telepítésének előkészítése

A Kaspersky Endpoint Security és a REST kliens közötti biztonságos interakció megköveteli a kérésazonosítás konfigurálását. Ehhez telepítenie kell egy tanúsítványt, majd alá kell írnia az egyes kérések adattartalmát.

Tanúsítvány létrehozásához használhatja például az OpenSSL-t.

Példa:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Használja az RSA titkosítási algoritmust 2048 bit vagy annál hosszabb kulcshosszal.

Ennek eredményeként kap egy `cert.pem` tanúsítványt és egy `key.pem` privát kulcsot.

Az alkalmazás telepítése a REST API támogatással

A Kaspersky Endpoint Security REST API támogatással történő telepítéséhez:

1. Futtassa az értelmező parancssort (cmd.exe) rendszergazdaként.
2. Menjen a mappába, ami tartalmazza a Kaspersky Endpoint Security 11.2.0 vagy későbbi verziójának terjesztőcsomagját.
3. Telepítse a Kaspersky Endpoint Security alkalmazást a következő beállításokkal:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     A felhasználónév, amivel kezelheti az alkalmazást a REST API-n keresztül. Adja meg a felhasználónevet a következő formátumban: `<DOMAIN>\<UserName>` (például `RESTAPI_User=COMPANY\Administrator`). Az alkalmazást csak ezzel a fiókkal kezelheti a REST API-n keresztül. A REST API-val történő munkálatokhoz csak egy felhasználót választhat ki.
   - `RESTAPI_Port=<port>`

     Az alkalmazás REST API felületen keresztül történő kezeléséhez használt port. A 6782 az alapértelmezett port. Győződjön meg arról, hogy a port szabad. Opcionális paraméterek.
   - `RESTAPI_Certificate=<path to certificate>`

     Tanúsítvány a kérések azonosítására (pl. `RESTAPI_Certificate=C:\cert.pem`).

     A tanúsítványt az alkalmazás telepítése után telepítheti, vagy a tanúsítvány lejárta után frissítheti.

     Tanúsítvány telepítése a REST API kérésazonosításhoz

     1. A Kaspersky Endpoint Security önvédelem letiltása

        Az önvédelmi mechanizmus megelőzi a merevlemezen lévő alkalmazásfájlok, a memóriafolyamatok és a rendszerleíró adatbázis bejegyzéseinek módosítását és törlését.

     2. Nyissa meg a REST API beállításait tartalmazó beállításkulcsot:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Adja meg a tanúsítvány elérési útját, pl. `Certificate = C:\Folder\cert.pem`.
     4. A Kaspersky Endpoint Security önvédelmének engedélyezése.
     5. Indítsa újra az alkalmazást.
   - `AdminKitConnector=1`

     Alkalmazáskezelés adminisztrációs rendszerek használatával. A kezelés alapértelmezetten engedélyezve van.

   Használhatja a setup.ini file fájlt is, hogy megadja a REST API felülettel történő műveletek beállításait.

   Példa:
   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
   /pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
   ```

Ennek eredményeképp kezelheti az alkalmazást a REST API-n keresztül. A működés hitelesítéséhez nyissa meg egy GET-kérelemmel a REST API dokumentumot.

Példa:
```
GET http://localhost:6782/kes/v1/api-docs
```

Ha az alkalmazást REST API támogatással telepítette, a Kaspersky Endpoint Security automatikusan létrehoz egy engedélyezési szabályt a Webfelügyelő beállításaiban a webes erőforrások eléréséhez (*Service Rule for REST API*). Erre a szabályra azért van szükség, hogy a REST-ügyfél mindig hozzáférhessen a Kaspersky Endpoint Security alkalmazáshoz. Ha például korlátozta a felhasználók hozzáférését a webes erőforrásokhoz, ez nem befolyásolja az alkalmazás REST API-n keresztül történő felügyeletét. Javasoljuk, hogy ne törölje a szabályt, és ne módosítsa a *Service Rule for REST API* beállításait. Ha törölte a szabályt, a Kaspersky Endpoint Security az alkalmazás újraindítása után visszaállítja azt.

Műveletek az API-val

Nem lehet korlátozni az alkalmazás hozzáférését a REST API-n keresztül a Jelszóvédelem használatával. Például nem lehet REST API-n keresztül megtiltani egy felhasználónak, hogy kikapcsolja a védelmet. A REST API-n keresztül megadhatja a Jelszavas védelmet, és korlátozhatja, hogy a felhasználó a helyi felületen keresztül érje el az alkalmazást.

Ahhoz, hogy a REST API-n keresztül kezelje az alkalmazást, először futtatnia kell a REST klienst azon fiók alatt, amit megadott az alkalmazás telepítése REST API támogatással lehetőségnél. A REST API-val történő munkálatokhoz csak egy felhasználót választhat ki.

NYISSA MEG A REST API DOKUMENTUMOT

Az alkalmazás REST API felületen keresztül történő kezelése a következő lépésekből áll:

1. Kérje le az alkalmazásbeállítások jelenlegi értékeit. Ehhez küldjön GET-kérelmet.
   Példa:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```
2. Az alkalmazás választ fog küldeni a beállítások struktúráival és értékeivel. A Kaspersky Endpoint Security az XML- és JSON-formátumokat támogatja.
   Példa:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```
3. Szerkessze az alkalmazás beállításait. Használja a GET-kérelemre kapott beállításstruktúrákat.
   Példa:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```
4. Mentse el az alkalmazás beállításait (az adattartalmat) egy JSON-fájlban (payload.json).

5. Írja alá a JSON-fájlt PKCS7 formátumban.

   Példa:
   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   Ennek eredményeként egy aláírt fájlt kap a kérés adattartalmával (`signed_payload.pem`).

6. Szerkessze az alkalmazás beállításait. Ehhez küldjön egy POST kérést, és csatolja az aláírt fájlt a kérés adattartalmával (`signed_payload.pem`).

Az alkalmazás alkalmazza az új beállításokat, és elküldi az alkalmazás konfigurációs eredményeit tartalmazó választ küld (a válasz üres is lehet). A beállítások frissítését GET kéréssel ellenőrizheti.

Az alkalmazással kapcsolatos információforrások

Ez a rész az alkalmazásra vonatkozó információforrásokat ismerteti.

A kérdés fontosságától és sürgősségétől függően kiválaszthatja a legmegfelelőbb információforrást.

A Kaspersky Endpoint Security oldal a Kaspersky webhelyén

A Kaspersky Endpoint Security oldalon általános információkat tekinthet meg az alkalmazásról, valamint annak funkcióiról és jellemzőiről.

A Kaspersky Endpoint Security oldal tartalmaz egy hivatkozást, amely az online áruházra mutat. Ott vásárolhatja vagy újíthatja meg az alkalmazást.

A Kaspersky Endpoint Security oldal a Tudásbázisban

A *Tudásbázis* a Terméktámogatás webhelyének egyik része.

A Tudásbázisban található Kaspersky Endpoint Security oldalon olyan cikkeket olvashat, amelyek hasznos információkat, ajánlásokat és válaszokat adnak a gyakran feltett kérdésekre az alkalmazás megvásárlásával, telepítésével és használatával kapcsolatban.

A Tudásbázis cikkei nemcsak a Kaspersky Endpoint Security termékkel, hanem más Kaspersky-alkalmazásokkal kapcsolatos kérdésekre is választ adhatnak. A Tudásbázisban található cikkek a Terméktámogatás híreit is tartalmazhatják.

A Kaspersky alkalmazásairól szóló beszélgetések a Fórumban

Ha kérdése nem igényel sürgős választ, megvitathatja azt a Kaspersky szakértőivel és más felhasználókkal a Fórumban.

A Fórumban megtekintheti az aktuális témákat, hozzászólásokat írhat, és új vitatémákat hozhat létre.

Kapcsolatfelvétel a Terméktámogatással

Ha nem talál megoldást a problémájára a dokumentációban vagy a Kaspersky Endpoint Security alkalmazással kapcsolatos információforrásokban, javasoljuk, hogy lépjen kapcsolatba a Terméktámogatással. A Terméktámogatási szakemberei választ adnak minden, a Kaspersky Endpoint Security telepítésére és használatára vonatkozó kérdésre.

A Kaspersky támogatást nyújt a Kaspersky Endpoint Security alkalmazáshoz annak életciklusa során (keresse fel az alkalmazás életciklusát ismertető oldalt). Mielőtt igénybe venné a terméktámogatási szolgáltatást, olvassa el a terméktámogatási szabályokat.

A terméktámogatással az alábbi módokon veheti fel a kapcsolatot:

- A Terméktámogatás webhelyének felkeresése
- Kérelem küldése a Kaspersky Terméktámogatás részére a Kaspersky CompanyAccount portálon keresztül

Miután értesíti a Kaspersky Terméktámogatás szakembereit a problémáról, előfordulhat, hogy *nyomkövetési fájl* előállítására kérik fel. A nyomkövetési fájl használatával lépésről lépésre nyomon követheti az alkalmazás parancsainak végrehajtását, illetve megállapíthatja, hogy az alkalmazás működésének melyik szakaszában történt a hiba.

A Terméktámogatás szakemberei további adatokat is igényelhetnek az operációs rendszerrel, a számítógépen futó folyamatokkal és az alkalmazásösszetevők működéséről szóló részletes jelentésekkel kapcsolatban.

Diagnosztika futtatásakor a Terméktámogatás szakértői felkérhetik, hogy módosítsa az alkalmazás beállításait az alábbi módokon:

- A funkció engedélyezése, ami bővített diagnosztikai információt fogad.
- Be kell állítani az alkalmazás egyes összetevőit úgy, hogy a szokásos felhasználói felületen nem hozzáférhető különleges beállításokat módosítja.
- A diagnosztikai adatok tárolási beállításainak módosítása.
- A hálózati forgalom elfogásának és naplózásának módosítása.

A Terméktámogatás szakemberei ezen műveletek elvégzéséhez minden szükséges tájékoztatást megadnak (a lépések sorrendjének ismertetését, a módosítandó beállításokat, konfigurációs fájlokat, szkriptfájlokat, további parancssori funkciókat, hibakereső modulokat, különleges segédprogramokat stb.), és tájékoztatják, hogy milyen adatok használatára kerül sor hibakeresési célokból. A kibővített diagnosztikai adatok mentésre kerülnek a felhasználó számítógépén. Az adatok Kaspersky részére történő továbbítása nem automatikus.

A fent felsorolt műveleteket kizárólag a Terméktámogatás szakembereinek felügyelete alatt, utasításaikat betartva szabad elvégezni. Ha az alkalmazásbeállításokat az online súgóban nem ismertetett, illetve a Terméktámogatás által nem ajánlott módon saját maga módosítja, akkor az operációs rendszer lelassulhat, illetve lefagyhat, csökkenhet a számítógép védelmi szintje, és kár eshet a feldolgozott adatok rendelkezésre állásában és épségében.

Nyomkövetési fájlok tartalma és tárolása

Személyesen Ön a felelős a számítógépén tárolt adatok biztonságáért, különösen az adatokhoz való hozzáférés megfigyeléséért és korlátozásáért mindaddig, amíg az adatokat el nem küldi a Kaspersky számára.

A nyomkövetési fájlok a számítógépen vannak tárolva az alkalmazás használata során, az alkalmazás eltávolításakor pedig véglegesen törlődnek.

A nyomkövetési fájlok, kivéve a Hitelesítési ügynökben lévő nyomkövetési fájlokat, a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappában vannak tárolva.

A nyomkövetési fájlok elnevezése a következő: `KES<14.1_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

A nyomkövetési fájlokban elmentett adatok megtekinthetők.

Minden nyomkövetési fájl tartalmazza az alábbi közös adatokat:

- Esemény ideje
- A végrehajtási szál száma

  A Hitelesítési ügynök nyomkövetési fájlja ezt az adatot nem tartalmazza.

- Az eseményt kiváltó alkalmazásösszetevő
- Az esemény súlyossági foka (tájékoztató jellegű, figyelmeztetés, kritikus esemény, hiba)
- Az esemény leírása az alkalmazás összetevőjének parancsvégrehajtásával és a végrehajtás eredményével együtt.

Az SRV.log, GUI.log és ALL.log nyomkövetési fájlok tartalma

Az `SRV.log`, a `GUI.log` és az `ALL.log` nyomkövetési fájlok az általános adatokon felül a következő információkat tartalmazhatják:

- Személyes adatok, köztük a vezeték-, középső és utónév, ha ezek az adatok helyi számítógépen lévő fájlok elérési útvonalában szerepelnek.
- A számítógépre telepített hardver adatai (például BIOS/UEFI firmware-adatok). Ezek az adatok belekerülnek a nyomkövetési fájlokba a Kaspersky teljes lemeztitkosítás végrehajtása során.
- A felhasználónév és jelszó, ha azok átvitele nyíltan történt. Ezek az adatok az internetes forgalom vizsgálata során nyomkövető fájlokba kerülhetnek.
- A felhasználónév és jelszó, ha azok HTTP-fejlécekben megtalálhatók.

- A Microsoft Windows fiók neve, ha az egy fájlnévben szerepel.
- Az Ön e-mail címe vagy fiókja nevét és jelszavát tartalmazó webcím, ha azok az észlelt objektum nevében találhatók.
- Az Ön által felkeresett webhelyek és átirányítások ezekről a webhelyekről. Ezek az adatok kerülnek nyomkövetési fájlokba, ha az alkalmazás webhelyeket vizsgál.
- Proxykiszolgáló címe, számítógépnév, port, IP-cím, valamint a proxykiszolgálóra való bejelentkezéshez szükséges felhasználónév. Ezek az adatok kerülnek nyomkövetési fájlokba, ha az alkalmazás proxykiszolgálót használ.
- Távoli IP-címek, melyekkel a számítógép kapcsolatokat létesített.
- Üzenet tárgya, azonosító, feladó neve és a feladó weblapjának címe közösségi hálózaton. Ezek az adatok kerülnek nyomkövetési fájlokba, ha a Webfelügyelő összetevő engedélyezve van.
- Hálózati forgalmi adatok. Ezek az adatok belekerülnek nyomkövetési fájlokba, ha engedélyezve vannak forgalomfelügyeleti összetevők (például a Webfelügyelő).
- A Kaspersky kiszolgálókról kapott adatok (például a víruskereső adatbázisok verziója).
- A Kaspersky Endpoint Security összetevők állapota és a műveleti adataik.
- Az alkalmazásban lévő felhasználói tevékenység adatai.
- Operációs rendszer események.

A HST.log, a BL.log, a Dumpwriter.log, a WD.log és az AVPCon.dll.log nyomkövetési fájl tartalma

A `HST.log` nyomkövetési fájl az általános adatokon felül információkat tartalmaz egy adatbázis- és alkalmazásmodul-frissítési feladatot végrehajtásával kapcsolatban.

A `BL.log` nyomkövetési fájl az általános adatokon felül információkat tartalmaz az alkalmazás működése közben bekövetkező eseményekkel, valamint az alkalmazáshibák hibakereséséhez szükséges adatokkal kapcsolatban. Ez a fájl akkor jön létre, ha az alkalmazást az avp.exe –bl paraméterrel indítják el.

A `Dumpwriter.log` nyomkövetési fájl az általános adatokon felül szervizinformációkat tartalmaz, melyek az alkalmazás memóriakiíratásának írásakor bekövetkező hibák hibaelhárításához szükségesek.

A `WD.log` nyomkövetési fájl az általános adatokon felül információkat tartalmaz az avpsus szolgáltatás működése közben bekövetkező eseményekkel, köztük az alkalmazásmodulok frissítési eseményeivel kapcsolatban.

Az `AVPCon.dll.log` nyomkövetési fájl az általános adatokon felül információkat tartalmaz a Kaspersky Security Center csatlakozási modul működése közben bekövetkező eseményekkel kapcsolatban.

A teljesítmény-nyomonkövetési fájlok tartalma

A teljesítmény-nyomkövetési fájlok elnevezése a következő:
`KES<14.1_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Az általános adatok mellett a teljesítmény-nyomonkövetési fájlok információkat tartalmaznak a processzor terheléséről, az operációs rendszer és az alkalmazások betöltéséről, valamint a futó programokról.

Az AMSI védelmi összetevő nyomkövetési fájljainak tartalma

Az általános adatokon felül az `AMSI.log` nyomkövetési fájljai a harmadik féltől származó alkalmazások által kezdeményezett vizsgálatok eredményeinek információit is tartalmazza.

A Levelezés védelem összetevő nyomkövetési fájljainak tartalma

Az `mcou.OUTLOOK.EXE.log` tartalmazhatja az e-mail-üzenetek részeit, köztük az e-mail-címeket, továbbá az általános adatokat.

A helyi menüből való vizsgálat összetevő nyomkövetési fájljainak tartalma

A `shellex.dll.log` nyomkövetési fájl információkat tartalmaz a vizsgálati feladat elvégzéséről és az alkalmazás hibakereséséhez szükséges adatokról, továbbá az általános információkról.

Az alkalmazás-webbővítmények nyomkövetési fájljainak tartalma

Az alkalmazás webes bővítményének nyomkövetési fájljai azon a számítógépen találhatók, ahol a Kaspersky Security Center Web Console üzembe van helyezve, a `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs` mappában.

Az alkalmazás webes bővítményének nyomkövetési fájljainak neve a következő: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. A Web Console a telepítése után megkezdi az adatok írását, az eltávolítása után pedig törli a nyomkövetési fájlokat.

Az alkalmazás-webbővítmények nyomkövetési fájljai az általános adatokon felül az alábbi információkat tartalmazzák:

- A KLAdmin felhasználói jelszót a Kaspersky Endpoint Security felület feloldásához (Jelszóvédelem).
- Átmeneti jelszót a Kaspersky Endpoint Security felület feloldásához (Jelszóvédelem).
- Felhasználónevet és jelszót az SMTP levelező kiszolgálókhoz. (E-mail értesítések).
- Felhasználónév és jelszó az internetes proxykiszolgálóhoz (Proxykiszolgáló).
- Felhasználónév és jelszó az *Alkalmazásösszetevők módosítása* feladathoz.
- A fiókbejelentkezési adatokat és az útvonalakat, amik meg vannak adva a Kaspersky Endpoint Security feladatokban és az irányelvek tulajdonságaiban.

A Hitelesítési ügynök nyomkövetési fájl tartalma

A Hitelesítési ügynök nyomkövetési fájlja a System Volume Information mappában tárolódik, és a következő a neve: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

A Hitelesítési ügynök nyomkövetési fájl az általános adatokon felül információkat tartalmaz a Hitelesítési ügynök működésével és a felhasználó által a Hitelesítési ügynökkel elvégzett műveletekkel kapcsolatban.

Alkalmazás tevékenységének követése

Az *Alkalmazás-nyomkövetés* az alkalmazás által végrehajtott műveletek és alkalmazás működése során bekövetkező eseményekről szóló üzenetek részletes nyilvántartása. A nyomkövetési folyamat során az alkalmazás fájlkészletet hoz létre a következővel: adatok a különböző alkalmazásösszetevők működéséről (például SRV.log, WD.log és mások).

Az alkalmazás-nyomkövetéseket a Kaspersky Terméktámogatás felügyelete alatt kell végezni.

Az alkalmazás-nyomkövetési fájl létrehozásához:

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az ablakban kattintson a **Támogató eszközök** gombra.
3. Az **Alkalmazás-nyomkövetés engedélyezése** kapcsolóval engedélyezze vagy tiltsa le az alkalmazásműködés nyomkövetését.
4. A **Nyomkövetés** legördülő listában válassza ki egy alkalmazás nyomkövetési módját:
   - **Méretkorlátozással**. Nyomkövetés mentése egy korlátozott méretű, megadott számú fájlkészletbe, és a régi fájlok felülírása, amikor elérte a maximális méretet. Ha ez a mód van kiválasztva, megadhatja a forgatáshoz szükséges fájlkészletek maximális számát és az egyes fájlkészletek maximális méretét.

     Alapértelmezés szerint az alkalmazás öt nyomkövetési fájlkészletet ment. Az egyes fájlkészletek mérete 3072 MB. Így 15 GB szabad lemezterületre van szükség a nyomkövetési fájlok mentéséhez.
   - **Korlátozások nélkül**. Egy nyomkövetési fájl mentése (nincs méretkorlát).
5. A **Szint** legördülő listán válassza ki a nyomkövetési szintet:
   - A **Normál** beállítás esetén a naplófájl minden hibáról és figyelmeztetésről, valamint az alkalmazás rendes működéséről is tárol üzeneteket (alapértelmezett).
   - A **Részletes** beállítás azt jelenti, hogy a naplófájl az alkalmazás működésével kapcsolatos összes információt menti.

   További nyomkövetési szintek állnak rendelkezésre, ha az alkalmazás nyomkövetési beállításait a parancssorból kezeli. Ajánlott a szükséges nyomkövetési szintet a Terméktámogatási szolgáltatás szakembereivel tisztázni. Ha nem kap útmutatást a Terméktámogatás szakemberétől, állítsa be a szintet **Normál** értékre.

Ha az alkalmazás nyomkövetése a parancssorból lett engedélyezve, és a nyomkövetési szint nem a **Normál** vagy a **Részletes** értékre lett beállítva, akkor a **Szint** legördülő lista értéke **Normál** lesz.

6. A nyomkövetési folyamat leállításához térjen vissza a **Támogató eszközök** ablakba, és tiltsa le a nyomkövetést.

Továbbá létrehozhat nyomkövetési fájlokat, ha telepíti az alkalmazást a parancssorból, például a setup.ini fájl használatával.

Ennek eredményeként az alkalmazásműködés nyomkövetési fájljai a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappában jönnek létre. A nyomkövetési fájlok létrehozása után küldje el a fájlt a Kaspersky Terméktámogatásnak.

A Kaspersky Endpoint Security az alkalmazás eltávolításakor automatikusan törli a nyomkövetési fájlokat. A fájlokat manuálisan is törölheti. Ehhez le kell tiltania a nyomkövetést, és le kell állítania az alkalmazást.

Alkalmazás teljesítményének követése

A Kaspersky Endpoint Security segítségével információt kaphat a számítógépről, ami hibát észlel az alkalmazás használata során. Például, információt kaphat az operációs rendszer terheléséről, ami az alkalmazás telepítése után lép fel. Ehhez a Kaspersky Endpoint Security létrehoz teljesítmény nyomonkövetési fájlokat. *A teljesítmény nyomkövetése* az alkalmazás által végzett műveletek naplózását jelenti, amelynek célja a Kaspersky Endpoint Security teljesítményével kapcsolatos hibák diagnosztizálása. Ennek az információnak a megszerzéséhez a Kaspersky Endpoint Security az Event Tracing for Windows (ETW) szolgáltatást használja. A Kaspersky Terméktámogatás felelős a Kaspersky Endpoint Security hibáinak diagnosztizálásáért és ezen hibák okainak meghatározásáért.

Az alkalmazás-nyomkövetéseket a Kaspersky Terméktámogatás felügyelete alatt kell végezni.

A nyomkövetési fájl létrehozásához:

1. Kattintson a fő alkalmazásablakban a gombra.
2. Az ablakban kattintson a **Támogató eszközök** gombra.
3. A **Teljesítmény-nyomkövetés engedélyezése** kapcsolóval engedélyezze vagy tiltsa le az alkalmazás teljesítményének nyomkövetését.
4. A **Nyomkövetés** legördülő listában válassza ki egy alkalmazás nyomkövetési módját:
   - **Méretkorlátozással**. Nyomkövetés mentése egy korlátozott méretű, megadott számú fájlba, és a régi fájlok felülírása, amikor elérte a maximális méretet. Ha ez a mód van kiválasztva, megadhatja az egyes fájlok maximális méretét.
   - **Korlátozások nélkül**. Egy nyomkövetési fájl mentése (nincs méretkorlát).

5. A **Szint** legördülő listán válassza ki a nyomkövetési szintet:

   - **Alacsony**. A Kaspersky Endpoint Security elemzi a teljesítménnyel kapcsolatos legfontosabb operációsrendszer-folyamatokat.

   - **Részletes**. A Kaspersky Endpoint Security elemzi a teljesítménnyel kapcsolatos összes operációsrendszer-folyamatot.

6. A **Nyomkövetési típus** legördülő listán válassza ki a nyomkövetés típusát:

   - **Alapinformáció**. A Kaspersky Endpoint Security elemzi a folyamatokat, miközben fut az operációs rendszer. Ezt a nyomonkövetési típust akkor használja, ha a probléma az operációs rendszer betöltése után áll fenn, például akkor, ha nem tudja elérni az internetet a böngészővel.

   - **Újraindításkor**. A Kaspersky Endpoint Security csak akkor elemzi a folyamatokat, amikor az operációs rendszer betöltődik. Miután betöltődik az operációs rendszer, a Kaspersky Endpoint Security befejezi a nyomkövetést. Ezt a nyomonkövetési típust akkor használja, ha a probléma az operációs rendszer betöltése lassú.

7. Indítsa újra a számítógépet, hogy megpróbálja újragenerálni a hibát.

8. A nyomkövetési folyamat leállításához térjen vissza a Támogató eszközök ablakba, és tiltsa le a nyomkövetést.

Ennek eredményeképpen a teljesítmény nyomonkövetési fájlok a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappában tárolódnak. A nyomkövetési fájl létrehozása után küldje el a fájlt a Kaspersky Terméktámogatásnak.

Memóriakiíratás

A memóriakiíratások minden Kaspersky Endpoint Security folyamat munkavégzésének memóriáját tartalmazzák a memóriakiíratás létrehozása idején.

A mentett memóriakiíratási fájlok bizalmas adatokat tartalmazhatnak. Az adathozzáférés szabályozása érdekében külön garantálnia kell a memóriakiíratási fájlok biztonságát.

A memóriakiíratások a számítógépen vannak tárolva az alkalmazás használata során, az alkalmazás eltávolításakor pedig véglegesen törlődnek. A memóriakép kiíratási fájlok a `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` mappában vannak tárolva.

Memóriakép írásának engedélyezése az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.

2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.

4. A **Hibakeresési adatok** részen kattintson a **Beállítások** gombra.

5. A megnyíló ablakban használja a **Memóriakép írásának engedélyezése** jelölőnégyzetet az alkalmazás memóriaképe írásának engedélyezéséhez vagy letiltásához.

6. Mentse el a módosításokat.

Memóriakép írásának engedélyezése a Web Console-ban és a Cloud Console-ban

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.

3. Válassza ki az **Application settings** lapot.

4. Nyissa meg a **General Settings** → **Technical Support** elemet.

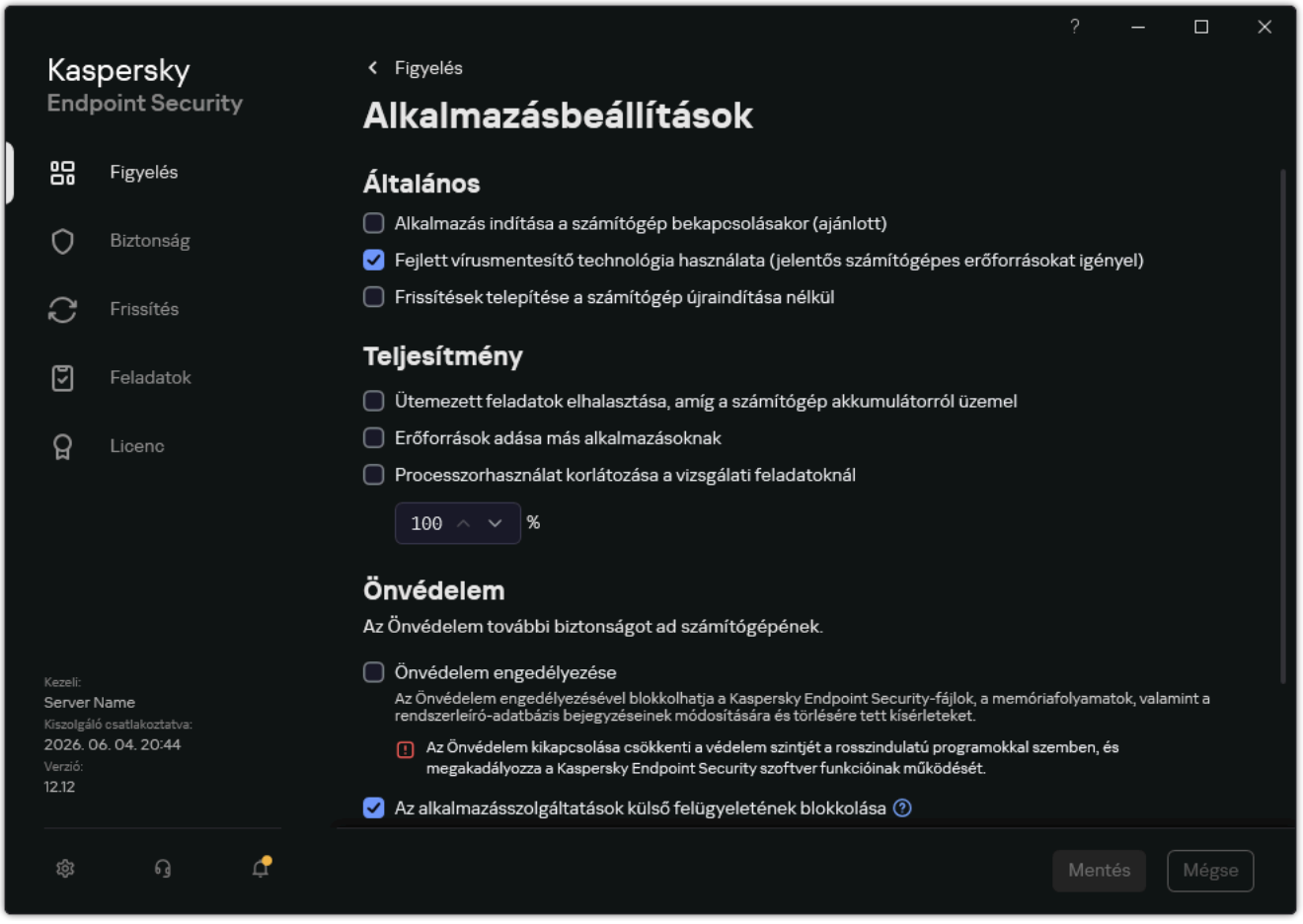
5. A(z) **Debug information** területen használja a(z) **Dump writing ENABLED** jelölőnégyzetet az alkalmazás memóriaképe írásának engedélyezéséhez vagy letiltásához.

6. Mentse el a módosításokat.

Memóriakép írásának engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. A **Hibakeresési adatok** blokkban használja a **Memóriakép írásának engedélyezése** jelölőnégyzetet az alkalmazás memóriaképe írásának engedélyezéséhez vagy letiltásához.

4. Mentse el a módosításokat.

Memóriakiíratási fájlok és nyomkövetési fájlok védelme

A kiíratási és a nyomkövetési fájlok az operációs rendszert és a felhasználói adatot érintő információkat is tartalmazhatnak. Az ilyen adatokhoz való illetéktelen hozzáférés megelőzése érdekében bekapcsolhatja a kiíratási és nyomkövetési fájlok védelmét.

A kiíratási és nyomkövetési fájlok védelmének bekapcsolása esetén a fájlokhoz az alábbi felhasználók férhetnek hozzá:

- A kiíratási fájlokhoz a rendszergazda és a helyi rendszergazda, valamint a kiíratási és nyomkövetési fájlok írását bekapcsoló felhasználó férhet hozzá.
- A nyomkövetési fájlokhoz kizárólag a rendszergazda és a helyi rendszergazda férhet hozzá.

A memóriakiíratási fájlok és a nyomkövetési fájlok védelmének engedélyezése az adminisztrációs konzolon (MMC)

1. A Kaspersky Security Center Administration Console fájában válassza ki a **Policies** lehetőséget.
2. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
3. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
4. A **Hibakeresési adatok** részen kattintson a **Beállítások** gombra.
5. A megnyíló ablakban a **Kiíratási és nyomkövetési fájlok védelmének engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le a fájlvédelmet.
6. Mentse el a módosításokat.

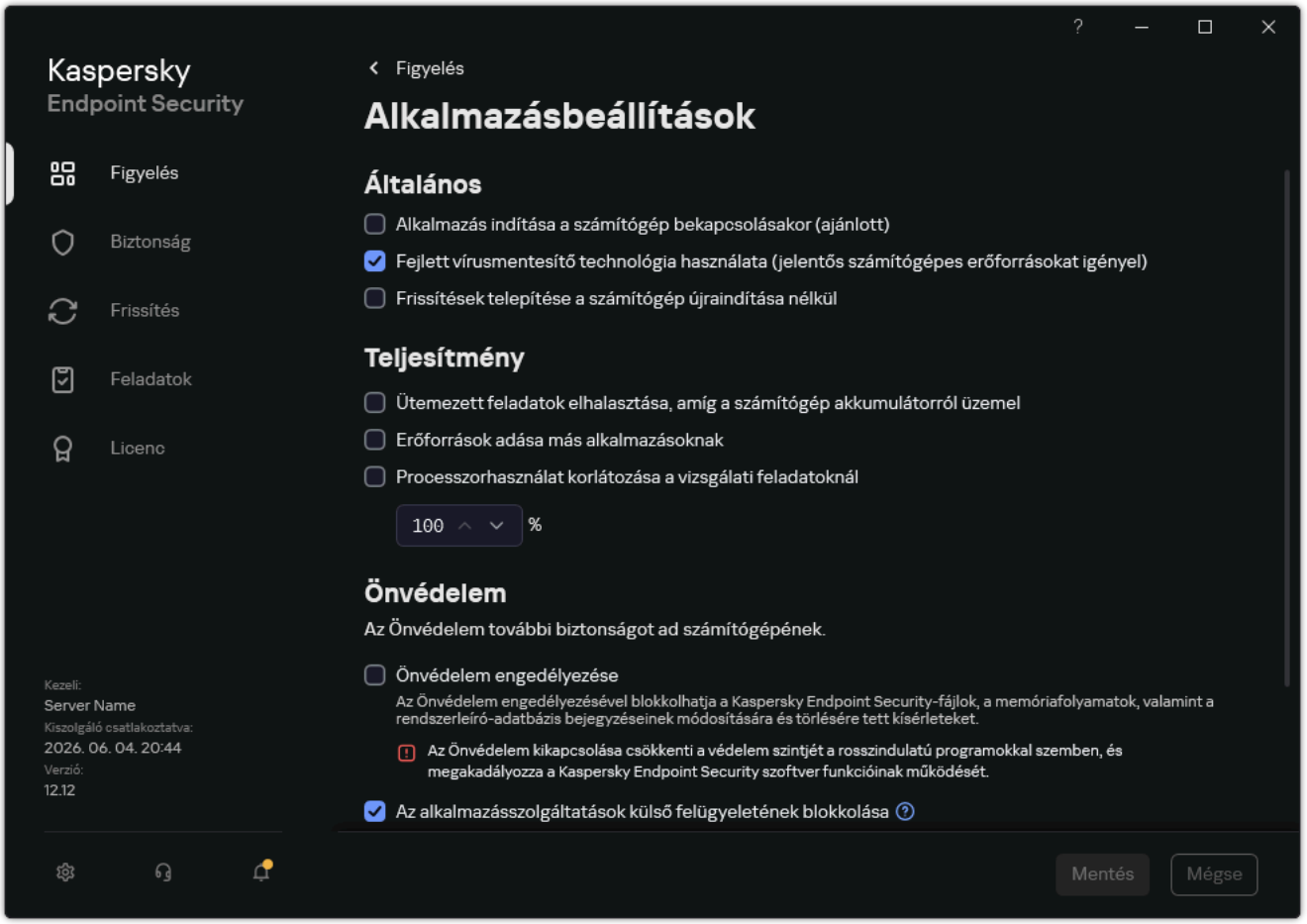
A memóriakiíratási fájlok és a nyomkövetési fájlok védelmének engedélyezése a Web Console-on és a Cloud Console-on

1. A Web Console fő ablakában válassza a **Asset management** → **Policies** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.

   Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** lapot.
4. Nyissa meg a **General Settings** → **Technical Support** elemet.
5. A(z) **Debug information** területen használja a(z) **Dump and trace files protection ENABLED** jelölőnégyzetet a fájlvédelem engedélyezéséhez vagy letiltásához.
6. Mentse el a módosításokat.

A memóriakiíratási fájlok és a nyomkövetési fájlok védelmének engedélyezése az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a ⚙ gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.



A Kaspersky Endpoint Security for Windows beállításai

3. A **Hibakeresési adatok** blokkban a **Kiíratási és nyomkövetési fájlok védelmének engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le a fájlvédelmet.
4. Mentse el a módosításokat.

A védelem bekapcsolt állapotában írt kiíratási és nyomkövetési fájlok védelme a funkció kikapcsolását követően is fennmarad.

Operációs rendszer adatainak lekérése (Kaspersky Get System Info)

A Kaspersky Endpoint Security alkalmazás telepítése után előfordulhat, hogy az operációs rendszer vagy egy alkalmazás nem működik megfelelően. Ütközés van az alkalmazás és a számítógép-összetevők szoftvere vagy illesztőprogramja között.

A probléma okának azonosításához a Kaspersky Teerméktámogatásnak egy jelentésre van szüksége a Kaspersky Get System Info segédprogramtól (a továbbiakban: GSI). A segédprogram használatával kapcsolatos további információkért lásd: Kaspersky Tudásbázis.

Korlátozások és figyelmeztetések

A Kaspersky Endpoint Security számos olyan korlátozást tartalmaz, amely az alkalmazás működése szempontjából nem létfontosságú.

Az alkalmazás telepítése

- A Microsoft Windows 10, Microsoft Windows Server 2016 és a Microsoft Windows Server 2019 operációs rendszerek támogatásának részleteiért lásd a Terméktámogatási tudásbázist.
- A Microsoft Windows 11 és a Microsoft Windows Server 2022 operációs rendszerek támogatásának részleteiért lásd a Terméktámogatási tudásbázist.
- Egy fertőzött számítógépre történő telepítést követően az alkalmazás nem tájékoztatja a felhasználót a számítógépes vizsgálat futtatásának szükségességéről. Problémákat tapasztalhat az alkalmazás aktiválásakor. A problémák megoldásához indítsa el a Kritikus területek vizsgálatát.
- Ha nem-ASCII karaktereket (például orosz betűket) használ a setup.ini és a setup.reg fájlokban, akkor azt javasoljuk, hogy a fájlt a notepad.exe fájl segítségével szerkessze, és a fájlt UTF-16LE kódolással mentse el. Más kódolás nem támogatott.
- Az alkalmazás nem támogatja nem-ASCII karakterek használatát az alkalmazás telepítési útvonalának megadásakor a telepítési csomag beállításaiban.
- Ha az alkalmazás beállításait CFG fájlból importálja, akkor a Kaspersky Security Networkben való részvételt meghatározó beállítás értéke nem lesz alkalmazva. A beállítások importálása után olvassa el a Kaspersky Security Network nyilatkozat szövegét, és erősítse meg beleegyezését a Kaspersky Security Networkben való részvételéhez. A Nyilatkozat szövegét elolvashatja az alkalmazás felületén vagy az alkalmazás terjesztőkészletét tartalmazó mappában található ksn_*.txt fájlban.
- Ha el szeretné távolítani, majd újratelepíteni a titkosítást (FLE vagy FDE) vagy az Eszközfelügyelő összetevőt, az újratelepítés előtt újra kell indítania a rendszert.
- A Microsoft Windows 10 operációs rendszer használatakor a Fájlszintű titkosítás (FLE) összetevő eltávolítása után újra kell indítania a rendszert.
- Amikor egyedi alkalmazás-összetevőket távolít el (például az *Alkalmazás-összetevők módosítása* feladattal), szükség lehet a számítógép újraindítására.
- Az *Alkalmazásösszetevők módosítása* feladat tulajdonságaiban, a telepítési módra váltásakor (**Külön mód** / **Kombinált mód**), az összetevőkészlet módok közötti szinkronizálása nem támogatott. Az alkalmazás a feladat tulajdonságainak újbóli megnyitása után szinkronizálja az összetevőkészletet a módok között.
- Az alkalmazás telepítése hibával zárulhat, amely szerint *Olyan alkalmazás van telepítve a számítógépen, amelynek neve hiányzik vagy nem olvasható*. Ez azt jelenti, hogy inkompatibilis alkalmazások vagy azok töredékei maradtak a számítógépen. Az inkompatibilis alkalmazások maradékainak eltávolításához küldjön a helyzet részletes leírását tartalmazó kérelmet a Kaspersky Lab Terméktámogatás részére a Kaspersky CompanyAccount használatával.
- Ha megszakította a Kaspersky Endpoint Security eltávolítását, a számítógép újraindítása után indítsa el az alkalmazás helyreállítását.

- Az alkalmazás megköveteli a Microsoft .NET Framework 4.0 vagy újabb használatát. A Microsoft .NET Framework 4.6.1 biztonsági réseket tartalmaz. Ha a Microsoft .NET Framework 4.6.1 verzióját használja, telepítenie kell a biztonsági frissítéseket. A Microsoft .NET Framework biztonsági frissítéseiről a Microsoft terméktámogatási webhelyén tájékozódhat.

- Ha az alkalmazás sikertelenül lett telepítve a kiszolgáló operációs rendszerében kiválasztott Kaspersky Endpoint Agent összetevővel, és megjelenik a *Windows Installer Coordinator Error* ablak, olvassa el a Microsoft támogatási webhelyén található utasításokat.

- Ha az alkalmazás helyben, nem interaktív módban lett telepítve, akkor a mellékelt setup.ini fájllal cserélje le a telepített összetevőket.

- Miután a Kaspersky Endpoint Security for Windows telepítve van, a Windows 7 egyes konfigurációiban a Windows Defender tovább működik. Javasoljuk, hogy manuálisan tiltsa le a Windows Defender alkalmazást, hogy megakadályozza a rendszer teljesítményének romlását.

- A Kaspersky Endpoint Security for Windows telepítésekor a Kaspersky Security for Windows Server (KSWS) és a Windows Defender alkalmazások telepítésével rendelkező kiszolgálón a rendszert újra kell indítani. A rendszer újraindítása akkor is szükséges, ha engedélyezte az alkalmazások rendszerújraindítás nélküli telepítését. A Windows Defender for Windows Server a Kaspersky Endpoint Security for Windows termékkel nem kompatibilis szoftverek listáján szerepel. Az alkalmazás telepítése előtt a telepítő eltávolítja a Windows Defender for Windows Server terméket. Az inkompatibilis szoftverek eltávolítása a rendszer újraindítását teszi szükségessé.

- A Kaspersky Endpoint Security for Windows (KES) telepítése előtt a Kaspersky Security for Windows Server (KSWS) telepítésével rendelkező kiszolgálón ki kell kapcsolni a KSWS jelszóvédelmét. A KSWS-ről a KES-re történő áttérés után engedélyezze a jelszóvédelmet az alkalmazás beállításaiban.

- Az alkalmazás Windows 7 vagy Windows Server 2008 R2 rendszert futtató olyan számítógépeken történő telepítéséhez, amelyeken a Veeam Backup & Replication szoftver telepítve van, előfordulhat, hogy újra kell indítania a számítógépet, és újra kell futtatnia a telepítést.

- A Kaspersky Small Office Security (KSOS) rendszerről a Kaspersky Endpoint Security (KES) rendszerre történő áttérés a Jelszóvédelem engedélyezésével a KSOS 21.16.*.*-os verziójától kezdve érhető el. A KSOS korábbi verzióinak áttelepítéséhez ki kell kapcsolnia a Jelszóvédelmet, vagy manuálisan el kell távolítania a KSOS-t. A KSOS rendszerről a KES rendszerre történő áttérés a Jelszóvédelem kikapcsolásával helyesen történik.

- A Kaspersky Endpoint Security nem telepíthető rendszerindításra alkalmas cserélhető meghajtón. A telepítés során a Kaspersky Endpoint Security egy hibaüzenetet jelenít meg: *Érvénytelen mappát vagy meghajtót választott ki. Az alkalmazást helyi merevlemezre kell telepíteni.* Ha külső eszközökkel sikerül cserélhető meghajtóra telepítenie az alkalmazást, ez az operációs rendszer összeomlását okozhatja a rendszerindítási folyamat során (kékképernyős összeomlás). Ez azt jelenti, hogy a Kaspersky Endpoint Security nem támogatja a Windows To Go és hasonló megoldásokat. A számítógép cserélhető meghajtóról történő vizsgálatához használhatja az ingyenesen használható Kaspersky Rescue Disk alkalmazást.

- A Kaspersky Endpoint Security hálózati összetevőinek telepítése többfelhasználós RDP-munkamenetekkel rendelkező terminálkiszolgálóra néhány speciális szempontot igényel. Az operációs rendszerek a rendszergazdai munkamenet vége után minden felhasználói munkamenetet leállítanak. A terminálkiszolgálóhoz való csatlakozáshoz újra kell indítania a kiszolgálót, vagy helyileg be kell jelentkeznie a rendszerbe. Az ilyen viselkedést a Windows operációs rendszer működésének sajátosságai határozzák meg.

- Ha a Kaspersky Endpoint Security for Windows (12.11.0.2004-es build) és a Kaspersky Endpoint Security for Linux (12.4.0.1354-es build) webes beépülő modulok telepítve vannak a Kaspersky Security Center 16.0-s vagy a Kaspersky Security Center 16.1-es verziójában, akkor a Kaspersky Endpoint Security for Windows webes bővítmény 12.11.0.6004-es verzióra való frissítése a Kaspersky Endpoint Security for Linux szabályzatok hibás működéséhez vezethet.

  Lehetséges megoldás: navigáljon a **Settings** → **Web plug-ins** ablakba, és távolítsa el a listából a Kaspersky Endpoint Security for Windows webes beépülő modult, a Kaspersky Endpoint Security for Linux webes beépülő modult és a Unified Protection and Management Plug-in beépülő modult. Ezután először telepítse a Kaspersky Endpoint Security for Linux webes beépülő modult, majd a Kaspersky Endpoint Security for Windows webes beépülő modult.

- A Web Console-on az összetevők listája hibásan jelenik meg a Kaspersky Endpoint Security 12.11 for Windows telepítőcsomag tulajdonságaiban. Az Anti-Cryptor különálló összetevőként nem érhető el az alkalmazás ezen verziójában. A megosztott mappák külső titkosítási funkciók elleni védelmét a Viselkedésészlelés összetevő tartalmazza. A Kaspersky Endpoint Security 12.12 for Windows verzióban ez a funkció különálló összetevő. Ugyanakkor az Adminisztrációs konzolon (MMC) az összetevők listája megfelelően jelenik meg.

Az alkalmazás frissítése

- A 11.0.0 alkalmazásverziótól kezdődően telepítheti a Kaspersky Endpoint Security for Windows MMC beépülő modult az előző beépülő modul verziójára. Egy korábbi bővítmény verzióhoz való visszatéréshez törölje az aktuális bővítményt, és telepítse a bővítmény egy korábbi verzióját.

- A Kaspersky Endpoint Security 11.0.0 vagy 11.0.1 for Windows frissítésekor az *Adatbázisok és alkalmazásmodulok frissítése*, a *Kritikus területek vizsgálata*, az *Egyéni vizsgálat* és az *Alkalmazásintegritás ellenőrzése* feladatok helyi feladatütemezési beállításai nem kerülnek mentésre.

- A Windows 10 1903 és 1909 verziójú operációs rendszert futtató számítógépeken a Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (10.3.3.275 számú build), Service Pack 2 Maintenance Release 4 (10.3.3.304 számú build), 11.0.0 és 11.0.1 a Fájlszintű titkosítás (FLE) összetevővel való telepítése hibával végződhet. Ez azért van, mert a fájlok titkosítását a Kaspersky Endpoint Security for Windows ezen verzióinál nem támogatják a Windows 10 1903 és 1909 verziói. A frissítés telepítése előtt javasoljuk, hogy távolítsa el a fájltitkosítás összetevőt.

- Az alkalmazás használatához szükség van a Microsoft .NET-keretrendszer 4.0 vagy újabb verziójára. A Microsoft .NET-keretrendszer 4.6.1 verziójában sebezhetőségek találhatók. Ha a Microsoft .NET-keretrendszer 4.6.1 verzióját használja, telepítenie kell a biztonsági frissítéseket. A Microsoft .NET-keretrendszer biztonsági frissítéseiről a Microsoft terméktámogatási webhelyén tájékozódhat.

- A Kaspersky Endpoint Security frissítésekor az alkalmazás letiltja a KSN használatát a Kaspersky Security Network nyilatkozat elfogadásáig. Ezenkívül a Kaspersky Security Centerben a számítógép állapota *Critical* állapotra módosítható; a *KSN kiszolgálói nem érhetők el* eseményt kapja. Ha a Kaspersky Managed Detection and Response szolgáltatást használja, eseményeket kap a megoldás használatakor történő szabálysértések esetén. A KSN használata szükséges a Kaspersky Managed Detection and Response működéséhez. A Kaspersky Endpoint Security engedélyezi a KSN használatát azon házirend alkalmazása után, amelyben a rendszergazda elfogadja a KSN használati feltételeit. A Kaspersky Security Network nyilatkozat elfogadása után a Kaspersky Endpoint Security folytatja működését.

- A Kaspersky Endpoint Security 11.10.0 vagy újabb verzióra történő, újraindítás nélküli frissítése után a számítógépen két Kaspersky Endpoint Security alkalmazás lesz telepítve. Ne távolítsa el manuálisan az alkalmazás előző verzióját. A számítógép újraindításakor az előző verzió automatikusan eltávolításra kerül.

- A Kaspersky Endpoint Security frissítése után a Microsoft Windows 11 rendszert futtató számítógépen a fájlok helyi menüjében megjelenhetnek az alkalmazás korábbi és új verzióinak elemei. Indítsa újra a számítógépet kétszer, hogy biztosítsa a fájlok helyi menüjének megfelelő működését.

- Ha az alkalmazás Önvédelem funkciója ki van kapcsolva, és az összes hálózati adapter leáll, akkor az alkalmazás hálózati összetevői nem fognak működni az alkalmazás frissítésének befejezése és a számítógép újraindítása között. Az alkalmazás hálózati összetevői közé tartozik a Web védelem, a Levelezés védelem, a Hálózati védelem, a Tűzfal, a Behatolásmegelőző rendszer és a Webfelügyelő. Indítsa újra a számítógépet, hogy az alkalmazás megfelelően működjön.

- A BadUSB védelem összetevő nem működik az alkalmazásfrissítés befejezése és a számítógép újraindítása között. Indítsa újra a számítógépet, hogy az alkalmazás megfelelően működjön.

- Az alkalmazás nem frissíthető, ha az előző frissítési folyamat nem fejeződött be. Indítsa újra a számítógépet, hogy az alkalmazás megfelelően működjön.

- Miután az alkalmazást a Kaspersky Endpoint Security 11 for Windows korábbi verziójáról frissítette, a számítógépet újra kell indítani.

- Ha a Kaspersky Endpoint Security szolgáltatást a Kaspersky Security Center Cloud Console segítségével kezeli, az alkalmazás helyi frissítése nem engedélyezett. Az alkalmazás helyi frissítése esetén nem lehet elfogadni a Kaspersky Security Center Cloud Console adatfeldolgozási szerződését.

ARM architektúra támogatása

- A Kaspersky Endpoint Security telepítése Light Agent üzemmódban Arm-alapú virtuális gépekre nem támogatott.

- A Kaspersky lemeztitkosítás az ARM-alapú számítógépeken nem támogatott.

- A fájltitkosítás nem támogatott az ARM-alapú számítógépeken.

- Az ARM-alapú számítógépek nem támogatják a cserélhető meghajtók titkosítását.

- A Windows 11 for Arm64 rendszert futtató számítógépeken az EDR Agent nem kompatibilis a következővel: Bitdefender Endpoint Security Tools.

- Az audiojel-védelmi funkció és a webkamera hozzáférés-védelmi funkciója nem támogatott az ARM-alapú számítógépeken.

- Az ARM-alapú számítógépeken a Levelezés védelem bővítmény az Outlook 2016, az Outlook 2021, az Outlook 2024 és az Outlook 365 for Arm64 32 bites és 64 bites verzióit támogatja.

- A Kaspersky Endpoint Security nem küld az ARM architektúrának szánt objektumokat a Kaspersky Sandbox számára.

- A nyomtatásvezérlés nem támogatott az ARM alapú számítógépeken.

- A Kaspersky Endpoint Detection and Response Expert (cloud) alkalmazás integrációja az ARM alapú számítógépeken nem támogatott.

- Az ARM alapú számítógépeken az *IOC Scan* feladat csak a következő levelezőprogramokból támogatja az e-mail-fájlokat: Outlook 2016 és Outlook 2021, 2024 és 365 for Arm64 32 és 64 bites verziói.

Kiszolgálói platformok támogatása

- Azokon a kiszolgálókon, amelyeken engedélyezve van az *adatdeduplikáció*, az fsdmhost.exe fájlt hozzá kell adnia a megbízható alkalmazások listájához. Ez segít optimalizálni az alkalmazás teljesítményét, és megakadályozza a CPU túlzott terhelését.

- A ReFS fájlrendszer korlátozottan támogatott:

  - A Kaspersky Endpoint Security helytelenül dolgozhatja fel a fenyegetések vírusmentesítési eseményeit. Például ha az alkalmazás törölt egy rosszindulatú fájlt, előfordulhat, hogy a jelentés tartalmaz egy „Az objektum nincs feldolgozva" bejegyzést. Ugyanakkor a Kaspersky Endpoint Security az alkalmazás beállításainak megfelelően vírusmentesíti a fenyegetéseket. A Kaspersky Endpoint Security egy másolatot is létrehozhat *Az objektum vírusmentesítése újraindításkor fog megtörténni* eseményről ugyanazon objektum esetében.

  - A Fájl védelem kihagyhat egyes fenyegetéseket. Ugyanakkor a Kártevő vizsgálata megfelelően működik.

  - A *Kártevő vizsgálata* feladat megkezdése után az iCheckerrel hozzáadott kizárások alaphelyzetbe kerülnek a kiszolgáló újraindításakor.

  - Az iSwift technológia nem támogatott. A Kaspersky Endpoint Security nem veszi figyelembe az iSwift technológia használatával hozzáadott vizsgálati kizárásokat.

  - A Kaspersky Endpoint Security nem észleli az eicar.com és a susp-eicar.com fájlokat, ha a meicar.exe fájl már létezett a számítógépen a Kaspersky Endpoint Security telepítése előtt.

  - Előfordulhat, hogy a Kaspersky Endpoint Security helytelenül jeleníti meg a fenyegetések vírusmentesítési értesítéseit. Például az alkalmazás megjeleníthet egy fenyegetésről szóló értesítést egy korábban vírusmentesített fenyegetésről.

- A Fájl szintű titkosítás (FLE) és a Kaspersky lemeztitkosítás (FDE) technológiái nincsenek támogatva a kiszolgálófelületeken. Ugyanakkor a Kaspersky Endpoint Security helytelenül dolgozhatja fel az adatok titkosítási eseményeit.

- A szerver operációs rendszerekben nem jelenik meg figyelmeztetés a fejlett vírusmentesítés szükségességéről.

- A Microsoft Windows Server 2008 ki van zárva a támogatásból. Az alkalmazást nem lehet Microsoft Windows Server 2008 operációs rendszert futtató számítógépre telepíteni.

- Az olyan kiszolgálóra telepített Kaspersky Endpoint Security, amelyen a Microsoft Data Protection Manager (DPM) telepítve van, a DPM hibás működését okozhatja. Ez a DPM működésének korlátaival függ össze. A hibás működés elhárításához adja hozzá a helyi kiszolgálómeghajtókat a Fájlvédelem összetevő és a *Kártevő vizsgálata* feladatok kizárásaihoz.

- A Server Core mode korlátozásokkal támogatott:

  - A helyi grafikus felhasználói felület nem érhető el, beleértve az értesítéseket, a felugró értesítéseket és az egyéb felületvezérlőket. Az alkalmazás nem tud üzenetablakokat megjeleníteni, beleértve a következő ablakokat:

    - Alkalmazásverzió és modulfrissítés megerősítését kérő üzenet;

    - A számítógép újraindítását kérő üzenet;

- Proxykiszolgáló hitelesítési adatait kérő üzenet;
- Rákérdezés az eszközökhöz való hozzáférésre (Eszközfelügyelő).

- A következő összetevők nem érhetők el: Web védelem, Levelezés védelem, Webfelügyelő, BadUSB védelem.
- Az Anti-Bridging nem érhető el.
- A Kaspersky Security Center konzol alkalmazási szabályzatában csak a Kaspersky Security Network nyilatkozatot fogadhatja el.
- A BitLocker meghajtótitkosítás csak a Trusted Platform Module (TPM) használatakor érhető el. PIN-kód/jelszó nem használható titkosításhoz, mert az alkalmazás nem tudja megjeleníteni a jelszót kérő ablakot az indítás előtti hitelesítéshez. Ha az operációs rendszerben engedélyezve van a Federal Information Processing szabványú kompatibilitási mód, a meghajtó titkosításának megkezdése előtt csatlakoztasson egy cserélhető meghajtót a titkosítási kulcs mentéséhez.

Támogatás virtuális platformokhoz

- A Hyper-V virtuális gépeken a Teljes lemeztitkosítás (FDE) nem támogatott.
- A Citrix virtuális platformokon a Teljes lemeztitkosítás (FDE) nem támogatott.
- A Windows 10 Enterprise többmunkamenetes támogatása korlátozott:
  - A Kaspersky Endpoint Security a felhasználó értesítése nélkül vírusmentesíti az aktív fenyegetéseket, ahogy a kiszolgálón lévő aktív fenyegetések vírusmentesítése esetében is teszi. Mivel az operációs rendszer továbbra is többmunkamenetes módban fut, más felhasználók elveszíthetik az adataikat, ha a fenyegetést nem sikerül azonnal megoldani.
  - A teljes lemeztitkosítás (FDE) nem támogatott.
  - A BitLocker felügyelete nem támogatott.
  - A Kaspersky Endpoint Security cserélhető meghajtókkal történő használata nem támogatott. A Microsoft Azure infrastruktúra a cserélhető meghajtókat hálózati meghajtókként definiálja.
- A Fájl szintű titkosítás (FLE) telepítése és használata a Citrix virtuális platformokon nem támogatott.
- A Kaspersky Endpoint Security for Windows és a Citrix PVS kompatibilitásának támogatásához hajtsa végre a telepítést az engedélyezett **A Citrix PVS megoldással való kompatibilitás biztosítása** opcióval. Ez az opció engedélyezhető a Telepítővarázslóban vagy a `/pCITRIXCOMPATIBILITY=1` parancssori paraméter használatával. Távoli telepítés esetén a KUD fájlt a következő paraméter hozzáadásával kell szerkeszteni: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. A klónozás megkezdése előtt ki kell kapcsolni az Önvédelmet a vDisket használó virtuális gépek klónozásához.
- Egy sablongépnek a Citrix XenDesktop mesterképhez előre telepített Kaspersky Endpoint Security for Windows és Kaspersky Security Center Network Hálózati ügynök alkalmazásokkal való előkészítésekor adja hozzá a következő kizárástípusokat a konfigurációs fájlhoz:

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
```

```
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

A Citrix XenDesktoppal kapcsolatos részletekért látogasson el a Citrix támogatás webhelyére.

- Bizonyos esetekben a cserélhető meghajtó biztonságos leválasztására tett kísérlet sikertelen lehet egy virtuális gépen, amely VMware ESXi hypervisorra lett telepítve. Próbálja meg ismét biztonságosan leválasztani az eszközt.

- A Kaspersky Endpoint Security az alábbi korlátozásokkal kompatibilis a VMware ESXi hipervizorral:

  - Előfordulhat, hogy a Kaspersky Endpoint Security nem kompatibilis a Guest Introspection illesztőprogramokkal (vnetWFP.sys, vnetFLT.sys és továbbiak). Az inkompatibilitás elhárításához frissítse az illesztőprogramokat a legújabb verzióra, vagy távolítsa el az illesztőprogramokat.

  - Egyes esetekben a virtuális gépen lévő cserélhető lemezek biztonságos eltávolítására tett kísérlet sikertelen lehet. Próbálja meg ismét biztonságosan leválasztani az eszközt.

- A Kaspersky Endpoint Security telepítése virtuális gépekre a Citrix VDA ügynökkel kompatibilitási hibával zárulhat. Ennek az az oka, hogy a Citrix Provisioning Services korlátozottan kompatibilis a víruskereső megoldásokkal. A Citrix Provisioning Services szolgáltatásokkal való vírusirtói megoldások használatának bevált gyakorlatairól a Citrix támogatási webhelyén találhat információkat.

- A Kaspersky Endpoint Security kihagyja a cserélhető meghajtók vizsgálatát, ha a meghajtó egy virtuális géphez csatlakozik a Citrix Hipervizoron (a *Cserélhető meghajtók vizsgálata* feladat). Az ilyen eszközökön az operációs rendszer hálózati meghajtóként észleli a csatlakoztatott cserélhető meghajtót. Ilyen esetekben használhatja az *Egyéni vizsgálat* feladatot. Az alkalmazás viselkedése normál és Light Agent üzemmódban ugyanaz.

- Ha a Kaspersky Endpoint Security egy olyan infrastruktúrában található virtuális gépre van telepítve, amely a Citrix App Layering technológiát használja, akkor az alkalmazás által fertőzöttként azonosított fájlok – amelyek állapota *Az objektum újraindításkor törlésre kerül* – nem kerülnek automatikusan eltávolításra a virtuális gép újraindításakor.

  Az ilyen fájlok törléséhez csatlakoztatnia kell a felhasználói réteget tartalmazó VHDX-fájlt a Citrix App Layering rendszergazdai számítógépén, majd futtatnia kell egy kártevő-ellenőrzést a csatlakoztatott lemezen.

Kompatibilitás a Kaspersky Security Centerrel

- A Kaspersky Security Center Web Console 14.1-es és korábbi verzióiban a Napló vizsgálata és a Fájlintegritás-figyelő összetevők funkcionális területeinek nevei nem jelennek meg megfelelően a Felügyeleti kiszolgáló tulajdonságainak felhasználói hozzáférési engedélyek beállítási szakaszában.

- Az alkalmazás javítását követően a számítógép és a Felügyeleti kiszolgáló kapcsolatának védelme le van tiltva. Az alkalmazás javítása után futtassa újra a *Felügyeleti kiszolgálói kapcsolatvédelem* feladatot.

- A Kaspersky Security Center Administration Console-on a **Felhasználó vagy felhasználók csoportjának kiválasztása** ablakban a Kaspersky Security Center felhasználói listájából csak az első 50 000 felhasználó jelenik meg. További részletekért lásd a Kaspersky Security Center súgóját.

- Amikor felügyelt eszközöket keres a Kaspersky Security Center Administration Console-on, az **Application components** lap egyszerre több változatot is megjeleníthet ugyanazon alkalmazás-összetevők nevével, beleértve a Kaspersky Endpoint Security régebbi verzióinak megfelelő neveket is. Egyes összetevők neve többször is előfordulhat.

  Az összetevők szerinti kereséshez egyszerűen ki kell választania egyet a megjelenített változatok közül. Az eszközök felismerésével kapcsolatos további részletekért olvassa el a Kaspersky Security Center súgóját.

Licencelés

- Ha megjelenik a *Hiba az adatok fogadásakor* rendszerüzenet, ellenőrizze, hogy az a számítógép, amelyen aktiválja, hálózati hozzáféréssel rendelkezik, vagy konfigurálja az aktiválási beállításokat a Kaspersky Security Center aktiválási proxyján keresztül.

- Az alkalmazás felületén a licenc lejárati dátuma a számítógép helyi idejében van megjelenítve.

- Az alkalmazás beágyazott kulcsfájlokkal instabil internet-hozzáféréssel rendelkező számítógépre történő telepítése olyan események ideiglenes megjelenítését eredményezheti, amelyek szerint az alkalmazás nincs aktiválva, vagy a licenc nem teszi lehetővé az összetevő működését. Ennek az az oka, hogy a telepítési folyamat során az alkalmazás először aktiválja a beágyazott próbalicencet. Ehhez internet-hozzáférésre van szükség.

- A próbaidőszak alatt bármilyen alkalmazásfrissítés vagy javítás instabil internet-hozzáféréssel rendelkező számítógépre történő telepítése olyan események ideiglenes megjelenítését eredményezheti, amelyek szerint az alkalmazás nincs aktiválva. Ennek az az oka, hogy a frissítési folyamat során az alkalmazás először aktiválja a beágyazott próbalicencet. Ehhez internet-hozzáférésre van szükség.

- Ha a próbalicenc automatikusan aktiválódott az alkalmazás telepítése során, majd az alkalmazást a licencinformációk mentése nélkül eltávolították, akkor az alkalmazás az újratelepítéskor nem aktiválódik automatikusan a próbalicenccel. Ebben az esetben manuálisan aktiválja az alkalmazást.

- Ha a Kaspersky Security Center 11-es verzióját és a Kaspersky Endpoint Security 14.1-es verzióját használja, az összetevők teljesítményjelentései helytelenül működhetnek. Ha olyan Kaspersky Endpoint Security-összetevőt telepít, amire a licenc nem terjed ki, a Hálózati Ügynök összetevő-állapothibát küldhet a Windows eseménynaplóba. A hibák elkerülése érdekében távolítsa el azokat az összetevőket, amikre a licenc nem terjed ki.

Levelezés védelem

- A levelek Microsoft Outlook levelezés védelem kiterjesztéssel történő vizsgálatakor javasoljuk, hogy használja a gyorsítótárazott Exchange módot (Gyorsítótárazott Exchange mód használata lehetőség).

- A Kaspersky Endpoint Security nem támogatja a Microsoft Outlook levelezőprogram 64 bites verzióját. Ez azt jelenti, hogy a Kaspersky Endpoint Security nem vizsgálja át a Microsoft Outlook-fájlokat (PST- és OST-fájlokat), ha a számítógépre a Microsoft Outlook 64 bites verziója van telepítve, még akkor sem, ha az e-mailek szerepelnek a vizsgálat hatókörében.

- A Kaspersky Endpoint Security nem támogatja a Microsoft Outlook New levelezőprogramot.

Kármentesítő motor

- Az alkalmazás csak olyan eszközökön állít vissza fájlokat, amiken NTFS vagy FAT32 fájlrendszer van.

- Az alkalmazás legfeljebb 100 MB méretű fájlokat állít vissza.

- Az alkalmazás a következő kiterjesztésű fájlokat állítja vissza: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.

- Nem lehet hálózati meghajtókon vagy újraírható CD/DVD lemezeken lévő fájlokat visszaállítani.

- Nem lehet olyan fájlokat visszaállítani, amik a Titkosító fájlrendszerrel (EFS) lettek titkosítva. Az EFS működésének részleteiért lásd a Microsoft weboldalt.

- Az alkalmazás nem figyel meg olyan fájlmódosításokat, amiket operációs rendszer kernel szintű folyamatok hajtottak végre.

Tűzfal

- Ha egy hálózati csomagszabály vagy alkalmazás hálózati szabálya DNS-neveket ad meg, a Kaspersky Endpoint Security kéréseket küldhet a DNS-kiszolgálónak ezen erőforrások IP-címének meghatározása céljából. A Tűzfal IP-címek segítségével figyeli a hálózati tevékenységet. Ezért az alkalmazás a DNS-neveket IP-címekké oldja fel. Javasoljuk, hogy a szabályokban csak a helyi hálózaton belüli számítógépek vagy belső szolgáltatások esetében használjon DNS-neveket.

- Az összes IPv6-címre vonatkozó szabály megadásához adja hozzá a ::-ffffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff címtartományt. A Tűzfal nem támogatja a ::/0 maszkot.

- A csomagok vagy kapcsolatok szűrése helyi cím, fizikai felület és a csomag élettartama (TTL) szerint a következő esetekben támogatott:

  - A kimenő csomagok vagy kapcsolatok helyi címe alapján a TCP és az UDP alkalmazási szabályaiban, valamint a csomagszabályokban.

  - A bejövő csomagok vagy kapcsolatok (az UDP kivételével) helyi címe szerint a blokkolási alkalmazás- és csomagszabályokban.

  - A bejövő vagy kimenő csomagok blokkcsomagszabályaiban a csomag élettartam (TTL) szerint.

  - Hálózati felületen keresztül bejövő és kimenő csomagokhoz, vagy a csomagszabályokban lévő kapcsolatokhoz.

- Ha egy hálózati adapter vagy csomag élettartamát konfigurálta egy engedélyezési csomagszabálynál, akkor ennek a szabálynak a prioritása alacsonyabb a blokkolási alkalmazásszabálynál. Más szavakkal, ha egy alkalmazás hálózati tevékenysége blokkolva van (például az alkalmazás a *Magas korlátozás* megbízhatósági csoportba tartozik), akkor nem engedélyezheti az alkalmazás hálózati tevékenységét egy ilyen beállításokkal rendelkező csomagszabály használatával. Minden más esetben a csomagszabály magasabb prioritású az alkalmazás hálózati szabályánál.

- A Tűzfal csomagszabályainak importálásakor a Kaspersky Endpoint Security módosíthatja a szabályneveket. Az alkalmazás azonos általános paraméterkészleteket határoz meg a szabályokhoz kapcsolódóan: protokoll, irány, távoli és helyi portok, csomag élettartama (TTL). Ha ez az általános paraméterkészlet több szabály esetén megegyezik, az alkalmazás ugyanazt a nevet rendeli hozzá ezekhez a szabályokhoz, vagy egy paramétercímkét fűz hozzá a névhez. Ez azt jelenti, hogy a Kaspersky Endpoint Security minden csomagszabályt importál, de az azonos általános paraméterkészlettel rendelkező szabályok neve megváltozhat.

- Ha egy hálózati szabályban engedélyezte az alkalmazás-események jelentését, az alkalmazás másik megbízhatósági csoportba történő áthelyezésekor az adott megbízhatósági csoport korlátozásai nem érvényesülnek. Így ha az alkalmazás a Megbízható megbízhatósági csoportban van, akkor nem vonatkoznak rá hálózati korlátozások. Ezzel engedélyezte az ezen alkalmazáshoz tartozó események jelentését, és áthelyezte azt a *Nem megbízható* megbízhatósági csoportba. A Tűzfal nem fog hálózati korlátozásokat érvényesíteni ennél az alkalmazásnál. Javasoljuk, hogy először helyezze át az alkalmazást a megfelelő megbízhatósági csoportba, majd engedélyezze az eseményjelentést. Ha ez a módszer nem megfelelő, manuálisan is konfigurálhatja az alkalmazás korlátozásait a hálózati szabály beállításaiban. A korlátozás csak az alkalmazás helyi felületére vonatkozik. Az alkalmazás megbízhatósági csoportok közötti áthelyezése a házirend szerint megfelelően működik.

- A Tűzfal és a Behatolásmegelőző rendszer összetevői közös beállításokkal rendelkeznek: alkalmazásjogok és védett erőforrások. Ha módosítja a Tűzfal beállításait, a Kaspersky Endpoint Security automatikusan alkalmazza az új beállításokat a Behatolásmegelőző rendszerben. Ha például engedélyezte a Tűzfal házirend általános beállításainak módosítását (a lakat nyitva van), akkor a Behatolásmegelőző rendszer beállításai is szerkeszthetővé válnak.

- Ha a Kaspersky Endpoint Security 11.6.0 vagy korábbi verziójában egy hálózati csomagszabály aktiválódik, a Tűzfal jelentés **Alkalmazásnév** oszlopában mindig a *Kaspersky Endpoint Security* értéke jelenik meg. Ezenkívül a Tűzfal minden alkalmazás esetében csomagszinten blokkolja a kapcsolatot. Ez a viselkedés megváltozott a Kaspersky Endpoint Security 11.7.0 vagy újabb verziója esetében. A Tűzfal jelentés kiegészült a **Szabály típusa** oszloppal. Hálózati csomagszabály indításakor az **Alkalmazásnév** oszlop értéke üres marad.

- Ha a Tűzfal használatával letiltott minden hálózati tevékenységet, a Hálózati védelem összetevő portvizsgálat típusú támadást észlelhet. Ez azért fordulhat elő, mert az alkalmazás a Tűzfal előtt indítja el a Hálózati védelmet, hogy észlelje a gyanús tevékenységet a hálózaton.

BadUSB védelem

- A Kaspersky Endpoint Security alaphelyzetbe állítja az USB-eszköz zárolásának időkorlátját, amikor a számítógép zárolva van (például a képernyőzár időkorlátja letelt). Vagyis, ha többször rossz engedélyezési kódot ad meg az USB-eszközhöz, és az alkalmazás zárolja az USB-eszközt, a Kaspersky Endpoint Security lehetővé teszi a hitelesítési kísérlet megismétlését a számítógép feloldása után. Ebben az esetben a Kaspersky Endpoint Security nem zárolja az USB-eszközt a BadUSB védelem összetevő beállításaiban meghatározott ideig.

- A Kaspersky Endpoint Security alaphelyzetbe állítja az USB-eszköz zárolásának időkorlátját, amikor a számítógép védelme szünetel. Vagyis, ha többször rossz engedélyezési kódot ad meg az USB-eszközhöz, és az alkalmazás zárolja az USB-eszközt, a Kaspersky Endpoint Security lehetővé teszi a hitelesítési kísérlet megismétlését a számítógép védelmének folytatása után. Ebben az esetben a Kaspersky Endpoint Security nem zárolja az USB-eszközt a BadUSB védelem összetevő beállításaiban meghatározott ideig.

Kaspersky Security Network

- A Kaspersky Endpoint Security nem támogatja a HTTPS-t a KSN Proxy-hoz való csatlakozáskor (**Use HTTPS** jelölőnégyzet bejelölve a KSN Proxy csatlakozási beállításaiban), ha a kiszolgáló címe nem latin betűket (nem ASCII szimbólumokat) tartalmaz.

- A Kaspersky Security Center alkalmazásban, amikor a globális Kaspersky Security Network használatáról a privát Kaspersky Security Network (KPSN) használatára, vagy fordítva vált, az adott termék házirendjében le van tiltva a Kaspersky Security Networkben való részvétel lehetősége. A váltás után olvassa el a Kaspersky Security Network nyilatkozat szövegét, és erősítse meg beleegyezését a KSN-ben való részvételhez. A Nyilatkozat szövegét az alkalmazás felületén vagy a termék házirendjének szerkesztésekor olvashatja el.

- A Kaspersky Endpoint Security 12.9 for Windows verziótól kezdve, amikor a KPSN-ről a globális KSN-re vált, újra meg kell erősítenie a Kaspersky Security Network nyilatkozat elfogadását. Ehhez engedélyeznie kell a Kaspersky Security Network használatát a házirend tulajdonságaiban vagy az alkalmazás felületén, és meg kell erősítenie a Kaspersky Security Network nyilatkozat elfogadását. Ha már használta a globális KSN-t, először le kell tiltania a KSN-használatot, majd újra engedélyeznie kell azt, és meg kell erősítenie a Kaspersky Security Network nyilatkozat elfogadását. Ha nem ért egyet a Kaspersky Security Network nyilatkozattal, az alkalmazás nem lesz képes hozzáférni a Kaspersky Security Network adataihoz.

- A Kaspersky Endpoint Security nem küld szöveges fájlokat (például TXT, CSV, LOG és DOCX fájlokat makrók nélkül) a Kaspersky Security Network részére vizsgálat céljából. Az alkalmazás vizsgálat céljából olyan fájlokat küld el, amelyek fenyegetést jelenthetnek a KSN számára. Ezek a fájlok tartalmazhatnak futtatható fájlokat vagy olyan fájlokat, amelyek futtatható kódot tartalmazhatnak (például makrókat a DOCX-fájlokban). Az alkalmazás más összetevői a szöveges fájlok vizsgálatáért felelősek. Manuálisan is ellenőrizheti a szöveges fájlok megbízhatóságát a fájl helyi menüjéből. Ha egy szöveges fájlnak *Nem megbízható (Kaspersky Security Network)* megbízhatósági állapota van, az alkalmazás figyelmen kívül hagyja az észlelt fenyegetésekre meghatározott műveletet.

Alkalmazásfelügyelő

- Az alkalmazásfelügyeleti szabályok használatakor nem ajánlott összesen 100 000-nél több bevonási és kizárási feltételt megadni a különböző kategóriájú alkalmazásokhoz, feltéve, hogy a Kaspersky Endpoint Security olyan számítógépen fut, amely megfelel a minimális hardverkövetelményeknek és Microsoft Windows 10 rendszeren működik.

- Csak a ZIP formátumú archívumok támogatottak, ha az Alkalmazásfelügyelő szabályaival dolgozik a Kaspersky Security Center Web Console-on. Más formátumú archívumok, például RAR vagy 7z, nem támogatottak. Nincs ilyen korlátozás, ha az adminisztrációs konzolon (MMC) dolgozik az Alkalmazásfelügyelő szabályaival.

- A Kaspersky Security Center Web Console alkalmazásfelügyeleti szabályaival való munka során a feltöltött fájl maximálisan támogatott mérete 104 MB. Nincs ilyen korlátozás, ha az adminisztrációs konzolon (MMC) dolgozik az Alkalmazásfelügyelő szabályaival.

- Ha a Microsoft Windows 10 alkalmazás tiltólista módban dolgozik, akkor a blokkolási szabályok hibás alkalmazása fordulhat elő, ami a szabályokban nem meghatározott alkalmazások blokkolását okozhatja.

- Ha új *előre meghatározott alkalmazásfelügyeleti szabályokat* ad hozzá a Kaspersky Endpoint Security frissítésekor, ezeket a szabályokat nem alkalmazhatja az alkalmazás korábbi verzióira.

- Amikor a progresszív webalkalmazásokat (PWA) blokkolja az Alkalmazásfelügyelő összetevő, akkor az appManifest.xml jelenik meg blokkolt alkalmazásként a jelentésben.

- A szabványos Jegyzettömb alkalmazás Windows 11-es alkalmazásvezérlési szabályhoz való hozzáadásakor nem ajánlott megadni az alkalmazás elérési útvonalát. A Windows 11 rendszert futtató számítógépeken az operációs rendszer a `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` mappában található Metro stílusú Notepadot használja. Az operációs rendszer korábbi verzióiban a Jegyzettömb a következő mappákban található:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Amikor a Jegyzettömböt hozzáadja egy alkalmazásfelügyeleti szabályhoz, megadhatja például az alkalmazás nevét és a fájl kivonatát a futó alkalmazás tulajdonságaiból.

- A KSWS házirend KES házirend-profilba történő áttelepítésekor a Házirendek és feladatok kötegelt konverziós varázsló (áttelepítési varázsló) átnevezi az alkalmazáskategóriákat, ha a kategóriák nevei tiltott karaktereket tartalmaznak: `'` `*` `<` `>` `?` `\` `:` `|`. Az áttelepítési varázsló ezeket a karaktereket `_` karakterekkel helyettesíti. Például a `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` alkalmazáskategóriát átnevezzük `KSWS_Everyone_[C61F-3B7C-4D89-96A1]` kategóriára.

Eszközfelügyelő

- A Kaspersky Endpoint Security képes naplózni a külső eszköz csatlakoztatási és leválasztási eseményeit. A Windows-szolgáltatások a rendszerfelhasználói fiókot használják az eszközök csatlakoztatására és leválasztására. Ez lehetetlenné teszi annak megállapítását, hogy melyik felhasználó csatlakoztatja vagy választja le az eszközt. A Kaspersky Endpoint Security az eseménynél megadja a rendszerfelhasználói fiókot.

- A megbízható listához hozzáadott nyomtatóeszközökhöz való hozzáférést az eszköz- és buszblokkolási szabályok blokkolják.

- MTP-eszközök esetén az Olvasás, Írás és Kapcsolódás műveletek vezérlése támogatott, ha az operációs rendszer beépített Microsoft illesztőprogramjait használja. Ha a felhasználó egyedi illesztőprogramot telepít egy eszközhöz (például az iTunes vagy az Android Debug Bridge részeként), akkor lehetséges, hogy az Olvasás és Írás műveletek ellenőrzése nem fog működni.

- MTP-eszközöknél az eszköz újbóli csatlakoztatása után megváltoznak a hozzáférési szabályok.

- Az Eszközfelügyelő összetevő regisztrálja a felügyelt eszközökkel kapcsolatos eseményeket, például egy eszköz csatlakoztatását és leválasztását, fájlolvasást eszközről, fájlírást eszközre és más eseményeket. A Kaspersky Endpoint Security csak a következő eszköztípusoknál regisztrálja a leválasztási eseményeket: Hordozható eszközök (MTP), Cserélhető meghajtók, Hajlékonylemezes meghajtók, CD/DVD-meghajtók. Más eszköztípusok esetén az alkalmazás nem regisztrálja a leválasztási eseményeket. Az alkalmazás minden eszköztípusnál regisztrálja az eszköz számítógéphez való csatlakoztatásának műveletét.

- Ha modellmaszk alapján ad hozzá eszközt a megbízható listához és olyan karaktereket használ, amelyek szerepelnek az azonosítóban, de nem szerepelnek a modell nevében, akkor ezek az eszközök nem lesznek hozzáadva. Egy munkaállomáson ezek az eszközök azonosító maszk alapján lesznek hozzáadva a megbízható listához.

- Ha az alkalmazást a számítógép újraindítása nélkül frissíti, az Eszközfelügyelő nem alkalmaz hozzáférési szabályokat az újracsatlakoztatott eszközökre. Ha azonban az eszközt a frissítés előtt csatlakoztatta, az Eszközfelügyelő megfelelően alkalmazza a szabályokat. Indítsa újra a számítógépet, hogy az alkalmazás megfelelően működjön az újracsatlakoztatott eszközökkel.

- A Kaspersky Endpoint Security 12.0-s verzióját telepített számítógépeken a **Hálózati nyomtatók** eszköztípushoz a nyomtatóhoz való hozzáférés **engedélyezése és nem naplózása** üzemmód a **kapcsolati busztól függ**, ha a számítógépen a Kaspersky Endpoint Security 12.1-es verziójú házirendje van érvényben. Ezekben az üzemmódokban az alkalmazás ugyanazokat a műveleteket hajtja végre. A Kaspersky Endpoint Security 12.1-es verziójában a hálózati nyomtatók hozzáférési módjának helyes neve **Engedélyezés és nem naplózás**.

- A Kaspersky Endpoint Security 12.0 for Windows verziótól kezdve az alkalmazás lehetővé teszi a nyomtatók nyomtatási szabályainak konfigurálását (nyomtatásvezérlés). Miután telepítette az alkalmazást nyomtatásvezérléssel, vagy frissítette az alkalmazást egy nyomtatásvezérléssel rendelkező verzióra, újra kell indítania a számítógépet. A számítógép újraindításáig a Kaspersky Endpoint Security nem alkalmaz nyomtatási szabályokat, és csak a nyomtatókhoz való hozzáférést tudja szabályozni. Ha a számítógép újraindítása hátrányosan befolyásolja a munkafolyamatokat a vállalatnál, akkor csak a spoolsv szolgáltatást (nyomtatási sorkezelő) indíthatja újra. A nyomtatásvezérlés nem támogatott az ARM alapú számítógépeken.

- A Kaspersky Endpoint Security for Windows 12.0 verziójától kezdve az alkalmazás támogatja a WPA3 protokollt a **Wi-Fi** típusú eszközök esetében. Ha a Kaspersky Endpoint Security 12.2 verziójú házirendjét alkalmazza egy számítógépen, a Kaspersky Endpoint Security 11.11.0 és korábbi verziójú számítógépeken a WPA2 protokoll van kiválasztva; a 12.0–12.1 verziók esetében a WPA2 / WPA3; a 12.2 és újabb verziók esetében a WPA3.

- Az Apple-eszközök hordozható eszközöknek (MTP) és iTunes-eszközöknek minősülnek. Az operációs rendszer tévesen azonosíthatja az Apple-eszköz kapcsolatát, és nem azonosíthatja az Apple-eszközt hordozható eszközként (MTP). Ezért az Apple-eszköz nem lesz elérhető a fájlkezelőben, de elérhető az iTunes alkalmazásban. Ennek eredményeképpen a Kaspersky Endpoint Security csak az iTunes alkalmazásban ellenőrzi az Apple-eszközhöz való hozzáférést. Az Apple-eszköz hordozható eszközként (MTP) történő eléréséhez nyissa meg az Eszközkezelőt, és távolítsa el az Apple-mobileszköz USB-illesztőprogramját az USB-vezérlők listájából. A számítógép újraindítása után az operációs rendszer hordozható eszközként (MTP) és iTunes-eszközként azonosítja az Apple-eszközt. A Kaspersky Endpoint Security az iTunes alkalmazásban és a fájlkezelőben is ellenőrzi az eszközhöz való hozzáférést.

- A Kaspersky Endpoint Security 12.3 for Windows esetében a hozzáférési beállítások eltérőek a **Bluetooth** eszköztípusnál. Ha **A csatlakozási busztól függ** értéket adta meg az alkalmazás előző verziójában, az alkalmazás 12.3 verzióra történő frissítése után a konfigurált érték a következőre változik: **Engedélyezés és nem naplózás**. Ez nem változtatja meg az eszköz viselkedését.

- Az Eszközfelügyelő csak a Microsoft Windows Bluetooth-implementáción keresztül támogatja a Bluetooth-eszközöket. Előfordulhat, hogy az Eszközfelügyelő helytelenül működik harmadik féltől származó Bluetooth-implementációkkal.

- Ha a Bluetooth-eszköz elrejti vagy meghamisítja az eszközosztályát (COD), előfordulhat, hogy az Eszközfelügyelő helytelenül fog működni.

- Bizonyos Realtek Bluetooth-illesztőprogramokkal rendelkező Windows 7 vagy Windows 8 rendszerű számítógépeken előfordulhat, hogy a Bluetooth-eszközök csak bemeneti eszközként (HID-osztály) történő csatlakoztatását nem lehet engedélyezni. Ez azt jelenti, hogy ha az alkalmazásbeállításokban megtiltja a Bluetooth-eszközökhöz való hozzáférést, és a bemeneti eszközöket a kizárásokhoz adja, az Eszközfelügyelő ehelyett megakadályozhatja az összes Bluetooth-eszközhöz való hozzáférést.

Webfelügyelő

- Az OGV és WEBM formátumok nem támogatottak.

- Az RTMP protokoll nem támogatott.

- A Webfelügyelő csak a WSL1 szabványt támogatja. Az alkalmazás nem ellenőrzi a WSL2 forgalmat.

Adaptív Anomáliafelügyelő

- Javasoljuk, hogy az esemény alapján automatikusan hozzon létre kizárásokat. Kizárás manuális hozzáadásakor adja hozzá a `*` karaktert az elérési út elejéhez, amikor megadja a célobjektumot.

- Adaptív Anomáliafelügyeleti szabályok jelentés nem hozható létre, ha a minta akár egy olyan eseményt is tartalmaz, amelynek neve meghaladja a 260 karaktert.

- Az Adaptív Anomáliafelügyelő Kiváltott szabályok tárolójából történő kizárások hozzáadása nem támogatott, ha egy objektum vagy egy folyamat tulajdonságainak értéke meghaladja a 256 karaktert (például célobjektum elérési útja). Kizárást manuálisan is hozzáadhat a Házirend beállításaiban. Kizárást az Adaptív Anomáliafelügyelő szabályok kiváltásáról szóló jelentésében is hozzáadhat.

- A Kaspersky Security Center 15.1 nem tud részletes **Jelentés az Adaptív Anomáliafelügyelői szabályok állapotáról** jelentést generálni egy adott szabályhoz.

Meghajtó titkosítása (FDE)

- A Kaspersky lemeztitkosítás az ARM-alapú számítógépeken nem támogatott.

- A BitLocker meghajtótitkosítás nem támogatott a Windows Home rendszert futtató számítógépeken.

- Az alkalmazás telepítése után újra kell indítania az operációs rendszert a merevlemez-titkosítás megfelelő működéséhez.

- A Hitelesítési ügynök nem támogatja a hieroglifákat és a `|` és `\` speciális karaktereket.

- A titkosítást követő optimális számítógép-teljesítmény érdekében a processzornak támogatnia kell az AES-NI utasításkészletet (Intel Advanced Encryption Standard New Instructions). Ha a processzor nem támogatja az AES-NI-t, a számítógép teljesítménye csökkenhet.

- Ha egyes folyamatok még azelőtt próbálnak hozzáférni a titkosított eszközökhöz, hogy az alkalmazás hozzáférést biztosított volna az ilyen eszközökhöz, az alkalmazás figyelmeztetést jelenít meg arról, hogy az ilyen folyamatokat le kell állítani. Ha a folyamatokat nem lehet leállítani, csatlakoztassa újra a titkosított eszközöket.

- A merevlemezek egyedi azonosítói az eszköztitkosítási statisztikában fordított formátumban vannak megjelenítve.

- Nem ajánlott az eszközök formázása, ha azok titkosítottak.

- Ha egyszerre több cserélhető meghajtó van csatlakoztatva a számítógéphez, a titkosítási házirend csak egy cserélhető meghajtóra alkalmazható. A cserélhető eszközök újbóli csatlakoztatásakor a titkosítási házirend helyesen lesz alkalmazva.

- Előfordulhat, hogy az erősen töredezett merevlemezen a titkosítás nem indul el. Töredezettségmentesítse a merevlemezt.

- A merevlemezek titkosításakor a hibernálás blokkolva lesz a titkosítási feladat kezdetétől a Microsoft Windows 7/8/8.1/10 rendszert futtató számítógép első újraindításáig, valamint a merevlemez-titkosítás telepítése után a Microsoft Windows 8/8.1/10 operációs rendszerek első újraindításáig. A merevlemezek visszafejtésekor a hibernálás blokkolva lesz a rendszerindító meghajtó teljes visszafejtésétől az operációs rendszer első újraindításáig. Ha az Első lépések opció engedélyezve van a Microsoft Windows 8/8.1/10 rendszerben, a hibernálás blokkolása megakadályozza az operációs rendszer leállítását.

- A Windows 7 rendszerű számítógépek nem engedélyezik a jelszó megváltoztatását a visszaállítás során, ha a lemez BitLocker technológiával van titkosítva. A visszaállítási kulcs megadása és az operációs rendszer betöltése után a Kaspersky Endpoint Security nem szólítja fel a felhasználót a jelszó vagy a PIN-kód módosítására. Így nem lehet új jelszót vagy PIN-kódot beállítani. A probléma az operációs rendszer sajátosságaiból származik. A folytatáshoz újra kell titkosítania a merevlemezt.

- Nem ajánlott az xbootmgr.exe eszköz használata, ha további szolgáltatók vannak engedélyezve. Például Dispatcher, Network vagy Drivers.

- A titkosított cserélhető meghajtó formázása nem támogatott olyan számítógépen, amelyre telepítve van a Kaspersky Endpoint Security for Windows.

- A titkosított cserélhető meghajtó FAT32 fájlrendszerrel való formázása nem támogatott (a meghajtó titkosítva jelenik meg). A formázáshoz formázza újra a meghajtót NTFS fájlrendszerre.

- Több letöltési ügynök nem lehet egyszerre egy titkosított számítógépen.

- A rendszerindító GPT-lemez nem titkosított állapotú lemezképének visszaállítására irányuló kísérlet során az operációs rendszer működésképtelenné teheti az operációs rendszert. Ennek elkerülése érdekében kövesse az alábbi ajánlásokat:

    - A lemezkép biztonsági mentésből való visszaállítása előtt teljesen fejtse vissza a lemez titkosítását.

    - A kép létrehozásakor használjon szektoronkénti másolást.

    - A lemezkép visszaállítása előtt törölje az adatokat a titkosított lemez első szektoraiból, majd inicializálja újra a lemezt.

- Nem lehet hozzáférni egy korábban egy másik számítógépen titkosított cserélhető meghajtóhoz, ha az alábbi feltételek mindegyike egyidejűleg teljesül:

  - Nincs kapcsolat a Kaspersky Security Center kiszolgálóval.

  - A felhasználó új tokennel vagy jelszóval próbál hitelesíteni.

  Ha hasonló helyzet fordul elő, indítsa újra a számítógépet. A számítógép újraindítása után hozzáférést kap a titkosított cserélhető meghajtóhoz.

- Előfordulhat, hogy az USB-eszközök Hitelesítési ügynök általi felfedezése nem támogatott, ha az USB-hez az xHCI mód engedélyezve van a BIOS-beállításokban.

- Az SSHD-eszközöknél az eszköz SSD-je leggyakrabban használt adatok gyorsítótárazásához használt részének Kaspersky-lemeztitkosítása (FDE) nem támogatott.

- A merevlemezek titkosítása UEFI módban futó 32 bites Microsoft Windows 8/8.1/10 operációs rendszerekben nem támogatott.

- Indítsa újra a számítógépet, mielőtt újból titkosít egy visszafejtett merevlemezt.

- A merevlemez-titkosítás nem kompatibilis a Kaspersky Anti-Virus for UEFI alkalmazással. Nem ajánlott merevlemez-titkosítást használni azokon a számítógépeken, amelyekre Kaspersky Anti-Virus for UEFI van telepítve.

- A Hitelesítési ügynök-fiókok Microsoft-fiókokon alapuló létrehozása a következő korlátozásokkal támogatott:

  - Az egyszeri bejelentkezés technológia nem támogatott.

  - A Hitelesítési ügynök-fiókok automatikus létrehozása nem támogatott, ha be van jelölve a fiókok létrehozásának lehetősége azon felhasználóknak, akik az elmúlt N napban jelentkeztek be a rendszerbe.

- Ha egy Hitelesítési ügynök-fiók neve `<domain>/<Windows account name>` formátumú, a számítógép nevének megváltoztatása után meg kell változtatni a számítógép helyi felhasználói számára létrehozott fiókok nevét is. Például, képzelje el, hogy van egy helyi `Ivanov` felhasználó az `Ivanov` számítógépen, és az `Ivanov/Ivanov` névvel Hitelesítési ügynök-fiók lett létrehozva ehhez a felhasználóhoz. Ha az `Ivanov` számítógépnév `Ivanov-PC` névre lett módosítva, a hitelesítési ügynök-fiók nevét is módosítani kell az `Ivanov` számítógép `Ivanov/Ivanov` felhasználója esetében az `Ivanov-PC/Ivanov` névre. A fiók nevét megváltoztathatja a Hitelesítési ügynök helyi fiókkezelési feladatával. A felhasználói fiók nevének megváltoztatása előtt a rendszerindítás előtti környezetben lehetőség van a régi név használatával (például `Ivanov/Ivanov`) való hitelesítésre is.

- Ha egy felhasználó csak egy token használatával férhet hozzá a Kaspersky lemeztitkosítási technológiával titkosított számítógéphez, és ennek a felhasználónak hozzáférés-helyreállítási eljárást kell befejeznie, győződjön meg arról, hogy a felhasználó jelszóalapú hozzáférést kapott a számítógéphez, miután a titkosított számítógéphez való hozzáférés vissza lett állítva. Előfordulhat, hogy a felhasználó által a hozzáférés visszaállításakor beállított jelszó nem lesz elmentve. Ebben az esetben a felhasználónak a számítógép következő újraindításakor újra el kell végeznie a titkosított számítógéphez való hozzáférés-helyreállítási eljárást.

- Ha egy merevlemezt visszafejt az FDE helyreállító eszközzel, a visszafejtési folyamat hibával zárulhat, ha a forráseszközön lévő adatok felülíródnak a visszafejtett adatokkal. A merevlemezen lévő adatok egy része titkosított marad. Javasoljuk, hogy válassza ki a visszafejtett adatok fájlba mentésére szolgáló opciót az eszközvisszafejtés beállításai között az FDE helyreállítóeszközt használatakor.

- Ha a Hitelesítési ügynök jelszava megváltozott, egy *A jelszó sikeresen megváltoztatva. Kattintson az OK gombra* szöveget tartalmazó üzenet jelenik meg, és a felhasználó újraindítja a számítógépet, az új jelszó nem lesz elmentve. A régi jelszót kell használni a későbbi hitelesítéshez a rendszerindítás előtti környezetben.

- A lemeztitkosítás nem kompatibilis az Intel Rapid Start technológiával.

- A lemeztitkosítás nem kompatibilis az ExpressCache technológiával.

- Bizonyos esetekben, amikor egy titkosított meghajtót az FDE helyreállító eszközzel próbál visszafejteni, az eszköz tévesen „titkosítatlannak" észleli az eszköz állapotát a „Kérés-válasz" eljárás befejeződése után. Az eszköz naplója olyan eseményt mutat, amely szerint az eszköz visszafejtése sikeres volt. Ebben az esetben az eszköz visszafejtéséhez újra kell indítani az adat-helyreállítási eljárást.

- Miután a Kaspersky Endpoint Security for Windows bővítményt a Web Console-ban frissítette, az ügyfélszámítógép tulajdonságai mindaddig nem jelenítik meg a BitLocker helyreállítási kulcsot, amíg a Web Console szolgáltatást újra nem indítja.

- A teljes lemeztitkosítás támogatásának egyéb korlátozásairól, valamint azon eszközök listájáról, melyek esetében a merevlemezek titkosítása korlátozásokkal támogatott, olvassa el a Terméktámogatás tudásbázisát.

Fájl szintű titkosítás (FLE)

- A fájltitkosítás nem támogatott az ARM-alapú számítógépeken.

- A Microsoft Windows Embedded operációs rendszerek nem támogatják a fájl- és mappatitkosítást.

- Az alkalmazás telepítése után a fájlok és mappák titkosításának megfelelő működéséhez újra kell indítania az operációs rendszert.

- Az alkalmazás csak az NTFS és a FAT32 fájlrendszerrel rendelkező eszközökön támogatja a fájlok titkosítását. Ha egy titkosított fájlt nem támogatott fájlrendszerrel (például exFAT) rendelkező eszközre továbbít, a fájl az adott eszközön nem lesz titkosítva, és módosítható lesz.

- Ha egy titkosított fájlt egy elérhető titkosítási funkciókkal rendelkező számítógépen van tárolva, és a fájlt olyan számítógépről szeretné elérni, ahol a titkosítás nem érhető el, akkor közvetlen hozzáférést kap a fájlhoz. A titkosítási funkciókkal rendelkező számítógép hálózati mappájában tárolt titkosított fájlokat visszafejtett formában lesz átmásolva egy olyan számítógépre, amely nem rendelkezik elérhető titkosítási funkciókkal.

- Azt javasoljuk, hogy az Encrypting File System-mel titkosított fájlokat a Kaspersky Endpoint Security for Windows rendszerrel való titkosítása előtt visszafejti.

- A titkosítás után a fájlok mérete 4 kB-tal nő.

- A fájl titkosítása után az *Archívum* attribútum a fájl tulajdonságaiban lesz beállítva.

- Amikor a visszafejtett fájlt például cserélhető adathordozóra másolja, a fájl titkosítva maradhat. Ez azért történhet meg, mert amikor a fájlkezelő (például az explorer.exe) megpróbál hozzáférni a titkosított fájlhoz, a fájl kivonatát a folyamat speciális listájába menti. A fájl visszafejtése után, amikor a fájlkezelő megpróbál hozzáférni a fájlhoz, a folyamat megkeresi a fájl kivonatát a listában. Ha a rendszer megtalálja a kivonatot, a Kaspersky Endpoint Security titkosítva hagyja a fájlt. Ennek elkerülése érdekében törölnie kell a folyamat listáját. Az operációs rendszer automatikusan törli a folyamatlistát, amint megtelik. A listát manuálisan is törölheti. Ehhez újraindíthatja a számítógépet, újraindíthatja azt a folyamatot, amelyet a fájlhoz való hozzáférésre használ (például explorer.exe), vagy használhat egy másik fájlkezelőt, amelyet nem használt a titkosított fájlhoz való hozzáférésre.

- Ha egy titkosított archívumból származó kicsomagolt fájl neve megegyezik egy a számítógépen már meglévő fájl nevével, akkor az utóbbit felülírja az új fájl, amelyet a titkosított archívumból csomagol ki. A felhasználó nem kap értesítést a felülírási műveletről.

- Mielőtt kicsomagolna egy titkosított archívumot, győződjön meg arról, hogy elegendő szabad lemezterület áll rendelkezésre a kicsomagolt fájlok tárolására. Ha nincs elég lemezterület, előfordulhat, hogy az archívum kicsomagolása befejeződik, de a fájlok megsérülnek. Ebben az esetben elképzelhető, hogy a Kaspersky Endpoint Security nem jelenít meg hibaüzenetet.

- A Hordozható fájlkezelő felület nem jelenít meg üzeneteket a működés közben fellépő hibákról.

- A Kaspersky Endpoint Security for Windows nem indítja el a Hordozható fájlkezelő alkalmazást olyan számítógépen, amelyre telepítve van a Fájlszintű titkosítás összetevő.

- Nem használhatja a Hordozható fájlkezelőt egy cserélhető meghajtó eléréséhez, ha az alábbi feltételek egyidejűleg teljesülnek:

  - Nincs kapcsolat a Kaspersky Security Centerrel;

  - A Kaspersky Endpoint Security for Windows telepítve van a számítógépen;

  - Adattitkosítás (FDE vagy FLE) nem lett végrehajtva a számítógépen.

  A hozzáférés akkor sem lehetséges, ha Ön ismeri a Hordozható fájlkezelő jelszavát.

- Fájltitkosítás használata esetén az alkalmazás nem kompatibilis a Sylpheed levelező klienssel.

- A Kaspersky Endpoint Security for Windows nem támogatja a titkosított fájlok hozzáférés-korlátozási szabályait bizonyos alkalmazások esetében. Ennek oka, hogy egyes fájlműveleteket egy harmadik féltől származó alkalmazás végez. Például a fájlmásolást a fájlkezelő végzi, nem maga az alkalmazás. Ily módon, ha a titkosított fájlokhoz való hozzáférés nem engedélyezett az Outlook levelezőprogram számára, a Kaspersky Endpoint Security lehetővé teszi a levelezőprogramnak a titkosított fájlhoz való hozzáférést, ha a felhasználó a vágólapon keresztül vagy a húzás funkcióval másolt fájlokat az e-mailbe. A másolási művelet egy olyan fájlkezelővel történt, amelynél a titkosított fájlokhoz való hozzáférés korlátozására vonatkozó szabályok nincsenek meghatározva, azaz a hozzáférés engedélyezett.

- Ha a cserélhető meghajtók a hordozható mód támogatásával vannak titkosítva, a jelszó életkor-szabályozása nem tiltható le.

- Az oldalfájl beállításainak módosítása nem támogatott. Az operációs rendszer az alapértelmezett értékeket használja a megadott paraméterértékek helyett.

- Használja a biztonságos eltávolítást, ha titkosított cserélhető meghajtókkal dolgozik. Nem tudjuk garantálni az adatok integritását, ha a cserélhető meghajtókat nem biztonságosan távolítja el.

- A fájlok titkosítása után a nem titkosított eredetijeik biztonságosan törlődnek.

- Az offline fájlok Client-Side Caching (CSC) használatával való szinkronizálása nem támogatott. Az offline fájlok titkosítása vagy a kiszolgálók SMB-n keresztüli Branch Caching technológiája sem támogatott. Javasoljuk, hogy a csoportházirend szintjén tiltsa le a megosztott erőforrások offline kezelését. Az offline módban lévő fájlok szerkeszthetők. A szinkronizálás után az offline fájlban végrehajtott módosítások elveszhetnek.

- Titkosított archívum létrehozása a rendszer merevlemezének gyökérkönyvtárában nem támogatott.

- Problémákat tapasztalhat a titkosított fájlok hálózaton keresztüli elérésekor. Javasoljuk, hogy helyezze át a fájlokat egy másik forrásba, vagy ellenőrizze, hogy a fájlszerverként használt számítógépet ugyanaz a Kaspersky Security Center felügyeleti kiszolgáló kezeli-e.

- A billentyűzetkiosztás megváltoztatása a titkosított önkicsomagoló archívum jelszóbeviteli ablakának lefagyását okozhatja. A probléma megoldásához zárja be a jelszómegadási ablakot, váltson az operációs rendszer billentyűzetkiosztására, és írja be újra a titkosított archívum jelszavát.

- Ha a fájltitkosítást egy lemezen több partícióval rendelkező rendszereken használják, javasoljuk, hogy használja a pagefile.sys fájl méretét automatikusan meghatározó beállítást. A számítógép újraindítása után a pagefile.sys fájl mozoghat a lemezpartíciók között.

- A fájltitkosítási szabályok, köztük a *Saját dokumentumok* mappában lévő fájlok alkalmazása után győződjön meg arról, hogy sikeresen hozzáférhetnek a titkosított fájlokhoz azok a felhasználók, akik számára a titkosítás alkalmazva lett. Ehhez minden felhasználónak be kell jelentkeznie a rendszerbe, amikor a Kaspersky Security Centerrel való kapcsolat elérhető. Ha a felhasználó a Kaspersky Security Centerhez való kapcsolódás nélkül próbál titkosított fájlokhoz hozzáférni, a rendszer lefagyhat.

- Ha valamilyen módon rendszerfájlok is beletartoznak a fájlszintű titkosítás hatókörébe, akkor a jelentésekben megjelenhetnek a fájlok titkosításával kapcsolatos hibákkal kapcsolatos események. Az ezekben az eseményekben megadott fájlok nincsenek titkosítva.

- A Pico folyamatok nem támogatottak.

- A kis- és nagybetűk között különbséget tevő elérési utak nem támogatottak. Titkosítási vagy visszafejtési szabályok alkalmazásakor a termékesemények elérési útjai kisbetűvel jelennek meg.

- Nem ajánlott titkosítani azokat a fájlokat, amelyeket a rendszer indításkor használ. Ha ezek a fájlok titkosítva vannak, a titkosított fájlokhoz való hozzáférésnek a Kaspersky Security Centerhez való kapcsolódás nélküli megkísérlése a rendszer lefagyását okozhatja, vagy a titkosítatlan fájlokhoz való hozzáférésre vonatkozó kéréseket eredményezhet.

- Ha több felhasználó FLE-szabályok alapján dolgozik egy fájlon a hálózaton, és ehhez fájl-memória leképezési módszerrel működő alkalmazást (például WordPad vagy FAR) és nagy fájlokkal való használatra tervezett alkalmazásokat (például Notepad ++) használnak, akkor a fájl titkosítatlan formában korlátlanul blokkolható anélkül, hogy elérhető lenne arról a számítógépről, amelyen tárolva van.

- A Kaspersky Endpoint Security nem titkosítja azokat a fájlokat, amelyek a OneDrive felhőalapú tárhelyen vagy más olyan mappákban találhatók, amelyek neve OneDrive. A Kaspersky Endpoint Security blokkolja a titkosított fájlok OneDrive mappákba másolását is, ha ezeket a fájlokat nem adják hozzá a visszafejtési szabályhoz.

- A fájlszintű titkosítási összetevő telepítésekor a felhasználók és csoportok kezelése WSL módban (Windows Subsystem for Linux) nem működik.

- A fájlszintű titkosító összetevő telepítésekor a fájlok átnevezéséhez és törléséhez a POSIX (Portable Operating System Interface) nem támogatott.

- Nem ajánlott az ideiglenes fájlok titkosítása, mert ez adatvesztést okozhat. Például a Microsoft Word ideiglenes fájlokat hoz létre egy dokumentum feldolgozása során. Ha az ideiglenes fájlok titkosítottak, de az eredeti fájl nem, a felhasználó *Hozzáférés megtagadva* hibát kaphat a dokumentum mentésekor. Az is előfordulhat, hogy a Microsoft Word menti a fájlt, de a következő alkalommal nem lehet megnyitni, tehát elvész az adat. Az adatvesztés elkerülése érdekében zárja ki az ideiglenes fájlokat a titkosítási szabályok hatóköréből.

Detection and Response (EDR, MDR, Kaspersky Sandbox)

- A *Move file to Quarantine* feladat miatt nem vizsgálhat karanténba helyezett objektumot.
- A 4 MB-nál nagyobb Alternate Data Stream (ADS) nem helyezhető karanténba. A Kaspersky Endpoint Security a felhasználó értesítése nélkül mellőzi az ilyen méretű adatfolyamokat.
- A Kaspersky Endpoint Security nem futtatja az *IOC Scan* feladatokat a hálózati meghajtókon, ha a feladat tulajdonságaiban a mappa elérési útja meghajtóbetűvel kezdődik. A Kaspersky Endpoint Security csak az UNC-útvonal formátumát támogatja az *IOC Scan* feladatokhoz a hálózati meghajtókon. Például: `\\server\shared_folder`.
- Annak érdekében, hogy az *IOC Scan* feladat az EmailItem feltételekkel megfelelően működjön, a Kaspersky Endpoint Security webes beépülő modult a legújabb verzióra kell frissíteni.
- Az ARM alapú számítógépeken az *IOC Scan* feladat csak a következő levelezőprogramokból támogatja az e-mail-fájlokat: Outlook 2016 és Outlook 2021, 2024 és 365 for Arm64 32 és 64 bites verziói.
- Az alkalmazás konfigurációs fájljának importálása hibával fejeződik be, ha a konfigurációs fájlban engedélyezve van az Integráció a Kaspersky Sandbox szolgáltatással beállítás. Az alkalmazásbeállítások exportálása előtt tiltsa le a Kaspersky Sandbox szolgáltatást. Ezután hajtsa végre az exportálási/importálási eljárást. A konfigurációs fájl importálása után engedélyezze a Kaspersky Sandbox szolgáltatást.
- Szabályzat KLP-fájlból történő importálásakor az a paraméterérték, amely a Kaspersky Detection and Response Expert Agreement feltételeinek elfogadását határozza meg, nem kerül alkalmazásra. Ennek eredményeként a szabályzat importálása után a Kaspersky Endpoint Security nem látja el az EDR Agent funkcióit. Az EDR Agent működéséhez nyissa meg a szabályzatot, módosítson bármely paramétert, és mentse a szabályzat beállításait.
- Ha az *IOC Scan* feladat futtatása során biztonsági sérülési indikátort észlel, az alkalmazás csak a FileItem kifejezésre vonatkozóan helyez egy fájlt karanténba. Fájl karanténba helyezése más kifejezések esetén nem támogatott.
- Kaspersky Endpoint Security for Windows 11.7.0 vagy újabb verziójú webes bővítményére van szükség az észlelések részleteinek kezeléséhez. Az értesítések adataira az Endpoint Detection and Response megoldásaival (EDR Optimum és EDR Expert) történő munka során van szükség. Az észlelés részletei a Kaspersky Security Center Web Console-on és a Kaspersky Security Center Cloud Console-on érhetők el.
- A [KES+KEA] konfiguráció [KES+beépített ügynök] konfigurációra történő átváltása a Kaspersky Endpoint Agent alkalmazás eltávolítási hibájával zárulhat. A Kaspersky Endpoint Agent legújabb verziójában javítottuk az alkalmazás eltávolítási hibáját. A Kaspersky Endpoint Agent eltávolításához indítsa újra a számítógépet, és hozzon létre egy alkalmazáseltávolítási feladatot.
- A [KES+KEA+beépített ügynök] konfiguráció nem támogatott. Az ilyen konfiguráció megzavarja az alkalmazások és a vállalatnál telepített Detection and Response megoldás közötti interakciót. Ezenkívül a Kaspersky Endpoint Agent és a beépített ügynök ugyanazon a számítógépen történő használata a telemetria duplikációjához és a számítógép és a hálózat fokozott terheléséhez vezethet. A [KES + beépített ügynök] konfigurációra való áttérés után győződjön meg arról, hogy a Kaspersky Endpoint Agent eltávolításra került a számítógépről. Ha a Kaspersky Endpoint Agent az áttérés után továbbra is működik, távolítsa el az alkalmazást manuálisan (például az *Uninstall application remotely* feladattal).

  A telepítő lehetővé teszi a Kaspersky Endpoint Agent telepítését olyan számítógépre, amelyen a Kaspersky Endpoint Security és a beépített ügynök telepítve van. A Kaspersky Endpoint Agent és a beépített ügynök is telepíthető egyetlen számítógépre az *Alkalmazásösszetevők módosítása feladat* eredményeként. A viselkedés a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent verzióitól függ.

- A riasztás részleteinek generálásakor az alkalmazás információkat ad az észlelt fenyegetésről, beleértve a módosított fájlok kivonatát is. A Kaspersky Endpoint Security a riasztás részleteinek generálása közben kiszámítja a fájl kivonatát. Vegye figyelembe, hogy a fájl eredeti kivonata a fájlmódosítási esemény létrehozásakor nem feltétlenül egyezik meg a riasztás részleteinek generálásakor számított kivonattal.

- A beépített ügynök, az EDR (KATA), a számítógép újraindítása után folytatja a számítógép hálózatelkülönítését, még akkor is, ha az elkülönítési időszak lejárt. A számítógép ismételt elkülönítésének elkerülése céljából ki kell kapcsolnia a hálózatelkülönítést a Kaspersky Anti Targeted Attack Platform konzolon.

- Javasoljuk, hogy frissítse az alkalmazást a hálózatelkülönítés befejezése után. A Kaspersky Endpoint Security frissítése után a hálózatelkülönítés leállítható.

- Az EDR (KATA), az EDR Optimum és az EDR Expert beépített ügynökei nem kompatibilisek egymással. Ezért a Kaspersky Endpoint Detection and Response bővítmény önálló licencével rendelkező beépített EDR-ügynök aktiválása kihagyható, ha a Kaspersky Endpoint Security terméket különböző EDR-funkciókkal aktiválta. Például a beépített EDR (KATA) ügynök önálló licenccel történő aktiválása kihagyásra kerül, ha a Kaspersky Endpoint Security terméket a [KES+EDR Optimum] licenccel aktiválta.

- A Kaspersky Endpoint Security 12.1-es verziójában a beépített EDR (KATA) Agent nem támogatja a következő metafájlokat az *NTFS metafájlok lekérdezése* feladathoz: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. A Kaspersky Endpoint Security 12.2 verziója támogatja ezeket a metafájlokat.

- A Kaspersky Endpoint Agent megoldásról a Kaspersky Endpoint Security for the Kaspersky Anti Targeted Attack Platform (EDR) megoldásra történő áttérés során előfordulhat, hogy a számítógép Central Node kiszolgálóihoz való csatlakoztatáskor hibák lépnek fel. Ennek oka, hogy a Web Console áttelepítési varázslója kihagyja a következő házirend-beállításokat, és nem telepíti át őket:

  - Beállítások módosításának tiltása **Connection settings** („zárolás”).

    Alapértelmezés szerint a beállítások módosíthatók (a „lakat” nyitva van). Ezért a beállítások nem kerülnek alkalmazásra a számítógépen. Meg kell tiltania a beállítások módosítását, és be kell zárnia a „lakatot”.

  - Kriptotároló.

    Ha kétirányú hitelesítést használ a Central Node kiszolgálóihoz való csatlakozáshoz, akkor újra fel kell vennie a kriptotárolót. Az áttelepítési varázsló helyesen telepíti át a kiszolgáló TLS-tanúsítványát.

  Az Adminisztrációs konzol (MMC) Házirend és feladatok áttelepítési varázslója áttelepíti a Kaspersky Anti Targeted Attack Platform (EDR) megoldás összes beállítását.

- Az alkalmazás aktiválási állapota helytelenül jelenik meg, ha az alkalmazás Endpoint Detection and Response Agent módban van telepítve a Kaspersky Managed Detection and Response megoldásának támogatására, és nincs kapcsolat a Kaspersky Security Centerrel. A BLOB fájl letöltése után, a Windows tálca értesítési területe hibás állapotot jelenít meg: *Az alkalmazás nincs aktiválva*. Az alkalmazás felülete azonban helyesen jeleníti meg az aktiválási állapotot. Indítsa újra a számítógépet, hogy az alkalmazás megfelelően működjön.

- A Kaspersky Endpoint Security lehetővé teszi az integrációt a Kaspersky Anti Targeted Attack Platform megoldással az EDR (KATA) összetevő vagy az Endpoint Sensor (nem támogatott) használatával. Vegye figyelembe, hogy az összetevők közül csak az egyiket használhatja a Kaspersky Anti Targeted Attack Platformmal való együttműködéshez. Az összetevő állapotának megtekintéséhez nyissa meg a számítógép tulajdonságait a felügyeleti konzolon (MMC) a következő helyen: az **Applications** részen nyissa meg a Kaspersky Endpoint Security for Windows tulajdonságait, és lépjen a **Components** szakaszra. A következő speciális szempontok vonatkoznak az összetevő állapotának megjelenítésére a Kaspersky Anti Targeted Attack Platformmal való együttműködés során:

  - A 12.0 és korábbi verziójú adminisztrációs bővítmény esetén az alkalmazás megjeleníti az **Endpoint Sensor** jelenlegi állapotát. A Kaspersky Endpoint Security 12.0 és korábbi verzióiban az EDR (KATA) összetevő nem érhető el. Az EDR (KATA) összetevő a 12.1-es verzióban jelent meg.

  - A 12.1-es és újabb verziójú adminisztrációs bővítmény esetében az alkalmazás megjeleníti az **Endpoint Detection and Response (KATA)** általános állapotát, ami jelentheti az Endpoint Sensor vagy az EDR (KATA) összetevő állapotát. Ez a felhasználó számítógépére telepített alkalmazás verziójától és a Kaspersky Anti Targeted Attack Platformmal való együttműködéshez rendelkezésre álló összetevőktől függ.

- A Kaspersky Endpoint Security 12.6-os és újabb verzióitól kezdve a Kaspersky Security Center Web Console 14.2-es és régebbi verziói nem megfelelően jelenítik meg az **Endpoint Detection and Response (KATA)** összetevő nevét a számítógép tulajdonságaiban. Az **Endpoint Detection and Response (KATA)** összetevő helyett az alkalmazás az **Endpoint Detection and Response Expert (KATA EDR)** összetevő nevét jeleníti meg. Az összetevők listájának megtekintéséhez nyissa meg a számítógép tulajdonságait a Web Console-on a következő helyen: az **Applications** részen nyissa meg a Kaspersky Endpoint Security for Windows tulajdonságait, és lépjen a **Components** szakaszra. A Kaspersky Security Center Web Console 15.1-es és újabb verzióitól kezdve az alkalmazás megfelelően jeleníti meg az összetevő nevét.

- Amikor a Kaspersky Endpoint Detection and Response adminisztrációs bővítményt a 15.3-as verzióra frissíti a Web Console 14.0–14.2-es verziójában, a riasztás részletei hibásan jelennek meg. A riasztási részletek megfelelő működéséhez indítsa újra a Kaspersky Security Center felügyeleti kiszolgálót.

- A Kaspersky Endpoint Detection and Response adminisztrációs bővítmény 15.4-es és újabb verziói nem támogatják a Kaspersky Security Center 14.0-s verzióját. Az adminisztrációs bővítmény frissítése után a riasztás részletei hibásan jelennek meg.

- A Kaspersky Extended Detection and Response (XDR) 1.4 verziójú megoldásai nem támogatják a Kaspersky Endpoint Security for Windows 12.12-es vagy újabb webes beépülő modulját. Meghagyhatja a webes beépülő modul jelenlegi verzióját, vagy frissítheti az XDR megoldást a 2.0 vagy újabb verzióra.

- A Kaspersky Endpoint Security nem küld az ARM architektúrának szánt objektumokat a Kaspersky Sandbox számára.

- A Kaspersky Endpoint Detection and Response Expert alkalmazás integrációja az ARM alapú számítógépeken nem támogatott.

- A Kaspersky Endpoint Security összesen akár 10 000 EDR Expert (on-premises) belefoglalási és kizárási eseményszűrési szabályt támogat.

- Az EDR Expert (on-premises) eseményszűrési szabályok nem kerülnek átadásra a szabályzatból a Kaspersky Endpoint Security 14.0-s vagy korábbi verzióját futtató felügyelt eszközökre, ha a tárolt szűrési szabályok támogatott korlátját túllépik. Az alkalmazás egy megfelelő figyelmeztetést jelenít meg.

Egyéb korlátozások

- A Windows operációs rendszerek a 11 24H2 verziótól kezdve támogatják az UDP Receive Segment Coalescing Offload (URO) technológiát. A technológia alapértelmezés szerint engedélyezve van, ha a számítógépen kompatibilis hálózati kártya és illesztőprogramok vannak telepítve. Az URO letiltása a felhasználó számítógépén jelentősen csökkentheti az alkalmazás teljesítményét.

- A Kaspersky Endpoint Security az alábbi korlátozásokkal támogatja a WSL alrendszert (Windows Subsystem for Linux):

  - WSL 1 Az alkalmazás a hálózati forgalmat figyeli, és HTTP/HTTPS protokollon keresztül észleli a fenyegetéseket. Mivel a Kaspersky Endpoint Security saját tanúsítványát használja a biztonságos HTTPS-kapcsolatok vizsgálatához, egyes harmadik féltől származó alkalmazások működése megszakadhat.

  - WSL 2 Az alkalmazás nem támogatja a WSL 2 verziót.

- Ha az alkalmazás hibákat jelez vagy működés közben lefagy, előfordulhat, hogy automatikusan újraindul. Ha az alkalmazás visszatérő hibákkal találkozik, melyek miatt összeomlik, az alábbi műveleteket végzi el:

  1. Letiltja a felügyeleti és védelmi funkciókat (a titkosítási funkciók bekapcsolva maradnak).

  2. Értesíti a felhasználót a funkciók letiltásáról.

  3. Megpróbálja az alkalmazást működőképes állapotúra visszaállítani, miután frissítette az antivírus adatbázisokat vagy alkalmazta az alkalmazásmodul-frissítéseket.

- Előfordulhat, hogy a megbízható listához hozzáadott webcímek helytelenül lesznek feldolgozva.

- A Kaspersky Security Center konzolon nem menthet fájlokat lemezre az **Advanced** → **Repositories** → **Active threats** mappából. A fájl mentéséhez vírusmentesíteni kell a fertőzött fájlt. A vírusmentesítés során az alkalmazás a fájl egy példányát a Biztonsági mentés mappába menti. Most már mentheti a fájlt lemezre az **Advanced** → **Repositories** → **Backup** mappából.

- Az adminisztrációs kiszolgálóra történő adatátvitel beállításainak öröklése (**Általános beállítások** → **Jelentések és tároló** → **Adatátvitel az adminisztrációs kiszolgálóra**) eltér más beállítások öröklésétől. Ha engedélyezte az adatátviteli beállítások módosítását a házirendben (a „lakat” nyitva van), akkor ezek a beállítások visszaállnak az alapértelmezett értékekre a helyi számítógép tulajdonságaiban a konzolon, ha korábban nem voltak megadva. Ha ezeket a beállításokat korábban megadta, akkor az értékeik visszaállnak. Házirend törlésekor a beállítások ugyanúgy öröklődnek. Ezekben az esetekben a helyi számítógép tulajdonságaiban a többi beállítás a házirendből öröklődik.

- A Kaspersky Endpoint Security figyeli az RFC 2616, RFC 7540, RFC 7541, RFC 7301 szabványoknak megfelelő HTTP-forgalmat. Ha a Kaspersky Endpoint Security egy másik adatcsere-formátumot észlel a HTTP-forgalomban, az alkalmazás blokkolja ezt a kapcsolatot, hogy megakadályozza a rosszindulatú fájlok letöltését az internetről.

- A Kaspersky Endpoint Security megakadályozza a QUIC protokollon keresztüli kommunikációt. A böngészők a szabványos átviteli protokollt (TLS vagy SSL) használják, függetlenül attól, hogy a QUIC támogatása engedélyezve van-e az adott böngészőben vagy sem.

- TLS-kapcsolati hibák léphetnek fel, ha a harmadik féltől származó szoftverek Libcurl tárral működnek együtt. Ez a Kaspersky-tanúsítvánnyal hozható összefüggésbe, amelyet a Kaspersky Endpoint Security a titkosított kapcsolatok vizsgálatához használ. A munka folytatásához letilthatja a harmadik féltől származó szoftverek tanúsítványérvényesítését (nem ajánlott), vagy hozzáadhat egy Kaspersky-tanúsítványtörzset a cURL tanúsítványtárhoz. Részletes információkért tekintse meg a Kaspersky Tudásbázist.

- A Kaspersky Endpoint Security for Windows első indításakor egy digitálisan aláírt alkalmazás átmenetileg rossz csoportba lehet áthelyezve. A digitálisan aláírt alkalmazás később a megfelelő csoportba kerül.

- Egy külső szoftver által blokkolt rosszindulatú objektum ismételt vizsgálata során a felhasználó nem kap értesítést a fenyegetés ismételt észleléséről. A fenyegetés ismételt észlelése esemény megjelenik az alkalmazásjelentésben és a Kaspersky Security Center jelentésben.

- A Kaspersky Security Center eszköztitkosításról szóló jelentése nem tartalmaz információkat azokról az eszközökről, amelyek a Microsoft BitLocker használatával lettek titkosítva kiszolgálóplatformokon vagy olyan munkaállomásokon, amelyekre az Eszközfelügyelő összetevő nincs telepítve.

- A Kaspersky Security Center Web Console-ban nem lehet az összes jelentésbejegyzés megjelenítését engedélyezni. A Web Console-ban csak a jelentésekben megjelenített bejegyzések számát módosíthatja. Alapértelmezés szerint a Kaspersky Security Center Web Console 1000 jelentésbejegyzést jelenít meg. Az összes jelentésbejegyzés megjelenítését a Felügyeleti konzolon (MMC) engedélyezheti.

- A Kaspersky Security Center Console-ban nem lehet 1000-nél több jelentésbejegyzés megjelenítését beállítani. Ha 1000-nél magasabb értéket állít be, a Kaspersky Security Center Console csak 1000 jelentésbejegyzést fog megjeleníteni.

- Házirend-hierarchia használatakor az gyermekházirend Cserélhető meghajtók titkosítása szakaszának beállításai akkor is szerkeszthetők, ha a szülőházirend tiltja a beállítások módosítását.

- Engedélyeznie kell a Bejelentkezés naplózása funkciót az operációs rendszer beállításaiban, hogy biztosítsa a kizárások megfelelő működését a megosztott mappák külső titkosítás elleni védelme érdekében.

- Ha a megosztott mappa védelme engedélyezve van, a Kaspersky Endpoint Security for Windows figyeli a megosztott mappák titkosítási kísérleteit minden olyan távoli hozzáférési munkamenetnél, amely a Kaspersky Endpoint Security for Windows indítása előtt lett elindítva, beleértve azt a számítógépet is, amelyről a távoli hozzáférési munkamenet indult és hozzá lett adva a kizárásokhoz. Ha nem szeretné, hogy a Kaspersky Endpoint Security for Windows figyelje a megosztott mappák titkosításának kísérleteit a kizárásokhoz hozzáadott számítógépről indított és a Kaspersky Endpoint Security for Windows indítása előtt indított távoli hozzáférési munkameneteknél, akkor kapcsolja ki és állítsa helyre a távoli hozzáférési munkamenetet, vagy indítsa újra a számítógépet, amelyre a Kaspersky Endpoint Security for Windows telepítve van.

- Ha a frissítési feladat egy adott felhasználói fiók jogosultságaival van futtatva, akkor a termékjavítások nem lesznek letöltve, amikor a frissítést hitelesítést igénylő forrásból hajtja végre.

- Előfordulhat, hogy az alkalmazás a rendszer elégtelen teljesítménye miatt nem indul el. A probléma megoldásához használja a Ready Boot opciót, vagy növelje az operációs rendszer szolgáltatások indítására vonatkozó időtúllépését.

- Az alkalmazás nem működik a Windows Safe Mode szolgáltatásában.

- Nem garantálhatjuk, hogy a Hangfelügyelő az alkalmazás telepítése utáni első újraindítást követően működni fog.

- A Felügyeleti konzol (MMC) alkalmazásengedélyek konfigurálására szolgáló ablakában, a behatolásmegelőzési beállításoknál az **Eltávolítás** gomb nem érhető el. Egy alkalmazást a megbízhatósági csoportból az alkalmazás helyi menüjén keresztül távolíthat el.

- Az alkalmazás helyi felületén, a Behatolásmegelőző rendszer beállításainál az alkalmazásjogok és a védett erőforrások nem tekinthetők meg, ha a számítógépet házirend felügyeli. A görgetés, keresés, szűrés és egyéb vezérlők nem állnak rendelkezésre. Az alkalmazásengedélyeket a Kaspersky Security Center konzol házirendjének tulajdonságaiban tekintheti meg.

- Ha az elforgatott nyomkövetési fájlok engedélyezve vannak, akkor az AMSI összetevő és az Outlook bővítmény nem hoz létre nyomkövetést.

- A teljesítmény nyomkövetések a Windows Server 2008 operációs rendszerben manuálisan nem gyűjthetők össze.

- Az „Újraindítás” nyomkövetéstípus teljesítmény nyomkövetései nem támogatottak.

- A memóriakép naplózása nem támogatott Pico folyamatok esetében.

- **A rendszerszolgáltatások külső kezelésének letiltása** opció kikapcsolása nem engedélyezi az `AMPPL=1` paraméterrel telepített alkalmazás szolgáltatásának leállítását (alapértelmezés szerint a Windows 10RS2 operációs rendszer verziójától kezdve a paraméter `1` értékre van beállítva). Az `1` értékű `AMPPL` paraméter lehetővé teszi a Védelmi folyamatok technológia termékszolgáltatáshoz való használatát.

- Egy mappa egyedi vizsgálatának futtatásához az egyéni vizsgálatot elindító felhasználónak jogosultságokkal kell rendelkeznie a mappa attribútumainak olvasásához. Ellenkező esetben az egyéni mappák vizsgálata nem fog működni és hibával zárul.

- Ha egy házirendben meghatározott vizsgálati szabály olyan elérési utat tartalmaz, amelynek végén nincs `\` karakter, például `C:\folder1\folder2`, akkor a vizsgálat a `C:\folder1\` elérési útra fog lefutni.

- Ha szoftverkorlátozó házirendeket (Software Restriction Policies, SRP) használ, előfordulhat, hogy a számítógép betöltése nem sikerül (fekete képernyő). A működési zavarok megelőzése céljából engedélyeznie kell az alkalmazáskönyvtárak használatát az SRP tulajdonságaiban. Az SRP tulajdonságaiban adja hozzá a khkum.dll fájlhoz a **Korlátlan** biztonsági szintű szabályt (**New Hash Rule** menüpont). A fájl a `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.1\klhk\klhk_x64\` mappában található. Ha ezt a módszert választotta, akkor a Kaspersky Endpoint Security *Frissítés* feladatának beállításaiban emellett törölnie kell az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzet bejelölését. Az SRP használatának részleteiért olvassa el a Microsoft dokumentációját.

  Az SRP-t le is tilthatja, és a Kaspersky Endpoint Security Alkalmazásfelügyelő összetevőjét használhatja az alkalmazáshasználat ellenőrzésére.

- Ha a számítógép a Windows csoportházirend-objektum (Group Policy Object, GPO) alatt egy tartományhoz tartozik, és a DriverLoadPolicy paramétere 8-ra van állítva (Good only), a telepített Kaspersky Endpoint Security-vel rendelkező számítógép újraindítása kékképernyős összeomlást okoz. A hiba megelőzése érdekében a csoportházirendben a Early Launch Antimalware (ELAM) paraméterét 1-re (Good and unknown) kell állítani. Az ELAM-beállítások a házirendben találhatók: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- Az Outlook bővítmény beállításainak kezelése a Rest API-n keresztül nem támogatott.

- Egy adott felhasználó feladatfuttatási beállításai konfigurációs fájllal nem vihetők át az eszközök között. Miután egy konfigurációs fájlból alkalmazta a beállításokat, manuálisan adja meg a felhasználónevet és a jelszót.

- A frissítés telepítése után az integritás-ellenőrzési feladat addig nem működik, amíg a rendszer a frissítés alkalmazásához nincs újraindítva.

- Amikor a távdiagnosztikai segédprogram megváltoztatja az elforgatott nyomkövetési szintet, a Kaspersky Endpoint Security for Windows hibásan üres értéket jelenít meg a nyomkövetési szinthez. A nyomkövetési fájlok ugyanakkor a helyes nyomkövetési szintnek megfelelően vannak megírva. Az elforgatott nyomkövetési szintnek az alkalmazás helyi felületén keresztül történő megváltoztatásakor a nyomkövetési szint helyesen van módosítva, de a távdiagnosztikai segédprogram hibásan a segédprogram által legutóbb meghatározott nyomkövetési szintet jeleníti meg. Ez azt eredményezheti, hogy a rendszergazdának nem lesznek naprakész információi az aktuális nyomkövetési szintről, és releváns információk hiányozhatnak a nyomkövetésekből, ha a felhasználó az alkalmazás helyi felületén manuálisan megváltoztatja a nyomkövetési szintet.

- A helyi felületen a Jelszóvédelem beállításai nem teszik lehetővé az adminisztrátori fiók nevének megváltoztatását (alapértelmezés szerint KLAdmin). Az adminisztrátori fiók nevének megváltoztatásához ki kell kapcsolnia a jelszóvédelmet, majd újból engedélyeznie kell a jelszóvédelmet, és meg kell adnia az adminisztrátori fiók új nevét.

- A Kaspersky Endpoint Security alkalmazás Windows Server 2019 kiszolgálón telepítve nem kompatibilis a Dockerrel. Ha Docker-tárolókat telepít egy olyan számítógépre, amelyen fut a Kaspersky Endpoint Security, a rendszer összeomlik (BSOD).

- Ha a Kaspersky Endpoint Security az SQL Server DBMS egyik kiszolgálójára van telepítve, az alkalmazás kéréseket küld a kiszolgáló példányának. Erre azért van szükség, hogy ellenőrizze az SQL Server Agent feladatait, és megakadályozza a rosszindulatú feladatok futtatását. A Kaspersky Endpoint Security az SQL Server felhasználói fiókot használja a feladatok vizsgálatához. Az alkalmazás kéréseket küld a kiszolgálónak a rendszermemória vizsgálatakor és a vírusadatbázisok frissítése után.

- A Kaspersky Endpoint Security és a Secret Net Studio szoftver kompatibilitása korlátozott:

  - A Kaspersky Endpoint Security alkalmazás nem kompatibilis a Secret Net Studio szoftver víruskereső összetevőjével.

    Az alkalmazás nem telepíthető olyan számítógépre, amelyen a Secret Net Studio a víruskereső összetevővel van telepítve. Az együttműködés lehetővé tételéhez el kell távolítania a víruskereső összetevőt a Secret Net Studio-ból.

  - A Kaspersky Endpoint Security alkalmazás nem kompatibilis a Secret Net Studio szoftver lemezvédelmi és adattitkosítási összetevőjével.

    Az alkalmazás nem telepíthető olyan számítógépre, amelyen a Secret Net Studio a lemezvédelmi és adattitkosítási összetevővel van telepítve. Az együttműködés lehetővé tételéhez el kell távolítania a lemezvédelmi és adattitkosítási összetevőt a Secret Net Studio szoftverből.

  - A Secret Net Studio nem kompatibilis a Kaspersky Endpoint Security Fájl szintű titkosítás (FLE) összetevőjével.

    Ha a Kaspersky Endpoint Security alkalmazást a Fájl szintű titkosítás (FLE) összetevővel telepíti, a Secret Net Studio hibásan működhet. Az együttműködés biztosítása érdekében el kell távolítania a Fájl szintű titkosítás (FLE) összetevőt a Kaspersky Endpoint Security alkalmazásból.

- A Rendszerintegritás-figyelő szabályainak importálásakor az alkalmazás ellenőrzi a szabály azonosítóját és nevét. Ha a szabályazonosítók megegyeznek, a Kaspersky Endpoint Security a meglévő szabályokat az új szabályokkal helyettesíti. Szabályok exportálásakor az alkalmazás automatikusan hozzárendeli az azonosítókat. Azonos azonosítóval rendelkező szabály létezhet, például ha kézzel szerkesztette az exportált XML-szabályfájlokat. Ha a szabályazonosítók egyediek, de a szabálynevek azonosak, a Kaspersky Endpoint Security a szabály nevéhez hozzáadja az `(1)` értéket és így tovább.

- A Kaspersky Endpoint Security for Windows 12.11-es verziójától kezdődően nem lehet megtekinteni a gyermekcsoportban megnyitott szülőházirend-beállításokat. A Web Console egy figyelmeztetést is megjelenít: *This policy is inherited. You can edit the policy settings only in the administration group in which it was created.*

- A 256 karakternél hosszabb felugró értesítések nem jelennek meg az Adminisztrációs konzolon (MMC).

- A szabályzatban és a telepítőcsomagban szereplő összetevők neve eltérő lehet. Például az Endpoint Detection and Response Expert (on-premises) neve Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) vagy Kaspersky Anti Targeted Attack Platform Integration is lehet. Az összetevők neve az alkalmazás verziójától függően eltérő lehet.

Szójegyzék

Adathalász webcímek adatbázisa

Olyan webcímek listája, amelyekről a Kaspersky szakemberei megállapították, hogy adathalászathoz kapcsolódnak. Az adatbázis rendszeresen frissül, és a Kaspersky alkalmazás terjesztőcsomagjának részét képezi.

Adminisztrációs csoport

Olyan eszközök készlete, amelyek közös funkciókon osztoznak, és a Kaspersky alkalmazásainak ugyanaz a készlete van rajtuk telepítve. Az eszközök azért vannak csoportosítva, hogy kényelmesen, egyetlen egységként lehessen kezelni őket. A csoport további csoportokat is tartalmazhat. A csoporton belül minden telepített alkalmazás számára csoportrendszabályokat és csoportfeladatokat lehet előállítani.

Aktív kulcs

Az a kulcs, amelyet az alkalmazás jelenleg használ.

Archívum

Egy vagy több, egyetlen tömörített fájlba csomagolt fájl. Az adatok be- és kicsomagolásához egy speciális, archiváló nevű alkalmazás szükséges.

Cloud Discovery

A Cloud Discovery kezeli a felhasználók felhőszolgáltatásokhoz való hozzáférését. A felhőszolgáltatások közé tartozik például a Microsoft Teams, a Salesforce és a Microsoft Office 365. A felhőszolgáltatások kategóriákba vannak csoportosítva, például *fájlmegosztás*, *üzenetküldés*, *e-mail*.

Feladat

A Kaspersky alkalmazásában feladatként végrehajtott funkciók, például: Valós idejű fájlvédelem, Teljes vizsgálat és Adatbázis-frissítés.

Fertőzhető fájl

Olyan fájl, amelyet szerkezetéből vagy formátumából adódóan a behatolók a rosszindulatú kódok tárolására és terjesztésére szolgáló „tárolóként" használhatnak fel. Ezek rendszerint végrehajtható fájlok, és kiterjesztésük például .com, .exe és .dll lehet. A rosszindulatú kódok aktiválódásának kockázata az ilyen fájloknál meglehetősen magas.

Fertőzött fájl

Rosszindulatú programokat tartalmazó fájl (a fájl vizsgálata során ismert rosszindulatú programok kódja észlelhető). A Kaspersky nem javasolja az ilyen fájlok használatát, mert azok megfertőzhetik a számítógépet.

Hitelesítési ügynök

A hitelesítés befejezésére szolgáló felület, mellyel hozzá lehet férni a titkosított merevlemezekhez, és be lehet tölteni az operációs rendszert a rendszerindításra alkalmaz merevlemez titkosítását követően.

Hordozható fájlkezelő

Olyan alkalmazás, amely felületet kínál a cserélhető meghajtókon lévő titkosított fájlokkal végezhető munkához, ha a számítógépen nem áll rendelkezésre titkosítási funkció.

Integrációs kiszolgáló

Kaspersky Endpoint Security for Virtualization Light Agent összetevő. A Kaspersky Endpoint Security összetevői és a virtuális infrastruktúra közötti interakciót biztosítja.

IOC

Biztonsági sérülési indikátor. Rosszindulatú objektumra vagy tevékenységre vonatkozó adatkészlet.

IOC-fájl

Olyan fájl, amely az indikátorkészleteket tartalmazza, és amellyel az alkalmazás egyezést próbál találni észlelés esetén. Az észlelés valószínűsége nagyobb lehet, ha a vizsgálat eredményeként az objektum pontos egyezést mutat több IOC-fájllal.

Kártékony webcímek adatbázisa

Olyan webcímek listája, amelyeknek tartalma veszélyesnek tekinthető. A listát a Kaspersky szakértői hozzák létre. Rendszeresen frissül, és a Kaspersky alkalmazás terjesztőkészletének részét képezi.

Kerberos hitelesítés

Az ügyfél és a kiszolgáló általi kölcsönös hitelesítés mechanizmusa a közöttük lévő kapcsolat létrehozása előtt, amely lehetővé teszi a nem biztonságos hálózatokon keresztüli kommunikációt. A mechanizmus egy jegyen alapul, amelyet a felhasználó egy megbízható hitelesítő központtól kap.

Licenctanúsítvány

Olyan dokumentum, amelyet a Kaspersky a felhasználónak a kulcsfájllal, illetve aktiváló kóddal együtt ad át. A felhasználó részére adott licencről tartalmaz információkat.

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent összetevő. Minden védendő virtuális gépen telepítve van.

Maszk

Helyettesítő karakterekkel megadott fájlnév és kiterjesztés.

A fájlmaszkok bármilyen, a fájlnevekben megengedett karaktert tartalmazhatnak, köztük helyettesítő karaktereket:

- A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).

- Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk. A** maszk csak a vizsgálati kizárásokhoz érhető el.

- A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

Network Agent

A Kaspersky Security Center egyik összetevője, mely lehetővé teszi az Adminisztrációs kiszolgáló és egy adott hálózati csomóponton (munkaállomáson vagy kiszolgálón) telepített Kaspersky alkalmazások közti interakciót. Ezt az összetevőt a Windows rendszeren futó összes Kaspersky alkalmazás közösen használja. A Hálózati ügynök dedikált verziói más operációs rendszereken futó alkalmazásokhoz valók.

OLE objektum

Csatolt fájl vagy más fájlba beágyazott fájl. A Kaspersky alkalmazásai lehetővé teszik a víruskeresést az OLE objektumokban. Ha például beilleszt egy Microsoft Office Excel® táblázatot egy Microsoft Office Word dokumentumba, a program OLE-objektumként vizsgálja meg a táblázatot.

OpenIOC

Biztonsági sérülési indikátorok (IOC) leírásának nyitott, XML alapú szabványa, amely legalább 500 különböző indikátort tartalmaz.

SVM

Biztonságos virtuális gép – egy speciális virtuális gép, amelyre a vizsgálói kiszolgálói szolgáltatás (Védelmi kiszolgáló, a Kaspersky Endpoint Security for Virtualization Light Agent egyik összetevője) telepítve van.

Tanúsítvány kibocsátója

A tanúsítványt kiállító tanúsítványközpont.

Téves riasztás

Akkor következik be téves riasztás, ha a Kaspersky alkalmazása egy nem fertőzött objektumot fertőzöttnek tekint, mivel az aláírása hasonló egy víruséhoz.

Trusted Platform Module

Egy biztonsághoz kapcsolódó alapvető funkciók nyújtására (például titkosítási kulcsok tárolására) szolgáló mikrocsip. A Trusted Platform Module általában a számítógép alaplapján helyezkedik el, és a rendszer többi összetevőjével a hardverbuszon keresztül lép kapcsolatba.

Védelem hatóköre

Futás közben a Fenyegetések elleni alapvető védelem összetevő által folyamatosan vizsgált objektumok. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak.

Vírusadatbázisok

Olyan adatbázisok, amelyek információkat tartalmaznak a kiadásuk napján a Kaspersky által ismert számítógépes biztonsági fenyegetésekre vonatkozóan. Az antivírus adatbázisokban lévő aláírások lehetővé teszik a kártékony kódok észlelését a vizsgált objektumokban. Az antivírus adatbázisokat a Kaspersky szakértői hozzák létre, és óránként frissülnek.

Vírusmentesítés

A fertőzött objektumok feldolgozására használt módszer, amely az adatok teljes vagy részleges helyreállítását eredményezi. Nem minden fertőzött objektum vírusmentesíthető.

Vizsgálat hatóköre

A Kaspersky Endpoint Security által a vizsgálati feladat végzése során vizsgált objektumok.

Webes erőforrás címének normalizált formája

A webes erőforrás címének normalizált formája a webes erőforrás címének szöveges ábrázolása, mely normalizálással áll elő. A *normalizálás* az a folyamat, melynek során a webes erőforrás címének szöveges ábrázolása adott szabályok alapján (például a felhasználói bejelentkezési név, jelszó és csatlakozási port webes erőforrás címének szöveges ábrázolásából való kizárásával, továbbá a webes erőforrás címének nagybetűsről kisbetűssé alakításával) megváltozik.

Tekintettel a védelmi összetevők működésére, a webes erőforrások címének normalizálása során az a cél, hogy ne kerüljön sor többször olyan webhelyek címeinek vizsgálatára, amelyek szintaxisa eltérő, de fizikailag azonosak.

Példa:

Egy cím nem normalizált formája: www.Pelda.com\.

A cím normalizált formája: www.pelda.com.

Függelékek

Ez a rész a dokumentum törzsének kiegészítő információit tartalmazza.

1. melléklet Alkalmazásbeállítások

A Kaspersky Endpoint Security konfigurálására használhatja a házirendet, a feladatokat vagy az alkalmazás felületét. Az alkalmazás összetevőinek részletes információi a megfelelő részekben találhatóak.

Fájl védelem

A Fájl védelem összetevő lehetővé teszi a számítógép fájlrendszerében a fertőzések megelőzését. Alapértelmezés szerint a Fájl védelem összetevő állandóan a számítógép RAM-jában található, és valós időben vizsgálja az összes megnyitott, mentett és futtatott fájlt. Ez az összetevő megvizsgálja a számítógép összes meghajtóján lévő fájlokat, beleértve a csatlakoztatott meghajtókat is. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

Az összetevő megvizsgálja a felhasználó és az alkalmazás által elért fájlokat. Ha az alkalmazás kártékony fájlt észlel, a Kaspersky Endpoint Security blokkolja a fájl működését. Az alkalmazás ezután kártevőmentesíti vagy törli a kártékony fájlt a „Fájl védelem" összetevő beállításainak megfelelően.

Amikor egy olyan fájlhoz próbál hozzáférni, amelynek tartalma OneDrive felhőalapú tárhelyen található, a Kaspersky Endpoint Security letölti és megvizsgálja a fájl tartalmát.

A Fájl védelem összetevő beállításai

Paraméter	Leírás
Biztonsági szint *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A Fájl védelemhez a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezek az alkalmazásban tárolt beállításcsoportokat *biztonsági szinteknek* nevezzük: • **Magas**. A Fájl védelem összetevő ennél a fájlbiztonsági szintnél ellenőrzi a legszigorúbban a megnyitott, mentett és elindított fájlokat. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján lévő összes fájltípust megvizsgálja. Ezenkívül vizsgálja az archívumokat, a telepítőcsomagokat és a beágyazott OLE-objektumokat is. • **Ajánlott**. A Kaspersky Lab szakértői ezt a fájlbiztonsági szintet ajánlják. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján csak a megadott fájlformátumokat és a beágyazott OLE objektumokat vizsgálja meg. A Fájl védelem összetevő nem vizsgálja az archívumokat és a telepítőcsomagokat. • **Alacsony**. E fájlbiztonsági szint beállításai biztosítják a maximális vizsgálati sebességet. A Fájl védelem összetevő a számítógép összes merevlemezén, cserélhető meghajtóján és hálózati meghajtóján csak a megadott kiterjesztésű fájlokat vizsgálja meg. A Fájl védelem összetevő nem vizsgálja az összetett fájlokat.
Fájltípusok *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	**Minden fájl**. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül). **Formátum alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejlécet a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres. **Kiterjesztés alapján vizsgált fájlok**. Ha ez a beállítás van kiválasztva, az alkalmazás csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.

Paraméter	Leírás
Vizsgálat hatóköre	Azon objektumokat tartalmazza, amelyeket megvizsgál a Fájl védelem összetevő. A vizsgálati objektum lehet merevlemez, cserélhető meghajtó, hálózati meghajtó, mappa, fájl vagy több fájlt meghatározó maszk. Alapértelmezés szerint a Fájl védelem összetevő minden, a merevlemezen, a hálózati meghajtókon vagy cserélhető meghajtón elindított fájlt megvizsgál. Az ilyen objektumok védelmi hatókörét nem lehet módosítani vagy törölni. Csak objektumot (például cserélhető meghajtót) zárhat ki a vizsgálat alól.
Gépi tanulás és aláíráselemzés *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A gépi tanulási és aláírás-elemzési módszer a Kaspersky Endpoint Security adatbázisait használja, melyek az ismert fenyegetések leírásait és semlegesítésük módszereit tartalmazzák. Az ezt a módszert alkalmazó védelem biztosítja a minimális elfogadható biztonsági szintet. A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.
Heurisztikus elemzés *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
Művelet fenyegetés észlelésekor	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, az alkalmazás törli a fájlt. **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ennek a lehetőségnek a kiválasztása esetén az alkalmazás automatikusan megpróbálja az észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés sikertelen, az alkalmazás blokkolja a fájlt. **Blokkolás**. Ha ezt a beállítást választja, az alkalmazás automatikusan blokkolja a fertőzött fájlt anélkül, hogy megpróbálná vírusmentesíteni vagy törölni azt. Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, az alkalmazás létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.
Csak új és módosult fájlok vizsgálata	Csak az új fájlokat és azokat a fájlokat vizsgálja, amelyeket a legutóbbi vizsgálatuk óta módosítottak. Ez csökkenti a vizsgálat idejét. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.
Archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.
Terjesztési csomagok vizsgálata	Harmadik féltől származó alkalmazások terjesztőcsomagjainak vizsgálata.
Microsoft Office formátumú fájlok vizsgálata	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.
E-mail formátumú fájlok vizsgálata	E-mail formátumú fájlok vizsgálata. Az alkalmazás megvizsgálja az MSG és EML típusú fájlokat. Az e-mail formátumú fájlok az OLE-objektumokat és MHT-fájlokat is magukban foglalják. A Kaspersky Endpoint Security megvizsgálja az archívumokból kibontott, 1 MB-nál kisebb, e-mail formátumú fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.
Ne csomagoljon ki nagy összetett fájlokat	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás minden összetett fájlt megvizsgál. Az alkalmazás megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.

Paraméter	Leírás
Összetett fájlok kicsomagolása a háttérben	Ha a jelölőnégyzet be van jelölve, az alkalmazás hozzáférést biztosít az összetett fájlokhoz, amelyek mérete meghaladja a fájlvizsgálatban meghatározott méret értékét. Ilyenkor a Kaspersky Endpoint Security a háttérben csomagolja ki és vizsgálja meg az összetett fájlokat. Az alkalmazás csak e fájlok kicsomagolása és vizsgálata után biztosít hozzáférést az ennél kisebb méretű összetett fájlokhoz. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás csak akkor biztosít hozzáférést bármilyen méretű fájlhoz, ha kicsomagolta és átvizsgálta a fájlokat.
Vizsgálat módja *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A Kaspersky Endpoint Security a felhasználó, az operációs rendszer vagy a felhasználó fiókja alatt futó alkalmazások által elért fájlokat vizsgálja. **Intelligens mód**. Ebben a módban a Fájl védelem az objektumot az azon végzett műveletek elemzése alapján vizsgálja meg. Ha például egy Microsoft Office dokumentummal dolgozik, a Kaspersky Endpoint Security a fájlt első megnyitásakor és utolsó bezárásakor vizsgálja meg. A fájlt felülíró köztes műveletek nem váltanak ki vizsgálatot. **Hozzáféréskor és módosításkor**. Ebben a módban a Fájl védelem megnyitási és módosítási kísérletek esetén mindig megvizsgálja az objektumokat. **Hozzáféréskor**. Ebben a módban a Fájl védelem az objektumokat csak a megnyitási kísérletek esetén vizsgálja meg. **Végrehajtáskor**. Ebben a módban a Fájl védelem az objektumokat csak a futtatási kísérletek esetén vizsgálja meg.
Használja az iSwift technológiát *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iSwift technológia az iChecker technológia továbbfejlesztése az NTFS fájlrendszer számára.
Használja az iChecker technológiát *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia lehetővé teszi a vizsgálat sebességének megnövelését bizonyos fájlok vizsgálatból való kihagyásával. A fájlok vizsgálatból való kizárása egy különleges algoritmus alapján történik, mely figyelembe veszi a Kaspersky Endpoint Security adatbázisok kiadásának dátumát, a fájl legutóbbi vizsgálatának dátumát, valamint a vizsgálati beállításokon végzett módosításokat. Az iChecker technológiának vannak korlátozásai is: nem működik nagy méretű fájlokkal, és csak olyan fájlokra érvényes, amelyek felépítését az alkalmazás felismeri (például EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP és RAR).
Fájl védelem szüneteltetése *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez ideiglenesen és automatikusan szünetelteti a Fájl védelem működését a megadott időpontban, vagy a megadott alkalmazásokkal való munka során.
A Windows-tárolókban végrehajtott fájlműveletek vizsgálata	Ha a rendszer fenyegetést észlel egy tárolón belül, az alkalmazás alkalmazza a a Fájl védelem összetevőhöz kiválasztott művelet. **A tároló leállítása, ha a vírusmentesítés sikertelen**. Előfordulhat, hogy az alkalmazás nem rendelkezik elegendő olvasási és írási jogosultsággal az észlelt objektumnál. Ebben az esetben az észlelt objektum vírusmentesítése vagy törlése nem lehetséges. Ha ez a jelölőnégyzet be van jelölve, az alkalmazás blokkolja az észlelt objektumot, és leállítja a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás csak az észlelt objektumot blokkolja. **Ne vizsgálja a Windows-tárolókban végrehajtott fájlműveleteket**. Ha ez a négyzet be van jelölve, az alkalmazás csak a tároló indításakor vizsgálja meg a tárolót. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás folyamatosan, valós időben vizsgálja a tárolót.

Web védelem

A Web védelem összetevő megelőzi, hogy rosszindulatú fájlok legyenek letöltve az internetről, valamint blokkolja a rosszindulatú és az adathalász weboldalakat. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

A Kaspersky Endpoint Security csak a HTTP, HTTPS és az FTP forgalmat figyeli meg. A Kaspersky Endpoint Security vizsgálja az URL-eket és az IP-címeket.

A Webfelügyelő használatához el kell végeznie az alkalmazás kezdeti konfigurálását:

- A HTTPS forgalom figyeléséhez, engedélyezze a titkosított kapcsolatok vizsgálatát (alapértelmezés szerint engedélyezve van).
- Válassza ki azokat a portokat, amelyeket a Kaspersky Endpoint Security megoldásnak figyelnie kell (alapértelmezés szerint az alkalmazás az összes portot figyeli).
- Válassza ki azokat az alkalmazásokat, amelyeknek a forgalmát a Kaspersky Endpoint Securityvel meg szeretné figyelni. A legtöbb böngésző már szerepel a Kaspersky által ajánlott alkalmazások listáján. Ha a böngészője hiányzik a listáról, adja hozzá manuálisan.
- Javasoljuk, hogy illesszen be egy weboldal-interakciós parancsfájlt a webes forgalomba (alapértelmezés szerint a parancsfájl beillesztése le van tiltva). Ez a parancsfájl lehetővé teszi a Web védelem eseményeinek regisztrációját az alkalmazás eseménynaplójában, az operációs rendszer eseménynaplójában és a jelentésekben.

Ha a felhasználó rosszindulatú vagy adathalász weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést és figyelmeztetést jelenít meg.

A Web védelem összetevő beállításai

Paraméter	Leírás
Biztonsági szint *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A Web védelemhez az alkalmazás különböző beállításcsoportokat alkalmazhat. Ezek az alkalmazásban tárolt beállításcsoportokat *biztonsági szinteknek* nevezzük: • **Magas**. Az a biztonsági szint, amely mellett a Web védelem a számítógépre HTTP-n és FTP-n keresztül érkező webes forgalom maximális vizsgálatát végzi. A Web védelem átfogó vizsgálatot végez minden objektumon az összes alkalmazás-adatbázis használatával, és elvégzi a lehető legalaposabb heurisztikus elemzést. • **Ajánlott**. Az alkalmazás teljesítménye és a webes forgalom biztonsága közti optimális egyensúlyt garantáló biztonsági szint. A Web védelem összetevő heurisztikus elemzése közepes vizsgálat szinten üzemel. A Kaspersky szakemberei ezt a webes forgalmi biztonsági szintet ajánlják. • **Alacsony**. A webes forgalom biztonsági szintjének ezen beállításai biztosítják a webes forgalom vizsgálatának maximális sebességét. A Web védelem összetevő heurisztikus elemzése egyszerű vizsgálat szinten üzemel.
Művelet fenyegetés észlelésekor	**Blokkolás**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Web védelem blokkolja az objektumhoz való hozzáférést, és üzenetet jelenít meg a böngészőben. **Tájékoztatás**. Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Kaspersky Endpoint Security engedélyezi az objektum letöltését a számítógépre, de a fertőzött objektumra vonatkozó információt fűz hozzá az aktív fenyegetések felsorolásához.
A webcím ellenőrzése a rosszindulatú webcímek adatbázisában *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A webes címek rosszindulatú URL-ek adatbázisában való ellenőrzésével nyomon követheti az elutasítási listához hozzáadott webhelyeket. A rosszindulatú webcímek adatbázisát a Kaspersky tartja karban, és az megtalálható az alkalmazás telepítőcsomagjában, továbbá a Kaspersky Endpoint Security adatbázisainak frissítésekor frissül.
Heurisztikus elemzés használata *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor a heurisztikus elemző vírusokat és más, fenyegetést jelentő alkalmazásokat keres a webes forgalomban, utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.

Paraméter	Leírás
A webcím ellenőrzése az adathalász webcímek adatbázisában *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Az adathalász webcímek adatbázisában megtalálhatók az adathalász támadások indítására használt, jelenleg ismert webhelyek webcímei. A Kaspersky az adathalász hivatkozások ezen adatbázisát egy az Anti-Phishing Working Groupként ismert nemzetközi szervezettől származó címekkel egészíti ki. Az adathalász webcímek adatbázisa megtalálható az alkalmazás telepítőcsomagjában, és a Kaspersky Endpoint Security adatbázisainak frissítésekor kiegészül.
Ne vizsgálja a megbízható webcímekről érkező webes forgalmat	Ha az opció be van jelölve, a Web védelem összetevő nem vizsgálja az olyan weboldalak/webhelyek tartalmát, amelyek címe szerepel a megbízható webcímek listáján. A megbízható webcímek listájára a megadott weboldal/webhely címét, illetve címmaszkját egyaránt felveheti. A titkosított kapcsolatokra vonatkozó kizárások általános listáját is létrehozhatja. Ebben az esetben a Kaspersky Endpoint Security nem vizsgálja a megbízható webcímek HTTPS-forgalmát, amikor a Web védelem, a Levelezés védelem és a Webfelügyelő összetevők végzik a munkájukat.

Levelezés védelem

A „Levelezés védelem" összetevő a bejövő és kimenő e-mail üzenetek mellékleteiben vizsgálja a vírusok és egyéb fenyegetések jelenlétét. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

A Levelezés védelem a bejövő és a kimenő üzeneteket is képes megvizsgálni. Az alkalmazás támogatja a POP3, SMTP, IMAP és NNTP protokollokat a következő levelezőprogramokban:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

A Mozilla Thunderbird, MyOffice Mail és R7-Office Organizer levelezőprogramok forgalmának vizsgálatához hozzá kell adnia a Kaspersky tanúsítványt a tanúsítványtárolóhoz, és ki kell választania a saját tanúsítványtárolót.

A Levelezés védelem nem támogat más protokollokat és levelezőprogramokat.

A Levelezés védelem nem mindig képes *protokollszintű* hozzáférést biztosítani az üzenetekhez (például a Microsoft Exchange megoldás használata esetén). Emiatt a Levelezés védelem tartalmaz egy bővítményt a Microsoft Office Outlookhoz. A bővítmény lehetővé teszi az üzenetek vizsgálatát a *levelezőprogram szintjén*. A Levelezés védelem bővítmény az Outlook 2010, 2013, 2016, 2019, 2021, 2024 és 365 32 bites és 64 bites verzióit támogatja. Az ARM-alapú számítógépeken a Levelezés védelem bővítmény az Outlook 2016, az Outlook 2021, az Outlook 2024 és az Outlook 365 for Arm64 32 bites és 64 bites verzióit támogatja.

A „Levelezés védelem" összetevő nem vizsgálja az üzeneteket, ha a levelezési ügyfélprogram böngészőben van megnyitva.

Egy rosszindulatú fájl csatolmányban történő észlelése esetén a Kaspersky Endpoint Security egy, a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Az üzenet feldolgozása megtörtént] <üzenet tárgysora>*.

Paraméter	Leírás
Biztonsági szint *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A Levelezés védelemhez az alkalmazás különböző beállításcsoportokat alkalmazhat. Ezek az alkalmazásban tárolt beállításcsoportokat *biztonsági szinteknek* nevezzük: • **Magas**. Ha ez az e-mail-biztonsági szint van kiválasztva, a Levelezés védelem összetevő a legalaposabban vizsgálja meg az e-mail-üzeneteket. A Levelezés védelem összetevő megvizsgálja a bejövő és kimenő e-mail-üzeneteket, és mély heurisztikus elemzést végez. A Magas levelezés biztonsági szint a magas kockázatú környezetekhez ajánlott. Például ilyen környezet egy ingyenes e-mail szolgáltatáshoz történő csatlakozás központi e-mail védelemmel nem rendelkező otthoni hálózatból. • **Ajánlott**. Az alkalmazás teljesítménye és az e-mail-biztonság közti optimális egyensúlyt garantáló biztonsági szint. A Levelezés védelem összetevő megvizsgálja a bejövő és kimenő e-mail-üzeneteket, és közepes szintű heurisztikus elemzést végez. Ezt a levélforgalmi biztonsági szintet ajánlják a Kaspersky szakemberei. • **Alacsony**. Ennél az e-mail-biztonsági szintnél a Levelezés védelem összetevő csak a bejövő e-mail üzeneteket vizsgálja, egyszerű heurisztikus elemzést végez, és nem vizsgálja az e-mail üzenetekhez mellékelt archívumokat. Ennél az e-mail-biztonsági szintnél a Levelezés védelem összetevő az e-mail üzenetek elemzését maximális sebességgel, az operációs rendszer erőforrásainak minimális kihasználása mellett végzi. Jól védett környezetben Alacsony e-mail-biztonsági szint ajánlott. Ilyen környezet lehet például a központi e-mail védelemmel rendelkező vállalati helyi hálózat.
Művelet fenyegetés észlelésekor	**Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás törli a fertőzött objektumot. Az alkalmazás a végrehajtott művelettel kapcsolatosan információt fűz az üzenet tárgysorához, például *[Üzenet fel lett dolgozva] <üzenet tárgysora>*. **Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül**. Ha fertőzött objektumot észlel egy bejövő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel egy kimenő üzenetben, az alkalmazás megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg. **Blokkolás**. Ha fertőzött objektumot észlel valamely bejövő üzenetben, az alkalmazás figyelmeztetést fűz az üzenet tárgysorához. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, az alkalmazás letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.
Védelem hatóköre *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	A *védelem hatóköre* magában foglalja azokat az objektumokat, amelyeket az összetevő a futtatáskor ellenőriz: bejövő és kimenő üzenetek vagy csak bejövő üzenetek. A számítógép védelméhez csak a bejövő üzeneteket kell megvizsgálni. Bekapcsolhatja a kimenő üzenetek vizsgálatát is, hogy megakadályozza a fertőzött fájlok archívumokban történő továbbítását. A kimenő üzenetek vizsgálatát akkor is bekapcsolhatja, ha meg akarja akadályozni, hogy bizonyos formátumú fájlok – például hang- és videofájlok – kerüljenek küldésre.
POP3, SMTP, NNTP és IMAP forgalom vizsgálata	Olyan forgalom Levelezés védelem összetevő általi vizsgálata, amelynek átvitele POP3, SMTP, NNTP és IMAP protokollal történik.
Microsoft Outlook-bővítmény csatlakoztatása	Ha a jelölőnégyzetben van jelölés, a POP3, az SMTP, az NNTP és az IMAP protokollal továbbított e-mail üzenetek vizsgálata a Microsoft Outlookba beépített bővítmény oldalán van engedélyezve. Ha az e-mailek vizsgálata a Microsoft Outlook bővítményével történik, akkor javasoljuk a Cached Exchange Mode használatát. A gyorsítótáras Exchange móddal kapcsolatban további információ, valamint a használatára vonatkozó ajánlások a Microsoft Tudásbázisban találhatók.
Heurisztikus elemzés *(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)*	Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve. Amikor rosszindulatú kódokat keres a fájlokban, a heurisztikus elemző utasításokat hajt végre a futtatható fájlokban. A heurisztikus elemző által végrehajtott utasítások száma a heurisztikus elemző számára megadott szinttől függ. A heurisztikus elemzés szintje állítja be az új fenyegetések vizsgálatának alapossága, az operációs rendszer erőforrásinak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
Csatolt archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését. Ha a vizsgálat során az alkalmazás egy archívum jelszavát észleli az üzenet szövegében, ezt a jelszót használja fel, hogy az archívumban rosszindulatú alkalmazásokat keressen. Ebben az esetben a jelszó nem kerül mentésre. A vizsgálat során az archívum ki lett csomagolva. Ha a kicsomagolási folyamat során alkalmazáshiba lép fel, manuálisan törölheti a kicsomagolt fájlokat, amelyek mentése a következő elérési útvonalon történik: %systemroot%\temp. A fájlok PR előtaggal rendelkeznek.
Microsoft Office formátumú csatolt fájlok vizsgálata	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.

Paraméter	Leírás
Ne legyen archívumok vizsgálata, ha a méret nagyobb, mint N MB	Ha ez a jelölőnégyzet be van jelölve, a Levelezés védelem összetevő a vizsgálatból kizárja azokat az e-mail üzenetekhez mellékelt archívumokat, melyeknek a mérete meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, a Levelezés védelem összetevő minden méretű e-mailhez mellékelt archívumot megvizsgál.
Archívumok ellenőrzésének korlátozása N másodpercre	Ha a jelölőnégyzet be van jelölve, akkor az e-mail üzenetekhez mellékelt archívumok vizsgálatára kijelölt időtartam a megadott időre korlátozódik.
Mellékletszűrő	A mellékletszűrő nincs alkalmazva a kimenő e-mail-üzenetekre. **Szűrés letiltása**. Ha ez az opció van kiválasztva, a Levelezés védelem összetevő nem szűri az e-mail üzenetekhez csatolt fájlokat. **Kiválasztott típusú mellékletek átnevezése**. Ha ezt a lehetőséget választja, a Levelezés védelem összetevő a megadott típusú csatolt fájlok kiterjesztésének utolsó karakterét aláhúzásjellel helyettesíti (például melléklet.doc_). Így a fájl megnyitásához a felhasználónak át kell neveznie a fájlt. **Kiválasztott típusú mellékletek törlése**. Ha ez az opció van kiválasztva, a Levelezés védelem összetevő törli az e-mail üzenetekből a megadott típusú mellékelt fájlokat. A fájlmaszkok listájában megadhatja az e-mail üzenetekben átnevezni vagy törölni kívánt csatolt fájlok típusait.

Hálózati védelem

A *Hálózati védelem* összetevő (más néven Intrusion Detection System, IDS) figyeli a bejövő hálózati forgalmat a hálózati támadásokra jellemző tevékenységek szempontjából. Ha az alkalmazás hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában. Az alkalmazás-adatbázisok tartalmazzák a már ismert hálózati támadások típusainak és az elhárításuk módszereinek leírását. A Hálózati védelem összetevő által észlelhető hálózati támadások listája az alkalmazás adatbázisainak és alkalmazásmoduljainak frissítésekor frissül.

A Hálózati védelem összetevő beállításai

Paraméter	Leírás
Portkeresés és hálózati elárasztás támadásként történő kezelése	A *hálózati elárasztás* a vállalat hálózati erőforrásainak (például webkiszolgálók) megtámadását jelenti. A támadás abból áll, hogy nagyszámú kérésekkel túlterhelik a hálózati erőforrások sávszélességét. Ilyenkor a felhasználók nem tudnak hozzáférni a vállalat hálózati erőforrásaihoz. A *portkereséses támadás* az UDP-portok, a TCP-portok és a számítógép hálózati szolgáltatásainak vizsgálatából áll. Lehetővé teszi a támadónak, hogy azonosítsa a számítógép sebezhetőségének mértékét, mielőtt veszélyesebb hálózati támadásokat hajtana végre. A portkereséssel a támadó a számítógépen lévő operációs rendszert is képes azonosítani, és kiválaszthatja az adott operációs rendszernek megfelelő hálózati támadásokat. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security figyeli a hálózati forgalmat az ilyen támadások észlelése céljából. Ha támadást észlel, az alkalmazás értesíti a felhasználót, és elküldi a megfelelő eseményt a Kaspersky Security Center számára. Az alkalmazás információkat szolgáltat a támadó számítógépről, amelyek szükségesek a fenyegetések időben történő elhárításához. Letilthatja az ilyen típusú támadások észlelését, ha az engedélyezett alkalmazások egy része ilyen típusú támadásokra jellemző műveleteket hajt végre. Ez segít elkerülni a téves riasztásokat.
Támadó eszközök blokkolása N percre	Ha a funkció engedélyezve van, a Hálózati védelem összetevő a támadó számítógépet felveszi a blokkolási listára. Ez azt jelenti, hogy a Hálózati védelem összetevő az első hálózati támadási próbálkozást követően a megadott ideig blokkolja a támadó számítógép hálózati kapcsolatát. A blokkolás automatikusan védi a felhasználó számítógépét az ugyanerről a címről érkező lehetséges további hálózati támadásoktól. A támadó számítógépnek legalább egy percet kell eltöltenie a blokkoltak listáján. A maximális időtartam 999 perc. A tiltólistát a Hálózatfigyelő eszköz ablakában tekintheti meg. A Kaspersky Endpoint Security törli a tiltólistát az alkalmazás újraindításakor és a Hálózati védelem beállításainak megváltoztatásakor.

Paraméter	Leírás
Kizárások	Ez a lista azokat az IP-címeket tartalmazza, amelyeken a Hálózati védelem a hálózati támadásokat nem blokkolja. Hozzáadhat egy IP-címet megadott porttal és protokollal. Az alkalmazás nem naplózza az olyan IP címekről érkező hálózati támadások információit, amik a kizárások listájában szerepelnek.
MAC-cím hamisítása elleni védelem	A *MAC-hamisítási támadás* a hálózati eszköz (hálózati kártya) MAC-címének megváltoztatásával történik. Ennek eredményeképpen a támadó átirányíthatja az eszköznek küldött adatokat másik eszközre, és hozzáférhet ezekhez az adatokhoz. A Kaspersky Endpoint Security segítségével blokkolhatja a MAC-hamisítási támadásokat, valamint értesítést kaphat a támadásokról.

Tűzfal

A Tűzfal blokkolja a jogosulatlan kapcsolódási kísérleteket a számítógépen az interneten vagy a helyi hálózaton végzett munka során. A Tűzfal felügyeli a számítógépen futó alkalmazások hálózati tevékenységét is. Ez lehetővé teszi, hogy védje a vállalat helyi hálózatát a személyes adatok ellopásával és más támadásokkal szemben. Az összetevő antivírus adatbázisok, a Kaspersky Security Network felhőszolgáltatás és előre definiált *hálózati szabályok.* segítségével biztosít védelmet a számítógépnek.

A Hálózati ügynök a Kaspersky Security Centerrel való kommunikációra szolgál. A Tűzfal automatikusan létrehozza az alkalmazás és a hálózati ügynök működéséhez szükséges hálózati szabályokat. Ennek eredményeként a Tűzfal több portot nyit meg a számítógépen. A megnyitott portok a számítógép szerepkörétől függenek (például terjesztési pont). Ha többet szeretne megtudni a számítógépen megnyíló portokról, olvassa el a Kaspersky Security Center súgóját.

Hálózati szabályok

A hálózati szabályokat a következő szinteken konfigurálhatja:

- *Hálózati csomagszabályok.* A hálózati csomagszabályok a hálózati csomagokat alkalmazástól függetlenül korlátozzák. Ezek a szabályok korlátozzák a bejövő és kimenő hálózati forgalmat a kiválasztott adatprotokoll adott portjain. A Kaspersky Endpoint Security alkalmazásban előre definiált hálózatiadatcsomag-szabályok érhetők el, a Kaspersky szakértői által javasolt jogosultságokkal.

- *Alkalmazás hálózati szabályai.* Az alkalmazások hálózati szabályai adott alkalmazások hálózati tevékenységét korlátozzák. Nem csupán a hálózati csomag jellemzőit veszik figyelembe, hanem azt a konkrét alkalmazást is, amelynek a hálózati csomag címezve van, illetve amely a hálózati csomagot elküldte.

Az alkalmazások szabályozott hozzáférést kapnak az operációs rendszer erőforrásaihoz, a folyamatokhoz és a személyes adatokhoz, amit a Behatolásmegelőző rendszer összetevő biztosít *alkalmazásjogok* használatával.

Az alkalmazás első indítása során a Tűzfal a következő műveleteket hajtja végre:

1. Ellenőrzi az alkalmazás biztonságát letöltött antivírus adatbázisok segítségével.

2. Ellenőrzi az alkalmazás biztonságát a Kaspersky Security Networkben.

   Javasoljuk, hogy vegyen részt a Kaspersky Security Networkben, amivel segíthet hatékonyabbá tenni a Tűzfal működését.

3. Az alkalmazást a megbízhatósági csoportok valamelyikébe helyezi: *Megbízható*, *Alacsony korlátozás*, *Magas korlátozás*, *Nem megbízható*.

   A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére használ. A Kaspersky Endpoint Security egy alkalmazást az alapján helyez megbízhatósági csoportba, hogy az alkalmazás milyen veszélyességi szintet képvisel a számítógép szempontjából.

   A Kaspersky Endpoint Security az alkalmazásokat a Tűzfal és a Behatolásmegelőző rendszer összetevő számára helyezi megbízhatósági csoportba. Nem lehet módosítani a megbízhatósági csoportot kizárólag a Tűzfal vagy a Behatolásmegelőző rendszer esetében.

   Ha nem vesz részt a KSN rendszerében vagy nincs hálózat, a Kaspersky Endpoint Security a Behatolásmegelőző rendszer összetevő beállításai alapján helyezi az alkalmazást megbízhatósági csoportba. Miután megérkezett az alkalmazás megítélése a KSN hálózattól, a rendszer automatikusan módosíthatja az alkalmazás megbízhatósági csoportját.

4. Blokkolja az alkalmazás hálózati tevékenységét a megbízhatósági csoportba tartozása alapján. Például a *Magas korlátozás* megbízhatósági csoportba tartozó alkalmazások egyáltalán nem használhatnak hálózati kapcsolatot.

Az alkalmazás következő indításakor a Kaspersky Endpoint Security ellenőrzi annak integritását. Amennyiben az alkalmazás nem változott meg, az összetevő az aktuális hálózati szabályokat alkalmazza. Ha az alkalmazás módosult, a Kaspersky Endpoint Security ugyanúgy végigelemzi, mintha az első elindítására kerülne sor.

A hálózati szabályok fontossági sorrendje

Minden szabálynak van valamilyen prioritása. Minél magasabban helyezkedik el egy szabály a szabályok listáján, annál magasabb a prioritása. Ha egy hálózati tevékenység több szabályhoz is társítva van, a Tűzfal a legmagasabb prioritású szabálynak megfelelően szabályozza a hálózati tevékenységet.

A hálózati csomagszabályok prioritása magasabb, mint az alkalmazások hálózati szabályaié. Ha ugyanazon típusú hálózati tevékenységre csomagszabályok és alkalmazásszabályok is meg vannak adva, a hálózati tevékenységet a csomagszabályok fogják szabályozni.

Az alkalmazások hálózati szabályai meghatározott módon működnek. Az alkalmazásokhoz tartozó hálózati szabály a hálózati állapot alapján foglal magában hozzáférési szabályokat: *nyilvános hálózat*, *helyi hálózat* vagy *megbízható hálózat*. Például a *Magas korlátozás* megbízhatósági csoportban lévő alkalmazások esetében alapértelmezetten minden hálózati állapotban le van tiltva a hálózati tevékenység. Ha egy hálózati szabály meg van adva egy egyéni alkalmazásra (szülőalkalmazásra) vonatkozóan, akkor az egyéb alkalmazások gyermekfolyamatai a szülőalkalmazás hálózati szabálya szerint fognak futni. Ha az alkalmazásnak nincs hálózati szabálya, az utódfolyamatok az alkalmazás megbízhatósági csoportjának hálózati szabálya szerint fognak futni.

Példa: Ön az alkalmazások számára az összes hálózati állapotban letiltotta a hálózati tevékenységet, kivéve az X böngésző számára. Ha az X böngészőből (szülőalkalmazás) elindítja az Y böngésző telepítését (gyermekfolyamat), az Y böngésző telepítője hozzáfér az internethez, és letölti a szükséges fájlokat. A telepítés után az Y böngésző a Tűzfal beállításai miatt nem fogja tudni elérni a hálózati kapcsolatokat. Ahhoz, hogy Ön az Y böngésző telepítője (gyermekfolyamat) számára megtiltsa a hálózati tevékenységet, hozzá kell adnia egy hálózati szabályt az Y böngésző telepítőjéhez.

Hálózati kapcsolati típusok

A Tűzfal lehetővé teszi Önnek a hálózat tevékenység felügyeletét a hálózati kapcsolat típusától függően. A Kaspersky Endpoint Security a számítógép operációs rendszerétől kapja meg a hálózati kapcsolatok típusát. Az operációs rendszerben a hálózati kapcsolat típusát a felhasználó szabhatja meg a kapcsolat létrehozásakor. Lehetősége van megváltoztatni a hálózati kapcsolat típusát a Kaspersky Endpoint Security beállításai között. A Tűzfal a Kaspersky Endpoint Security beállításaiban, és nem az operációs rendszerben megadott hálózattípustól függően figyeli a hálózati tevékenységet.

A következő hálózati kapcsolattípusok érhetők el:

- **Nyilvános hálózat**. A hálózatot nem védi víruskereső alkalmazás, tűzfal és szűrő (például wifi egy kávézóban). Az ilyen hálózathoz kapcsolódó számítógép felhasználója számára a Tűzfal blokkolja a számítógép fájljaihoz és nyomtatóihoz való hozzáférést. A külső felhasználók megosztott mappákon keresztül sem férhetnek hozzá adatokhoz, illetve a számítógép asztalához sincs távoli hozzáférésük. A Tűzfal az egyes alkalmazások hálózati tevékenységét az azokhoz beállított hálózati szabályok alapján szűri ki.

  A Tűzfal alapértelmezés szerint az internetnek *Nyilvános hálózat* típust oszt ki. Az internet típusa nem módosítható.

- **Helyi hálózat**. Hálózat olyan felhasználóknak, akik korlátozott hozzáféréssel rendelkeznek a jelen számítógép fájljaihoz és nyomtatóihoz (például vállalati LAN vagy otthoni hálózat).

- **Megbízható hálózat**. Biztonságos hálózat, amelyen a számítógép nincs kitéve támadásoknak, sem az adatok illetéktelen elérésére irányuló próbálkozásoknak. A Tűzfal az ilyen állapotú hálózaton belül minden hálózati tevékenységet engedélyez.

A Tűzfal összetevő beállításai

Paraméter	Leírás
Csomagszabályok	A hálózati csomagszabályok listáját tartalmazó táblázat. A hálózati csomagszabályok a hálózati csomagok alkalmazástól független korlátozására szolgálnak. Ezek a szabályok korlátozzák a bejövő és kimenő hálózati forgalmat a kiválasztott adatprotokoll adott portjain. A táblázatban a Kaspersky által a Microsoft Windows operációs rendszereket futtató számítógépek hálózati forgalmának optimális védelme érdekében ajánlott előre beállított hálózati csomagszabályok szerepelnek. Az egyes hálózati csomagszabályok végrehajtási prioritását a Tűzfal szabja meg. A Tűzfal a hálózati csomagszabályokat abban a sorrendben dolgozza fel, ahogy fentről lefelé a hálózati csomagszabályok listáján elhelyezkednek. A Tűzfal megkeresi a hálózati kapcsolatra vonatkozó legfelső hálózati csomagszabályt, és az érintett hálózati tevékenység engedélyezése, illetve blokkolása formájában végrehajtja. A Tűzfal ezután minden más hálózati csomagszabályt ignorál az adott hálózati kapcsolathoz. A hálózati csomagszabályok prioritása magasabb, mint az alkalmazások hálózati szabályaié.
Elérhető hálózatok	Ebben a táblázatban információk találhatók a Tűzfal által a számítógépen észlelt hálózati kapcsolatokról. Alapértelmezés szerint az internet *Nyilvános hálózat* állapotot kap. Az internet állapota nem módosítható.
Szabályok az alkalmazásokhoz	**Alkalmazás**. A „Tűzfal” összetevő által felügyelt alkalmazások táblázata. Az alkalmazások megbízhatósági csoportokba vannak besorolva. A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security használ az alkalmazások hálózati tevékenységének felügyelete során. Lehetősége van kiválasztani egy alkalmazást a számítógépeken telepített összes alkalmazás egyszerű felsorolásából valamely rendszabály alapján, majd felvenni az alkalmazást egy megbízható csoportba. **Hálózati szabályok**. Valamely megbízható csoportba tartozó alkalmazások hálózati szabályainak táblázata. Ezen szabályoknak megfelelően a Tűzfal szabályozza az alkalmazások hálózati tevékenységét. A táblázatban szerepelnek a Kaspersky szakértői által javasolt, előre definiált hálózati szabályok. Ezek a hozzáadott hálózati szabályok optimális védelmet nyújtanak a Windows operációs rendszert futtató számítógépek hálózati adatforgalmának. Az előre definiált hálózati szabályok törlésére nincs mód.

BadUSB védelem

Egyes vírusok az USB eszközök firmware-ét módosítva becsapják az operációs rendszert, így az az USB eszközt billentyűzetként észleli. Ennek eredményeképpen a vírus parancsokat hajthat végre az Ön felhasználói fiókja alatt, például rosszindulatú programok letöltésére.

A BadUSB védelem összetevő megakadályozza azt, hogy a billentyűzetet emuláló fertőzött USB eszközök a számítógéphez csatlakozzanak.

Ha egy USB eszközt a számítógéphez való csatlakoztatásakor az operációs rendszer billentyűzetként azonosít, akkor felkéri a felhasználót, hogy írjon be ezen a billentyűzeten vagy a képernyőn megjelenő billentyűzeten, ha elérhető, egy általa előállított számkódot (lásd az alábbi táblázatot). Ezt az eljárást nevezik billentyűzethitelesítésnek.

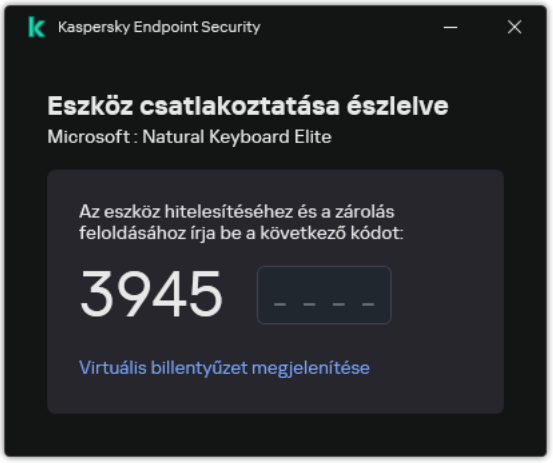
A kód megfelelő beírása esetén az alkalmazás menti az azonosító paramétereket — a billentyűzet VID/PID azonosítóját és a csatlakoztatás portszámát — a hitelesített billentyűzetek listájára. A billentyűzethitelesítést a billentyűzet ismételt csatlakoztatásakor és az operációs rendszer újraindításakor nem kell újra elvégezni.

Ha a hitelesített billentyűzetet a számítógép egy másik USB portjához csatlakoztatja, az alkalmazás megjeleníti a billentyűzet újbóli hitelesítési kérését.

Ha a számkód beírása nem sikerül, az alkalmazás új kódot állít elő. Beállíthatja a számkód beírására tett kísérletek számát. Ha a számkódot többször helytelenül adják meg, vagy a billentyűzethitelesítés engedélyezési ablaka be van zárva (lásd az alábbi ábrát), az alkalmazás letiltja a billentyűzetről történő bevitelt. Amikor letelik az USB-eszköz blokkolási ideje, vagy az operációs rendszer újraindul, az alkalmazás ismét felkéri a felhasználót, hogy végezze el a billentyűzet hitelesítését.

Az alkalmazás a hitelesített billentyűzet használatát engedélyezi, a nem hitelesítettét pedig blokkolja.

A BadUSB védelem összetevőt alapértelmezés szerint nem telepíti a rendszer. Ha szüksége van a BadUSB védelem összetevőre, hozzáadhatja az alkalmazás telepítése előtt a telepítőcsomag tulajdonságaiban, vagy módosíthatja az elérhető alkalmazásösszetevőket az alkalmazás telepítését után.



Billentyűzethitelesítés

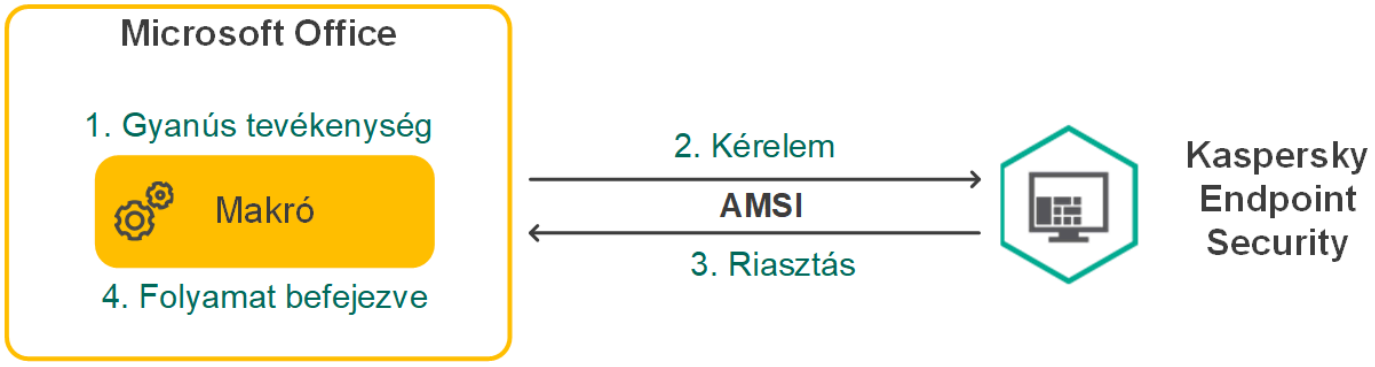
A BadUSB Védelem összetevő beállításai

Paraméter	Leírás
Virtuális billentyűzet használatának tiltása az USB-eszközök hitelesítésére	Ha a kapcsológomb be van kapcsolva, az alkalmazás blokkolja a Képernyőn megjelenő billentyűzet használatát olyan USB eszköz hitelesítésénél, amelyen nem lehet megadni hitelesítési kódot
Vonalkód használatának tiltása az USB-eszközök hitelesítésére	Ha ez a kapcsológomb be van kapcsolva, az alkalmazás nem jeleníti meg a vonalkódot a vonalkódolvasó hitelesítési értesítésében.
Az USB-készülékhitelesítési kísérletek maximális száma	Automatikusan blokkolja az USB-eszközt, ha a megadott számú alkalommal helytelenül adják meg a hitelesítési kódot. Az érvényes értékek 1 és 10 között vannak. Ha például 5 kísérletet engedélyez a hitelesítési kód megadására, az alkalmazás az ötödik sikertelen kísérlet után blokkolja az USB-eszközt. A Kaspersky Endpoint Security megjeleníti az USB-eszköz blokkolásának időtartamát. Ezen idő letelte után ismét öt alkalommal próbálkozhat a hitelesítési kód megadásával.
A próbálkozások maximális számának időkorlátja	Az USB-eszköz letiltásának időtartama a megadott számú sikertelen engedélyezési kísérlet után. Az érvényes értékek 1 és 180 (perc) között vannak.

AMSI védelem

Az AMSI védelmi összetevő a Microsoft által az Antimalware Scan Interface számára nyújtott támogatás. Az *Antimalware Scan Interface (AMSI)* engedélyezi a harmadik féltől származó, AMSI támogatással rendelkező alkalmazásoknak, hogy objektumokat küldjenek (például PowerShell szkripteket) a Kaspersky Endpoint Security számára további vizsgálat érdekében, valamint azt, hogy vizsgálati eredményeket kapjanak ezen objektumokról. Harmadik féltől származó alkalmazások közé tartozhatnak például a Microsoft Office alkalmazások (lásd az alábbi ábrát). Az AMSI részleteiért lásd a Microsoft dokumentációt.

Az AMSI védelem a fenyegetéseket csak észlelni tudja, valamint értesíteni a harmadik féltől származó alkalmazásokat ezekről. A harmadik féltől származó alkalmazás, miután értesítést kap a fenyegetésről, nem engedi a rosszindulatú tevékenységek végrehajtását (például leállítja a műveletet).



AMSI művelet – példa

Az AMSI védelmi összetevő elutasíthatja a harmadik féltől származó szolgáltató kérelmét, például akkor, ha az alkalmazás túllépte a megadott időtartamra meghatározott maximális kérelmek számát. A Kaspersky Endpoint Security információkat küld a harmadik féltől származó alkalmazások elutasított kérelmeiről az adminisztrációs kiszolgálónak. Az AMSI védelmi összetevő nem tagadja meg azoktól a külső alkalmazásoktól származó kéréseket, amelyekhez a folyamatos integráció az AMSI védelmi összetevővel engedélyezve van.

Az AMSI védelem a következő – munkaállomásokon, illetve kiszolgálókon futó – operációs rendszereken érhető el:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / több munkamenetes Enterprise
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

- Windows Server 2016 Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2019 Essentials / Standard / Datacenter (beleértve a Server Core mode megoldást is)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (beleértve a Server Core mode megoldást is)
- Windows Server 2025 Standard / Datacenter

AMSI védelem beállításai

Paraméter	Leírás
Archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb archívumok vizsgálata. Az alkalmazás kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat. Az archívumok ellenőrzése során az alkalmazás rekurzív kibontást végez. Ez lehetővé teszi a többszintű archívumokban (archívum az archívumon belül) lévő fenyegetések észlelését.
Terjesztési csomagok vizsgálata	Harmadik féltől származó alkalmazások terjesztőcsomagjainak vizsgálata.
Microsoft Office formátumú fájlok vizsgálata	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják. Az alkalmazás az 1 MB-nál kisebb, Office formátumú fájlokat vizsgálja, függetlenül attól, hogy a jelölőnégyzet be van-e jelölve vagy sem.
Ne csomagoljon ki nagy összetett fájlokat	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás minden összetett fájlt megvizsgál. Az alkalmazás megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.

Biztonsági rések kihasználásának megelőzése

A Biztonsági rések kihasználásának megelőzése összetevő észleli azon programkódokat, amik a számítógép sebezhetőségeinek segítségével kihasználják a rendszergazda jogait vagy rosszindulatú tevékenységeket hajtanak végre. Például, ezek a kihasználások puffertúlcsordulást eredményezhetnek. Ennek eléréséhez a kihasználás nagy mennyiségű adatot küld a sebezhető alkalmazásnak. Az adatok feldolgozásakor a sebezhető alkalmazás végrehajtja a rosszindulatú kódot. A támadás eredményeképp a kihasználás engedély nélkül indíthatja el a rosszindulatú program telepítését. Ha a Kaspersky Endpoint Security egy sebezhető alkalmazásból származó végrehajtható fájl futtatására irányuló olyan kísérletet észlel, amelyet nem a felhasználó végzett el, akkor blokkolja a fájl indítását vagy értesíti a felhasználót.

A Biztonsági rések kihasználásának megelőzése összetevő emellett a hálózati portokat is figyeli az olyan alkalmazások folyamatai után, amelyek veszélyt jelenthetnek a számítógép biztonságára. Az alkalmazás vírusadatbázisok segítségével szerez információt az ilyen folyamatokról.

A biztonsági rések kihasználását megelőző összetevő beállításai

Paraméter	Leírás
Sebezhetőség kihasználásának észlelésekor	**Blokkolás**. Ha a kihasználás észlelése során ez az elem van kiválasztva, a Kaspersky Endpoint Security blokkolja a kihasználás műveleteit és egy naplóbejegyzést készít, benne a kihasználás adataival. **Tájékoztatás**. Ha ez az elem van kiválasztva, amikor a Kaspersky Endpoint Security észlel egy kihasználást, egy naplóbejegyzést készít, benne a kihasználás adataival, majd hozzáadja az adatokat az aktív fenyegetések listához.
Rendszerfolyamatok memóriavédelmének engedélyezése	Ha a kapcsológomb be van kapcsolva, akkor a Kaspersky Endpoint Security blokkolja az olyan külső folyamatokat, amelyek megpróbálnak hozzáférni a rendszerfolyamatok memóriájához.

Viselkedésészlelés

A Viselkedésészlelés összetevő a számítógépen futó alkalmazások műveleteiről fogad adatokat, és a teljesítmény növelése érdekében átadja ezeket az információkat a többi védelmem összetevőinek. A Viselkedésészlelés összetevő Viselkedésfolyam-aláírásokat (BSS) alkalmaz az alkalmazásokhoz. Ha egy alkalmazás aktivitása megegyezik egy viselkedésfolyam-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet. A Kaspersky Endpoint Security funkciói viselkedésfolyam-aláíráson alapulnak, és a számítógép számára proaktív védelmet nyújtanak.

A Viselkedésészlelés összetevő emellett a hálózati portokat is figyeli az olyan alkalmazások folyamatait illetően, amelyek veszélyt jelenthetnek a számítógép biztonságára nézve. Az alkalmazás vírusadatbázisok segítségével szerez információt az ilyen folyamatokról.

A Viselkedésészlelés összetevő beállításai

Paraméter	Leírás
Művelet kártevő tevékenységének észlelésekor	**Törlés**. Ha ez az opció van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security törli az alkalmazás végrehajtható fájlját, miközben a fájlról biztonsági másolatot készít a Biztonsági mentésben. **Blokkolás**. Ha ez az opció van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security az érintett alkalmazást bezárja. **Tájékoztatás**. Ha ez a lehetőség be van jelölve, és a rendszer egy alkalmazás rosszindulatú tevékenységét észleli, a Kaspersky Endpoint Security nem szakítja meg az alkalmazás futását, de az alkalmazás rosszindulatú tevékenységére vonatkozó információt fűz az aktív fenyegetések listájához.

Behatolásmegelőző rendszer

A Behatolásmegelőző rendszer összetevő megelőzi, hogy az alkalmazások az operációs rendszerre esetleg veszélyes műveletbe kezdjenek, így felügyelve a hozzáférést az operációs rendszer erőforrásaihoz és a személyes adatokhoz. Az összetevő antivírus adatbázisok és a Kaspersky Security Network felhőszolgáltatás segítségével biztosít védelmet a számítógépnek.

Az összetevő *alkalmazásjogosultságok* használatán keresztül felügyeli az alkalmazások működését. Az alkalmazásjogosultságok a következő hozzáférési paramétereket tartalmazzák:

- hozzáférés az operációs rendszer erőforrásaihoz (például automatikus rendszerindítási beállításokhoz, beállításkulcsokhoz);
- Hozzáférés a személyes adatokhoz (például fájlokhoz és alkalmazásokhoz).

Az alkalmazások hálózati műveleteit a Tűzfal felügyeli *hálózati szabályok* alkalmazásával.

Az alkalmazás első indítása során a „Behatolásmegelőző rendszer” összetevő a következő műveleteket hajtja végre:

1. Ellenőrzi az alkalmazás biztonságát letöltött antivírus adatbázisok segítségével.
2. Ellenőrzi az alkalmazás biztonságát a Kaspersky Security Networkben.

Javasoljuk, hogy vegyen részt a Kaspersky Security Networkben, amivel eredményesebbé teheti a „Behatolásmegelőző rendszer” összetevő működését is.

3. Az alkalmazást a megbízhatósági csoportok valamelyikébe helyezi: *Megbízható*, *Alacsony korlátozás*, *Magas korlátozás*, *Nem megbízható*.

   A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére használ. A Kaspersky Endpoint Security egy alkalmazást az alapján helyez megbízhatósági csoportba, hogy az alkalmazás milyen veszélyességi szintet képvisel a számítógép szempontjából.

   A Kaspersky Endpoint Security az alkalmazásokat a Tűzfal és a Behatolásmegelőző rendszer összetevő számára helyezi megbízhatósági csoportba. Nem lehet módosítani a megbízhatósági csoportot kizárólag a Tűzfal vagy a Behatolásmegelőző rendszer esetében.

   Ha nem vesz részt a KSN rendszerében vagy nincs hálózat, a Kaspersky Endpoint Security a Behatolásmegelőző rendszer összetevő beállításai alapján helyezi az alkalmazást megbízhatósági csoportba. Miután megérkezett az alkalmazás megítélése a KSN hálózattól, a rendszer automatikusan módosíthatja az alkalmazás megbízhatósági csoportját.

4. Blokkolja az alkalmazás műveleteit a megbízhatósági csoporttól függően. Például a *Magas korlátozás* megbízhatósági csoportba sorolt alkalmazások nem kapnak hozzáférést az operációs rendszer moduljaihoz.

Az alkalmazás következő indításakor a Kaspersky Endpoint Security ellenőrzi annak integritását. Amennyiben az alkalmazás nem változott meg, az összetevő használni fogja a meglevő alkalmazásjogot. Ha az alkalmazás módosult, a Kaspersky Endpoint Security ugyanúgy végigelemzi, mintha az első elindítására kerülne sor.

A Behatolásmegelőző rendszer összetevő beállításai

Paraméter	Leírás
Alkalmazásjogok	A „Behatolásmegelőző rendszer” összetevő által figyelt alkalmazások táblázata. Az alkalmazások megbízhatósági csoportokba vannak besorolva. A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére használ. Lehetősége van kiválasztani egy alkalmazást a számítógépeken telepített összes alkalmazás egyszerű felsorolásából valamely rendszabály alapján, majd felvenni az alkalmazást egy megbízható csoportba. Az alkalmazások hozzáférési jogai a következő táblázatokban szerepelnek: • **Fájlok és rendszerleíró adatbázis**. Az operációs rendszer erőforrásaihoz való hozzáférési jogosultságok és a megbízhatósági csoportba tartozó alkalmazások személyes adatainak táblázata. • **Jogok**. Az operációs rendszer folyamataihoz és erőforrásaihoz tartozó hozzáférési jogosultságok táblázata a megbízhatósági csoportba tartozó alkalmazásokra vonatkozóan. • **Hálózati szabályok**. Valamely megbízható csoportba tartozó alkalmazások hálózati szabályainak táblázata. Ezen szabályoknak megfelelően a Tűzfal szabályozza az alkalmazások hálózati tevékenységét. A táblázatban szerepelnek a Kaspersky szakértői által javasolt, előre definiált hálózati szabályok. Ezek a hozzáadott hálózati szabályok optimális védelmet nyújtanak a Windows operációs rendszert futtató számítógépek hálózati adatforgalmának. Az előre definiált hálózati szabályok törlésére nincs mód.
Védett erőforrások	A táblázat kategorizált számítógépes erőforrásokat tartalmaz. A Behatolásmegelőző rendszer figyeli a többi alkalmazás hozzáférési próbálkozásait a táblázatban található erőforrásokhoz. Az erőforrás lehet egy beállításkategória, fájl, mappa vagy beállításkulcs.
A Kaspersky Endpoint Security előtt indított alkalmazások megbízhatósági csoportja	Megbízható csoport, amelybe a Kaspersky Endpoint Security felveszi azokat az alkalmazásokat, amelyek indítására a Kaspersky Endpoint Security indítása előtt kerül sor.
Szabályok frissítése a korábban ismeretlen alkalmazásokhoz a KSN-ről	Ha a jelölőnégyzet be van jelölve, a Behatolásmegelőző rendszer frissíti a korábban ismeretlen jogokat a Kaspersky Security Network adatbázisai segítségével.
Megbízik a digitálisan aláírt alkalmazásokban	Ha ez a jelölőnégyzet be van jelölve, a Behatolásmegelőző rendszer összetevő a megbízható gyártók digitális aláírásaival rendelkező alkalmazásokat a *Megbízható* csoportba helyezi. A *megbízható gyártók* olyan szoftvergyártók, amelyekben a Kaspersky megbízik. A gyártói tanúsítványt manuálisan is hozzáadhatja a megbízható tanúsítványtárolóhoz. Ha a jelölőnégyzet nincs bejelölve, a Behatolásmegelőző rendszer összetevő nem tekinti megbízhatónak az ilyen alkalmazásokat, és más paraméterek alapján dönti el megbízhatósági csoportjukat.

Paraméter	Leírás
Azon alkalmazások szabályainak törlése, amelyek már több mint N napja (1–90) nem lettek elindítva	Ha a jelölőnégyzet ki van jelölve, a Kaspersky Endpoint Security automatikusan törli az alkalmazás információit (megbízhatósági csoport és hozzáférési jogok), ha a következő feltételek teljesülnek: • Ön manuálisan is beteheti az alkalmazást egy megbízhatósági csoportba, és konfigurálhatja a hozzáférési jogait. • Az alkalmazás nem indult el a megadott időtartamon belül. Ha az alkalmazás megbízhatósági csoportja és jogai automatikusan ki lettek választva, a Kaspersky Endpoint Security 30 nap után törli ezeket az adatokat. Nem lehet módosítani az alkalmazás információinak tárolási feltételeit, illetve nem lehet kikapcsolni az automatikus törlést. Ha legközelebb elindítja az alkalmazást, a Kaspersky Endpoint Security úgy fogja elemezni azt, mintha legelőször indítaná el.
Más csoportokban nem szereplő alkalmazások megbízhatósági csoportja	Az ezen a legördülő listán lévő elemek szabják meg, melyik megbízhatósági csoportba osztja be a Kaspersky Endpoint Security az ismeretlen alkalmazásokat. Az alábbi elemek közül választhat egyet: • **Alacsony korlátozás**. • **Magas korlátozás**. • **Nem megbízható**.

Kármentesítő motor

A Kármentesítő motor összetevő révén a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben végrehajtott műveleteket visszagörgetni.

A rosszindulatú programok operációs rendszerben végzett tevékenységeinek visszagörgetésekor a Kaspersky Endpoint Security a rosszindulatú programok alábbi típusú tevékenységeit kezeli:

- **Fájl tevékenysége**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Törli a rosszindulatú program által létrehozott végrehajtható fájlokat (minden médián, kivéve a hálózati meghajtókon).
  - Törli az olyan végrehajtható fájlokat, amiket a rosszindulatú programokkal fertőzött fájlok hoztak létre.
  - Visszaállítja a rosszindulatú program által módosított vagy törölt fájlokat.

  A fájlvisszaállítás funkciónak számos korlátozása van.

- **Beállításjegyzék-tevékenység**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Törli a rosszindulatú program által létrehozott beállításkulcsokat.
  - Nem állítja vissza a rosszindulatú program által módosított vagy törölt beállításkulcsokat.

- **Rendszertevékenység**

A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

- Megszűnteti a rosszindulatú program által kezdeményezett folyamatokat.
- Megszakítja azokat a folyamatokat, amelyekbe a rosszindulatú alkalmazás bejutott.
- Nem folytatja a rosszindulatú program által megállított folyamatokat.

- **Hálózati tevékenység**

  A Kaspersky Endpoint Security az alábbi feladatokat végzi el:

  - Blokkolja a rosszindulatú program hálózati tevékenységét.
  - Blokkolja a rosszindulatú programok által fertőzött folyamatok hálózati tevékenységét.

A rosszindulatú tevékenységek utáni visszagörgetés elindítható a Fájl védelem vagy Viselkedésészlelés összetevővel, illetve a Kártevő vizsgálata során.

A rosszindulatú programok műveleteinek visszagörgetése szigorúan meghatározott adatkészletet érint. A visszagörgetés semmilyen negatív következménnyel nem jár az operációs rendszerre és a számítógép adatainak integritására nézve.

Kaspersky Security Network

A számítógép védelmének fokozása érdekében a Kaspersky Endpoint Security a felhasználóktól a világ minden tájáról kapott adatokat használja. A Kaspersky Security Network feladata ezen adatok fogadása.

A KSN-funkciók nem lesznek elérhetők a szoftverben az Egyesült Államok területén.

A *Kaspersky Security Network (KSN)* felhőalapú szolgáltatások egy olyan infrastruktúrája, amely hozzáférést nyújt a Kaspersky online tudásbázisához, ahonnan információkat kaphat fájlok, webes erőforrások és szoftverek megbízhatóságáról. A Kaspersky Security Network adatait felhasználva a Kaspersky Endpoint Security gyorsabban reagál az új típusú fenyegetésekre, egyes védelmi összetevők teljesítménye nő, a téves riasztások valószínűsége pedig csökken. Ha tagja a Kaspersky Security Networknek, a KSN szolgáltatások a Kaspersky Endpoint Security számára információkat nyújtanak a vizsgált webcímek megbízhatóságáról, valamint a vizsgált fájlok kategóriájáról és megbízhatóságáról. A KSN-hez való hozzáférés konfigurálásával kapcsolatos további részletekért lásd a Kaspersky Security Center súgóját.

A Kaspersky Security Network használata önkéntes. Az alkalmazás a kezdeti beállítás során kéri a felhasználót, hogy használja a KSN szolgáltatást. A felhasználók bármikor megszüntethetik részvételüket a KSN-ben.

A KSN-ben való részvétel során keletkező statisztikai adatok Kaspersky részére történő elküldésével és az ilyen adatok tárolásával és megsemmisítésével kapcsolatos részletes információk a Kaspersky Security Network nyilatkozatában és a Kaspersky webhelyén találhatók. A Kaspersky Security Network nyilatkozatának szövegét tartalmazó ksn_<nyelv azonosítója>.txt fájl megtalálható az alkalmazás terjesztőkészletében.

A Kaspersky megbízhatósági adatbázisainak infrastruktúrája

A Kaspersky Endpoint Security a következő infrastrukturális megoldásokat támogatja a Kaspersky megbízhatósági adatbázisaival való együttműködéshez:

- A *Kaspersky Security Network (KSN)* a legtöbb Kaspersky-alkalmazás által használt megoldás. A KSN-résztvevők információkat kapnak a Kaspersky-től, és elküldik a Kaspersky számára a felhasználó számítógépén észlelt objektumokat, hogy a Kaspersky is elemezze azokat, és belevegye a megbízhatósági és statisztikai adatbázisába.

- A *Kaspersky Private Security Network (KPSN)* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky megbízhatósági adatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a Kaspersky-nek a saját számítógépükről. A KPSN vállalati felhasználóknak ajánlott, akik a következő okokból nem tudnak részt venni a Kaspersky Security Networkben:

    - A helyi munkaállomások nem csatlakoznak az internethez.

Az adatok vállalati LAN-hálózaton vagy az országon kívüli továbbítását tiltja a törvény vagy a vállalat biztonsági rendszabálya.

Kaspersky Security Network beállítások

Paraméter	Leírás
Kiterjesztett KSN mód engedélyezése	A *Kiterjesztett KSN mód* egy olyan mód, melyben a Kaspersky Endpoint Security további adatokat küld a Kaspersky számára. A Kaspersky Endpoint Security KSN használatával észleli a fenyegetéseket, pozíciótól függetlenül.
Felhő mód engedélyezése	A *Felhő mód* arra az alkalmazásműveleti módra vonatkozik, amiben a Kaspersky Endpoint Security az antivírus adatbázisok egyszerű verzióját használja. A Kaspersky Security Network támogatja az alkalmazásműveletet, ha az antivírus adatbázisok egyszerű verziója van használva. Az antivírus adatbázisok egyszerű verziójával körülbelül fele annyi RAM-ot használ a számítógépen, amit az átlagos adatbázisokkal használna. Ha nem vesz részt a Kaspersky Security Networkben, vagy ha a felhő mód ki van kapcsolva, a Kaspersky Endpoint Security letölti az antivírus adatbázisok teljes verzióját a Kaspersky szerverekről. Ha a kapcsológomb be van kapcsolva, a Kaspersky Endpoint Security az antivírus adatbázisok egyszerű verzióit használja, ami csökkenti az operációs rendszer erőforrásainak igénybevételét. A jelölőnégyzet bejelölése után a Kaspersky Endpoint Security a következő frissítés során letölti az antivírus adatbázisok egyszerű verzióját. Ha a kapcsológomb ki van kapcsolva, a Kaspersky Endpoint Security az antivírus adatbázisok teljes verzióját használja. A jelölőnégyzet kitörlése után a Kaspersky Endpoint Security a következő frissítés során letölti az antivírus adatbázisok teljes verzióját.
Számítógép státusza, ha a KSN kiszolgálók elérhetetlenek *(csak a Kaspersky Security Center konzolon érhető el)*	A legördülő listában lévő elemek meghatározzák a számítógép állapotát a Kaspersky Security Centerben, ha a KSN kiszolgálók elérhetetlenek.

Paraméter	Leírás
Adminisztrációs kiszolgáló használata KSN-proxykiszolgálóként *(csak a Kaspersky Security Center konzolon érhető el)*	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a KSN proxykiszolgálót használja. A KSN proxyszolgáltatás beállításait az Adminisztrációs kiszolgáló tulajdonságaiban adhatja meg.
A Kaspersky Security Network kiszolgálóinak használata, ha a KSN-proxykiszolgáló nem érhető el *(csak a Kaspersky Security Center konzolon érhető el)*	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a KSN kiszolgálókat használja, ha a KSN Proxykiszolgáló elérhetetlen. A KSN kiszolgálók egyaránt lehetnek a Kaspersky oldalán és harmadik felek oldalán (a Privát Kaspersky Security Network használata esetén).

Naplóvizsgálat

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt.

A 11.11.0 verziótól kezdődően a Kaspersky Endpoint Security for Windows tartalmazza a Napló vizsgálata összetevőt. A Napló vizsgálata figyelemmel kíséri a védett környezetek integritását a Windows eseménynapló-elemzése alapján. Ha az alkalmazás szokatlan magatartást érzékel a rendszerben, jelzi a rendszergazdának, mert ez a magatartás kibertámadásra tett kísérlet jele is lehet.

A Kaspersky Endpoint Security elemzi a Windows eseménynaplóit, és észleli a szabálysértéseket. Az összetevő előre definiált szabályokat tartalmaz. Az előre definiált szabályok heurisztikus elemzésen alapulnak. Saját szabályokat (egyéni szabályokat) is hozzáadhat. Egy szabály aktiválódásakor az alkalmazás *Critical* állapotú eseményt hoz létre (lásd az alábbi ábrát).

Ha a Naplóvizsgálatot szeretné használni, győződjön meg arról, hogy az auditálási házirend biztonsági beállításai megfelelően vannak konfigurálva, és a rendszer naplózza a vonatkozó eseményeket (részleteket a Microsoft terméktámogatási webhelyén találhat).



Naplóvizsgálati értesítés

Paraméter	Leírás
Előre definiált szabályok	Naplóvizsgálati szabályok listája. Az előre definiált szabályok a védett számítógépeken előforduló rendellenes tevékenységek sablonjait tartalmazzák. A rendellenes tevékenységek támadási kísérletet jelezhetnek.
Egyéni szabályok	A felhasználó által hozzáadott naplóvizsgálati szabályok listája. Saját feltételeit is beállíthatja a naplóvizsgálati szabály kiváltásához. Ehhez meg kell adnia egy eseményazonosítót, és ki kell választania egy eseményforrást. Az eseményforrást kiválaszthatja a standard naplók közül: *Application*, *Security* vagy *System*. Egy harmadik féltől származó alkalmazás naplóját is megadhatja.

Anti-Cryptor

Az Anti-Cryptor összetevő a megosztott mappákban végzett tevékenységeket elemzi. Ha ez a tevékenység megegyezik a külső titkosításra jellemző viselkedésfolyamat-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet.

A Kaspersky Endpoint Security csak azoknak a fájloknak a külső titkosítását akadályozza meg, amelyek NTFS fájlrendszert tartalmazó adathordozón találhatók, és nincsenek EFS rendszerrel titkosítva.

Paraméter	Leírás
Kizárások név vagy IP-cím alapján	**Kizárások név vagy IP-cím alapján**. Azon külső számítógépek listája, amelyekről a megosztott mappák titkosításának kísérleteit a rendszer nem kíséri figyelemmel. Ahhoz, hogy kizárja a listában megadott számítógépeket a külső titkosítás elleni megosztott mappák védelme alól, először engedélyeznie kell a Bejelentkezés naplózása funkciót a Windows biztonsági naplórendjéből. A Bejelentkezés naplózása funkció alapértelmezetten ki van kapcsolva. A Windows biztonsági naplórendjéről szóló további információkért, kérjük látogassa meg a Microsoft weboldalt. **Kizárások maszk szerint**. A védelem hatókörének kizárásai. Egy mappa kizárása a védelem hatóköréből csökkentheti az álpozitív találatok számát, ha a cég adattitkosítást használ a megosztott mappák segítségével történő fájlcsere során. A Viselkedelemzés például vakriasztást okozhat, ha a felhasználó ENC kiterjesztésű fájlokkal dolgozik egy megosztott mappában. Ez a tevékenység megfelel a külső titkosításra jellemző viselkedési mintának. Ha az adatok védelme céljából titkosított fájlokat tárol egy megosztott mappában, vegye fel a mappát a kizárások közé. maszkok használata: • A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák). • Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk. • A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.
Művelet fenyegetés észlelésekor	• **Tájékoztatás**. Ha ez a beállítás be van jelölve, a megosztott mappákban lévő fájlok módosítási kísérletének észlelésekor a Kaspersky Endpoint Security a módosítási kísérletről szóló információkat hozzáadja az aktív fenyegetések listájához, bejegyzést add hozzá a helyi alkalmazásfelület jelentéseibe, és az észlelt rosszindulatú tevékenységről információt küld a Kaspersky Security Center számára. • **Kapcsolódás blokkolása (perc) N percig**. Ha ez az opció be van jelölve, a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észlelve blokkolja a fájlmódosításhoz való hozzáférést a rosszindulatú tevékenységet kezdeményező munkamenet számára, és biztonsági másolatokat készít a módosított fájlokról. Ha a Kármentesítő motor összetevő engedélyezve van, és a **Kapcsolat blokkolása (perc) N percig** lehetőség ki van választva, a módosított fájlok a biztonsági mentésekből kerülnek visszaállításra.
Védelem hatóköre	A *védelem hatóköre* azon megosztott mappák elérési útvonalainak listája, amelyekben a Kaspersky Endpoint Security figyeli a fájltevékenységet. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. Alapértelmezés szerint az alkalmazás automatikusan azonosítja a megosztott mappákat, és minden mappában figyeli a fájltevékenységet.

Webfelügyelő

A Webfelügyelő kezeli a felhasználók hozzáférését a webes erőforrásokhoz. Ez csökkenti a forgalmat és a munkaidő nem megfelelő használatát. Ha a felhasználó a Webfelügyelő által korlátozott weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést vagy figyelmeztetést jelenít meg (lásd az alábbi ábrát).

A Webfelügyelő használatához el kell végeznie az alkalmazás kezdeti konfigurációját:

- A HTTPS forgalom figyeléséhez, engedélyezze a titkosított kapcsolatok vizsgálatát (alapértelmezés szerint engedélyezve van).
- Válassza ki azokat a portokat, amelyeket a Kaspersky Endpoint Security megoldásnak figyelnie kell (alapértelmezés szerint az alkalmazás az összes portot figyeli).

- Válassza ki azokat az alkalmazásokat, amelyeknek a forgalmát a Kaspersky Endpoint Securityvel meg szeretné figyelni. A legtöbb böngésző már szerepel a Kaspersky által ajánlott alkalmazások listáján. Ha a böngészője hiányzik a listáról, adja hozzá manuálisan.

- Javasoljuk, hogy illesszen be egy weboldal-interakciós parancsfájlt a webes forgalomba (alapértelmezés szerint a parancsfájl beillesztése le van tiltva). Ez a parancsfájl lehetővé teszi a Webfelügyelő események regisztrációját az alkalmazás eseménynaplójában, az operációs rendszer eseménynaplójában és a jelentésekben.

A weboldalak elérésének kezelési módszerei

A Webfelügyelővel a következő módszerekkel konfigurálhatja a weboldalak elérését:

- **Weboldalkategória**. A weboldalak a Kaspersky Security Network felhőszolgáltatás, a heurisztikus elemzés és az ismert weboldalak adatbázisai (köztük az alkalmazás-adatbázisok) alapján vannak besorolva. Például korlátozhatja a felhasználói hozzáférést a *Közösségi hálózatok* kategóriához vagy más kategóriákhoz.

- **Adattípus**. Például korlátozhatja egy felhasználó hozzáférését a webhely adataihoz, elrejthet képeket. A Kaspersky Endpoint Security a fájl formátuma alapján határozza meg az adattípust, nem pedig a kiterjesztése alapján.

  > A Kaspersky Endpoint Security nem vizsgálja a fájlokat az archívumokban. Például, ha képfájlok vannak egy archívumban, a Kaspersky Endpoint Security *Archívumok* adattípusként azonosítja azokat, nem pedig *Grafika*.

- **Egyedi címek**. Megadhat webcímet vagy használhat maszkokat.

Egyszerre több módszert is használhat a weboldalak elérésének szabályozására. Például korlátozhatja az *Office-alkalmazások fájljai* adattípus elérést a *Webalapú e-mail* webhely-kategória számára.

Weboldalhozzáférési szabályok

A Webfelügyelő szabályozza a weboldalakhoz történő hozzáférést a *hozzáférési szabályokkal*. A következő speciális beállításokat alkalmazhatja a weboldal hozzáférési szabályához:

- A felhasználók, akikre a szabály vonatkozik.

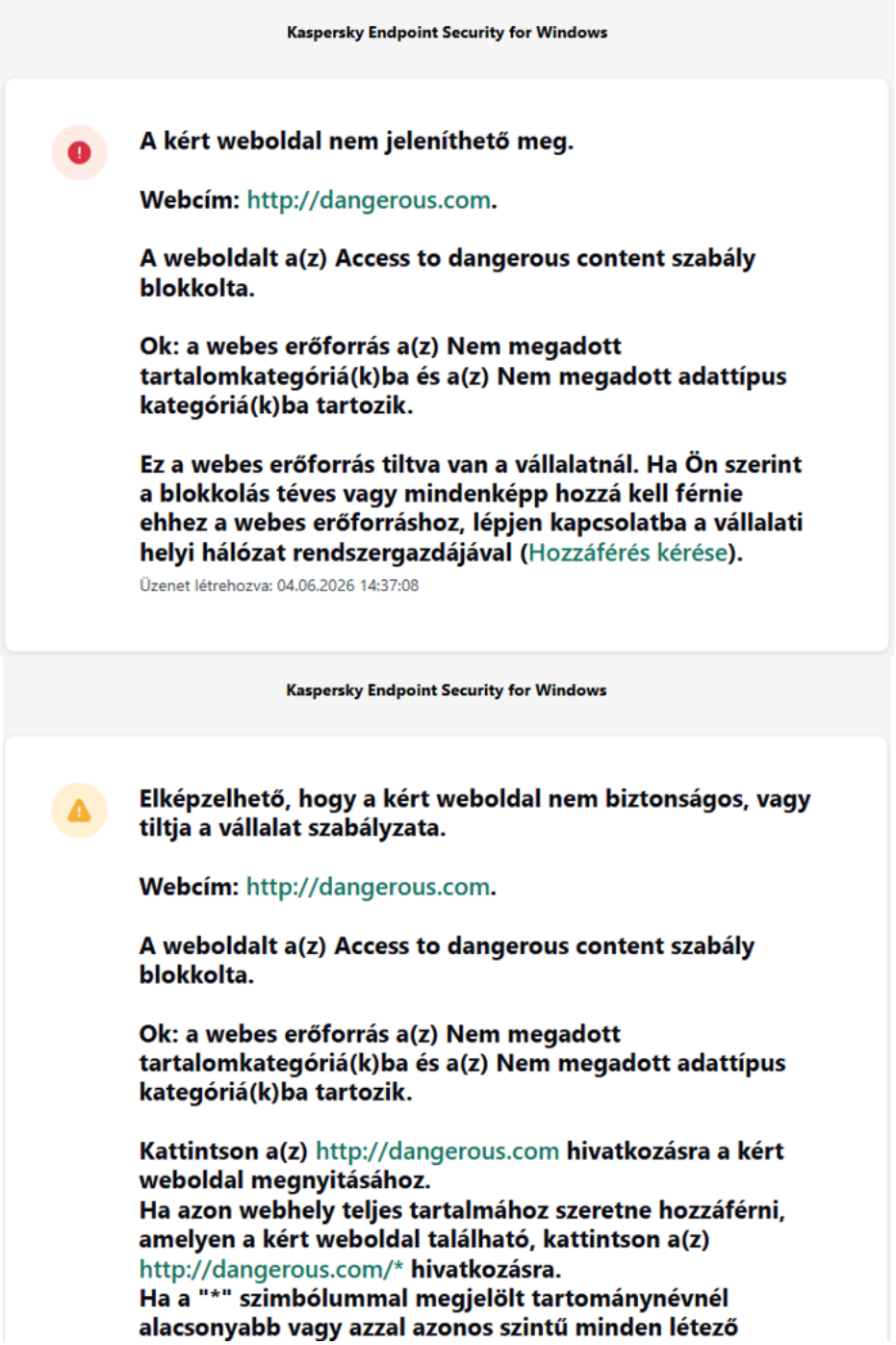
  Például korlátozhatja minden olyan felhasználó számára a böngészőn keresztül történő internetelérést, akik nem az IT osztályon vannak.

- Szabályütemezés.

  Korlátozhatja a böngészőn keresztül történő internetelérést a munkaidő alatt.

Hozzáférési szabály prioritásai

Minden szabálynak van valamilyen prioritása. Minél magasabban helyezkedik el egy szabály a szabályok listáján, annál magasabb a prioritása. Ha egy weboldal számos szabályhoz lett hozzáadva, a Webfelügyelő a legmagasabb prioritású szabály alapján szabályozza a weboldal elérését. Például, a Kaspersky Endpoint Security a vállalati portált közösségi hálózatként azonosíthatja. A közösségi hálózatok elérésének korlátozásához és a vállalati webportál elérésének biztosításához hozzon létre két szabályt: egy blokkoló szabályt, ami a *Közösségi hálózatok* weboldalkategóriára vonatkozik, és egy engedélyező szabályt, ami a vállalat webportáljára vonatkozik. A vállalati webportál hozzáférési szabályának magasabb prioritásúnak kell lennie, mint a közösségi hálózatok hozzáférési szabályának.



Webfelügyelő üzenet

Paraméter	Leírás
Szabályok a webes erőforrásokhoz való hozzáférésre	A webes erőforrások hozzáférési szabályait tartalmazó lista. Minden szabálynak van valamilyen prioritása. Minél magasabban helyezkedik el egy szabály a szabályok listáján, annál magasabb a prioritása. Ha egy weboldal számos szabályhoz lett hozzáadva, a Webfelügyelő a legmagasabb prioritású szabály alapján szabályozza a weboldal elérését.
Alapértelmezett szabály	Az *Alapértelmezett szabály* azt a webes erőforráshoz hozzáférő szabályt jelenti, amire nem vonatkozik egyetlen más szabály sem. A következők közül választhat: • **Az összes engedélyezése, kivéve a szabálylistát**, ami tiltólistaként is ismert a tiltott webhelyekhez. • **Az összes megtagadása, kivéve a szabálylistát**, ami engedélyezési listaként is ismert az engedélyezett webhelyekhez.
Az aktív felhasználói böngészői munkamenetek megszüntetése a szabály alkalmazása után	Ha a jelölőnégyzet be van jelölve, a Webfelügyelő a házirend alkalmazása után azonnal megszünteti a kapcsolatot a blokkolt webes erőforrásokkal. A böngésző azonnal leállítja az adatok letöltését a weboldalról. Amikor frissíti a weboldalt, vagy egy másik tiltott weboldalra lép, az alkalmazás figyelmeztetést jelenít meg. A Webfelügyelő csak a böngészőkben teszi lehetővé a webes erőforrások azonnali leválasztását. Más alkalmazások esetében a Webfelügyelő csak az új kapcsolatokat korlátozza. Ha a jelölőnégyzet nincs bejelölve, a Webfelügyelő csak a tiltott webes erőforrásokra korlátozza az új kapcsolatokat. A Webfelügyelő nem szünteti meg az aktív kapcsolatokat.
Sablonok	**Figyelmeztetés**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely nem kívánatos webes erőforráshoz való hozzáférési próbálkozásra figyelmeztet. **Üzenet a blokkolásról**. Ez a beviteli mező annak az üzenetnek a sablonját tartalmazza, amely akkor jelenik meg, ha kiváltódik egy szabály, amely blokkolja a hozzáférést a webes erőforráshoz. **Üzenet a rendszergazdának**. A LAN rendszergazda részére küldendő üzenet sablonját tartalmazza, ha a felhasználó egy blokkolást tévedésnek tekint. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Weboldal hozzáférésének blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre. Az üzenetsablonok kezeléséhez speciális változók állnak rendelkezésre (pl. `%USER_NAME%`). A változók lehetővé teszik egyetlen üzenetsablon használatát a különböző számítógépeken.
Az engedélyezett oldalak megnyitásának naplózása	A Kaspersky Endpoint Security naplózza a weboldalak látogatását, köztük az engedélyezett weboldalakét is. A Kaspersky Endpoint Security eseményeket küld a Kaspersky Security Center, a Kaspersky Endpoint Security helyi naplója és a Windows eseménynapló számára. Az internettevékenység megfigyeléséhez meg kell adnia az események mentésének beállításait. A figyelési funkciót támogató böngészők: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. A felhasználói tevékenység figyelése más böngészőkben nem működik. Az internettevékenység megfigyelése több számítógépes erőforrást vehet igénybe HTTPS-forgalom visszafejtése során.

Eszközfelügyelő

Az Eszközfelügyelő felügyeli az olyan eszközökhöz történő felhasználói elérést, amik csatlakoztatva vannak a számítógéphez (például merevlemezek, kamerák vagy Wi-Fi modulok). Ez lehetővé teszi, hogy megvédje számítógépét a fertőzésektől, ha ilyen eszközök vannak csatlakoztatva, valamint megelőzi az adatvesztést vagy -szivárgást.

Ha az Eszközfelügyelő engedélyezve van, az alkalmazás továbbítja a csatlakoztatott eszközökre vonatkozó információkat a Kaspersky Security Centernek. A csatlakoztatott eszközök listáját a Kaspersky Security Center **Advanced** → **Repositories** → **Hardware** mappájában tekintheti meg.

Eszközhozzáférési szintek

Az Eszközfelügyelő a következő szinteken felügyeli a hozzáférést:

- **Eszköztípus**. Például nyomtatók, cserélhető meghajtók és CD/DVD meghajtók.

  Az eszköz hozzáférésének beállításait az alábbiak szerint lehet megadni:

  - Engedélyezés – .
  - Blokkolás – .
  - Szabályokkal (csak nyomtatók és hordozható eszközök) – .
  - A csatlakozási busztól függ (kivéve Wi-Fi) – .
  - Blokkolás kivételekkel (csak Wi-Fi) – .

- **Csatlakozási busz**. A *csatlakozási busz* egy felület, amivel csatlakoztatni lehet eszközöket a számítógéphez (például USB vagy FireWire). Ha **A csatlakozási busztól függ** mód van kiválasztva az eszköztípusnál, az alkalmazás a csatlakozási felülettől függően engedélyezi vagy letiltja az eszköz elérését (pl. USB).

  Az eszköz hozzáférésének beállításait az alábbiak szerint lehet megadni:

  - Engedélyezés – .
  - Blokkolás – .

- **Megbízható eszközök**. A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

  Az alábbi adatok alapján hozzáadhat megbízható eszközöket:

  - **Eszközök azonosító alapján**. Minden eszköz egyedi azonosítóval rendelkezik (Hardverazonosítóval, azaz HWID-vel). Megtekintheti az azonosítót az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. Példa az eszközazonosítóra: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Azonosító alapján kényelmesen lehet eszközöket hozzáadni, ha bizonyos meghatározott eszközöket akar hozzáadni.

  - **Eszközök típus alapján**. Minden eszköz rendelkezik egy gyártóazonosítóval (VID) és termékazonosítóval (PID). Megtekintheti az azonosítókat az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. A VID és PID számok megadására szolgáló sablon: `VID_1234&PID_5678`. Modell alapján kényelmesen lehet eszközöket hozzáadni, amennyiben a szervezetében használt bizonyos készülékmodelleket akarja használni. Ilyen módon az adott modell valamennyi példányát hozzáadhatja.

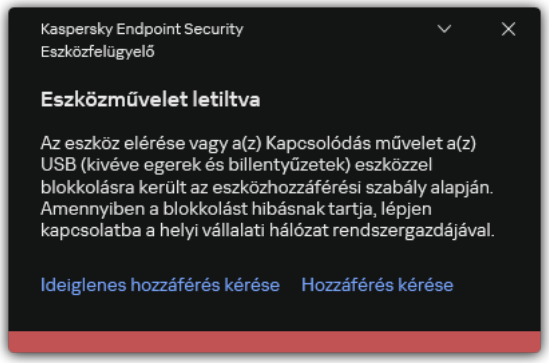
  - **Eszközök azonosítómaszk alapján**. Ha több eszközt használ, amelyek azonosítója megegyezik, akkor maszkok segítségével veheti fel azokat a megbízható listára. A `*` karakter akármilyen karakterláncot helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `WDC_C*`.

  - **Eszközök modellmaszk alapján**. Ha több eszközt használ hasonló VID vagy PID azonosítóval (például ugyanattól a gyártótól származó eszközök), akkor maszkokkal hozzáadhat készülékeket a megbízható listához. A `*` karakter akármilyen karakterláncot helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `VID_05AC&PID_*`.

Az Eszközfelügyelő szabályozza az eszközökhöz történő hozzáférést a *hozzáférési szabályokkal*. Az Eszközfelügyelővel elmentheti a készülék kapcsolódási/lecsatlakozási eseményeit. Az események elmentéséhez meg kell adnia a szabályzatban az események regisztrációját.

Ha a készülék elérése a csatlakozóbusztól függ (a állapot), akkor a Kaspersky Endpoint Security nem menti el a készülék kapcsolódási/leválasztási eseményeket. Ahhoz, hogy engedélyezze, hogy a Kaspersky Endpoint Security elmentse az eszköz kapcsolódási/leválasztási eseményeket, engedélyezze a megfelelő típusú készülék elérését (a állapot), vagy adja hozzá a készüléket a megbízható listához.

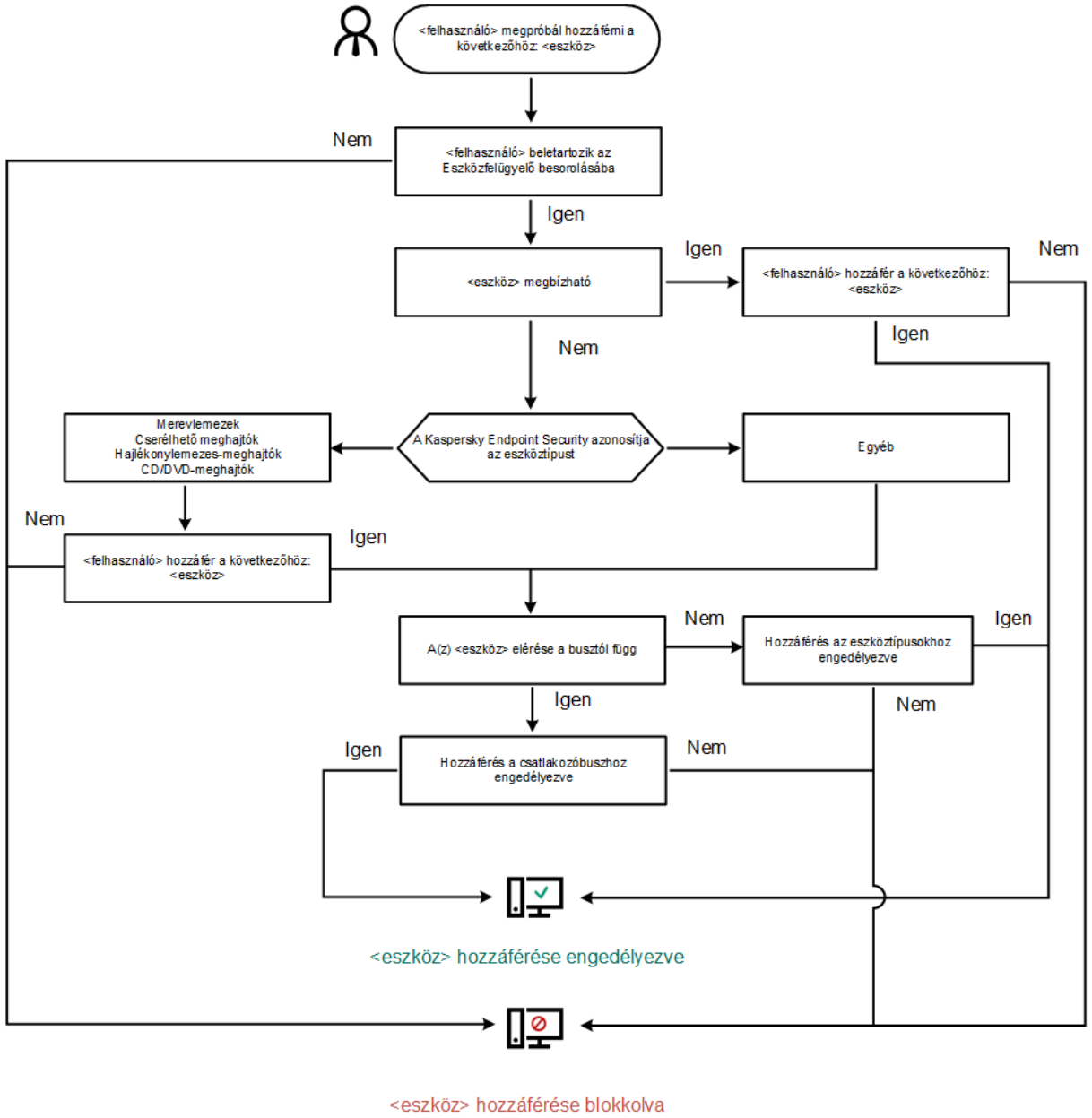
Ha egy olyan eszköz csatlakozik a számítógéphez, ami blokkolva van az Eszközfelügyelő által, akkor a Kaspersky Endpoint Security blokkolja az elérést, és megjelenít egy értesítést (lásd az alábbi ábrát).



Eszközfelügyelő értesítés

Eszközfigyelő műveleti algoritmus

A Kaspersky Endpoint Security döntést hoz az eszközök hozzáférésének engedélyezéséről, miután a felhasználó a számítógéphez csatlakoztatja őket (lásd az alábbi ábrát).



Eszközfigyelő műveleti algoritmus

Ha az eszköz csatlakoztatva van és hozzáférhető, akkor szerkesztheti a hozzáférési és a blokkolási szabályt. Ebben az esetben, ha legközelebb valaki megpróbál hozzáférni az eszközhöz (például ha meg akarja tekinteni a mappalistát, vagy olvasási és írási műveleteket akar elvégezni), akkor a Kaspersky Endpoint Security blokkolja a hozzáférést. A fájlrendszer nélküli eszköz csak a következő csatlakoztatás alkalmával blokkolódik.

Ha telepített Kaspersky Endpoint Security alkalmazással rendelkező számítógép felhasználójának hozzáférést kell kérnie egy olyan eszközhöz, amely a felhasználó szerint tévedésből van blokkolva, küldje el a felhasználónak a hozzáférés-kérési utasításokat.

Paraméter	Leírás
Ideiglenes hozzáférési kérések engedélyezése *(csak a Kaspersky Security Center konzolon érhető el)*	Ha a jelölőnégyzet be van jelölve, a **Hozzáférés kérése** gombra használható a Kaspersky Endpoint Security helyi felületén. Ezzel a gombbal a felhasználó ideiglenes hozzáférést kérhet egy blokkolt eszközhöz.
Készülékek és Wi-Fi hálózatok	Ez a táblázat tartalmazza az összes lehetséges eszköztípust az Eszközfelügyelő összetevő osztályozásának megfelelően, ideértve hozzáférési állapotukat is.
Csatlakozási buszok	Az összes rendelkezésre álló csatlakozási busz listája az Eszközfelügyelő összetevő osztályozásának megfelelően, ideértve hozzáférési állapotukat is. A Kaspersky Endpoint Security a csatlakozási busz típusától függően engedélyezi vagy tagadja meg a hozzáférést az eszközökhöz, ha **A csatlakozási busztól függ** mód ki van választva.
Megbízható eszközök	A megbízható eszközök listája, valamint a felhasználók, akik hozzáférést adtak ezekhez az eszközökhöz.
Értékek egyesítése öröklésekor *(csak a Kaspersky Security Center konzolon érhető el)*	Ez egyesíti a megbízható eszközök listáját a Kaspersky Security Center szülői és gyermek házirendjeiben. A listák egyesítéséhez a gyermekházirendet úgy kell beállítani, hogy örökölje a Kaspersky Security Center szülőházirendjének beállításait. Ha a jelölőnégyzet be van jelölve, a Kaspersky Security Center szülőházirendjének listaelemei megjelennek a gyermekházirendekben. Így például létrehozhatja a megbízható eszközök összevont listáját az egész vállalat számára. A gyermekházirend örökölt listaelemei nem törölhetők és nem szerkeszthetők. Az öröklés során összevont megbízható eszközök listáján szereplő elemek csak a szülő házirendben törölhetők és szerkeszthetők. Az alacsonyabb szintű irányelvekben lehetősége van hozzáadni, módosítani és eltávolítani a listaelemeket. Ha a gyermek- és szülőházirend listák elemei egyeznek, ezek az elemek a szülőházirend ugyanazon elemeként jelennek meg. Ha a jelölőnégyzet nincs bejelölve, akkor a lista elemeit nem egyesíti a rendszer, amikor a Kaspersky Security Center házirendek beállításainak öröklése zajlik. Ez a funkció lehetővé teszi a házirend-profilok listáinak összevonását is. A listák egyesítéséhez a legmagasabb prioritású profilban engedélyezze a beállítások öröklését egy alacsonyabb prioritású profilból. A házirend-profilok prioritásaival kapcsolatos további részletekért olvassa a Kaspersky Security Center súgóját.
Anti-Bridging	Az Anti-Bridging gátolja a hálózati hidak létrehozását azzal, hogy megelőzi, hogy a számítógépen egyszerre több hálózati kapcsolat legyen létrehozva. Ezzel megvédheti a vállalati hálózatát a védtelen, engedély nélküli hálózatokon keresztül érkező támadásoktól. Az Anti-Bridging az eszközprioritások alapján nem teszi lehetővé a több csatorna létrehozását. Minél magasabban helyezkedik el egy eszköz a listán, annál magasabb a prioritása. Ha egy aktív és egy új kapcsolatnak ugyanaz a típusa (például Wi-Fi), a Kaspersky Endpoint Security blokkolja az aktív kapcsolatot, és lehetővé teszi az új kapcsolat létrehozását. Ha egy aktív és egy új kapcsolatnak különböző a típusa (például hálózati adapter és Wi-Fi), a Kaspersky Endpoint Security blokkolja az alacsonyabb prioritású kapcsolatot, és engedélyezi a magasabb prioritásút. Az Anti-Bridging a következő típusú eszközökön támogatja a műveletet: hálózati adapter, Wi-Fi és modem.
Üzenetsablonok	**Üzenet a blokkolásról**. Annak az üzenetnek a sablonja, ami akkor jelenik meg, amikor a felhasználó megpróbál hozzáférni egy blokkolt készülékhez. Ez az üzenet akkor is megjelenik, amikor a felhasználó megpróbál végrehajtani egy olyan műveletet a készülék tartalmán, ami blokkolva van számára. **Üzenet a rendszergazdának**. Annak az üzenetnek a sablonja, amelyet a LAN-rendszergazda kap, ha a felhasználó úgy véli, hogy az eszközhöz való hozzáférés blokkolása, illetve az eszköz tartalmával végzett művelet tiltása tévedés. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Eszközhozzáférés blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

Alkalmazásfelügyelő

Az Alkalmazásfelügyelő kezeli az alkalmazások indítását a felhasználók számítógépén. Ez lehetővé teszi a vállalati biztonsági házirend bevezetését az alkalmazások használatára vonatkozóan. Az Alkalmazásfelügyelő emellett csökkenti a számítógép megfertőződésének kockázatát is azzal, hogy korlátozza a hozzáférést az alkalmazásokhoz.

Az Alkalmazásfelügyelő konfigurálásának lépései a következők:

1. Alkalmazáskategóriák létrehozása.

   A rendszergazda létrehoz kategóriákat az általa kezelni kívánt alkalmazásokhoz. Az alkalmazáskategóriák a vállalati hálózat minden számítógépére vonatkoznak, függetlenül a rendszergazdai csoportoktól. Kategória létrehozásához a következő feltételeket használhatja: KL-kategória (például *Böngészők* vagy más kategória), fájlkivonat, az alkalmazás gyártója és egyéb feltételek.

2. Alkalmazásfelügyeleti szabályok létrehozása.

   A rendszergazda alkalmazásfelügyeleti szabályokat hoz létre a rendszergazdai csoport házirendjében. A szabályban alkalmazáskategóriák szerepelnek, és ezen kategóriák alkalmazásainak rendszerindításkori állapota lehet „letiltva" vagy „engedélyezett". Az adminisztrátor sok szabályt hozhat létre. Egy alkalmazás több szabály feltételeinek is megfelelhet. A blokkoló szabályok prioritása magasabb az engedélyező szabályokénál. A Kaspersky Endpoint Security minden indításkor ellenőrzi, hogy az alkalmazás megfelel-e a szabálynak. A Kaspersky Endpoint Security egymás után elvégzi az alkalmazás összes Alkalmazásfelügyeleti szabályának megfelelőségét.

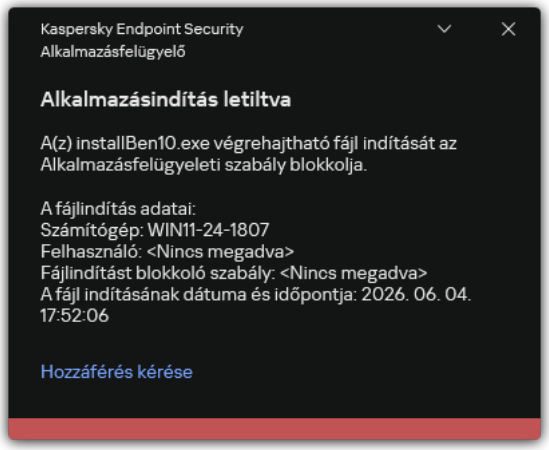
3. Az Alkalmazásfelügyelő módjának kiválasztása.

   A rendszergazda kiválasztja azt a módot, amelyet a szabályok egyikében sem szereplő alkalmazásokkal folytatott munka során használni kíván (alkalmazás tiltólista és engedélyezési lista).

Ha egy felhasználó megkísérli egy tiltott alkalmazás elindítását, a Kaspersky Endpoint Security blokkolja az alkalmazás elindítását, és értesítést jelenít meg (részletek az alábbi ábrán).

Elérhető a *tesztelési mód*, amellyel ellenőrizheti az Alkalmazásfelügyelő beállításait. Ebben a módban a Kaspersky Endpoint Security a következőt teszi:

- lehetővé teszi az alkalmazások betöltését rendszerindításkor, köztük a letiltottakét is;
- értesítést jelenít a tiltott alkalmazások elindításáról, és a felhasználó számítógépére vonatkozó információt rögzít a jelentésben;
- adatokat küld a tiltott alkalmazások indításáról a Kaspersky Security Center számára.



Az Alkalmazásfelügyelő értesítései

Az Alkalmazásfelügyelő üzemmódjai

Az Alkalmazásfelügyelő összetevő két módban működhet:

- **Tiltólista**. Ebben a módban az Alkalmazásfelügyelő a felhasználók számára engedélyezi minden alkalmazás elindítását, kivéve az Alkalmazásfelügyelő blokkolási szabályai által letiltottakat.

  Alapértelmezés szerint ez a mód van engedélyezve az Alkalmazásfelügyelőben.

- **Engedélyezési lista**. Ebben a módban az Alkalmazásfelügyelő a felhasználók számára blokkolja az összes olyan alkalmazás elindítását, amely engedélyezett, és nincs letiltva az Alkalmazásfelügyeleti szabályaiban.

  Ha az Alkalmazásfelügyelő engedélyezési szabályai teljes mértékben meg vannak adva, az összetevő minden, a helyi hálózati rendszergazda által nem ellenőrzött új alkalmazás indítását blokkolja, miközben engedélyezi az operációs rendszer és a felhasználók számára munkájukhoz szükséges megbízható alkalmazások működését.

  Elolvashatja az Alkalmazásfelügyelői szabályok engedélyezési lista módban történő konfigurálására vonatkozó ajánlásokat.

Az Alkalmazásfelügyelő e módokban való működése egyaránt beállítható a Kaspersky Endpoint Security helyi felületén, illetve a Kaspersky Security Center segítségével.

A Kaspersky Security Center azonban olyan eszközöket is kínál, amelyek a Kaspersky Endpoint Security helyi felületén nem találhatók meg, köztük az alábbi feladatokhoz szükséges eszközöket:

- Alkalmazáskategóriák létrehozása.

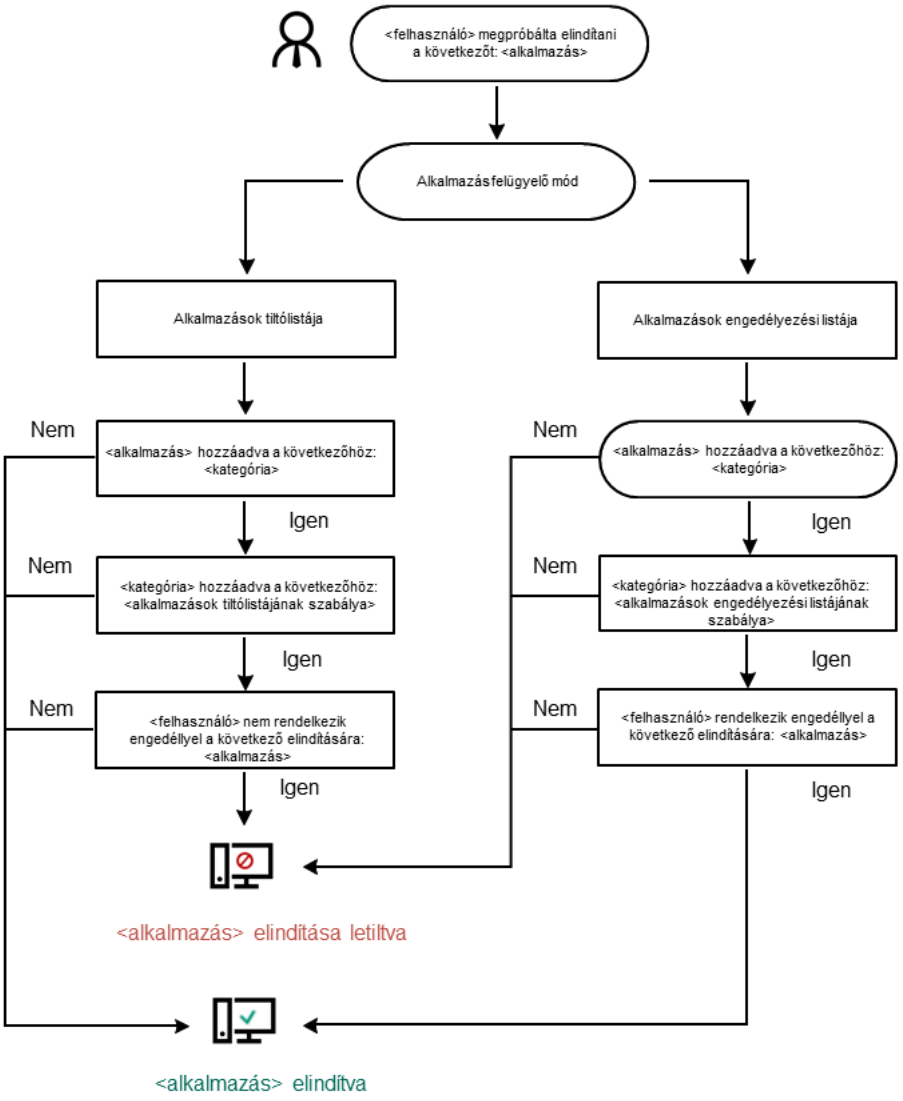
  A Kaspersky Security Center Adminisztrációs Konzolban előállított Alkalmazásfelügyeleti szabályok egyedi alkalmazáskategóriákon alapulnak, nem pedig szerepeltetési és kizárási feltételeken, mint a Kaspersky Endpoint Security helyi felülete esetén.

- A vállalati LAN számítógépeken telepített alkalmazásokra vonatkozó információk fogadása.

Ezért javasoljuk az Alkalmazásfelügyelő összetevő működésének beállítását a Kaspersky Security Center segítségével.

Alkalmazásfelügyelő műveleti algoritmusa

A Kaspersky Endpoint Security algoritmust használva hoz döntést egy adott alkalmazás elindításáról (részletek a lentebbi ábrán).



Alkalmazásfelügyelő műveleti algoritmusa

Az Alkalmazásfelügyelő összetevő beállításai

Paraméter	Leírás
Művelet szabályok által blokkolt alkalmazások indításakor	**Szabályok alkalmazása**. A Kaspersky Endpoint Security a kiválasztott módnak megfelelően kezeli az alkalmazások indítását. **Tesztszabályok**. A Kaspersky Endpoint Security lehetővé teszi az Alkalmazásfelügyelő jelenlegi módjában blokkolt alkalmazás elindítását, azonban az indítás információit a jelentésben rögzíti.
Alkalmazásindítás vezérlésének módja	Az alábbi opciók közül választhat: • **Tiltólista**. Ha ez az opció van kiválasztva, az Alkalmazásfelügyelő az összes felhasználó számára engedélyezi bármely alkalmazás elindítását, kivéve, ha teljesülnek az Alkalmazásfelügyelő blokkolási szabályainak feltételei. • **Engedélyezési lista**. Ha ez az opció van kiválasztva, az Alkalmazásfelügyelő az összes felhasználó számára blokkolja bármely alkalmazás elindítását, kivéve, ha teljesülnek az Alkalmazásfelügyelő engedélyezési szabályainak feltételei. Ha az **Engedélyezési lista** mód van kiválasztva, két Alkalmazásfelügyeleti szabály automatikusan létrejön: • **Golden Image**. • **Megbízható frissítéstelepítők**. Az automatikusan létrehozott szabályok nem törölhetők, és beállításaik nem szerkeszthetők. A szabályok letilthatók és engedélyezhetők.
A DLL-modulok betöltésének figyelése	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security szabályozza a DLL modulok betöltését, ha a felhasználó alkalmazásokat próbál elindítani. A DLL modullal és az azt betöltő alkalmazással kapcsolatos információk bekerülnek a jelentésbe. Amikor engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, győződjön meg arról, hogy az Alkalmazásfelügyelő beállításaiban engedélyezve van a következő szabályok egyike: **Golden Image** szabály, illetve egy másik szabály, amely tartalmazza a **Golden Image\Trusted Certificates** KL-kategóriát, és gondoskodik a megbízható DLL-modulok és illesztőprogramok betöltéséről a Kaspersky Endpoint Security indítása előtt. Ha úgy engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, hogy a **Golden Image** szabály ki van kapcsolva, az instabilitást okozhat az operációs rendszerben. A Kaspersky Endpoint Security kizárólag a jelölőnégyzet bejelölését követően betöltött DLL modulokat és illesztőprogramokat figyeli. A jelölőnégyzet bejelölése után ajánlott a számítógép újraindítása annak érdekében, hogy az alkalmazás minden DLL-modult és illesztőprogramot figyeljen, beleértve a Kaspersky Endpoint Security indítása előtt betöltött modulokat is.
Szigorú digitális aláírás-ellenőrzés használata	Kiválaszthat egy tanúsítványt egy alkalmazásfelügyeleti szabály kiváltó feltételeként. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security csak a megbízható rendszertanúsítvány-tárhelytől származó tanúsítványokkal aláírt alkalmazásokra alkalmaz szabályokat. Az ilyen tanúsítvánnyal aláírt alkalmazásokat a védelmi összetevők is megbízhatónak tekintik, például a *Kártevő vizsgálata* feladat. Ha azonban egy másik tárolóból származó tanúsítványt ad meg egy alkalmazásfelügyeleti szabályban, a Kaspersky Endpoint Security nem alkalmaz ilyen szabályt. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security szabályokat alkalmaz a Windows Megbízható főtanúsítványok tárolójából származó tanúsítvánnyal aláírt alkalmazásokra. Az ilyen alkalmazások nem részei a megbízható zónának. A védelmi összetevők figyelik az ilyen alkalmazások tevékenységét.
Alkalmazásblokkolással kapcsolatos üzenetsablonok	**Üzenet a blokkolásról**. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja. **Üzenet a rendszergazdának**. Üzenetsablon olyan üzenet írásához, amelyet a felhasználó küldhet a vállalati LAN rendszergazdájának, ha a felhasználó véleménye szerint egy alkalmazást tévedésből blokkol a rendszer. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Alkalmazásindítás hozzáférésének blokkolására vonatkozó üzenet az adminisztrátornak**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

Adaptív Anomáliafelügyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

Az Adaptív Anomáliafelügyelő összetevő megfigyeli és letiltja azokat a tevékenységeket, amelyek nem megszokottak a cég hálózatán található számítógépeken. Az Adaptív Anomáliafelügyelő egy szabálycsoport alapján követi nyomon a nem jellemző viselkedést (például a *Start of Microsoft PowerShell from office application* szabályt). A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján. Konfigurálhatja, hogy az Adaptív Anomáliafelügyelő miként kezelje az egyes szabályokat és engedélyezheti olyan PowerShell szkriptek végrehajtását, amelyek bizonyos feladatokat automatizálnak. A Kaspersky Endpoint Security az alkalmazás adatbázisával együtt frissíti a szabálycsoportokat. A szabálycsoportok frissítését manuálisan kell megerősíteni.

Az Adaptív Anomáliafelügyelő beállításai

Az Adaptív Anomáliafelügyelő beállítása a következő lépésekből áll:

1. Az Adaptív Anomáliafelügyelő betanítása.

   Miután engedélyezte az Adaptív Anomáliafelügyelőt, a szabályok *tanuló módban* vannak. A tanulás során az Adaptív Anomáliafelügyelő nyomon követi a szabályok végrehajtását kiváltó tevékenységeket és eseményriasztásokat küld a Kaspersky Security Center részére. Minden szabálynak megvan a saját tanulási ideje. A tanulási mód időtartamát a Kaspersky szakemberei határozták meg. Normális esetben a tanulási mód két hétig aktív.

   Ha egy szabály betartását a tanulási időszak során egyszer se váltották ki, akkor az Adaptív Anomáliafelügyelő az adott szabályhoz kapcsolódó tevékenységeket gyanúsnak fogja minősíteni. A Kaspersky Endpoint Security le fog tiltani az adott szabályhoz kapcsolódó minden tevékenységet.

   Ha egy szabály végrehajtását kiváltották a tanulási időszakban, akkor a Kaspersky Endpoint Security naplóbejegyzést készít az eseményekről a szabálykiváltó jelentésben és a **Rule triggers in Smart Training state** gyűjteményben.

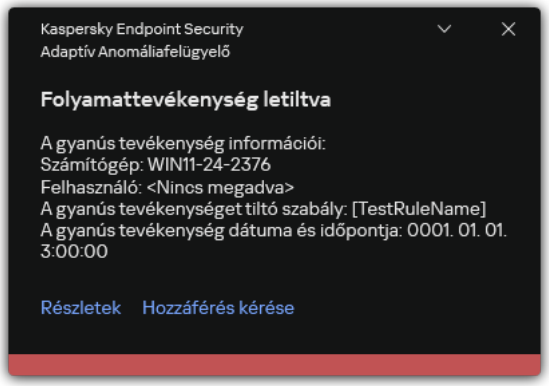
2. A szabálykiváltó jelentés értelmezése.

   A szabálykiváltó jelentést vagy a **Rule triggers in Smart Training state** gyűjteményt a rendszergazdának kell értelmezni. A rendszergazda ezt követően kiválaszthatja az Adaptív Anomáliafelügyelő viselkedését az adott helyzetben, hogy blokkolja vagy engedélyezi a szabály betartását. A rendszergazda emellett folyamatosan nyomon követheti az adott szabály működését és kibővítheti a tanulási mód időtartamát. Ha a rendszergazda nem tesz semmit, az alkalmazás továbbra is tanulási módban fog működni. Az útmutató mód feltételek újraindultak.

Az Adaptív Anomáliafelügyelő konfigurálása valós időben a következő csatornákon történik:

- Az Adaptív Anomáliafelügyelő automatikusan letiltja vagy engedélyezi a szabályokhoz társított tevékenységeket, amelyek nem lettek kiváltva tanulási módban.
- A Kaspersky Endpoint Security új szabályokat ad hozzá és eltávolítja az elavultakat.
- A rendszergazda azt követően konfigurálja az Adaptív Anomáliafelügyelő működését, hogy áttekintette a szabálykiváltó jelentést és a **Rule triggers in Smart Training state** gyűjtemény tartalmát. Javasoljuk, hogy ellenőrizze a szabályokat kiváltó jelentést és a **Rule triggers in Smart Training state** tárhely tartalmát.

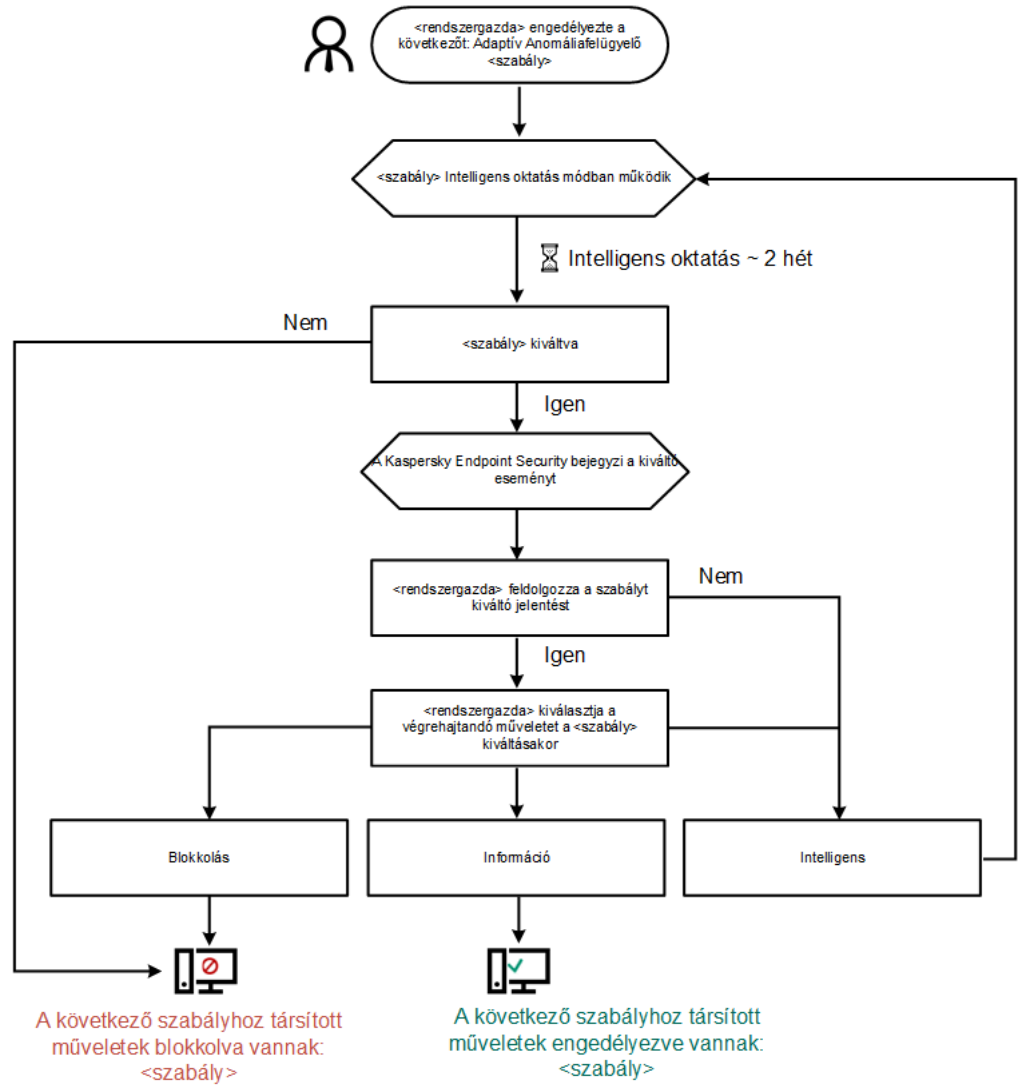
Amikor egy rosszindulatú alkalmazás megpróbál műveletet végrehajtani, a Kaspersky Endpoint Security letiltja a műveletet és értesítést jelenít meg (lásd az alábbi ábrát).



Adaptív Anomáliafelügyeleti értesítés

Adaptive Anomaly Control operating algorithm

A Kaspersky Endpoint Security a következő algoritmus alapján dönti el, hogy engedélyezze vagy letiltsa az adott szabályhoz társított műveletet (lásd az alábbi ábrán).



Adaptive Anomaly Control operating algorithm

Adaptive Anomaly Control component settings

Paraméter	Leírás
Jelentés az Adaptív Anomáliafelügyeleti szabályok állapotáról *(csak a Kaspersky Security Center konzolon érhető el)*	Ez a jelentés az Adaptív Anomáliafelügyelő észlelései szabályainak állapotáról tartalmaz információkat (például *Letiltva* vagy *Blokkolva*). A jelentés minden rendszergazdai csoport számára létrejön.
Jelentés az Adaptív Anomáliafelügyelő aktívan alkalmazott szabályairól *(csak a Kaspersky Security Center konzolon érhető el)*	Ez a jelentés tartalmazza az Adaptív Anomáliafelügyelő által észlelt gyanús tevékenységek információit. A jelentés minden rendszergazdai csoport számára létrejön.

Paraméter	Leírás
Szabályok	Adaptív Anomáliafelügyeleti szabályok táblázata A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján.
Sablonok	**Üzenet a blokkolásról**. Üzenetsablon, ami akkor jelenik meg a felhasználónak, amikor aktiválódik az Adaptív Anomáliafelügyelő egy olyan szabálya, amely blokkolja a gyanús tevékenységet. **Üzenet a rendszergazdának**. Üzenetsablon a felhasználó számára, ami t a felhasználó a helyi hálózat rendszergazdája részére tud küldeni abban az esetben, ha a művelet letiltása szerinte téves döntés volt. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: **Alkalmazástevékenység blokkolásáról szóló üzenet a rendszergazdának**. Az esemény leírása egy üzenetet tartalmaz a rendszergazdának behelyettesített változókkal. Ezeket az eseményeket a Kaspersky Security Center konzolján tekintheti meg az előre meghatározott **User requests** eseményválasztással. Ha a vállalatnál nincs telepítve a Kaspersky Security Center, vagy nincs kapcsolat a Felügyeleti kiszolgálóval, az alkalmazás üzenetet küld a rendszergazdának a megadott e-mail-címre.

Rendszerintegritás-figyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt.

A 12.6-os verziótól kezdve a Kaspersky Endpoint Security for Windows a Fájlintegritás-figyelő összetevő helyett a Rendszerintegritás-felügyelet összetevőt tartalmazza. A Rendszerintegritás-figyelő összetevő a Fájlintegritás-figyelő összes funkcióját tartalmazza, és lehetővé teszi a beállításjegyzék-változások és a külső eszközök csatlakoztatásának figyelését.

A Rendszerintegritás-figyelő figyeli az operációs rendszerben bekövetkező olyan változásokat, amelyek a számítógépes biztonság sérülésére utalhatnak. Ilyen változások észlelésekor a Kaspersky Endpoint Security megfelelő eseményeket generál, és figyelmezteti a rendszergazdát. A Rendszerintegritás-figyelő valós idejű üzemmódban működhet, és kérésre rendszerintegritás-ellenőrzéseket is végezhet.

Valós idejű rendszerintegritás-figyelő

Valós idejű üzemmódban a Rendszerintegritás-figyelő nyomon követi az összetevő hatókörébe tartozó objektumok változásait (a *figyelési hatókör*). A Rendszerintegritás-figyelő lehetővé teszi az ilyen objektumokhoz való illetéktelen hozzáférés valós idejű blokkolását is.

Igény szerinti rendszerintegritás-ellenőrzés

Az igény szerinti rendszerintegritás-ellenőrzés egy manuálisan vagy ütemezetten futtatható feladat. A *Rendszerintegritás-ellenőrzés* feladat futtatásához konfigurálnia kell az összetevő hatókörét (a *figyelési hatókör*), és létre kell hoznia egy alapszintet. Az *alapszint* a rendszerben lévő objektumok rögzített állapota, amelyet az alkalmazás referenciaként használ az aktuális állapottal való összehasonlításkor.

Paraméter	Leírás
A blokkolási szabályok működési módja	• **Blokkolás**. Ebben a módban a Rendszerintegritás-figyelő blokkolja a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt. • **Tájékoztatás**. Ebben a módban a Rendszerintegritás-figyelő engedélyezi a figyelési hatókörben lévő fájlokkal és beállításkulcsokkal kapcsolatos műveleteket, és létrehoz egy megfelelő eseményt.
Valós idejű rendszerintegritás-figyelő	Valós idejű üzemmódban a Rendszerintegritás-figyelő nyomon követi az összetevő hatókörébe tartozó objektumok változásait (a *figyelési hatókör*). A Rendszerintegritás-figyelő lehetővé teszi az ilyen objektumokhoz való illetéktelen hozzáférés valós idejű blokkolását is.
Eszközök figyelése	A Rendszerintegritás-figyelő figyeli a külső eszközök csatlakoztatását és leválasztását.
Fájlok és a beállításjegyzék figyelése	A Rendszerintegritás-figyelő figyeli a fájlok, mappák és beállításjegyzékek változásait.
Rendszerintegritás ellenőrzése	Az igény szerinti rendszerintegritás-ellenőrzés egy manuálisan vagy ütemezetten futtatható feladat. A *Rendszerintegritás-ellenőrzés* feladat futtatásához konfigurálnia kell az összetevő hatókörét (a *figyelési hatókör*), és létre kell hoznia egy alapszintet. Az *alapszint* a rendszerben lévő objektumok rögzített állapota, amelyet az alkalmazás referenciaként használ az aktuális állapottal való összehasonlításkor.

Végponti szenzor

A Végponti szenzor nem része a Kaspersky Endpoint Security 11.4.0 terméknek.

A Végponti szenzor összetevőt a Kaspersky Security Center Web Console és a Kaspersky Security Center Adminisztrációs konzol helyeken kezelheti. A Végponti szenzor kezelésére nincs mód a Kaspersky Security Center Cloud Console-ban.

A *Végponti szenzor* kialakítása szerint a Kaspersky Anti Targeted Attack Platform (KATA) programmal működik. A *Kaspersky Anti Targeted Attack Platform* egy megoldás, ami a kifinomult fenyegetések, például célzott támadások és speciális, állandó veszélyek (APT), valamint nagy kockázatú veszélyforrások időszerű észlelésére szolgál. A Kaspersky Anti Targeted Attack Platform három funkcionális egységet tartalmaz:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Az összes funkcionális egységet vagy az egyes funkcionális egységeket külön is megvásárolhatja. A megoldás részleteivel kapcsolatos információért lásd a Kaspersky Anti Targeted Attack Platform útmutatót.

A Végponti szenzor kezelésére a következő korlátozások vonatkoznak:

- Lehetősége van módosítani a Végponti szenzor beállításait egy irányelven belül, ha a számítógépre a Kaspersky Endpoint Security verziószáma 11.0.0 és 11.3.0 közötti. A Végponti szenzor összetevőnek irányelv segítségével történő konfigurálására vonatkozó, további részleteket a Kaspersky Endpoint Security korábbi verzióinak súgócikkeiben olvashat.
- Ha a Kaspersky Endpoint Security 11.4.0-s vagy újabb verziója van telepítve a számítógépre, nem áll módjában konfigurálni a Végponti szenzor összetevőt az irányelv segítségével.

A Végponti szenzor telepítése ügyfélszámítógépeken történik. Ezeken a számítógépeken az összetevő folyamatosan figyeli a folyamatokat, az aktív hálózati kapcsolatokat és a módosított fájlokat. A Végponti érzékelő adatokat ad tovább a KATA kiszolgáló számára.

Az összetevő a következő operációs rendszerek alatt működik:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-bit).

A KATA működésével kapcsolatos részletes információért lásd a Kaspersky Anti Targeted Attack Platform súgót.

Sandbox

A Kaspersky Endpoint Security for Windows tartalmaz egy beépített ügynököt a Kaspersky Sandbox megoldással való integrációhoz. *A Sandbox* összetevő észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (a Sandbox-kiszolgálók). A megoldás részleteivel kapcsolatos információkat a Kaspersky Sandbox súgóban és a Kaspersky Anti Targeted Attack Platform súgóban találja.

A 12.7-es verziótól kezdve a Kaspersky Endpoint Security for Windows támogatja a Sandbox összetevőt, amely a Kaspersky Anti Targeted Attack Platform megoldás részét képezi. A Kaspersky Sandbox megoldással ellentétben a KATA Sandbox összetevő lehetővé teszi a fájlok automatikus, valamint manuális vizsgálatát is a fájl helyi menüjéből.

A KATA Sandbox használatához a Kaspersky Anti Targeted Attack Platform 7.0 vagy újabb verziójának telepítése szükséges.

Az összetevőt csak a Kaspersky Security Center Web Console használatával lehet felügyelni. Ezt az összetevőt nem felügyelheti az Adminisztrációs Konzol (MMC) használatával.

Paraméter	Leírás
Integration mode	**Kaspersky Sandbox**. Integráció a Kaspersky Sandbox megoldással. Az alkalmazás csak automatikus módban küldi el a Kaspersky Sandboxban vizsgálat alá vont fájlokat. **KATA Sandbox**. Integráció a Kaspersky Anti Targeted Attack Platform megoldás Sandbox összetevőjével. Kiválaszthatja a vizsgálathoz a fájl beküldési módját: • **Manually**. A felhasználó manuálisan küldi be a fájlt vizsgálatra a helyi menüből (**Küldés a Sandboxba**). • **Automatically**. Az alkalmazás automatikusan észleli az objektumokat, és vizsgálat céljából elküldi azokat a Sandboxba. • **Combined**.
Server connection settings	**Timeout (msec)**. Időtúllépés történt a Sandbox-kiszolgáló (Kaspersky Sandbox esetén) vagy a Central Node-kiszolgáló (KATA esetén) csatlakoztatásakor. A beállított időtúllépés letelte után a Kaspersky Endpoint Security kérést küld a következő kiszolgálónak. Növelheti a kiszolgáló kapcsolódási időtúllépését, ha a kapcsolat sebessége alacsony, vagy ha a kapcsolat instabil. A kérések ajánlott időtúllépése 0.5 másodperc vagy kevesebb. **Request queue**. A kérési várólista mappájának mérete. Ha több objektumot küld vizsgálatra a Sandboxban, a Kaspersky Endpoint Security egy kérés-várólistát hoz létre. Alapértelmezés szerint a kérési várólista mappamérete 100 MB-ra van korlátozva. A maximális méret elérése után a Sandbox leállítja az új kérések hozzáadását a várólistához, és elküldi a megfelelő eseményt a Kaspersky Security Centernek. A kiszolgáló konfigurációjától függően konfigurálhatja a kérési várólista mappaméretét. **Server TLS certificate**. A Sandbox-kiszolgálóval (Kaspersky Sandbox esetén) vagy a Central Node-kiszolgálóval (KATA esetén) való megbízható kapcsolat konfigurálásához TLS-tanúsítványt kell készítenie. Ezután hozzá kell adnia a tanúsítványt a számítógéphez egy házirend segítségével. A tanúsítványt a Sandbox-kiszolgálóhoz (Kaspersky Sandbox esetén) vagy a Central Node-kiszolgálóhoz (KATA esetén) is hozzá kell adnia. **Use two-way authentication** (csak a KATA Sandboxhoz). Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.
Connection to Sandbox servers	**Kaspersky Sandbox**. A Sandbox-kiszolgáló kapcsolódási beállításai. A kiszolgálók a Microsoft Windows operációs rendszerek telepített virtuális képeit használják a vizsgálandó objektumok futtatására. Megadhat egy IP-címet (IPv4 vagy IPv6) vagy egy teljes tartománynevet. **KATA Sandbox**. Central Node-kiszolgáló kapcsolódási beállításai. A Central Node kiválasztja az optimális beállításokat a vizsgálathoz, és elosztja a terhelést a Sandbox-kiszolgálók között.
Action on threat detection	**Move copy to Quarantine, delete object**. Ha ezt az opciót választja, a Kaspersky Endpoint Security törli a számítógépen talált rosszindulatú objektumot. Az objektum törlése előtt a Kaspersky Endpoint Security biztonsági másolatot készít arra az esetre, ha az objektumot később vissza kell állítani. A Kaspersky Endpoint Security a biztonsági másolatot karanténba helyezi. **Run Critical Areas Scan**. Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a *Critical Areas Scan* feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja. **Create IOC Scan task**. Ha ezt az opciót választja, a Kaspersky Endpoint Security automatikusan létrehozza az *IOC Scan (autonóm IOC vizsgálati feladat)* elemet. Ehhez a feladathoz konfigurálhatja a futásmódot, a vizsgálat hatókörét és az IOC észlelési műveletet (*Move copy to Quarantine, delete object* vagy *Run Critical Areas Scan*). Az *IOC Scan* feladat beállításainak módosításához nyissa meg a feladat beállításait.
IOC Scan scope	**Critical file areas**. Ha ezt az opciót választja, a Kaspersky Endpoint Security csak a számítógép kritikus fájlterületein végez IOC vizsgálatot: rendszermag memóriája és rendszerindítási szektorok. **File areas on system drive of the computer**. Ha ez az opció van kiválasztva, a Kaspersky Endpoint Security IOC vizsgálatot végez a számítógép rendszermeghajtóján.
Run IOC Scan task	**Manually**. A futásmód, amelyben manuálisan elindíthatja az *IOC Scan* feladatot, amikor az Önnek kényelmes. **Automatically**. Olyan futtatási mód, amelyben a Kaspersky Endpoint Security egy fenyegetés észlelését követően automatikusan elindítja az *IOC Scan* szolgáltatást. **Run only when the computer is idle**. A futásmód, amelyben a Kaspersky Endpoint Security futtatja az *IOC vizsgálat* feladatot, ha a képernyővédő aktív, vagy a képernyő zárolva van. Ha a felhasználó feloldja a számítógép zárolását, a Kaspersky Endpoint Security felfüggeszti a feladatot. Ez azt jelenti, hogy a feladat végrehajtása több napot is igénybe vehet.

Managed Detection and Response

A Kaspersky Endpoint Security for Windows támogatja a Managed Detection and Response megoldással való integrációt. A *Kaspersky Managed Detection and Response (MDR)* megoldás automatikusan észleli és elemzi az infrastruktúrában bekövetkező biztonsági incidenseket. Ehhez az MDR a végpontoktól és a gépi tanulásból kapott telemetriai adatokat használja. Az MDR incidensadatokat küld a Kaspersky szakértőinek. A szakértők ezután feldolgozhatják az incidenst, és például új bejegyzést adhatnak hozzá a vírusadatbázisokhoz. Alternatív megoldásként a szakértők javaslatokat tehetnek az incidens feldolgozására, és például javasolhatják a számítógép leválasztását a hálózatról. A megoldás működéséről részletes információt a Kaspersky Managed Detection and Response súgójában talál.

A Managed Detection and Response beállításai

Paraméter	Leírás
MDR konfigurációs fájl	A BLOB fájl tartalmazza az ügyfélazonosítót és a Kaspersky Managed Detection and Response licencére vonatkozó információkat. A BLOB fájl az MDR konfigurációs fájl ZIP-archívumában található. A ZIP-archívumot a Kaspersky Managed Detection and Response konzoljában szerezheti be. A BLOB fájlról részletes információt a Kaspersky Managed Detection and Response súgójában talál.

Endpoint Detection and Response

A Kaspersky Endpoint Security for Windows beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Optimum megoldáshoz (a továbbiakban: „EDR Optimum"). A 11.8.0 verzióval kezdődően a Kaspersky Endpoint Security for Windows beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Expert megoldáshoz (a továbbiakban: „EDR Expert"). A *Kaspersky Endpoint Detection and Response* megoldáscsomag a vállalat informatikai infrastruktúrájának védelmét biztosítja a fejlett számítógépes fenyegetések ellen. A megoldások ötvözik a fenyegetések különböző automatikus észlelését, és képesek reagálni ezekre a fenyegetésekre, hogy ellensúlyozzák a speciális támadásokat, beleértve az új biztonsági réseket, a zsarolóprogramokat, a fájlmentes támadásokat, valamint a legitim rendszereszközöket használó módszereket. Az EDR Expert több fenyegetésfigyelési és reagálási funkciót kínál, mint az EDR Optimum. A megoldásokról részletesen a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban olvashat.

A Kaspersky Endpoint Detection and Response felügyeli és elemzi a fenyegetések fejlődését, és olyan információkat szolgáltat a *biztonsági személyzetnek* vagy a *rendszergazdának* a lehetséges támadásról, amely szükséges az időben történő reagáláshoz. A Kaspersky Endpoint Detection and Response külön ablakban jeleníti meg az észlelés részleteit. A *riasztás* olyan esemény a vállalati IT-infrastruktúrában, amelyet az alkalmazás szokatlan vagy gyanús eseményként azonosított, és amely biztonsági fenyegetést jelenthet a vállalati IT-infrastruktúrára. Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére. Az észlelési részletek közé tartoznak például a számítógépen megjelenő fájlok előzményei. Az észlelések kezelésével kapcsolatos részleteket a Kaspersky Endpoint Detection and Response Optimum súgóban és a Kaspersky Endpoint Detection and Response Expert súgóban találja.

A Endpoint Detection and Response Optimum összetevőt a Web Console és a Cloud Console segítségével konfigurálhatja. A Endpoint Detection and Response Expert (cloud) összetevő beállításai csak a Cloud Console-ban érhetők el.

Paraméter	Leírás
Enable advanced system activity logging	A kiterjesztett telemetria javítja az IOC-észlelés pontosságát, de a számítógép ilyenkor több erőforrást használ. Javasoljuk, hogy engedélyezze a kiterjesztett telemetriát a számítógépen az utólagos IOC-vizsgálathoz. A *Visszamenőleges IOC vizsgálat* az *IOC Scan* egyik módja, amelyben a Kaspersky Endpoint Security egy bizonyos időszak adatai alapján a sérülésekre utaló jelek után kutat. Ez az üzemmód arra szolgál, hogy a védett számítógép telemetriai adatai – például a hálózati tevékenység, a folyamatok, a fájlok és egyéb telemetriai adatok – alapján felderítse a biztonsági incidensekre utaló jeleket. Ha a kiterjesztett telemetria le van tiltva, a Kaspersky Endpoint Security rotálhatja az észlelt sérülési indikátorokra vonatkozó információkat.
Network Isolation	A számítógép automatikus leválasztása a hálózatról válaszul az észlelt fenyegetésekre. Amikor a hálózatelkülönítés be van kapcsolva, az alkalmazás leválaszt minden aktív kapcsolatot, és blokkol minden új TCP/IP-kapcsolatot a számítógépen. Az alkalmazás csak a következő kapcsolatokat hagyja aktívan: • A Hálózatelkülönítés kizárásaiban felsorolt kapcsolatok. • A Kaspersky Endpoint Security szolgáltatásai által kezdeményezett kapcsolatok. • A Kaspersky Security Center Network Agent által kezdeményezett kapcsolatok.
Automatically unlock isolated device in (hours)	A hálózatelkülönítés meghatározott idő elteltével automatikusan vagy manuálisan kikapcsolható. Alapértelmezés szerint a Kaspersky Endpoint Security 5 órával az elkülönítés megkezdése után kapcsolja ki a hálózatelkülönítést.
Network isolation exclusions	A hálózatelkülönítési kizárásokhoz tartozó szabályok listája. Az e szabályoknak megfelelő hálózati kapcsolatok nincsenek blokkolva a számítógépeken, ha a Hálózatelkülönítés be van kapcsolva. A Hálózatelkülönítés kizárásainak konfigurálásához használhatja a *szabványos hálózati profilok* listáját. Alapértelmezés szerint a kizárások közé tartoznak azok a hálózati profilok, amelyek a DNS-/DHCP-kiszolgálóval és a DNS-/DHCP-ügyfélszerepkörrel rendelkező eszközök zavartalan működését biztosító szabályokat tartalmazzák. Módosíthatja a szabványos hálózati profilok beállításait, vagy manuálisan is megadhat kizárásokat. A házirend tulajdonságaiban megadott kizárások csak akkor alkalmazhatók, ha a hálózatelkülönítés automatikusan bekapcsol az észlelt fenyegetés hatására. A számítógép tulajdonságaiban megadott kizárások csak akkor érvényesek, ha a hálózatelkülönítést a Kaspersky Security Center konzoljának számítógép-tulajdonságaiban vagy a riasztási részletekben manuálisan kapcsolják be.
Execution Prevention	A végrehajtható fájlok és szkriptek futtatásának és az Office formátumú fájlok megnyitásának vezérlése. Például megakadályozhatja a nem biztonságosnak ítélt alkalmazások futtatását a kiválasztott számítógépen. A végrehajtás megakadályozása támogatja az Office-fájlkiterjesztések és a szkriptértelmezők készletét. A Végrehajtás megelőzése összetevő használatához hozzá kell adnia végrehajtás-megelőzési szabályokat. A *végrehajtás-megelőzési szabály* olyan kritériumok összessége, amelyeket az alkalmazás figyelembe vesz, amikor egy objektum végrehajtására reagál, például amikor blokkolja az objektum végrehajtását. Az alkalmazás elérési utak vagy az MD5 és SHA256 kivonatolási algoritmusokkal kiszámított ellenőrzőösszegek alapján azonosítja a fájlokat.
Action on execution or opening of forbidden object	**Block and add to event log**. Ebben az üzemmódban az alkalmazás blokkolja a megelőzési szabály kritériumainak megfelelő objektumok végrehajtását vagy dokumentumok megnyitását. Az alkalmazás egy eseményt is közzétesz az objektumok végrehajtására vagy dokumentumok megnyitására irányuló kísérletekről a Windows eseménynaplójában és a Kaspersky Security Center eseménynaplójában. **Add to event log**. Ebben az üzemmódban a Kaspersky Endpoint Security közzétesz egy eseményt a Windows eseménynaplójában és a Kaspersky Security Center eseménynaplójában a végrehajtható objektumok futtatására vagy a megelőzési szabály kritériumainak megfelelő dokumentumok megnyitására tett kísérletről, de nem blokkolja az objektum vagy a dokumentum futtatási vagy megnyitási kísérletét. Alapértelmezésben ez a mód van kiválasztva.
Execution prevention rules	A *végrehajtás-megelőzési szabály* olyan kritériumok összessége, amelyeket az alkalmazás figyelembe vesz, amikor egy objektum végrehajtására reagál, például amikor blokkolja az objektum végrehajtását. Az alkalmazás elérési utak vagy az MD5 és SHA256 kivonatolási algoritmusokkal kiszámított ellenőrzőösszegek alapján azonosítja a fájlokat.

Paraméter	Leírás
Cloud Sandbox	*Cloud Sandbox* egy olyan technológia, amely lehetővé teszi a speciális fenyegetések észlelését egy számítógépen. A Kaspersky Endpoint Security elemzés céljából automatikusan továbbítja az észlelt fájlokat a Cloud Sandbox részére. A Cloud Sandbox elszigetelt környezetben futtatja ezeket a fájlokat, hogy azonosítsa a rosszindulatú tevékenységeket és döntsön a megbízhatóságukról. Ezen fájlok adatai ezután Kaspersky Security Network részére elküldésre kerülnek. Ezért, ha a Cloud Sandbox rosszindulatú fájlt észlelt, a Kaspersky Endpoint Security, a fenyegetésnek a megszüntetése érdekében az összes olyan számítógépen el fogja végezni a megfelelő műveletet, amelyen ez a fájl észlelhető. A Cloud Sandbox technológia folyamatosan engedélyezve van és minden Kaspersky Security Network felhasználó számára elérhető, függetlenül attól, milyen típusú licencet használnak. Ha ez a jelölőnégyzet ki van választva, a Kaspersky Endpoint Security engedélyezi a Cloud Sandbox segítségével észlelt fenyegetések számlálóját a fő alkalmazásablaknak a **Fenyegetésészlelő technológiák** alatt. A Kaspersky Endpoint Security a Cloud Sandbox fenyegetés észlelő technológiát az alkalmazás eseményekben és a Kaspersky Security Center konzol *Report on threats* is jelzi.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

A Kaspersky Endpoint Security for Windows támogatja az integrációt a Kaspersky Endpoint Detection and Response Expert (on-premises) megoldással. *Kaspersky Endpoint Detection and Response Expert (on-premises)* egy vállalati kiberbiztonsági megoldás, amely olyan Kaspersky-alkalmazásokat tartalmaz, amelyek segítségével a vállalatok a legtöbb típusú kiberkockázattal szemben védekezhetnek, és a legfontosabb fenyegetés-terjesztési forgatókönyveket lefedhetik. Az EDR Expert (on-premises) összetevők az Open Single Management Platformon (OSMP) vannak telepítve. Ez a platform egyetlen felületen futtat platformokon átívelő forgatókönyveket, és lehetővé teszi a Kaspersky-alkalmazások és a harmadik féltől származó alkalmazások egy átfogó biztonsági rendszerbe való integrálását.

A megoldás egyik központi eleme a *SIEM*. A SIEM nyomon követi az összes összetevőből érkező eseményeket, és a gyártó és a felhasználó által meghatározott szabályok segítségével korrelálja ezeket az eseményeket egymással. Az EDR Expert (on-premises) a vállalati infrastruktúrából kapott naplókat és telemetriát vizsgálja a támadások automatikus észlelése érdekében, és lehetővé teszi az incidensek egységes vizsgálati grafikon segítségével való kivizsgálását, amely az összes, az EDR Expert (on-premises) alkalmazásban gyűjtött eseményt egyesíti, beleértve a Kaspersky alkalmazásokból és harmadik fél információbiztonsági termékeiből származó eseményeket is.

Az összetett incidensekre való reagáláshoz az EDR Expert (on-premises) előre beállított és felhasználó által meghatározott forgatókönyveket használ. Harmadik féltől származó alkalmazásokból származó válaszakciókat és több alkalmazást is érintő válaszforgatókönyveket is használhat.

Endpoint Detection and Response (KATA)

A Kaspersky Endpoint Security for Windows támogatja a Kaspersky Endpoint Detection and Response összetevővel való együttműködést a Kaspersky Anti Targeted Attack Platform (EDR (KATA)) megoldás részeként. A *Kaspersky Anti Targeted Attack Platform* egy megoldás, ami a kifinomult fenyegetések, például célzott támadások és speciális, állandó veszélyek (APT), valamint nagy kockázatú veszélyforrások időszerű észlelésére szolgál. A Kaspersky Anti Targeted Attack Platform három funkcionális egységet tartalmaz:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Az összes funkcionális egységet vagy az egyes funkcionális egységeket külön is megvásárolhatja. A megoldás részleteivel kapcsolatos információért lásd a Kaspersky Anti Targeted Attack Platform útmutatót.

A Kaspersky Endpoint Security a vállalati IT-infrastruktúra egyes számítógépeire van telepítve, és folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítás alatt álló fájlokat. A számítógépen zajló eseményekkel kapcsolatos információk (telemetriai adatok) elküldésre kerülnek a Kaspersky Anti Targeted Attack Platform kiszolgálóra. Ebben az esetben a Kaspersky Endpoint Security információkat küld a Kaspersky Anti Targeted Attack Platform kiszolgálónak az alkalmazás által észlelt fenyegetésekről, valamint az ilyen fenyegetések feldolgozási eredményeiről is.

Az EDR (KATA) és NDR (KATA) integráció a Kaspersky Security Center konzolon van konfigurálva. A beépített ügynök ezután a Kaspersky Anti Targeted Attack Platform konzol segítségével kezelhető, beleértve a feladatok futtatását, a karanténba helyezett objektumok kezelését, a jelentések megtekintését és az egyéb műveleteket.

Endpoint Detection and Response Expert (on-premises)

Paraméter	Leírás
Connection to telemetry collection servers	A *telemetriagyűjtő kiszolgáló* egy olyan SIEM-megoldás részét képező kiszolgáló, amely a számítógépen bekövetkező eseményekre vonatkozó információkat gyűjti, normalizálja, korrelálja, elemzi és tárolja. A telemetriagyűjtő kiszolgálókhoz (KUMA) való csatlakozáshoz állítsa be a következőket: • **Timeout (sec)**. A kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik kiszolgálóhoz. • **Server certificate**. TLS-tanúsítvány a kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). • **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). A kiszolgáló beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót. A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.
Address és **Port** (telemetriagyűjtő kiszolgálók)	A telemetriagyűjtő kiszolgálókhoz való csatlakozás beállításai. Megadhat egy IP-címet (IPv4 vagy IPv6). Több telemetriagyűjtő kiszolgáló címét is hozzáadhatja. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
Send telemetry to telemetry collection servers	Ezzel a funkcióval teljesen kikapcsolhatja a telemetriai adatok KATA-kiszolgálóra való küldését. Ha például a Kaspersky Anti Targeted Attack Platformot egy másik, szintén telemetriát használó megoldással együtt használja, kikapcsolhatja a KATA (EDR) platformnak való telemetriaküldést. Ez lehetővé teszi a kiszolgálói terhelés optimalizálását ezekhez a megoldásokhoz. Ha telepítette a Managed Detection and Response megoldást és a KATA (EDR) megoldást, használhatja az MDR-telemetriát, és létrehozhat Fenyegetésekre adott válasz típusú feladatokat a KATA (EDR) megoldásban. • **Send telemetry with IOA only**. Lehetővé teszi a telemetria optimalizálását és csak a telemetria küldését IOA segítségével. A *támadásjelző (IOA)* szabály a rendszeren belüli olyan gyanús viselkedések leírását tartalmazza, amelyek célzott támadásra utalhatnak. Az alkalmazás összehasonlítja a rendszerben zajló viselkedést ezekkel a szabályokkal, és naplózza a célzott támadásra utaló eseményeket. Az alkalmazás *streameléses vizsgálati* technológiát használ, amely lehetővé teszi az ilyen események valós idejű nyomon követését. • **Maximum event transmission delay (sec)**. Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc. • **Limit the number of event packets per transmission**. Az alkalmazás akkor szinkronizál a kiszolgálóval, amikor a puffer megtelik eseményekkel. Az alapértelmezett beállítás 1024 esemény. Ez a funkció lehetővé teszi az események pufferelésének letiltását a kiszolgálóval való szinkronizálás előtt.
Enable request throttling	Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését. Telemetriabeállítások konfigurálása: • **Maximum number of events per hour**. Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni. • **Percentage of event limit excess**. Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.
Send sync request to server every (min)	A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security információkat küld a módosított alkalmazásbeállításokról és feladatokról.

Paraméter	Leírás
Connection to response servers	A *válaszkiszolgáló* egy olyan kiszolgáló, amely adatokat fogad és vizsgál, tanulmányozza az objektumok viselkedését, és közzéteszi az ilyen tanulmányok eredményeit. Konfigurálja a következőket a válaszkiszolgálói kapcsolathoz: • **Timeout (sec)**. A kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik kiszolgálóhoz. • **Server certificate**. TLS-tanúsítvány a kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). • **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. Kriptokonténert szerezhet az Open Single Management Platformon (az utasításokat a Kaspersky Endpoint Detection and Response Expert (on-premises) súgójában találja). A kiszolgáló beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót.
Address és **Port** (válasz kiszolgálók)	A válaszkiszolgálókhoz való csatlakozás beállításai. Megadhat egy IP-címet (IPv4 vagy IPv6). Több telemetriagyűjtő kiszolgáló címét is hozzáadhatja. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

Az Endpoint Detection and Response (KATA) beállításai

Paraméter	Leírás
Send sync request to server every (min)	A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security információkat küld a módosított alkalmazásbeállításokról és feladatokról.
Connection to KATA servers	Konfigurálja a következőket a Central Node-kiszolgáló kapcsolódási beállításaira voatkozóan: • **Timeout (sec)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz. • **Server certificate**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). • **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót. A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.
Address és **Port** (KATA-kiszolgálók)	A Kaspersky Anti Targeted Attack Platform kiszolgálókhoz való csatlakozáshoz szükséges beállítások. Adja meg a csatlakozáshoz szükséges Central Node-kiszolgáló IP-címét (IPv4 vagy IPv6) és portját. Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
Send telemetry to KATA	Ezzel a funkcióval teljesen kikapcsolhatja a telemetriai adatok KATA-kiszolgálóra való küldését. Ha például a Kaspersky Anti Targeted Attack Platformot egy másik, szintén telemetriát használó megoldással együtt használja, kikapcsolhatja a KATA (EDR) platformnak való telemetriaküldést. Ez lehetővé teszi a kiszolgálói terhelés optimalizálását ezekhez a megoldásokhoz. Ha telepítette a Managed Detection and Response megoldást és a KATA (EDR) megoldást, használhatja az MDR-telemetriát, és létrehozhat Fenyegetésekre adott válasz típusú feladatokat a KATA (EDR) megoldásban. Telemetriabeállítások konfigurálása: • **Maximum event transmission delay (sec)**. Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc. • **Maximum number of event packages**. Az alkalmazás akkor szinkronizál a kiszolgálóval, amikor a puffer megtelik eseményekkel. Az alapértelmezett beállítás 1024 esemény.

Paraméter	Leírás
Enable request throttling	Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését. Telemetriabeállítások konfigurálása: • **Maximum number of events per hour**. Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni. • **Percentage of event limit excess**. Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.

Network Detection and Response (KATA)

A Kaspersky Endpoint Security for Windows támogatja a Kaspersky Network Detection and Response összetevővel való együttműködést a Kaspersky Anti Targeted Attack Platform (EDR (KATA)) megoldás részeként. A *Kaspersky Anti Targeted Attack Platform* egy megoldás, ami a kifinomult fenyegetések, például célzott támadások és speciális, állandó veszélyek (APT), valamint nagy kockázatú veszélyforrások időszerű észlelésére szolgál. A Kaspersky Anti Targeted Attack Platform három funkcionális egységet tartalmaz:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Az összes funkcionális egységet vagy az egyes funkcionális egységeket külön is megvásárolhatja. A megoldás részleteivel kapcsolatos információért lásd a Kaspersky Anti Targeted Attack Platform útmutatót.

A Kaspersky Endpoint Security a vállalati IT-infrastruktúra egyes számítógépeire van telepítve, és folyamatosan figyeli a folyamatokat, a nyitott hálózati kapcsolatokat és a módosítás alatt álló fájlokat. A számítógépen zajló eseményekkel kapcsolatos információk (telemetriai adatok) elküldésre kerülnek a Kaspersky Anti Targeted Attack Platform kiszolgálóra. Ebben az esetben a Kaspersky Endpoint Security információkat küld a Kaspersky Anti Targeted Attack Platform kiszolgálónak az alkalmazás által észlelt fenyegetésekről, valamint az ilyen fenyegetések feldolgozási eredményeiről is.

Az EDR (KATA) és NDR (KATA) integráció a Kaspersky Security Center konzolon van konfigurálva. A beépített ügynök ezután a Kaspersky Anti Targeted Attack Platform konzol segítségével kezelhető, beleértve a feladatok futtatását, a karanténba helyezett objektumok kezelését, a jelentések megtekintését és az egyéb műveleteket.

Paraméter	Leírás
Kiszolgáló kapcsolódási beállításai	**Időtúllépés (mp)**. A Central Node kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik Central Node-kiszolgálóhoz. **Kiszolgálói TLS-tanúsítvány hibája**. TLS-tanúsítvány a Central Node-kiszolgálóval való megbízható kapcsolat létrehozásához. A TLS-tanúsítványt beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). **Kétirányú hitelesítés használata**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a Central Node-kiszolgáló közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához engedélyeznie kell a kétirányú hitelesítést a Central Node-kiszolgáló beállításaiban, majd be kell szereznie egy kriptotárolót, és be kell állítania egy jelszót a kriptotároló védelméhez. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A kriptotárolót beszerezheti a Kaspersky Anti Targeted Attack Platform konzolon (az utasításokat a Kaspersky Anti Targeted Attack Platform Súgóban találja). A Central Node beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót. A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.
Cím és **port**	A Kaspersky Anti Targeted Attack Platform kiszolgálókhoz való csatlakozáshoz szükséges beállítások. Adja meg a csatlakozáshoz szükséges Central Node-kiszolgáló IP-címét (IPv4 vagy IPv6) és portját. Több Central Node-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.
Szinkronizálási kérés küldése a NDR kiszolgálójának ennyi percenként (perc)	A kiszolgálónak küldött szinkronizálási kérések gyakorisága. A szinkronizálás során a Kaspersky Endpoint Security információkat küld a módosított alkalmazásbeállításokról és feladatokról.
Maximális eseményátviteli késleltetés (mp)	Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc.
Kérésszabályzás engedélyezése	Ez a funkció segíti a kiszolgáló terhelésének optimalizálását. Ha ez a funkció engedélyezve van, az alkalmazás korlátozza az események továbbítását. Ha az események száma meghaladja a beállított korlátokat, a Kaspersky Endpoint Security leállítja az események küldését.
Események maximális száma óránként	Az alkalmazás elemzi a telemetriai adatfolyamot, és korlátozza az események küldését, ha az eseményfolyam meghaladja a konfigurált események óránkénti korlátját. A Kaspersky Endpoint Security egy óra elteltével folytatja az események küldését. Az alapértelmezett beállítás óránként 3000 esemény. Ha az alkalmazás kiszolgálóra van telepítve, a telemetriai adatfolyam magasabb. Kiszolgálóknál ajánlott az értéket óránként 60 000 eseményre növelni.
Eseménykorlát túllépésének százalékos aránya	Az alkalmazás típusok szerint rendezi az eseményeket (például "Változások a beállításjegyzékben" események), és korlátozza az események továbbítását, ha az azonos típusú események aránya az események teljes számához viszonyítva meghaladja a beállított százalékos korlátot. A Kaspersky Endpoint Security akkor folytatja az események küldését, amikor a többi esemény aránya az események teljes számához képest ismét elég nagy lesz. Az alapértelmezett beállítás 15%.

Integráció az KUMA-rel

A Kaspersky Endpoint Security for Windows támogatja a Kaspersky Unified Monitoring and Analysis Platform megoldást. A *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* egy biztonsági információ- és eseménykezelő megoldás (SIEM) a vállalatok IT-infrastruktúrájához. A KUMA lehetővé teszi a biztonsági fenyegetések észlelését, elemzését és elhárítását, mielőtt azok kárt okozhatnának.

Paraméter	Leírás
Maximum delay when sending events (sec)	Az alkalmazás szinkronizál a kiszolgálóval, hogy a szinkronizálási intervallum lejárta után eseményeket küldjön. Az alapértelmezett beállítás 30 másodperc.
Connection to KUMA servers	**Timeout (sec)**. A KUMA kiszolgálójának maximális válaszideje. Amikor lejár az időkorlát, a Kaspersky Endpoint Security megpróbál csatlakozni egy másik KUMA-kiszolgálóhoz. **Server certificate**. TLS-tanúsítvány a KUMA-kiszolgálóval való megbízható kapcsolat létrehozásához. TLS-tanúsítványt a Kaspersky Unified Monitoring and Analysis Platform konzolon szerezhet be (az utasításokat lásd: Kaspersky Unified Monitoring and Analysis Platform). A megbízható kapcsolat létrehozásához a KUMA-konzolon a tcp-csatlakozó beállításai között a **With verification** TLS módot kell kiválasztania (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában). **Use two-way authentication**. Kétirányú hitelesítés a Kaspersky Endpoint Security és a KUMA közötti biztonságos kapcsolat létrehozásakor. A kétirányú hitelesítés használatához a KUMA-konzolon a tcp-csatlakozó beállításai között a **Custom PFX** TLS módot kell kiválasztania (lásd a tcp típusú csatlakozó beállításait a Kaspersky Unified Monitoring and Analysis Platform súgójában). Ezután szereznie kell egy kriptokonténert, és be kell állítania egy jelszót a kriptokonténer védelmére. A *kriptotároló* egy PFX archívum tanúsítvánnyal és privát kulccsal. A KUMA beállításainak konfigurálása után engedélyeznie kell a kétirányú hitelesítést is a Kaspersky Endpoint Security beállításaiban, és be kell töltenie egy jelszóval védett kriptotárolót. A kriptotárolót jelszóval kell védeni. Üres jelszóval nem lehet kriptotárolót hozzáadni.
KUMA-kiszolgálók	A Kaspersky Unified Monitoring and Analysis Platform kiszolgálóihoz való kapcsolat beállításai. Megadhat egy IP-címet (IPv4 vagy IPv6). Több KUMA-kiszolgálócímet is megadhat. A Kaspersky Endpoint Security az első IP-címen keresztül próbál csatlakozni a kiszolgálóhoz. Ha nem sikerül kapcsolatot létesíteni, a Kaspersky Endpoint Security a listán szereplő második IP-címet használja a csatlakozáshoz, és így tovább.

Teljes lemeztitkosítás

Kiválaszthatja a titkosítási technológiát: Kaspersky lemeztitkosítás vagy BitLocker meghajtótitkosítás (a továbbiakban egyszerűen „BitLocker” is).

Kaspersky lemeztitkosítás

A Kaspersky lemeztitkosítás az ARM-alapú számítógépeken nem támogatott.

A rendszermerevlemezek titkosítását követően a számítógép legközelebbi indításakor a felhasználónak a Hitelesítési ügynök segítségével hitelesítést kell végeznie, mielőtt hozzáférhetne a merevlemezekhez, és betöltődhetne az operációs rendszer. Ehhez meg kell adni a token vagy a számítógéphez csatlakoztatott okoskártya jelszavát, vagy a helyi hálózati rendszergazda által a *Hitelesítési ügynök fiókok kezelése* feladat segítségével létrehozott Hitelesítési ügynök-fiók felhasználónevét és jelszavát. Ezek a fiókok azon Microsoft Windows fiókokon alapulnak, amelyekkel a felhasználó az operációs rendszerbe bejelentkezik. Emellett használhatja az Single Sign-On (SSO) technológiát is, amely lehetővé teszi, hogy automatikusan bejelentkezzen az operációs rendszerbe a Hitelesítési ügynök-fiókja felhasználónevével és jelszavával.

A Hitelesítési ügynök segítségével kétféleképpen lehet a felhasználói hitelesítést elvégezni:

- Adja meg a hálózati rendszergazda által a Kaspersky Security Center eszközeivel létrehozott Hitelesítési ügynök-fiók felhasználónevét és jelszavát.
- Adja meg a token vagy a számítógéphez csatlakoztatott okoskártya jelszavát.

  Akkor lehet tokent vagy okoskártyát használni, ha a számítógép merevlemezeit az AES256 titkosítási algoritmus titkosította. Ha a számítógép merevlemezei az AES56 algoritmussal vannak titkosítva, a rendszer elutasítja az elektronikus tanúsítványfájl parancshoz való hozzáadását.

BitLocker meghajtótitkosítás

A *BitLocker* a Windows operációs rendszerek beépített titkosítási technológiája. A Kaspersky Endpoint Security lehetővé teszi, hogy a Kaspersky Next infrastruktúra segítségével vezérelje és kezelje a Bitlockert. A BitLocker logikai köteteket titkosít. A BitLocker használatával nem lehet cserélhető meghajtókat titkosítani. A BitLocker részleteiért lásd a Microsoft dokumentációját.

A lemez titkosításakor a BitLocker a system partition helyre helyezi a rendszerbetöltőt és az egyéb segédfájlokat. Ez a partíció nem titkosított. Az operációs rendszer a Windows telepítése során automatikusan létrehozza a rendszerpartíciót. Ha a lemez teljesen particionálva van a Windows telepítése előtt, az operációs rendszer nem tud rendszerpartíciót létrehozni. Ebben az esetben a BitLocker-lemeztitkosítás indításakor az operációs rendszer arra kéri Önt, hogy particionálja újra a lemezt, és hozzon létre rendszerpartíciót. A rendszerpartíció létrehozása után az operációs rendszer elindítja a BitLocker titkosítást.

A BitLocker egy Trusted Platform Module segítségével a hozzáférési kulcsok biztonságos tárolását biztosítja. A *Trusted Platform Module* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapján helyezkedik el, és a rendszer többi összetevőjével a hardverbuszon keresztül lép kapcsolatba. A TPM-ek használatával lehet a legbiztonságosabb módon tárolni a BitLocker hozzáférési kulcsokat, mivel a TPM indítás előtti rendszerintegráció-hitelesítést nyújt. A számítógépen továbbra is titkosíthat meghajtókat TPM nélkül. Ilyen esetben a hozzáférési kulcs jelszó nélkül lesz titkosítva. A BitLocker a következő hitelesítési módszereket használja:

- TPM.
- TPM és PIN-kód.
- Jelszó.

Miután titkosítja a rendszer merevlemezét, a felhasználónak végig kell mennie a BitLocker hitelesítések, hogy elindítsa az operációs rendszert. Hitelesítés után a BitLocker lehetővé teszi a felhasználó számára a bejelentkezést. A BitLocker nem támogatja az egyszeri bejelentkezési technológiát (SSO).

Egy meghajtó titkosítása után a BitLocker létrehoz egy helyreállítási kulcsot. A Kaspersky Endpoint Security elküldi a helyreállítási kulcsot a Kaspersky Security Centernek, hogy visszaállíthassa a lemezhez való hozzáférést, például ha egy felhasználó elfelejtette a jelszavát.

Ha egy felhasználó BitLocker használatával titkosít egy lemezt, a Kaspersky Endpoint Security elküldi a helyreállítási kulcsot és a lemeztitkosítással kapcsolatos információkat a Kaspersky Security Centernek.

Ha Windows csoportrendszabályokat használ, kapcsolja ki a BitLocker kezelést a rendszabály-beállításokban. A Windows rendszabály-beállítások összeférhetetlenek lehetnek a Kaspersky Endpoint Security rendszabály-beállításaival. Meghajtó titkosításakor hiba léphet fel.

A Kaspersky lemeztitkosítási összetevő beállításai

Paraméter	Leírás
Titkosítási mód	**Összes merevlemez titkosítása**. Ha ez az opció ki van választva, az alkalmazás a rendszabály alkalmazásakor titkosítja az összes merevlemezt. Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak az az operációs rendszer tölthető be, amelyeken az alkalmazás telepítve van. **Összes merevlemez visszafejtése**. Ha ez az opció ki van választva, az alkalmazás a rendszabály alkalmazásakor visszafejti az összes korábban titkosított merevlemezt. **Maradjon változatlan**. Ha ez az elem ki van választva, az alkalmazás az irányelv alkalmazásakor a meghajtókat korábbi állapotukban hagyja. Ha a meghajtó titkosítva van, akkor titkosítva marad. Ha a meghajtó vissza van fejtve, akkor visszafejtve marad. Alapértelmezés szerint ez az elem van kiválasztva.
A titkosítás során Hitelesítési ügynöki fiókok automatikus létrehozása Windows-felhasználóknak	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás a Hitelesítési ügynöki fiókokat a számítógépen található Windows felhasználói fiókok listája alapján hozza létre. Alapértelmezés szerint a Kaspersky Endpoint Security minden helyi és tartományi fiókot felhasznál, amelynek használatával a felhasználó bejelentkezett az operációs rendszerbe az utolsó 30 nap során.
Hitelesítési ügynök fióklétrehozási beállítások	**A számítógépen lévő összes fiók**. A számítógépen lévő összes fiók, amely bármikor aktív volt. **A számítógépen lévő összes tartományfiók**. A számítógépen lévő összes olyan fiók, amely valamilyen tartományhoz tartozik, és amely bármikor aktív volt. **A számítógépen lévő összes helyi fiók**. Minden olyan helyi fiók a számítógépen, amely bármikor aktív volt. **Szolgáltatási fiók egyszeri jelszóval**. A szolgáltatásfiók szükséges a számítógéphez való hozzáféréshez, például ha a felhasználó elfelejti a jelszavát. A szolgáltatásfiókot tartalék fiókként is használhatja. Meg kell adnia a fiók nevét (alapértelmezés szerint `ServiceAccount`). A Kaspersky Endpoint Security automatikusan létrehoz egy jelszót. A jelszót megtalálja a Kaspersky Security Center konzolon. **Helyi rendszergazda**. A Kaspersky Endpoint Security létrehoz egy hitelesítési ügynöki felhasználói fiókot a számítógép helyi rendszergazdájának. **Számítógép kezelője** A Kaspersky Endpoint Security létrehoz egy hitelesítési ügynöki felhasználói fiókot a számítógépkezelő fiókjának. Az Active Directory számítógép-tulajdonságai között megtekintheti, hogy melyik fiók rendelkezik számítógépkezelői szerepkörrel. Alapértelmezés szerint a számítógépkezelői szerepkör nincs meghatározva, vagyis nem felel meg egyetlen fióknak sem. **Aktív fiók**. A Kaspersky Endpoint Security automatikusan létrehoz egy hitelesítési ügynöki fiókot a lemeztitkosításkor aktív fióknak.
Hitelesítési ügynöki fiókok automatikusa létrehozása a számítógép összes felhasználójának bejelentkezéskor	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás a Hitelesítési ügynök elindítása előtt ellenőrzi a számítógépen található Windows felhasználói fiókok adatait. Ha a Kaspersky Endpoint Security olyan Windows felhasználói fiókot észlel, amely nem rendelkezik Hitelesítési ügynöki fiókkal, az alkalmazás új fiókot hoz létre a titkosított meghajtók eléréséhez. Az új Hitelesítési ügynöki fiók a következő alapértelmezett beállításokkal rendelkezik: csak jelszóvédett bejelentkezés és jelszó megváltoztatása az első hitelesítéskor. Ezért a már titkosított meghajtókkal rendelkező számítógépek esetében nem kell manuálisan hozzáadnia Hitelesítési ügynöki fiókokat a *Hitelesítési ügynök fiókok kezelése* feladattal.
Hitelesítési ügynökben megadott felhasználónév mentése	Ha a jelölőnégyzet ki van jelölve, az alkalmazás elmenti a Hitelesítési ügynök fiókjának nevét. Ily módon nem szükséges a fióknevet a legközelebbi alkalommal megadnia, amikor ugyanabban a fiókban a Hitelesítési ügynökben hitelesítést szeretne végezni.

Paraméter	Leírás
Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)	Ez a jelölőnégyzet engedélyezi/letiltja azt a lehetőséget, amely a titkosítási területet kizárólag a foglalt merevlemez-szektorokra korlátozza. A korlátozás révén csökkentheti a titkosítási időt. A **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemezek visszafejtése. A titkosítás megkezdése előtt kell a jelölőnégyzetet bejelölni, illetve törölni. Ha a jelölőnégyzet be van jelölve, akkor a merevlemeznek csak a fájlok által elfoglalt részei kerülnek titkosításra. A Kaspersky Endpoint Security az új adatokat hozzáadásukkor automatikusan titkosítja. Ha a jelölőnégyzet nincs bejelölve, a teljes merevlemez titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit. Ez a lehetőség új merevlemezek esetén javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha már használatban lévő merevlemezen alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről, még a törölt, esetlegesen helyreállítható adatokról is. Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.
Legacy USB Support (nem ajánlott)	Ez a jelölőnégyzet engedélyezi vagy letiltja a Legacy USB Support funkciót. A *Legacy USB Support* olyan BIOS/UEFI-funkció, amely lehetővé teszi USB-eszközök (például biztonsági token) használatát a számítógép rendszerindítási fázisában, az operációs rendszer elindítása előtt (BIOS-mód). A Legacy USB Support nem befolyásolja az USB-eszközök támogatását az operációs rendszer indulását követően. Ha a jelölőnégyzet be van jelölve, engedélyezve van az USB eszközök támogatása a számítógép indulásakor. Ha a Legacy USB Support funkció engedélyezve van, a Hitelesítési ügynök BIOS-módban nem támogatja a tokenekkel való működést USB-kapcsolaton keresztül. Ezt a lehetőséget csak akkor ajánlott alkalmazni, ha hardverkompatibilitási probléma áll fenn, és csak azokon a számítógépeken, amelyeken fennáll a probléma.
Jelszóbeállítások	A Hitelesítési ügynök-fiók jelszóerősségi beállításai. A Single Sign-On technológia használata során a Hitelesítési ügynök figyelmen kívül hagyja a Kaspersky Security Centerben meghatározott jelszóerősségi követelményeket. A jelszóerősségi követelményeket az operációs rendszer beállításai között lehet megadni.
Egyszeri bejelentkezés (SSO) technológia használata	Az SSO technológia révén ugyanazon hitelesítési adatokkal férhet hozzá a titkosított merevlemezekhez és jelentkezhet be az operációs rendszerbe. Ha a jelölőnégyzet be van jelölve, akkor meg kell adni a fiók belépési adatait a titkosított merevlemezekhez való hozzáféréshez, majd az operációs rendszerbe való automatikus bejelentkezéshez. Ha a jelölőnégyzet nincs bejelölve, akkor a titkosított merevlemezekhez való hozzáféréshez, majd az operációs rendszerbe való bejelentkezéshez külön-külön meg kell adni a titkosított merevlemezek hozzáférési hitelesítő adatait, majd az operációs rendszer felhasználói fiókjának hitelesítő adatait.
Külső hitelesítésszolgáltatók bevonása	A Kaspersky Endpoint Security támogatja a külső ADSelfService Plus hitelesítési szolgáltatót. Amikor harmadik féltől származó hitelesítésszolgáltatóval dolgozik, a Hitelesítési ügynök még az operációs rendszer betöltése előtt elfogja a jelszót. Ez azt jelenti, hogy a felhasználónak csak egyszer kell megadnia a jelszót a Windowsba történő bejelentkezéskor. Windowsba történő bejelentkezés után a felhasználó használhatja harmadik fél hitelesítőadat-szolgáltató képességeit például a vállalati szolgáltatásokban történő hitelesítéshez. A harmadik fél hitelesítésszolgáltatók szintén lehetővé teszik a felhasználóknak, hogy önállóan állítsák vissza saját jelszavukat. Ebben az esetben a Kaspersky Endpoint Security automatikusan frissíti a Hitelesítési ügynök jelszavát. Ha az alkalmazás által nem támogatott harmadik fél általi hitelesítóadat-szolgáltatót használ, az egyszeri bejelentkezési technológia működése közben korlátozásokba ütközhet.
Súgó	**Hitelesítés**. Súgószöveg, amely a fiók bejelentkezési adatainak megadásakor jelenik meg a Hitelesítési ügynök ablakában. **Jelszó módosítása**. Súgószöveg, amely a Hitelesítési ügynök-fiók jelszavának módosításakor jelenik meg a Hitelesítési ügynök ablakában. **Jelszó visszaállítása**. Súgószöveg, amely a Hitelesítési ügynök-fiók jelszavának visszaállításakor jelenik meg a Hitelesítési ügynök ablakában.

A BitLocker meghajtótitkosítás összetevő beállításai

Paraméter	Leírás
Titkosítási mód	**Összes merevlemez titkosítása**. Ha ez az opció ki van választva, az alkalmazás a rendszabály alkalmazásakor titkosítja az összes merevlemezt. Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak az az operációs rendszer tölthető be, amelyeken az alkalmazás telepítve van. **Összes merevlemez visszafejtése**. Ha ez az opció ki van választva, az alkalmazás a rendszabály alkalmazásakor visszafejti az összes korábban titkosított merevlemezt. **Maradjon változatlan**. Ha ez az elem ki van választva, az alkalmazás az irányelv alkalmazásakor a meghajtókat korábbi állapotukban hagyja. Ha a meghajtó titkosítva van, akkor titkosítva marad. Ha a meghajtó vissza van fejtve, akkor visszafejtve marad. Alapértelmezés szerint ez az elem van kiválasztva.
Rendszerindítás előtt, billentyűzeten keresztül történő BitLocker hitelesítés bekapcsolása táblagépeken	Adatbevitelt igénylő hitelesítés használata rendszerindítás előtti környezetben, még akkor is, ha a platformon nem lehetséges a bevitel rendszerindítás előtt (például táblagépek érintőképernyős billentyűzetei esetén). A táblagépek érintőképernyője nem érhető el rendszerindítás előtt. Ahhoz, hogy a felhasználó befejezze a BitLocker hitelesítést a táblagépeken, először csatlakoztatnia kell egy USB-billentyűzetet például. Ha a jelölőnégyzet be van jelölve, a rendszerindítás előtti bevitelt igénylő hitelesítés engedélyezve van. Javasoljuk, hogy ezt a beállítást csak olyan eszközöknél használja, amelyek az érintőképernyős billentyűzeteken kívül alternatív adatbeviteli eszközöket – például USB-billentyűzetet – is tartalmaznak a rendszerindítás előtti környezetben. Ha a jelölőnégyzet üres, a BitLocker meghajtótitkosítás nem érhető el táblagépeken.
Hardveres titkosítás használata (Windows 8 és újabb verziók)	Ha a jelölőnégyzet be van jelölve, az alkalmazás hardveres titkosítást használ. Ennek köszönhetően felgyorsul a titkosítás, és kevesebb számítógépes erőforrásra lesz szükség.
Csak a felhasznált lemezterület titkosítása (Windows 8 és újabb verziók)	Ez a jelölőnégyzet engedélyezi/letiltja azt a lehetőséget, amely a titkosítási területet kizárólag a foglalt merevlemez-szektorokra korlátozza. A korlátozás révén csökkentheti a titkosítási időt. A **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemezek visszafejtése. A titkosítás megkezdése előtt kell a jelölőnégyzetet bejelölni, illetve törölni. Ha a jelölőnégyzet be van jelölve, akkor a merevlemeznek csak a fájlok által elfoglalt részei kerülnek titkosításra. A Kaspersky Endpoint Security az új adatokat hozzáadásukkor automatikusan titkosítja. Ha a jelölőnégyzet nincs bejelölve, a teljes merevlemez titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit. Ez a lehetőség új merevlemezek esetén javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha már használatban lévő merevlemezen alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről, még a törölt, esetlegesen helyreállítható adatokról is. Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.

Paraméter	Leírás
Hitelesítési módszer	**Csak jelszó (Windows 8 és újabb verziók)** Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security jelszót kér a felhasználótól, ha a felhasználó megpróbál egy titkosított meghajtóhoz hozzáférni. Ezt a lehetőséget akkor lehet kiválasztani, ha nincs használatban Trusted Platform Module (TPM). **Trusted Platform Module (TPM)** Ha ez a lehetőség van kiválasztva, a BitLocker Trusted Platform Module-t (TPM) használ. A *Trusted Platform Module* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapján helyezkedik el, és a rendszer többi összetevőjével a hardverbuszon keresztül lép kapcsolatba. A Windows 7 vagy Windows Server 2008 R2 rendszert futtató számítógépeknél csak TPM-modul használata érhető el. Ha nincs telepítve TPM-modul, akkor a BitLocker titkosítás nem lehetséges. Az ilyen számítógépeken nem támogatott a jelszó használata. A Trusted Platform Module-lal rendelkező eszköz olyan titkosítási kulcsokat tud előállítani, amelyeket csak az adott eszközzel lehet visszafejteni. A Trusted Platform Module a titkosítási kulcsokat saját gyökértárolási kulcsával titkosítja. A gyökértárolási kulcs tárolása a Trusted Platform Module-on belül történik. Ez további védelmi szintet nyújt a titkosítási kulcsok feltörési próbálkozásai ellen. Alapértelmezésben ez a művelet van kiválasztva. A titkosítási kulcshoz való hozzáféréshez további védelmi szintet állíthat be, és a kulcsot jelszóval vagy PIN-kóddal titkosíthatja: • **PIN-kód használata a TPM-nél**. Ennek a négyzetnek a bejelölésével a felhasználó használhatja a PIN-kódot a Trusted Platform Module-ban (TPM) tárolt titkosítási kulcshoz való hozzáférés megszerzéséhez. Ha a jelölőnégyzet törölve van, a felhasználók nem használhatják a PIN-kódokat. A titkosítási kulcs eléréséhez a felhasználónak meg kell adnia a jelszót. • **Trusted Platform Module (TPM) vagy jelszó, ha a TPM nem érhető el**. Ha ez az opció van kiválasztva, a felhasználó jelszó segítségével férhet hozzá a titkosítási kulcshoz, ha nem áll rendelkezésre Trusted Platform Module (TPM). Ha a jelölőnégyzet törölve van és a TPM nem érhető el, nem indul el a teljes lemeztitkosítás. A kiválasztott hitelesítési módszert jelszó- vagy PIN-kódkövetelmények megadásával kell konfigurálni: • **PIN-kód minimális hossza (karakter)**. • **Jelszó minimális hossza (karakter)**. • **A jelszó/PIN-kód érvényességi idejének korlátozása a TPM-nél (nap)**. • **Bővített PIN-kód használata (betűk és számok)**. A *bővített PIN-kód* lehetővé teszi a számokon kívül más karakterek használatát is: latin nagy- és kisbetűket, speciális karaktereket és szóközöket.
Helyreállítási kulcs automatikus újragenerálása (nap)	A jelszó automatikus frissítése a BitLocker által védett meghajtóhoz való hozzáférés visszaállításához. Ha a jelölőnégyzet be van jelölve, adja meg a helyreállítási kulcs jelszavának érvényességi idejét. Ez segít megelőzni a helyreállítási kulcs jelszavának ismételt használatát.

Fájl szintű titkosítás

A fájltitkosítás nem támogatott az ARM-alapú számítógépeken.

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

A fájlok listáit összeállíthatja kiterjesztés vagy kiterjesztések csoportja alapján, illetve a számítógép helyi meghajtóin tárolt mappák listái szerint, és létrehozhat adott alkalmazások által előállított fájlok titkosítására vonatkozó szabályokat. Rendszabály alkalmazását követően a Kaspersky Endpoint Security az alábbi fájlokat titkosítja és fejti vissza:

- a listákra titkosítás és visszafejtés céljából egyedileg felvett fájlok;
- a listákra titkosítás és visszafejtés céljából felvett mappákban tárolt fájlok;
- külön alkalmazások által előállított fájlok.

A fájltitkosítás a következő speciális tulajdonságokkal rendelkezik:

- A Kaspersky Endpoint Security csak az operációs rendszer helyi felhasználói profiljai esetén titkosítja és fejti vissza az előre megadott mappákban lévő fájlokat. A Kaspersky Endpoint Security a barangoló felhasználói profilok, a kötelező felhasználói profilok, az ideiglenes felhasználói profilok előre megadott mappáiban és az átirányított mappákban lévő fájlokat nem titkosítja és nem fejti vissza.
- A Kaspersky Endpoint Security nem végzi el a fájlok titkosítását, ha módosításuk kárt tehet az operációs rendszerben és a telepített alkalmazásokban. Az alábbi fájlok és mappák az összes beágyazott mappával együtt a titkosítási kizárások listáján vannak:
  - %WINDIR%;
  - %PROGRAMFILES% és %PROGRAMFILES(X86)%;
  - Windows beállításjegyzékfájlok.

  A titkosítási kizárások listája nem tekinthető meg és nem szerkeszthető. Noha a titkosítási kizárások listáján szereplő fájlokat és mappákat fel lehet venni a titkosítási listára, a fájltitkosítási feladat végrehajtásakor nem kerül sor a titkosításukra.

A fájlszintű titkosítási összetevő beállításai

Paraméter	Leírás
Titkosítási mód	**Maradjon változatlan**. Ha ez az elem ki van választva, a Kaspersky Endpoint Security a fájlokat és mappákat titkosítás és visszafejtés nélkül változatlanul hagyja. **A szabályoknak megfelelően**. Ha ez az elem ki van választva, a Kaspersky Endpoint Security a titkosítási szabályoknak megfelelően titkosítja a fájlokat és mappákat, a visszafejtési szabályoknak megfelelően visszafejti a fájlokat és mappákat, az alkalmazások fájlhozzáféréseit pedig az alkalmazásszabályok szerint határozza meg. **Összes visszafejtése**. Ha ez az elem ki van választva, a Kaspersky Endpoint Security az összes titkosított fájlt és mappát visszafejti.

Paraméter	Leírás
Titkosítás	Ezen a lapon a helyi meghajtókon tárolt fájlok titkosítási szabályai láthatók. Fájlt a következőképpen lehet hozzáadni: • **Előre megadott mappák**. A Kaspersky Endpoint Security a következő területek hozzáadását teszi lehetővé: **Dokumentumok**. Az operációs rendszer szokványos *Dokumentumok* mappájában, valamint az azon belüli almappákban található fájlok. **Kedvencek**. Az operációs rendszer szokványos *Kedvencek* mappájában, valamint az azon belüli almappákban található fájlok. **Asztal**. Az operációs rendszer szokványos *Asztal* mappájában, valamint az azon belüli almappákban található fájlok. **Ideiglenes fájlok**. A számítógépre telepített alkalmazások működéséhez kapcsolódó ideiglenes fájlok. Például a Microsoft Office alkalmazások olyan ideiglenes fájlokat hoznak létre, amelyek a dokumentumok biztonsági mentését tartalmazzák. **Outlook fájlok**. Az Outlook levelezőprogram működéséhez kapcsolódó fájlok: adatfájlok (PST), offline adatfájlok (OST), offline címjegyzékfájlok (OAB) és személyes címjegyzékfájlok (PAB). • **Egyéni mappa**. A mappa elérési útját kézzel is megadhatja. Mappa elérési útjának megadásakor tartsa be a következő szabályokat: Használjon környezeti változót (például: `%FOLDER%\UserFolder\`). Egy környezeti változót csak egyszer lehet használni, és kizárólag az elérési út kezdetén. Ne használjon relatív útvonalat. Ne használja a `*` (csillag) és a `?` (kérdőjel) karaktert. Ne használjon UNC-útvonalat. Használjon `;` (pontosvessző) vagy `,` (vessző) karaktert elválasztókarakterként. • **Fájlok kiterjesztés alapján**. Kiválaszthat kiterjesztéscsoportokat a listából, például az *Archívumok* kiterjesztéscsoportot. Lehetősége van kézzel is hozzáadni fájlkiterjesztést.
Visszafejtés	Ezen a lapon a helyi meghajtókon tárolt fájlok visszafejtési szabályai láthatók.
Szabályok az alkalmazásokhoz	A lapon egy táblázat jelenik meg, amely az alkalmazások titkosított fájlokhoz való hozzáférési szabályait és az egyedi alkalmazások által létrehozott, illetve módosított fájlok titkosítási szabályait tartalmazza.
Titkosított csomagok	Jelszóerősség követelményei a titkosított csomagok létrehozásánál.

Cserélhető meghajtók titkosítása

Az ARM-alapú számítógépek nem támogatják a cserélhető meghajtók titkosítását.

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security alkalmazás telepítése munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépre történt. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security alkalmazás kiszolgálókra szánt Windows rendszert futtató számítógépre van telepítve.

A Kaspersky Endpoint Security a FAT32 fájlok és az NTFS fájlrendszerek titkosítását támogatja. Ha egy nem támogatott fájlrendszerű cserélhető meghajtó van csatlakoztatva a számítógéphez, a cserélhető meghajtó titkosítási feladata hibás lesz, a Kaspersky Endpoint Security pedig csak olvasható állapotot rendel a cserélhető meghajtóhoz.

A cserélhető meghajtón tárolt adatok védelme érdekében a következő titkosítási típusokat használhatja:

- Full Disk Encryption (FDE).

  A teljes cserélhető meghajtó titkosítása, annak fájlrendszerét is beleértve.

  Nincs mód a titkosított adatok elérésére a vállalati hálózaton kívülről. A titkosított adatok elérése a vállalti hálózaton belül sem lehetséges, ha a számítógép nincs csatlakoztatva a Kaspersky Security Centerhez (pl „vendég” számítógépen).

- File Level Encryption (FLE).

  Csak a fájlok titkosítása egy cserélhető meghajtón. A fájlrendszer változatlan marad.

  > A cserélhető meghajtón tárolt fájlok titkosítása lehetőséget biztosít az adatok elérésére a vállalati hálózaton kívülről egy speciális mód, az úgynevezett *hordozható mód* segítségével.

A titkosítási folyamat során a Kaspersky Endpoint Security főkulcsot hoz létre. A Kaspersky Endpoint Security a következő tárhelyekre menti a főkulcsot:

- Kaspersky Security Center.
- A felhasználó számítógépe.

  A főkulcs titkosítása a felhasználó titkos kulcsával történik.
- Cserélhető meghajtó.

  A főkulcs titkosítása a Kaspersky Security Center nyilvános kulcsával történik.

A titkosítás befejezését követően a cserélhető meghajtón tárolt adatok a vállalati hálózaton belülről úgy érhetők el, mintha szokványos cserélhető meghajtóról lenne szó, titkosítás nélkül.

A titkosított adatok elérése

Titkosított adatokat tartalmazó cserélhető meghajtó csatlakoztatásakor a Kaspersky Endpoint Security a következő műveleteket hajtja végre:

1. Ellenőrzi a főkulcs meglétét a felhasználó számítógépének helyi adattárolóján.

   Ha a főkulcs megtalálható, a felhasználó hozzáférést kap a cserélhető meghajtón tárolt adatokhoz.

   Ha nem található a főkulcs, a Kaspersky Endpoint Security a következő műveleteket hajtja végre:

   a. Kérelmet küld a Kaspersky Security Center felé.

      A kérelem beérkezését követően a Kaspersky Security Center választ küld, amely tartalmazza a főkulcsot.

   b. A Kaspersky Endpoint Security menti a főkulcsot a felhasználó számítógépének helyi adattárolójában a titkosított cserélhető meghajtón később végzett műveletekhez.
2. Visszafejti az adatokat.

A cserélhető meghajtó titkosításának speciális jellemzői

A cserélhető meghajtók titkosításának folyamata a következő speciális jellemzőkkel bír:

- A cserélhető meghajtók titkosításának előre megadott beállításait tartalmazó rendszabály a kezelt számítógépek egy adott csoportja számára van kialakítva. Emiatt a cserélhető meghajtók titkosításához és visszafejtéséhez beállított Kaspersky Security Center-rendszabály alkalmazásának eredménye attól a számítógéptől függ, amelyhez a cserélhető meghajtót csatlakoztatja.
- A Kaspersky Endpoint Security a cserélhető meghajtókon tárolt csak olvasható fájlokat nem titkosítja és nem fejti vissza.
- Az alábbi eszköztípusok cserélhető meghajtókként vannak támogatva:
  - USB buszon keresztül csatlakoztatott adathordozók
  - USB és FireWire buszokon keresztül csatlakoztatott merevlemezek
  - USB és FireWire buszokon keresztül csatlakoztatott SSD-meghajtók

Cserélhető meghajtók titkosításának beállításai

Paraméter	Leírás
Titkosítási mód	**Teljes cserélhető meghajtó titkosítása**. E lehetőség kiválasztása esetén a rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtókat fájlrendszerükkel együtt szektoronként titkosítja. **Összes fájl titkosítása**. E lehetőség kiválasztása esetén a rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtókon tárolt összes fájlt titkosítja. A Kaspersky Endpoint Security nem titkosítja újra a már titkosított fájlokat. Az alkalmazás nem titkosítja a cserélhető meghajtók fájlrendszereit, így a titkosított fájlok neveit és a mappaszerkezeteket, és ezek hozzáférhetők maradnak. **Csak az új fájlok titkosítása**. E lehetőség kiválasztása esetén a rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security csak azokat a fájlokat titkosítja, amelyek a Kaspersky Security Center rendszabály legutóbbi alkalmazása óta kerültek a cserélhető meghajtókra, illetve már korábban ott voltak, de azóta módosultak. Ez a titkosítási mód akkor jön jól, ha egy cserélhető meghajtót személyes célokra és munkára egyaránt használja. Ezzel a titkosítási móddal az összes régi fájlt változatlanul hagyhatja, és titkosíthatja csak azokat a fájlokat, amelyeket a felhasználó olyan számítógépen hoz létre, amelyen telepítve van a Kaspersky Endpoint Security, és be van kapcsolva a titkosítási funkció. Ily módon a személyes fájlokhoz attól függetlenül mindig hozzá lehet férni, hogy a számítógépen telepítve van-e a Kaspersky Endpoint Security, és azon be van-e kapcsolva a titkosítási funkció. **Teljes cserélhető meghajtó visszafejtése**. E lehetőség kiválasztása esetén a rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtókon lévő összes titkosított fájlt visszafejti a cserélhető meghajtók fájlrendszereivel együtt, ha azok titkosítására korábban sor került. **Maradjon változatlan**. Ha ez az elem ki van választva, az alkalmazás az irányelv alkalmazásakor a meghajtókat korábbi állapotukban hagyja. Ha a meghajtó titkosítva van, akkor titkosítva marad. Ha a meghajtó vissza van fejtve, akkor visszafejtve marad. Alapértelmezés szerint ez az elem van kiválasztva.
Hordozható mód	Ez a jelölőnégyzet engedélyezi/letiltja a cserélhető meghajtók előkészítését, ami lehetővé teszi a cserélhető meghajtón lévő fájlokhoz való hozzáférést a vállalati hálózaton kívüli számítógépeken. Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security jelszó megadására kéri a felhasználót, mielőtt a cserélhető meghajtón lévő fájlokat a rendszabályt alkalmazva titkosítaná. A jelszó az olyan számítógépeken titkosított, cserélhető meghajtón lévő fájlokhoz való hozzáféréshez szükséges, amelyek a vállalati hálózaton kívül találhatók. Lehetősége van konfigurálni a jelszó erősségét. A hordozható mód az **Összes fájl titkosítása** és a **Csak az új fájlok titkosítása** beállításhoz érhető el.

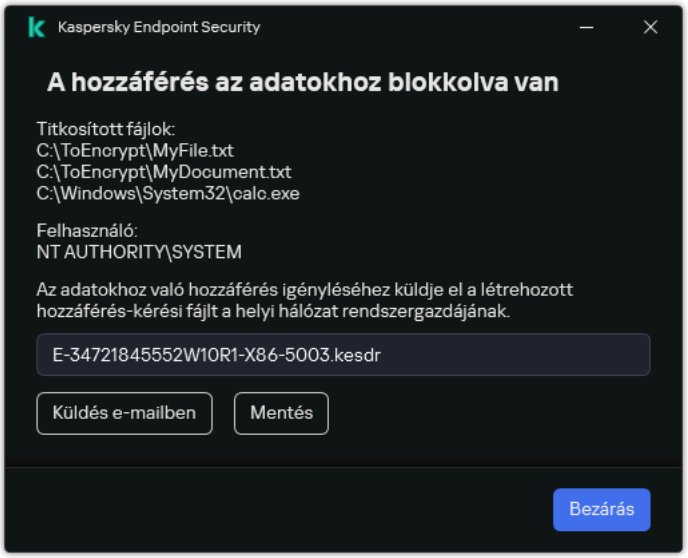
Paraméter	Leírás
Csak a használt lemezterület titkosítása	Ez a jelölőnégyzet engedélyezi/letiltja azt a titkosítási módot, amelynél csak a foglalt lemezszektorok titkosítására kerül sor. Ez a mód új meghajtók esetén javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha a jelölőnégyzet be van jelölve, akkor a meghajtónak csak a fájlok által elfoglalt részei lesznek titkosítva. A Kaspersky Endpoint Security az új adatokat hozzáadásukkor automatikusan titkosítja. Ha a jelölőnégyzet nincs bejelölve, a teljes meghajtó titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit. A csak a foglalt terület titkosításának képessége kizárólag a **Teljes cserélhető meghajtó titkosítása** módban áll rendelkezésre. A titkosítás megkezdését követően a **Csak a használt lemezterület titkosítása** funkció be- és kikapcsolása nem változtatja meg ezt a beállítást. A titkosítás megkezdése előtt kell a jelölőnégyzetet bejelölni, illetve törölni.

Egyéni szabályok	Ez a táblázat azokat az eszközöket tartalmazza, amelyekhez egyéni visszafejtési szabályok vannak megadva.f Lehetősége van létrehozni titkosítási szabályokat az egyes cserélhető meghajtókhoz a következő módokon:
	
	• Adjon hozzá egy cserélhető meghajtót az Eszközfelügyelő megbízható eszközeinek listájáról.
	
	• Kézzel adjon hozzá cserélhető meghajtót:
	
	  • Eszközazonosító alapján (Hardware ID vagy HWID)
	
	  • Eszközmodell szerint: Vendor ID (VID) és Product ID (PID)

Cserélhető meghajtók titkosításának engedélyezése offline módban	Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security akkor is titkosítja a cserélhető meghajtókat, ha nincs kapcsolat a Kaspersky Security Centerrel. Ilyenkor a cserélhető meghajtó visszafejtéséhez szükséges adatok annak a számítógépnek a merevlemezén tárolódnak, amelyhez a cserélhető meghajtó csatlakozik, és nem kerülnek be a Kaspersky Security Centerbe. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem titkosítja a cserélhető meghajtókat, ha nincs kapcsolat a Kaspersky Security Centerrel.
Titkosítási jelszó beállításai/Hordozható fájlkezelő	A hordozható fájlkezelő jelszóerősségére vonatkozó beállítások.

Sablonok (adattitkosítás)

Az adatok titkosítását követően a Kaspersky Endpoint Security korlátozhatja az adatok elérhetőségét, például a szervezet infrastruktúrájának változása vagy a Kaspersky Security Center felügyeleti kiszolgálójának változása miatt. Ha egy felhasználónak nincs hozzáférése a titkosított adatokhoz, a felhasználó kérhet hozzáférést az adatokhoz a rendszergazdától. Másképpen megfogalmazva: a felhasználónak hozzáférés-kérési fájlt kell küldenie a rendszergazda felé. Ezután a felhasználónak fel kell töltenie a rendszergazdától kapott válaszfájlt a Kaspersky Endpoint Security alkalmazásba. A Kaspersky Endpoint Security lehetővé teszi, hogy e-mailben hozzáférést kérjen a rendszergazdától (részletek a lentebbi ábrán).



Hozzáférés kérése titkosított adatokhoz

Rendelkezésre áll egy sablon, amelynek segítségével jelenteni lehet a titkosított adatok hozzáférhetőségének hiányát. A felhasználói kényelem érdekében lehetősége van kitölteni a következő mezőket:

- **Eddig**. Adja meg az adattitkosítási funkciók jogosultságait kezelő rendszergazdai csoport e-mail-címét.
- **Tárgy**. Adja meg az e-mail tárgyát a titkosított fájlokhoz való hozzáférés kérésével. Lehetősége van például hozzáadni címkéket az üzenetek szűrése érdekében.
- **Felhasználó üzenete**. Ha szükséges, módosítsa az üzenet tartalmát. Használhat változókat a szükséges adatok beemeléséhez (például a `%USER_NAME%` változót).

Kizárások

A *megbízható zóna* olyan, a rendszergazda által beállított objektumok és alkalmazások listája, melyeket a Kaspersky Endpoint Security aktív módban nem figyel.

A megbízható zónát a rendszergazda függetlenül, a kezelt objektumok tulajdonságai és a számítógépen telepített alkalmazások alapján hozhatja létre. Akkor válhat szükségessé objektumok és alkalmazások felvétele a megbízható zónába, ha a Kaspersky Endpoint Security egy olyan objektumhoz vagy alkalmazáshoz való hozzáférést blokkol, amelyről biztosan tudja, hogy ártalmatlan. A rendszergazda engedélyezheti a felhasználónak, hogy létrehozza a saját helyi megbízható zónáját egy adott számítógéphez. Így a felhasználók a házirendben található általános megbízható zóna mellett létrehozhatják a kizárásokra és megbízható alkalmazásokra vonatkozó saját listájukat is.

A Kaspersky Endpoint Security 12.5 for Windowstól kezdve lehetőség van az EDR telemetria hozzáadására a megbízható zónához. Ez lehetővé teszi az alkalmazás által a telemetriagyűjtő kiszolgálónak küldött adatok optimalizálását a Kaspersky Anti Targeted Attack Platform (EDR) megoldás számára.

A Kaspersky Endpoint Security 12.6 for Windows verziótól kezdve a vizsgálati kizárások és a megbízható alkalmazások hozzáadódnak a megbízható zónához. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segítik a Kaspersky Endpoint Security gyors konfigurálását SQL-kiszolgálókon, Microsoft Exchange-kiszolgálókon és a System Center Configuration Manager-ben. Ez azt jelenti, hogy nem kell manuálisan beállítania egy megbízható zónát az alkalmazáshoz a kiszolgálókon.

A Kaspersky Endpoint Security 12.8 for Windows verziótól kezdve az alkalmazást Light Agent üzemmódban is telepítheti a virtuális környezetek védelme céljából. Az előre definiált vizsgálati kizárások és megbízható alkalmazások segíthetnek a Kaspersky Endpoint Security gyors konfigurálásában Citrix és VMware virtuális környezetekben.

Kizárás a vizsgálatból

A *vizsgálatból való kizárás* olyan feltételkészlet, amelyet teljesíteni kell, hogy a Kaspersky Endpoint Security ne vizsgálja a vírusok és egyéb fenyegetések jelenlétét. A vizsgálatból való kizárások révén biztonsággal használhatók az olyan jogszerű szoftverek, amelyekkel a bűnözők károsíthatják a számítógépet vagy a személyes adatokat. Miközben ezeknek az alkalmazásoknak nincs rosszindulatú funkciója, a behatolók felhasználhatják őket rosszindulatú eljárásaik során. A betolakodók által a számítógép vagy a személyes adatok károsítására használható legitim szoftverekről részletes információkat a Kaspersky IT Encyclopedia webhelyen találhat.

Az ilyen alkalmazásokat a Kaspersky Endpoint Security blokkolhatja. A blokkolás megelőzése érdekében a használatban lévő alkalmazásoknál vizsgálatból való kizárásokat adhat meg. Ehhez fel kell venni a megbízható zónába a Kaspersky IT Encyclopedia által felsorolt nevet vagy névmaszkot. Például gyakran használhatja a Radmin alkalmazást a számítógépek távoli adminisztrációjához. A Kaspersky Endpoint Security az ilyen tevékenységet gyanúsnak tekinti, és előfordulhat, hogy blokkolja. Az alkalmazás blokkolásának megelőzése érdekében készítsen vizsgálatból való kizárást a Kaspersky IT Encyclopedia által megadott névvel vagy névmaszkkal.

Ha a számítógépre egy adatokat gyűjtő és azokat feldolgozásra továbbító alkalmazás van telepítve, a Kaspersky Endpoint Security rosszindulatú programként sorolhatja be ezt az alkalmazást. Ennek elkerülésére a Kaspersky Endpoint Security jelen dokumentumban leírt módon való konfigurálásával kizárhatja az alkalmazást a vizsgálatból.

A vizsgálatból való kizárásokat az alábbi alkalmazásösszetevők, valamint a rendszergazda által beállított feladatok használhatnak:

- Viselkedésészlelés
- Biztonsági rések kihasználásának megelőzése
- Behatolásmegelőző rendszer
- Fájl védelem
- Web védelem

- Levelezés védelem
- *Kártevő vizsgálata* feladat

Megbízható alkalmazások listája

A *megbízható alkalmazások listája* azon alkalmazások listája, amelyeknek fájl- és hálózati tevékenységét (ideértve a rosszindulatú tevékenységet is) és a rendszer beállításjegyzékéhez való hozzáférését a Kaspersky Endpoint Security nem kíséri figyelemmel. A Kaspersky Endpoint Security alapértelmezés szerint figyeli a megnyitott, végrehajtott vagy bármilyen alkalmazásfolyamat által mentett objektumokat, és felügyeli az összes alkalmazás tevékenységét és az általuk generált hálózati forgalmat. Miután egy alkalmazás felkerült a megbízható alkalmazások listájára, a Kaspersky Endpoint Security nem figyeli tovább az alkalmazás tevékenységét.

A különbség a vizsgálati kizárások és a megbízható alkalmazások között az, hogy a kizárások esetében a Kaspersky Endpoint Security nem vizsgálja a fájlokat, míg a megbízható alkalmazások esetében nem ellenőrzi az indított folyamatokat. Ha egy megbízható alkalmazás rosszindulatú fájlt hoz létre egy olyan mappában, amely nem szerepel a vizsgálati kizárások között, a Kaspersky Endpoint Security észleli a fájlt, és megszünteti a fenyegetést. Ha a mappa hozzá van adva a kizárásokhoz, a Kaspersky Endpoint Security kihagyja ezt a fájlt.

Ha például a Microsoft Windows Jegyzettömb szabványos alkalmazás által használt objektumokat biztonságosnak tekinti, azaz megbízik ebben az alkalmazásban, akkor felveheti a megbízható alkalmazások listájára, így az általa használt objektumok nem kerülnek megfigyelésre. Ez növeli a számítógép teljesítményét, ami különösen fontos a kiszolgálói alkalmazások használatakor.

Ezenkívül bizonyos, a Kaspersky Endpoint Security által gyanúsként osztályzott műveletek számos alkalmazás funkcióinak kontextusában biztonságos lehet. A billentyűzeten begépelt szöveg rögzítése például az automatikus billentyűzetkiosztás-átváltók esetén rutinszerű eljárás (ilyen például a Punto Switcher). Az ilyen alkalmazások jellemzőinek figyelembe vételéhez és tevékenységük figyelésből való kizárásához célszerű őket a megbízható alkalmazások listájára felvenni.

A megbízható alkalmazások segítenek elkerülni a Kaspersky Endpoint Security és más alkalmazások közötti kompatibilitási problémákat (például egy külső számítógép hálózati forgalmának a Kaspersky Endpoint Security és egy másik vírusirtó alkalmazás általi kettős vizsgálatát).

A megbízható alkalmazás végrehajtható fájljában és folyamatában ugyanakkor továbbra is sor kerül a vírusok és egyéb rosszindulatú programok jelenlétének vizsgálatára. Egy alkalmazás teljes mértékben kizárható a Kaspersky Endpoint Security vizsgálatából a vizsgálati kizárások segítségével.

Paraméter	Leírás

Észlelt objektumok típusai

A megadott alkalmazásbeállításoktól függetlenül a Kaspersky Endpoint Security mindig észleli és blokkolja a vírusokat, férgeket és trójaiakat. Ezek jelentős károkat okozhatnak a számítógépen.

- **Vírusok és férgek**

  Alkategória: vírusok és férgek (Viruses_and_Worms)

  Veszély szintje: magas

  A klasszikus vírusok és férgek a felhasználó által nem jóváhagyott műveleteket végeznek. Olyan másolatokat hozhatnak létre önmagukról, amelyek szintén képesek önmaguk másolására.

  Klasszikus vírus

  Miután egy klasszikus vírus a számítógépbe jut, megfertőz egy fájlt, aktiválódik, rosszindulatú műveleteket hajt végre, és önmaga másolataival lát el további fájlokat.

  A klasszikus vírus csak a számítógép helyi erőforrásaiban sokszorozódik meg, saját magától másik számítógépre nem tud átjutni. Csak akkor kerül át másik számítógépre, ha saját magát bemásolja egy megosztott könyvtárba, egy behelyezett CD-re, vagy, ha a felhasználó továbbít egy email üzenetet, amelynek a csatolt fájlja fertőzött.

  A klasszikus vírus kódja a számítógépek, operációs rendszerek vagy alkalmazások számos területét elérheti. A környezettől függően a vírusok lehetnek *fájl vírusok*, *boot vírusok*, *script vírusok* vagy *makróvírusok*.

  A vírusok rendkívül sokféle módon fertőzhetnek fájlokat. A(z) *Overwriting* vírusok saját kódjukkal felülírják a fertőzött fájlt, így törölve annak tartalmát. A fertőzött fájl működése leáll, így nem lehet helyreállítani. A(z) *Parasitic* vírusok csak módosítják a fájlokat, azokat teljesen vagy részlegesen működőképes állapotban hagyva. A(z) *Companion* nem módosítják a fájlokat, csak másolatot készítenek róluk. Egy fertőzött fájlt megnyitva annak másolata (azaz tulajdonképpen a vírus) indul el. Az alábbi vírusok szintén megtalálhatók: *Link vírusok*, *OBJ-vírusok*, *LIB-vírusok*, *forráskódú* vírusok és számos egyéb.

  Worm

  A klasszikus vírusokhoz hasonlóan a férgek kódja akkor aktiválódik és hajt végre rosszindulatú műveleteket, ha már elterjedt a rendszerben. Azért féreg a neve, mert képes „átmászni" az egyik számítógépről a másikra a felhasználó engedélye nélkül, hogy számos adatcsatornán keresztül elterjessze a másolatait.

  A különböző férgeket megkülönböztető fő tulajdonság az elterjedésük módja. Az alábbi táblázat áttekintést nyújt a férgek különféle típusairól, azok terjedésének módja alapján.

  A férgek terjedésének módjai

Típus	Name	Leírás
E-mail-féreg	E-mail-féreg	Ezek e-mailen keresztül terjednek. A fertőzött e-mail tartalmaz egy a féreg másolatát tartalmazó csatolt fájlt, vagy egy hivatkozást egy webhelyre feltöltött, kifejezetten erre a célra feltört vagy létrehozott fájlhoz. Ha a felhasználó megnyitja a csatolt fájlt, a féreg aktiválódik. A hivatkozásra kattintva a fájlt letöltve, majd megnyitva a féreg szintén megkezdi a rosszindulatú műveleteket. Ezután megkezdi lemásolni saját magát, újabb e-mail címek keresésébe kezd, és terjeszteni kezdi a fertőzött üzeneteket.
IM-Worm	IM kliens férgek	Azonnali üzenetküldőkön keresztül terjednek. Az ilyen férgek rendszerint a felhasználó partnerlistáját felhasználva üzenetet küldenek, benne egy adott webhelyen, a féreg másolatát tartalmazó fájlra mutató hivatkozással. Amikor a felhasználó letölti és megnyitja a fájlt, a féreg aktiválódik.
IRC-Worm	Internetes csevegési férgek	Ezek olyan Internet Relay Chats szolgáltatásokon keresztül terjednek, amelyek valós idejű kommunikációt biztosítanak az interneten keresztül. Az ilyen férgek az internetes csevegésben egy önmagukat tartalmazó fájlt adnak közre, vagy egy hivatkozást a fájlra. Amikor a felhasználó letölti és megnyitja a fájlt, a féreg aktiválódik.
Net-Worm	Hálózati férgek	Ezek a férgek számítógépes hálózatokon terjednek. A többi féreggel ellentétben a tipikus hálózati féreg a felhasználó beavatkozása nélkül terjed. A féreg átvizsgálja a helyi hálózaton található számítógépeket, és sebezhetőséget jelentő programokat keres. Ehhez erre a célra létrehozott hálózati programcsomagokat küld szét (amik a biztonsági rések kiaknázását végzik), benne a féreg kódjával. Ha egy „sebezhető" számítógép található a hálózaton, az megkapja az ilyen hálózati csomagot. Amint a féreg teljesen bejutott a számítógépbe, azonnal aktiválódik.
P2P-Worm	Fájlcserélő hálózati férgek	Fájlcserélő (Peer-to-Peer) hálózatokon keresztül terjednek. A P2P hálózatba való bejutáshoz a féreg bemásolja magát a fájlcsere mappába, amely rendszerint a felhasználó számítógépén található. A P2P hálózat információkat jelenít meg a fájlról, így a felhasználó a többi fájlhoz hasonlóan „megtalálja" a fertőzött fájlt a hálózaton, majd letölti és megnyitja. A kifinomultabb férgek adott P2P-hálózat protokollját is képesek emulálni: ezek pozitív válaszokat küldenek a keresésekre, majd felajánlják saját másolatukat letöltésre.
Worm	Egyéb típusú férgek	Az egyéb típusú férgek a következők lehetnek: • Saját másolataikat hálózati erőforrásokon át terjesztő férgek. Az operációs rendszer funkcióit kihasználva ezek megvizsgálják az elérhető hálózati mappákat, más számítógépekhez kapcsolódnak az interneten keresztül, és megkísérlik azok lemezmeghajtói felett átvenni a teljes uralmat. A fent ismertetett férgekkel ellentétben mások maguktól nem aktiválódnak, csak akkor, ha a felhasználó megnyitja a féreg egy másolatát tartalmazó fájlt. • Olyan férgek, amelyek a táblázatban ismertetett módok egyikét sem használják az elterjedésre (pl. a mobiltelefonokon terjedő férgek).

- **Trójai programok (köztük zsarolóprogramok)**

  Alkategória: Trójai programok

Veszély szintje: magas

A férgekkel és vírusokkal ellentétben a trójai programok nem szaporítják magukat. A számítógépet például e-mailen vagy böngészőn át szállják meg, amikor a felhasználó fertőzött weboldalt látogat meg. A trójai programok a felhasználó közreműködésével indulnak el. Rosszindulatú működésüket közvetlenül az elindulásukat követően kezdik meg.

A különböző trójai programok eltérően viselkednek a fertőzött számítógépeken. A „trójai" fő funkciói az információk blokkolása, módosítása vagy megsemmisítése, leállítva ezzel számítógépeket, hálózatokat. Ezen kívül a trójai programok fájlokat fogadnak és küldenek, futtatják azokat, üzeneteket jelenítenek meg a képernyőn, weboldalaknak küldenek kérést, programokat töltenek le és telepítenek, valamint újraindítják a számítógépet.

A hackerek gyakran különböző trójai programok „készletét" alkalmazzák.

Az alábbi táblázat a trójai programok viselkedéstípusait ismerteti.

Trójai programok viselkedése fertőzött számítógépen

Típus	Name	Leírás
Trojan-ArcBomb	Trójai programok – „archívumbombák"	Kicsomagoláskor az archívumok mérete megnő, ami kihat a számítógép működésére. Az ilyen archívum kicsomagolásakor a számítógép működése lelassul, esetleg lefagy és a merevlemez megtelhet „üres" adatokkal. Az „archívumbombák" különösen nagy veszélyt jelentenek fájl és levelező kiszolgálókra. Ha a kiszolgáló automatikus rendszert használ a beérkező információk feldolgozására, az „archívumbomba" leállíthatja a működését.
Backdoor	Távoli rendszerfelügyeletet lehetővé tevő trójai programok	Az összes közül ezek a legveszélyesebb trójai programok. Funkciójuk alapján hasonlítanak a számítógépre telepített rendszerfelügyeleti alkalmazásokhoz. Ezek a programok a felhasználó tudtán kívül telepítik magukat a számítógépre, lehetővé téve, hogy a betolakodó távolról átvegye az uralmat a gép felett.
Trojan	Trójai programok	Ez a kategória az alábbi rosszindulatú alkalmazásokat tartalmazza: • **Klasszikus trójai programok**. Ezek a programok csak a trójai programok fő funkcióit látják el, melyek a következők: az információk blokkolása, módosítása vagy megsemmisítése és a számítógépek, hálózatok leállítása. Nem rendelkeznek olyan speciális funkciókkal, mint a táblázatban szereplő más típusok. • **Sokoldalú trójai programok**. Ezek a programok számos trójai programra jellemző speciális funkcióval rendelkeznek.
Trojan-Ransom	Váltságdíj trójai	Ezek a felhasználó adatait „túszul ejtik", módosítva vagy blokkolva azt, esetleg meggátolják a számítógép működését, hogy a felhasználó számára elvesszenek az adatok. A betolakodó váltságdíjat követel a felhasználótól, azt ígérve, hogy küld egy alkalmazást, amellyel visszaállítható a számítógép normál állapota az elveszett adatokkal együtt.
Trojan-Clicker	Trójai kattintók	Ezek a felhasználó számítógépéről weboldalakat látogatnak meg, saját maguk utasítva a webböngészőt, vagy módosítva az operációs rendszer fájljaiban megadott webcímet. Az ilyen programokkal a betolakodó hálózati támadást indíthat, valamint webhelyek látogatottságát növelheti, hogy a reklámcsíkhirdetések megjelenítésének a száma növekedjen.
Trojan-Downloader	Trójai-letöltők	Ezek a betolakodó weboldaláról további rosszindulatú alkalmazásokat töltenek le és telepítenek a felhasználó számítógépére. A letöltendő rosszindulatú alkalmazás fájlnevét tartalmazhatják, illetve megkaphatják a meglátogatott weboldalról is.
Trojan-Dropper	Trójaitelepítők	Más trójai programokat tartalmaznak, melyeket a számítógép merevlemezére mentenek, majd telepítenek. A betolakodók a telepítő típusú trójai programokat az alábbi célokból használhatják: • Rosszindulatú alkalmazás telepítése a felhasználó tudtán kívül: A trójai telepítőprogramok nem jelenítenek meg rendszerüzeneteket, vagy hamis információkat jelenítenek meg például tömörített fájl hibájáról, esetleg az operációs rendszer inkompatibilis verziójáról. • Más ismert rosszindulatú alkalmazások megvédése a felfedezéstől: nem minden vírusirtó szoftver képes felismerni a trójai telepítőprogramon belül a rosszindulatú alkalmazást.
Trojan-Notifier	Trójai-értesítők	Tájékoztatják a betolakodót, hogy a fertőzött számítógép hozzáférhető, és elküldik neki a számítógép adatait: az IP-címet, a megnyitott port számát, illetve az e-mail-címet. Kapcsolatba lépnek a betolakodóval e-mailben vagy FTP-n, weboldalának meglátogatásával vagy más módon. Ezek a programok gyakran több trójai programból álló programcsomag részét képezik. Ezek értesítik a betolakodót a többi trójai program sikeres telepítéséről.
Trojan-Proxy	Trójai-proxyk	Segítségükkel a betolakodó névtelenül érhet el weboldalakat a felhasználó számítógépéről; gyakran alkalmazzák őket levélszemét küldésére.
Trojan-PSW	Jelszólopó programok	A jelszólopók olyan típusú trójai programok, amelyek felhasználói fiókokat törnek fel, például szoftver regisztrációs adatait szerzik meg. A bizalmas adatokat a rendszerfájlokban és a regisztrációs adatbázisban érik el, majd elküldik azokat a „támadónak" e-mail, FTP útján, meglátogatva a weboldalát, esetleg más módon. Néhány ilyen trójai program a táblázat által tárgyalt külön kategóriába sorolható. Ezek a bankfiók adatokat lopó trójai programok (Trojan-Banker), az azonnali üzenetküldő programok felhasználóitól adatokat lopó trójai programok (Trójai-IM) valamint online játékok felhasználóitól adatokat lopó trójai programok (Trojan-GameThief).
Trojan-Spy	Trójai-kémek	Ezek kémkednek a felhasználó után, információkat gyűjtenek az általa a számítógépen végzett műveletekről. Eltéríthetik a felhasználó által a billentyűzeten begépelt adatokat, képernyőképet készíthetnek, vagy elkészíthetik az aktív alkalmazások teljes listáját. Miután megszerezték az információkat, eljuttatták azokat a betolakodónak e-mail, FTP útján, a weboldalát meglátogatva vagy más módon.
Trojan-DDoS	Trójai hálózattámadók	Az ilyen programok a felhasználó számítógépéről rengeteg kérést küldenek egy távoli kiszolgálóra. A kiszolgáló az összes kérésre reagálva kifogy az erőforrásaiból, és leáll (Denial-of-Service, vagy DoS). A hackerek gyakran több számítógépet is megfertőznek ilyen programokkal, hogy több párhuzamos támadást indíthassanak egyetlen kiszolgáló ellen. A DoS programok egy számítógépről a felhasználó tudtával indítanak támadást. A DDoS (elosztott DoS) programok több számítógépről a fertőzött számítógép felhasználójának a tudta nélkül indítanak elosztott támadást.
Trojan-IM	Azonnali üzenetküldő ügyfelek felhasználóitól adatokat lopó trójai programok	Ellopják az azonnali üzenetküldők felhasználóinak számlaszámait és jelszavait. Az információkat eljuttatják a betolakodónak e-mail, FTP útján, a weboldalát meglátogatva vagy más módon.

Rootkit	Rootkitek	Ezek más rosszindulatú alkalmazásokat és azok tevékenységét maszkolják, így meghosszabbítva azok jelenlétét az operációs rendszerben. Emellett a fertőzött számítógép memóriájában olyan fájlokat, folyamatokat vagy beállításkulcsokat rejtenek el, amelyek rosszindulatú alkalmazásokat futtatnak. A rootkitek maszkolhatnak adatcserét alkalmazások között a felhasználó számítógépén és a hálózaton található számítógépek között.
Trojan-SMS	SMS-üzenetek formájában megjelenő trójai programok	Ezek mobiltelefonokat fertőznek meg, SMS-üzeneteket küldve fizetős telefonszámokra.
Trojan-GameThief	Online játékok felhasználóitól adatokat lopó trójai programok	Ezek online játékok résztvevőitől lopnak fiókbejelentkezéseket, aztán eljuttatják a betolakodónak e-mailben, FTP-n, a weboldala meglátogatásával vagy más módon.
Trojan-Banker	Bankszámlaadatokat lopó trójai programok	Ezek bankszámlaadatokat vagy elektronikus fizetési rendszeradatokat lopnak, aztán → eljuttatják a hackernek e-mailben, FTP-n, a weboldala meglátogatásával vagy más módon.
Trojan-Mailfinder	E-mail címeket gyűjtő trójai programok	Ezek a számítógépen található e-mail címeket gyűjtik össze, aztán eljuttatják a betolakodónak e-mail, FTP útján, a weboldalát meglátogatva vagy más módon. A betolakodók az összegyűjtött címekre aztán levélszemetet küldenek.

- **Rosszindulatú eszközök**

  Alkategória: Rosszindulatú eszközök

  Veszély szintje: közepes

  A többi rosszindulatú programmal ellentétben a rosszindulatú eszközök az elindítás után közvetlenül nem kezdik el a működésüket. Ily módon biztonságosan menthetők és elindíthatók a felhasználó számítógépén. A betolakodók az ilyen programok funkcióit gyakran használják vírusok, férgek és trójai programok létrehozására, hálózati támadások indítására távoli kiszolgálók ellen, számítógépek feletti uralom átvételére vagy más rosszindulatú műveletek végrehajtására.

  A rosszindulatú eszközök különböző funkciói az alábbi táblázat szerint csoportosíthatók.

  Rosszindulatú eszközök funkciói

Típus	Name	Leírás
Constructor	Konstruktorok	Ezek segítségével hozhatók létre új vírusok, férgek és trójai programok. Néhány konstruktor szabványos ablakalapú felülettel rendelkezik, ahol a felhasználó kiválaszthatja a létrehozni kívánt rosszindulatú alkalmazás típusát, a hibakeresésre adandó választ és egyéb tulajdonságokat.
Dos	Hálózati támadások	Az ilyen programok a felhasználó számítógépéről rengeteg kérést küldenek egy távoli kiszolgálóra. A kiszolgáló az összes kérésre reagálva kifogy az erőforrásaiból, és leáll (Denial-of-Service, vagy DoS).
Exploit	Biztonsági rések	Az *exploit* olyan adatcsomag vagy programkód, amely az alkalmazás sebezhetőségét megkeresve, azt kihasználva rosszindulatú műveletbe kezd a számítógépen. Például az exploit fájlokat ír és olvas, vagy kérést küld „fertőzött" weboldalaknak. A különböző exploitok különböző alkalmazások vagy hálózati szolgáltatások sebezhetőségét használják ki. Az exploit hálózati csomagnak álcázva magát a hálózaton keresztül számos számítógépbe eljut, sebezhető hálózati szolgáltatásokkal rendelkező számítógépeket keresve. A DOC fájlban működő exploit a szövegszerkesztő program sebezhetőségét használja ki. A készítője által beprogramozott műveletet akkor kezdi végrehajtani, amikor a felhasználó megnyitja a fertőzött fájlt. Az e-mail üzenetbe ágyazott exploit az e-mail kliens sebezhetőségeit keresi. A rosszindulatú műveletet akkor kezdi végrehajtani, amikor a felhasználó megnyitja a fertőzött üzenetet az e-mail kliensben. A hálózati férgek a hálózaton exploitok segítségével terjednek. A Nuker exploitok számítógépeket leállító hálózati csomagok.
FileCryptor	Titkosítók	Ezek más rosszindulatú alkalmazásokat titkosítanak, hogy elrejtsék azokat a víruskereső alkalmazások elől.
Flooder	Hálózatokat „szennyező" programok	Ezek nagy mennyiségű üzenetet küldenek hálózati csatornákon. Az ilyen eszközök között találhatók az internetes csevegéseket szennyező programok is. Az elárasztó eszközök nem tartalmaznak e-mail, IM-kliens és mobilkommunikációs rendszerek csatornáit „eltömítő" programokat. Az ilyen programok külön típusként (e-mail-elárasztó, IM-elárasztó és SMS-elárasztó) szerepelnek ebben a táblázatban.
HackTool	Hackelő eszközök	Az ilyenek teszik lehetővé azon számítógép feletti uralom átvételét, amelyre feltelepültek, vagy más számítógépek megtámadását (például új rendszerfiók felvételét a felhasználó engedélye nélkül, a rendszernapló törlését, hogy elrejthető legyen a jelenlétük az operációs rendszerben). Ebbe a típusba tartoznak némely szimatoló programok, amelyek jelszavakat térítenek el. A Szimatolók olyan programok, amelyek a hálózati forgalmat képesek megjeleníteni.
Hoax	Hoaxok	Az ilyenek a felhasználót vírus jellegű üzenetekkel riogatják: ezek nem fertőzött fájlban is „észlelik a vírust", vagy olyan formázásról értesítik a felhasználót, ami a valóságban nem történik meg.
Spoofer	Hamisító eszközök	Ezek a feladó hamis címéről küldenek üzeneteket és hálózati kéréseket. A behatolók hamisító jellegű eszközöket alkalmaznak, hogy például üzenetek valódi feladóinak adják ki magukat.
VirTool	Rosszindulatú alkalmazásokat módosító eszközök	Ezek lehetővé teszik más rosszindulatú programok módosítását, hogy elrejtsék azokat víruskereső alkalmazások elől.
Email-Flooder	E-mail címeket „szennyező" programok	Ezek nagy mennyiségű üzenetet küldenek számos e-mail címre, így„szennyezve" azokat. A nagy mennyiségű beérkező üzenet gátolja a felhasználót a hasznos üzenetei kezelésében.
IM-Flooder	Az azonnali üzenetküldők forgalmát SMS üzenetekkel „szennyező" programok	Az azonnali üzenetküldők felhasználóit elárasztják üzenetekkel. Az üzenetek nagy száma akadályozza a felhasználót a hasznos üzenetek kezelésében.
SMS-Flooder	A forgalmat SMS üzenetekkel „szennyező" programok	Ezek nagy mennyiségű SMS-üzenetet küldenek a mobiltelefonra.

- **Reklámprogram**

  Alkategória: hirdetési szoftver (reklámprogram)

  Veszély szintje: közepes

  A reklámprogram a felhasználó számára biztosít reklámokat. A reklámprogram más program kezelőfelületén reklámcsík hirdetést jelenít meg, és a kereső kérését a hirdető weboldalára irányítja. Néhányuk marketinginformációkat gyűjt a felhasználóról, majd elküldi a fejlesztőnek: ezek az információk a felhasználó által meglátogatott weboldalak neveit, az általa használt keresési kulcsszavakat tartalmazhatják. A trójai kémprogramokkal ellentétben a reklámprogramok ezeket az adatokat a felhasználó beleegyezésével küldik el a fejlesztőnek.

- **Autotárcsázók**

  Alkategória: legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.

  Veszély szintje: közepes

  A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetek IRC-kliensek, tárcsázók, fájlletöltő programok, számítógépes rendszertevékenység-figyelők, jelszókezelők, internetkiszolgálók FTP, HTTP, és Telnet szolgáltatásokhoz.

  Mindazonáltal ha a betolakodók hozzáféréssel rendelkeznek az ilyen programokhoz vagy bejuttatják a felhasználó számítógépébe, akkor néhány funkciójukat a biztonság feltörésére használhatják.

  Ezeknek az alkalmazásoknak eltérőek a funkcióik; az alábbi táblázat a típusaikat tartalmazza.

Típus	Name	Leírás
Client-IRC	Internet csevegő kliensek	A felhasználó az ilyen programokat másokkal való kapcsolattartásra használja internetes csevegéseken. A betolakodók ezeken a programokon keresztül terjesztik a rosszindulatú programokat.
Downloader	Letöltéshez használható programok	Ezek rejtve töltenek le fájlokat különböző weboldalakról.
Monitor	Monitorozásra alkalmas programok	Ezek monitorozást tesznek lehetővé azon a számítógépen, amelyre feltelepültek (azt figyelve, hogy mely alkalmazások aktívak, és azok miként folytatják az adatcserét más számítógépekre telepített programokkal).
PSWTool	Jelszó visszaállítók	Ezek elfelejtett jelszavak megtekintését és helyreállítását teszik lehetővé. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal:
RemoteAdmin	Távoli rendszerfelügyeletet lehetővé tevő programok	Ezeket széles körben alkalmazzák rendszergazdák. A programok a távoli számítógép kezelőfelületét teszik elérhetővé, annak monitorozása és felügyelése céljából. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal: a távoli számítógép monitorozása és felügyelete céljából. A legális távfelügyeleti programok különböznek a hátsó kapu típusú trójai távfelügyeleti programoktól. A trójai programok jellegzetessége, hogy függetlenül bejutnak az operációs rendszerbe, és magukat feltelepítik; a jogszerű programok nem rendelkeznek ilyen funkcióval.
Server-FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Server-Proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Server-Telnet	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Server-Web	Webkiszolgálók	Ezek webkiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy HTTP-n keresztül távoli elérést nyissanak hozzá.
RiskTool	Helyi számítógépen történő munkavégzésre szolgáló eszközök	A felhasználó számára további lehetőségeket biztosítanak, amikor a számítógépén dolgozik. Az eszköz segítségével a felhasználó aktív alkalmazások ablakait, fájljait rejtheti el, és aktív folyamatokat állíthat le.
NetTool	Hálózati eszközök	A felhasználó számára további lehetőségeket biztosítanak, amikor a hálózaton más számítógépeken dolgozik. Segítségével újraindíthatja a távoli gépeket, felderítheti a nyitott portokat, és a távoli gépre telepített alkalmazásokat futtathat.
Client-P2P	P2P hálózati ügyfelek	Segítségükkel a felhasználó fájlcserélő (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.
Client-SMTP	SMTP-kliensek	E-mail üzeneteket küldenek a felhasználó tudta nélkül. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
WebToolbar	Webes eszköztárak	Ezek eszköztárakkal egészítik ki más alkalmazások kezelőfelületeit, keresőmotorok elérését megkönnyítve.
FraudTool	Pszeudoprogramok	Ezek más programoknak adják ki magukat. Lehetnek például pszeudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.

- **Legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait**

  Alkategória: legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.

  Veszély szintje: közepes

  A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetek IRC-kliensek, tárcsázók, fájlletöltő programok, számítógépes rendszertevékenység-figyelők, jelszókezelők, internetkiszolgálók FTP, HTTP, és Telnet szolgáltatásokhoz.

Mindazonáltal ha a betolakodók hozzáféréssel rendelkeznek az ilyen programokhoz vagy bejuttatják a felhasználó számítógépébe, akkor néhány funkciójukat a biztonság feltörésére használhatják.

Ezeknek az alkalmazásoknak eltérőek a funkcióik; az alábbi táblázat a típusaikat tartalmazza.

Típus	Name	Leírás
Client-IRC	Internet csevegő kliensek	A felhasználó az ilyen programokat másokkal való kapcsolattartásra használja internetes csevegéseken. A betolakodók ezeken a programokon keresztül terjesztik a rosszindulatú programokat.
Downloader	Letöltéshez használható programok	Ezek rejtve töltenek le fájlokat különböző weboldalakról.
Monitor	Monitorozásra alkalmas programok	Ezek monitorozást tesznek lehetővé azon a számítógépen, amelyre feltelepültek (azt figyelve, hogy mely alkalmazások aktívak, és azok miként folytatják az adatcserét más számítógépekre telepített programokkal).
PSWTool	Jelszó visszaállítók	Ezek elfelejtett jelszavak megtekintését és helyreállítását teszik lehetővé. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal:
RemoteAdmin	Távoli rendszerfelügyeletet lehetővé tevő programok	Ezeket széles körben alkalmazzák rendszergazdák. A programok a távoli számítógép kezelőfelületét teszik elérhetővé, annak monitorozása és felügyelése céljából. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal: a távoli számítógép monitorozása és felügyelete céljából. A legális távfelügyeleti programok különböznek a hátsó kapu típusú trójai távfelügyeleti programoktól. A trójai programok jellegzetessége, hogy függetlenül bejutnak az operációs rendszerbe, és magukat feltelepítik; a jogszerű programok nem rendelkeznek ilyen funkcióval.
Server-FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Server-Proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Server-Telnet	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Server-Web	Webkiszolgálók	Ezek webkiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy HTTP-n keresztül távoli elérést nyissanak hozzá.
RiskTool	Helyi számítógépen történő munkavégzésre szolgáló eszközök	A felhasználó számára további lehetőségeket biztosítanak, amikor a számítógépén dolgozik. Az eszköz segítségével a felhasználó aktív alkalmazások ablakait, fájljait rejtheti el, és aktív folyamatokat állíthat le.
NetTool	Hálózati eszközök	A felhasználó számára további lehetőségeket biztosítanak, amikor a hálózaton más számítógépeken dolgozik. Segítségével újraindíthatja a távoli gépeket, felderítheti a nyitott portokat, és a távoli gépre telepített alkalmazásokat futtathat.
Client-P2P	P2P hálózati ügyfelek	Segítségükkel a felhasználó fájlcserélő (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.
Client-SMTP	SMTP-kliensek	E-mail üzeneteket küldenek a felhasználó tudta nélkül. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
WebToolbar	Webes eszköztárak	Ezek eszköztárakkal egészítik ki más alkalmazások kezelőfelületeit, keresőmotorok elérését megkönnyítve.
FraudTool	Pszeudoprogramok	Ezek más programoknak adják ki magukat. Lehetnek például pszeudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.

- **Csomagolt objektumok, melyek tömörítése felhasználható károkozásra képes kód védelmére**

  Alkategória: csomagolt fájlok, amelyek kárt okozhatnak.

  Veszély szintje: közepes.

  A fájl csomagolása egy speciális csomagolóprogrammal történik, amelyet rosszindulatú programok (vírusok, férgek, trójaiak) csomagolására használnak. A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található önkicsomagoló modult ellenőrzi.

  A hackerek a kártevőket speciális csomagolóprogramok segítségével csomagolják be, hogy elrejtsék azokat a vírusirtók észlelése elől. A Kaspersky szakértői azonosították a hackerek által leggyakrabban alkalmazott csomagolóprogramokat.

- **Többszörösen csomagolt objektumok**

  Alkategória: csomagolt fájlok, amelyek kárt okozhatnak.

  Veszély szintje: közepes.

  A fájl csomagolása egy speciális csomagolóprogrammal történik, amelyet rosszindulatú programok (vírusok, férgek, trójaiak) csomagolására használnak. A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található önkicsomagoló modult ellenőrzi.

  A hackerek a kártevőket speciális csomagolóprogramok segítségével csomagolják be, hogy elrejtsék azokat a vírusirtók észlelése elől. A Kaspersky szakértői azonosították a hackerek által leggyakrabban alkalmazott csomagolóprogramokat.

Kizárások

Ez a táblázat a vizsgálati kizárásokkal kapcsolatos adatokat tartalmaz.

Javasoljuk, hogy abszolút elérési utak helyett relatív útvonalakat adjon meg. Ez lehetővé teszi nemcsak a fájlrendszer-objektumok, hanem a fájl nélküli objektumok kizárását is. Például: `*\Program Files`

`(x86)\Folder\Subfolder`.

A következő módszerekkel kizárhat objektumokat a vizsgálat alól:

- A fájl vagy mappa elérési útjának megadása.
- Az objektum ellenőrzőösszeg megadása.
- maszkok használata:
  - A `*` (csillag) karakter, mely helyettesít bármely karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\*\*.txt` maszk a minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a C: meghajtón lévő mappákban található (kivéve az almappák).
  - Két egymást követő `*` karakter bármely karakterhalmazt helyettesíthet (az üres halmazt is) a fájlban, beleértve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\**\*.txt` maszk a `Folder` nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a `Folder`. A maszknak legalább egy beágyazási szintet kell tartalmaznia. A `C:\**\*.txt` maszk nem érvényes maszk.
  - A `?` (kérdőjel) karakter, mely helyettesít bármely egyedülálló karaktert, kivéve a `\` és `/` karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a `C:\Folder\???.txt` maszk tartalmazni fogja a `Folder` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

    A maszkokat bárhol használhatja a fájl vagy mappa elérési útjában. Ha például a vizsgálat hatókörét szeretné kiterjeszteni a számítógépen található összes felhasználói fiók Letöltések mappájára, írja be a `C:\Users\*\Downloads\` maszkot.

    A Kaspersky Endpoint Security támogatja a környezeti változókat

    > A Kaspersky Endpoint Security nem támogatja a `%userprofile%` környezeti változót, amikor a Kaspersky Security Center konzol segítségével hozza létre a kizárások listáját. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a * karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást.

- Adja meg az objektumtípus nevét a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például `Email-Worm`, `Rootkit` vagy `RemoteAdmin`). Használhat maszkokat a `?` karakterrel (bármely karaktert helyettesíti) és a `*` karakterrel (tetszőleges számú karaktert helyettesít). Például, ha a `Client*` maszk van megadva, az alkalmazás kizárja a `Client-IRC`, `Client-P2P` és a `Client-SMTP` objektumokat is a vizsgálatokból.

> A Kaspersky Endpoint Security elrejti a vizsgálati kizárások listáját az alkalmazás felhasználói felületén, ha a konzolon a rendszergazda letiltotta a vizsgálati kizárások konfigurálását („zárt lakat" szimbólum), és a helyi vizsgálati kizárások tiltva vannak (a **Helyi kizárások használatának engedélyezése** jelölőnégyzet nincs bejelölve).

Megbízható alkalmazások	Ebben a táblázatban azoknak a megbízható alkalmazásoknak a listája található, amelyeknek a tevékenységét a Kaspersky Endpoint Security működése közben nem figyeli. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor. A Kaspersky Endpoint Security nem támogatja a `%userprofile%` környezeti változót a megbízható alkalmazások listájának létrehozásakor a Kaspersky Security Center konzolon. Ha a bejegyzést minden felhasználói fiókra alkalmazni szeretné, használhatja a `*` karaktert (például `C:\Users\*\Documents\File.exe`). Amikor új környezeti változót ad hozzá, újra kell indítania az alkalmazást. Az Alkalmazásfelügyelő összetevő szabályozza az egyes alkalmazások elindulását, függetlenül attól, hogy az adott alkalmazás szerepel-e a megbízható alkalmazások listáján. A Kaspersky Endpoint Security elrejti a megbízható alkalmazások összevont listáját az alkalmazás felhasználói felületén, ha a rendszergazda a konzolon letiltotta a megbízható alkalmazások konfigurálását („zárt lakat" szimbólum), és a helyi megbízható alkalmazások tiltva vannak (a **Helyi megbízható alkalmazások használatának engedélyezése** jelölőnégyzet nincs bejelölve).
Értékek egyesítése öröklésekor *(csak a Kaspersky Security Center konzolon érhető el)*	Ez egyesíti a Kaspersky Security Center szülő- és gyermekházirendjében szereplő vizsgálati kizárások és megbízható alkalmazások listáját. A listák egyesítéséhez a gyermekházirendet úgy kell beállítani, hogy örökölje a Kaspersky Security Center szülőházirendjének beállításait. Ha a jelölőnégyzet be van jelölve, a Kaspersky Security Center szülőházirendjének listaelemei megjelennek a gyermekházirendekben. Így például létrehozhatja a megbízható alkalmazások összesített listáját a teljes szervezet számára. A gyermekházirend örökölt listaelemei nem törölhetők és nem szerkeszthetők. A vizsgálati kizárások listájában szereplő elemek és az öröklődés során egyesített megbízható alkalmazások listája csak a szülőházirendben törölhető és szerkeszthető. Az alacsonyabb szintű irányelvekben lehetősége van hozzáadni, módosítani és eltávolítani a listaelemeket. Ha a gyermek- és szülőházirend listák elemei egyeznek, ezek az elemek a szülőházirend ugyanazon elemeként jelennek meg. Ha a jelölőnégyzet nincs bejelölve, akkor a lista elemeit nem egyesíti a rendszer, amikor a Kaspersky Security Center házirendek beállításainak öröklése zajlik. Ez a funkció lehetővé teszi a házirend-profilok listáinak összevonását is. A listák egyesítéséhez a legmagasabb prioritású profilban engedélyezze a beállítások öröklését egy alacsonyabb prioritású profilból. A házirend-profilok prioritásaival kapcsolatos további részletekért olvassa a Kaspersky Security Center súgóját.
Helyi kizárások használatának engedélyezése/Helyi megbízható alkalmazások használatának engedélyezése *(csak a Kaspersky Security Center konzolon érhető el)*	*Helyi kizárások és helyi megbízható alkalmazások (helyi megbízható zóna)* – a felhasználó által a Kaspersky Endpoint Security alkalmazásban meghatározott objektumok és alkalmazások listája egy adott számítógépen. A Kaspersky Endpoint Security nem figyeli a helyi megbízható zónából származó objektumokat és alkalmazásokat. Így a felhasználók a házirendben található általános megbízható zóna mellett létrehozhatják a kizárásokra és megbízható alkalmazásokra vonatkozó saját listájukat is. Ha a jelölőnégyzet be van jelölve, a felhasználó létrehozhat egy helyi listát a vizsgálati kizárásokról és egy helyi listát a megbízható alkalmazásokról. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket. Ha a jelölőnégyzet nincs bejelölve, a felhasználó csak a házirendben létrehozott vizsgálati kizárások általános listájához és megbízható alkalmazások általános listájához férhet hozzá.
EDR (KATA) / NDR (KATA) telemetria *(csak a Kaspersky Security Center konzolon érhető el)*	Ez a táblázat az EDR telemetria kizárásaival kapcsolatos információkat tartalmazza.
KUMA telemetria *(csak a Kaspersky Security Center konzolon érhető el)*	A Kaspersky Unified Monitoring and Analysis Platform (KUMA) számára küldendő események listája. A Kaspersky Endpoint Security a következő módokban működik: • **Összes esemény küldése**. Ebben a módban az alkalmazás az összes eseményt a Windows naplójából küldi el, kivéve a kizárási szabályokhoz hozzáadott eseményeket. • **Csak kiválasztott események küldése**. Ebben a módban az alkalmazás csak a belefoglalási szabályokban hozzáadott eseményeket küldi el.
Megbízható rendszertanúsítvány tárhelye	Valamelyik megbízható rendszertanúsítvány-áruházat kiválasztva a Kaspersky Endpoint Security kizárja a vizsgálatból a megbízható digitális aláírással aláírt alkalmazásokat. A Kaspersky Endpoint Security automatikusan hozzárendeli ezeket az alkalmazásokat a **Megbízható** csoporthoz. Ha a **Ne használja** lehetőség van kiválasztva, a Kaspersky Endpoint Security megvizsgálja az alkalmazásokat, függetlenül attól, hogy rendelkeznek-e digitális aláírással. A Kaspersky Endpoint Security egy alkalmazást az alapján helyez megbízhatósági csoportba, hogy az alkalmazás milyen veszélyességi szintet képvisel a számítógép szempontjából.

Alkalmazásbeállítások

A következő általános beállításokat adhatja meg az alkalmazáshoz:

- Működési mód
- Önvédelem
- Teljesítmény
- Hibakeresési adatok
- A számítógép állapota a beállítások alkalmazásakor

Alkalmazásbeállítások

Paraméter	Leírás
Az alkalmazás indítása a számítógép indításakor (ajánlott)	Ha az opció ki van választva, a Kaspersky Endpoint Security az operációs rendszer betöltését követően elindul, és a teljes munkamenet során védi a számítógépet. Ha ez az opció nincs kijelölve, a Kaspersky Endpoint Security nem indul el az operációs rendszer indításakor, amíg a felhasználó kézileg el nem indítja. A számítógép védelme le van tiltva, és a felhasználói adatok fenyegetéseknek lehetnek kitéve.
Fejlett vírusmentesítő technológia használata (jelentős számítógépes erőforrásokat igényel)	A Kaspersky Endpoint Security általában még a számítógép megfertőződése előtt megszünteti az észlelt kártevőket. A Fejlett vírusmentesítési technológia megvédi a számítógépet a már aktív rosszindulatú programoktól (aktív fertőzés), ezáltal minimalizálja az adatvesztés és a fertőzés terjedésének kockázatát. Ha ez a technológia engedélyezve van, a Kaspersky Endpoint Security rosszindulatú tevékenység észlelésekor egy felugró értesítést jelenít meg. Az értesítésben a Kaspersky Endpoint Security felajánlja a számítógép Fejlett vírusmentesítésének elvégzését. Miután a felhasználó jóváhagyja az eljárást, a Kaspersky Endpoint Security semlegesíti a fenyegetést, majd újraindítja a számítógépet. A fejlett vírusmentesítő technológia jelentős számítógépes erőforrásokat vesz igénybe, amitől a többi alkalmazás lelassulhat. Amikor az alkalmazás aktív fertőzés észlelését végzi, elképzelhető, hogy az operációs rendszer bizonyos funkciói nem érhetők el. Az operációs rendszer funkciói a Fejlett vírusmentesítés befejeződésével és a számítógép újraindulásával ismét elérhetővé válnak. Ha a Kaspersky Endpoint Security alkalmazás Windows for Servers operációs rendszert futtató számítógépre van telepítve, a Kaspersky Endpoint Security nem jeleníti meg az értesítést. Ezért Ön nem választhatja ki az aktív fenyegetés vírusmentesítésére szolgáló műveletet. A fenyegetések vírusmentesítéséhez engedélyeznie kell a fejlett vírusmentesítő technológiát az alkalmazásbeállításokban, és engedélyeznie kell az azonnali fejlett vírusmentesítést a *Kártevő vizsgálata* feladat beállításaiban. Ezután el kell indítania a *Kártevő vizsgálata* feladatot.
A Kaspersky Security Center használata proxykiszolgálóként az aktiváláshoz *(csak a Kaspersky Security Center konzolon érhető el)*	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás a Kaspersky Security Center felügyeleti kiszolgálót használja proxykiszolgálóként az aktiváló kiszolgálókhoz való csatlakozáshoz. Erre akkor van szükség, ha aktiváló kódot használ az alkalmazás aktiválásához egy elszigetelt, internet-hozzáférés nélküli hálózati szegmensben. Ha az alkalmazást kulcsfájl segítségével aktiválja, nincs szükség internet-hozzáférésre.
Önvédelem engedélyezése	Ha ez a funkció engedélyezve van, a Kaspersky Endpoint Security megakadályozza a merevlemezen lévő alkalmazásfájlok, a memóriafolyamatok és a beállításjegyzék bejegyzései módosítását és törlését.

Paraméter	Leírás
Alkalmazásszolgáltatások külső felügyeletének blokkolása	Ha ez a funkció engedélyezve van, a Kaspersky Endpoint Security nem teszi lehetővé az alkalmazásszolgáltatások harmadik féltől származó alkalmazások (például CMD) használatával való kezelését. Az alkalmazásszolgáltatások harmadik féltől származó alkalmazások használatával történő kezelésére tett kísérlet esetén a Microsoft Windows tálcán az alkalmazás ikonja fölött értesítés jelenik meg (kivéve, ha az értesítési szolgáltatást a felhasználó letiltotta). Az alkalmazásszolgáltatások külső kezelését csak olyan számítógépeken engedélyezheti, amelyek nem támogatják az AM-PPL technológiát, illetve olyan számítógépeken, amelyeken a technológia le van tiltva.
Ütemezett feladatok elhalasztása, amíg a számítógép akkumulátorról üzemel	Ha ez a négyzet be van jelölve, az energiatakarékos mód akkor lesz engedélyezve, ha a számítógép akkumulátorról működik. A Kaspersky Endpoint Security elhalasztja az ütemezett feladatokat. Szükség esetén manuálisan indíthatja el a vizsgálati és frissítési feladatokat. Ha az energiatakarékos mód be van kapcsolva, a számítógép pedig akkumulátorról működik, az alábbi feladatok akkor sem futnak, ha be vannak ütemezve: • *Teljes vizsgálat* • *Kritikus területek vizsgálata* • *Egyéni vizsgálat* • *Alkalmazás integritás-ellenőrzése* • *IOC vizsgálat* • *Adatbázisok és alkalmazásmodulok frissítése* (csak javítások) Az alkalmazás csak akkor hagyja ki az ütemezett adatbázis-frissítéseket, ha a laptop akkumulátorról működik, és az akkumulátor töltöttségi szintje 30% alatt van. Minden más esetben a Kaspersky Endpoint Security az ütemterv szerint frissíti az adatbázisokat, függetlenül attól, hogy a laptop csatlakoztatva van-e a hálózathoz vagy akkumulátorról működik, illetve hogy az alkalmazás energiatakarékos módban van-e.
Erőforrások adása más alkalmazásoknak	A számítógép erőforrásainak Kaspersky Endpoint Security általi felhasználása a számítógép átvizsgálása során növelheti a processzor és a merevlemez alrendszereinek terhelését. Ez lassíthatja más alkalmazások működését. A teljesítmény optimalizálása céljából a Kaspersky Endpoint Security biztosítja *az erőforrások más alkalmazásoknak történő átadásának módját*. Ebben az üzemmódban az operációs rendszer csökkentheti a Kaspersky Endpoint Security vizsgálati feladatszálainak prioritását, ha a processzorterhelés magas. Ez lehetővé teszi az operációs rendszer erőforrásainak más alkalmazások számára történő újraelosztását. Így a vizsgálati feladatok kevesebb processzoridőt kapnak. Ennek eredményeképpen a Kaspersky Endpoint Security számára tovább tart a számítógép vizsgálata. Az alkalmazás alapértelmezés szerint úgy van beállítva, hogy az erőforrásokat átadja más alkalmazásoknak.
A CPU-használat korlátozása vizsgálati feladatoknál	A Kaspersky Endpoint Security teljesítményének optimalizálása érdekében korlátozhatja a CPU-használatot a *Kártevő vizsgálata* feladatnál. Ha a jelölőnégyzet be van jelölve, a *Kártevő vizsgálata* feladat által az összes processzormagra jutó átlagos terhelés megközelíti a megadott értéket. Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.
Memóriakép írásának engedélyezése	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security összeomláskor kiíratási fájlt ír. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem ír kiíratási fájlt. Az alkalmazás a számítógép merevlemezén található kiíratási fájlokat is törli.
Kiíratási és nyomkövetési fájlok védelmének engedélyezése	Ha a jelölőnégyzet be van jelölve, akkor a kiíratási fájlokhoz a rendszerszintű és helyi rendszergazdák, valamint a kiíratási és követési fájlok írását engedélyező felhasználó férhet hozzá. A nyomkövető fájlokhoz csak a rendszerszintű és helyi rendszergazdák férnek hozzá. Ha a jelölőnégyzet nincs bejelölve, bármely felhasználó hozzáférhet a kiíratási és nyomkövetési fájlokhoz.
A számítógép állapota a beállítások alkalmazásakor *(csak a Kaspersky Security Center konzolon érhető el)*	A Kaspersky Endpoint Security alkalmazást telepített ügyfélszámítógépek állapotának megjelenítésének beállításai a Webfelügyelőben, ha hiba lép fel a rendszabály alkalmazása vagy feladat végrehajtása közben. A következő állapotok állnak rendelkezésre: *OK*, *Figyelmeztetés* és *Kritikus*.

Paraméter	Leírás
Frissítések telepítése a számítógép újraindítása nélkül	Az alkalmazás frissítése a számítógép újraindítása nélkül lehetővé teszi a kiszolgálók zavartalan működésének biztosítását. Az alkalmazást a 11.10.0 verzióval kezdődően újraindítás nélkül frissítheti. Az alkalmazás korábbi verziójának frissítéséhez újra kell indítania a számítógépet. A 11.11.0-s verziótól kezdve a következő műveleteket hajthatja végre a számítógép újraindítása nélkül: • javítások telepítése • az alkalmazásösszetevők készletének módosítása • a Kaspersky Endpoint Security telepítése a Kaspersky Security for Windows Server termékre A paraméter alapértelmezett értéke az operációs rendszer típusától függően változik. Ha az alkalmazás munkaállomásra van telepítve, az alkalmazás újraindítás nélküli frissítése le van tiltva. Ha az alkalmazás kiszolgálóra van telepítve, az alkalmazás újraindítás nélküli frissítése engedélyezve van.
Kompatibilitás távfelügyeleti szoftverekkel *(csak a Kaspersky Security Center konzolon érhető el)*	Ha a Kaspersky Endpoint Security távfelügyeleti eszközökkel való használata problémákat okoz, engedélyezheti a kompatibilitási módot. A problémák a távfelügyeleti eszközök és az alkalmazás Secure Desktop funkciójával való inkompatibilitásból fakadhatnak. A funkciónak az a célja, hogy megerősítse azokat a műveleteket, amelyek potenciálisan csökkenthetik a számítógép biztonsági szintjét. Ez a funkció lehetővé teszi, hogy az alkalmazás egy olyan megerősítő párbeszédpanelt jelenítsen meg, amely elkülönül a többi folyamattól. Ez a funkció megemelt jogosultsági szintet használ a kérés teljesítéséhez. Ily módon csak a felhasználó tudja megerősíteni a műveletet, a rosszindulatú program nem. Ha ez az opció ki van választva, a távfelügyeleti eszközökkel való kompatibilitási mód engedélyezve van. Az alkalmazás egy megerősítő párbeszédpanelt jelenít meg e funkció nélkül. Ez csökkentheti a számítógép biztonsági szintjét. Nem javasoljuk a kompatibilitási mód engedélyezését, ha a Kaspersky Endpoint Security távfelügyeleti eszközökkel való használata nem okoz problémát. Ha az opció nincs bejelölve, a távfelügyeleti eszközökkel való kompatibilitási mód le van tiltva. Alapértelmezés szerint a jelölőnégyzet nincs bejelölve. Példa: ha a böngészőt RemoteApp módban használja, előfordulhat, hogy a Kaspersky Endpoint Security nem jelenít meg megerősítési ablakot, amikor egy nem megbízható tanúsítvánnyal rendelkező webhelyet keres fel, mert a RemoteApp nem támogatja az alkalmazás biztonsági asztal funkcióját. Ez azt okozhatja, hogy a böngésző nem reagál. Ahhoz, hogy a böngésző megfelelően működjön RemoteApp módban, engedélyeznie kell a kompatibilitási módot. Akkor is megpróbálhatja engedélyezni a kompatibilitási módot, ha más, harmadik féltől származó szoftverek használata során problémákat tapasztal a biztonsági asztal funkcióval kapcsolatban.

Jelentések és tároló

Jelentések

Az egyes Kaspersky Endpoint Security összetevők működésére, az egyes vizsgálati feladatok, frissítési feladatok, integritási ellenőrzési feladatok teljesítményére, valamint az alkalmazás általános működésére vonatkozó információk jelentésekbe kerülnek.

A jelentések a `C:\ProgramData\Kaspersky Lab\KES.14.1\Report` mappában vannak tárolva.

Biztonsági mentés

A *Biztonsági mentés* tárolja az olyan fájlok másolatait, amelyek törölve vagy módosítva lettek a vírusmentesítés során. A *biztonsági másolat* egy másolt fájl, mely a fájl vírusmentesítése vagy törlése előtt lett létrehozva. A fájlok biztonsági másolatai különleges formátumban vannak tárolva, és nem jelentenek fenyegetést.

A fájlok biztonsági másolatai a `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` mappában vannak tárolva.

A Rendszergazda csoportban lévő felhasználók számára elérhető ez a mappa. A felhasználó, akinek a fiókjáról telepítve lett a Kaspersky Endpoint Security, korlátozott hozzáféréssel rendelkezik ehhez a mappához.

A Kaspersky Endpoint Security nem biztosít lehetőséget a fájlok biztonsági másolatához való felhasználói hozzáférések beállítására.

Karantén

A *karantén* egy speciális helyi tároló a számítógépen. A felhasználó karanténba helyezheti azokat a fájlokat, amelyeket veszélyesnek ítél meg a számítógépen. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha az integrálva van a Kaspersky Detection and Response megoldásokkal. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a Biztonsági mentésbe helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért olvassa el a Kaspersky Sandbox súgót, a Kaspersky Endpoint Detection and Response Optimum súgót, a Kaspersky Endpoint Detection and Response Expert súgót, a Kaspersky Anti Targeted Attack Platform súgót és a Kaspersky Endpoint Detection and Response Expert (on-premises) súgót.

A karantén csak a Web Console segítségével konfigurálható. A Web Console segítségével karanténba helyezett objektumokat is kezelhet (visszaállítás, törlés, hozzáadás stb.). Az objektumokat a számítógépen helyileg visszaállíthatja a parancssor használatával.

A Kaspersky Endpoint Security a rendszerfiókot (SYSTEM) használja a fájlok karanténba helyezéséhez.

A jelentések és tároló beállításai

Paraméter	Leírás
Delete reports after (days)	Ha a jelölőnégyzet be van jelölve, a maximális jelentéstárolási időtartamot a meghatározott időintervallum korlátozza. A jelentések maximális tárolási időtartama alapértelmezett esetben 30 nap. Ezt követően a Kaspersky Endpoint Security automatikusan törli a jelentésfájlban lévő legrégebbi bejegyzéseket.
Limit the size of report file to (MB)	Ha a jelölőnégyzet be van jelölve, a maximális jelentésfájlméretet a megadott érték korlátozza. Alapértelmezés szerint a maximális fájlméret 1024 MB. A jelentésfájlok maximális méretének túllépését elkerülendő a Kaspersky Endpoint Security automatikusan törli a jelentésfájlok legrégebbi bejegyzéseit a maximális méret elérésekor.
Delete objects after (days)	Ha a jelölőnégyzet be van jelölve, a maximális fájltárolási időtartamot a meghatározott időintervallum korlátozza. A fájlok maximális tárolási időtartama alapértelmezett esetben 30 nap. A maximális tárolási időtartam lejárata után a Kaspersky Endpoint Security törli a legrégebbi fájlokat a Biztonsági mentésből.
Limit the size of Backup to (MB)	Ha a jelölőnégyzet be van jelölve, a maximális tárhelyet a meghatározott érték korlátozza. Alapértelmezés szerint a maximális méret 1024 MB. A tárhely maximális méretének túllépését elkerülve a Kaspersky Endpoint Security automatikusan törli a tárhely legrégebbi fájljait a maximális méret elérésekor.
Limit the size of Quarantine	Ha a jelölőnégyzet be van jelölve, a karantén maximális tárhelyét a meghatározott érték korlátozza. Alapértelmezés szerint a maximális méret 1024 MB. Amikor a karantén eléri a maximális méretet, a Kaspersky Endpoint Security elküldi a *Nincs elegendő hely a karantén tárhelyen* eseményt a Kaspersky Security Centernek, és közzéteszi az eseményt a Windows Eseménynaplóban. Eközben az alkalmazás leállítja az új objektumok karanténba helyezését. A karantént kézzel kell kiürítenie.
Notify when the Quarantine storage reaches (%)	A karantén küszöbértéke. Például beállíthatja a karantén küszöbértékét 50%-ra. Amikor a karantén eléri a küszöbértéket, a Kaspersky Endpoint Security elküldi a megfelelő eseményt a Kaspersky Security Centernek, és közzéteszi az eseményt a Windows Eseménynaplóban. Eközben az alkalmazás folytatja az új objektumok karanténba helyezését.

Paraméter	Leírás
Adatátvitel az adminisztrációs kiszolgálóra *(csak a Kaspersky Security Centeren érhető el)*	Az események kategóriája az ügyfélszámítógépen, amik információit el kell küldeni az Adminisztrációs kiszolgálóra. A lemezterület optimalizálása érdekében a felügyeleti kiszolgálón letilthatja egyes adatok átvitelét. Az alkalmazás a következő kategóriákba tartozó eseményeket küldi: • **About Quarantine files**. A karanténba helyezett fájlok listáját a Kaspersky Security Center konzolban tekintheti meg a **Advanced** → **Repositories** → **Quarantine** mappában. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha az integrálva van a Kaspersky Detection and Response megoldásokkal. • **About files in Backup**. A Biztonsági másolat mappában található fájlok listáját a Kaspersky Security Center konzolban tekintheti meg a **Advanced** → **Repositories** → **Backup** mappában. • **About unprocessed files**. A feldolgozatlan fájlok listáját a Kaspersky Security Center konzolban tekintheti meg a **Advanced** → **Repositories** → **Active threats** mappában. • **About installed devices**. A csatlakoztatott eszközök listáját a Kaspersky Security Center konzolban tekintheti meg a **Advanced** → **Repositories** → **Hardware** mappájában. Az eszközök listája a számítógép tulajdonságaiban és a Kaspersky Endpoint Security for Windows házirendjében is elérhető (**Eszközfelügyelő** szakasz). • **About started applications**. A futtatható fájlok listáját a Kaspersky Security Center konzolon tekintheti meg a **Advanced** → **Application management** → **Executable files** mappában. A végrehajtható fájlok listája a Számítógép tulajdonságaiban is elérhető. • **About file encryption errors**. A fájltitkosítási hibák listáját a Kaspersky Security Center konzolban tekintheti meg a **Advanced** → **Data encryption and protection** → **Encryption events** mappában. A hibalista a számítógép tulajdonságaiban is elérhető. • **Report on Adaptive Anomaly Control rules state**. A jelentést a Kaspersky Security Center konzolban tekintheti meg a **Administration Server** csomópontban a **Reports** lapon. Ez a jelentés a Kaspersky Endpoint Security for Windows házirend tulajdonságaiban is elérhető (**Adaptív Anomáliafelügyelő** szakasz). • **Report on triggered Adaptive Anomaly Control rules**. A jelentést a Kaspersky Security Center konzolban tekintheti meg a **Administration Server** csomópontban a **Reports** lapon. Ez a jelentés a Kaspersky Endpoint Security for Windows házirend tulajdonságaiban is elérhető (**Adaptív Anomáliafelügyelő** szakasz). • **About a threat development chain**. Az észlelési részleteket a Kaspersky Security Center Web Console-on tekintheti meg a **Monitoring** → **Alerts** szakaszban. A fenyegetés-fejlődési láncról szóló információkat a Kaspersky Endpoint Detection and Response megoldások használják.

Hálózati beállítások

Megadhatja az internethez való csatlakozáshoz és az antivírus adatbázisok frissítéséhez használt proxykiszolgálót, kiválaszthatja a hálózati port figyelő módját, beállíthat titkosítottkapcsolat-vizsgálatokat.

Hálózati opciók

Paraméter	Leírás
Forgalom csökkentése díjköteles kapcsolatoknál	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás korlátozott internetkapcsolat esetén korlátozza a saját hálózati forgalmát. A Kaspersky Endpoint Security a nagy sebességű mobil internetkapcsolatokat korlátozott kapcsolatként, a Wi-Fi kapcsolatokat korlátlan kapcsolatként azonosítja. A Költségtudatos hálózati figyelés a Windows 8 vagy újabb rendszert futtató számítógépeken működik.
Szkript beillesztése a webforgalomba a weboldalakkal való interakcióhoz	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security beilleszt egy a weboldallal való interakciót szolgáló parancsfájlt a webes forgalomba. Ez a parancsfájl biztosítja, hogy a Webfelügyelő összetevő megfelelően működjön. A parancsfájl lehetővé teszi a Webfelügyelő események regisztrációját. A parancsfájl nélkül nem engedélyezheti a felhasználó internetes tevékenységének figyelését. A Kaspersky szakértői azt javasolják, hogy a Webfigyelő helyes működésének biztosítása érdekében injektálja be a weboldal-interakciós parancsfájlt a forgalomba.
Proxykiszolgáló beállításai	A felhasználók vagy ügyfélszámítógépek internet-hozzáféréshez használt proxykiszolgálójának beállításai. A Kaspersky Endpoint Security ezeket a beállításokat több védelmi összetevőnél, valamint az alkalmazás adatbázisainak és moduljainak frissítésekor is használja. A proxykiszolgáló automatikus beállításához a Kaspersky Endpoint Security a WPAD protokollt használja (Web Proxy Auto-Discovery). Ha a proxykiszolgáló IP-címe a protokoll segítségével nem állapítható meg, az alkalmazás a Microsoft Internet Explorer böngészőbeállításaiban megadott proxykiszolgáló címét használja fel.
Proxykiszolgáló kihagyása helyi címek esetén	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem használ proxykiszolgálót megosztott mappából történő frissítéshez.

Paraméter	Leírás
Proxykiszolgáló-hitelesítési beállítások	A proxykiszolgálón az alkalmazás internet-hozzáféréshez való hitelesítéséhez meg kell adnia a felhasználó hitelesítő adatait. A Kaspersky Endpoint Security támogatja az automatikus hitelesítést a proxykiszolgálón. Ha az automatikus hitelesítés sikertelen, az alkalmazás kéri a hitelesítő adatok megadását. **Ne használjon hitelesítést**. **NTLM hitelesítés**. NTLM hitelesítés az aktuális felhasználói fiókkal (alapértelmezett). **NTLM hitelesítés felhasználónévvel és jelszóval**. NTLM hitelesítés manuálisan megadott hitelesítő adatokkal. **Felhasználónév és jelszó**. Hitelesítés manuálisan megadott hitelesítő adatokkal. **Automatikus hitelesítés**. **Kerberos hitelesítés**. Kerberos hitelesítés az aktuális felhasználói fiókkal (alapértelmezett). Ahhoz, hogy a Kerberos-hitelesítés megfelelően működjön, ha a proxykiszolgáló címéhez CNAME-bejegyzéseket használ, minden egyes CNAME-bejegyzéshez regisztrálnia kell egy egyszerű szolgáltatásnevet (SPN). **Kerberos hitelesítés felhasználónévvel és jelszóval**. Kerberos hitelesítés manuálisan megadott hitelesítő adatokkal. Ha a Kerberos hitelesítés van kiválasztva, a Kaspersky Endpoint Security a proxykiszolgáló beállításaitól függően a Kerberos vagy az NTLM protokollt használva végezheti el a hitelesítést.
Figyelt portok	**Minden hálózati port figyelése**. Ebben a hálózati portmegfigyelési módban a védelmi összetevők (Fájl védelem, Web védelem és Levelezés védelem) a számítógép minden nyitott hálózati portján továbbított adatfolyamot figyelnek. **Csak a kijelölt hálózati portok figyelése**. Ebben a hálózati portfigyelési módban a védelem összetevői figyelemmel kísérik a számítógép kiválasztott portjait és a kiválasztott alkalmazások hálózati tevékenységét. Az e-mailekhez és a hálózati forgalomhoz általában használt hálózati portok listája, amik a Kaspersky szakértők javaslatai alapján lettek megadva. **A Kaspersky által javasolt alkalmazások összes portjának figyelése**. Olyan alkalmazások előre meghatározott listáját használja, amelyek hálózati portjait a Kaspersky Endpoint Security figyeli. Például ebben a listában szerepel a Google Chrome, az Adobe Reader, a Java és más alkalmazások. **A megadott alkalmazások figyelése minden porton**. Olyan alkalmazások listáját használja, amelyek hálózati portjait a Kaspersky Endpoint Security figyeli.
Titkosított kapcsolatok vizsgálata	A Kaspersky Endpoint Security a következő protokollokon keresztül továbbított titkosított hálózati forgalmat vizsgálja: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. A Kaspersky Endpoint Security az alábbi vizsgálati módokat támogatja a titkosított kapcsolatok tekintetében: • **Ne vizsgálja a titkosított kapcsolatokat**. A Kaspersky Endpoint Security nem fog hozzáférni az olyan webhelyek tartalmához, amelyek címének a kezdete `https://`. • **Titkosított kapcsolatok vizsgálata a védelmi összetevők kérésére**. A Kaspersky Endpoint Security csak akkor vizsgálja a titkosított forgalmat, ha a Web védelem, a Levelezés védelem vagy a Webfelügyelő összetevő ezt kéri. • **Mindig vizsgálja a titkosított kapcsolatokat**. A Kaspersky Endpoint Security akkor is vizsgálni fogja a titkosított hálózati forgalmat, ha a védelem összetevői nem működnek. A Kaspersky Endpoint Security nem vizsgálja azokat a titkosított kapcsolatokat, amelyeket olyan megbízható alkalmazások hoztak létre, amelyeknél a forgalomvizsgálat le van tiltva. A Kaspersky Endpoint Security nem vizsgálja a titkosított kapcsolatokat a megbízható webhelyek előre meghatározott listájáról. A megbízható webhelyek előre meghatározott listáját a Kaspersky szakértői hozták létre. Ez a lista az alkalmazás vírusadatbázisaival frissül. A megbízható webhelyek előre meghatározott listáját csak a Kaspersky Endpoint Security felületen tekintheti meg. Nem tudja megtekinteni a listát a Kaspersky Security Center konzolon.

Paraméter	Leírás
Megbízható főtanúsítványok	A megbízható főtanúsítványok listája. A Kaspersky Endpoint Security lehetővé teszi, hogy megbízható főtanúsítványokat telepítsen a felhasználói számítógépekre, ha például új tanúsítványközpontot kell telepítenie. Az alkalmazás lehetővé teszi, hogy tanúsítványt adjon hozzá egy speciális Kaspersky Endpoint Security tanúsítványtárolóhoz. Ebben az esetben a tanúsítvány csak a Kaspersky Endpoint Security alkalmazás esetében tekinthető megbízhatónak. Más szóval a felhasználó az új tanúsítvánnyal a böngészőben hozzáférhet egy webhelyhez. Ha egy másik alkalmazás megpróbál hozzáférni a webhelyhez, akkor tanúsítványprobléma miatt kapcsolódási hiba jelentkezhet. A rendszer tanúsítványtárolójához való hozzáadáshoz használhatja az Active Directory csoportházirendjeit.
Nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása	• **Engedélyezés**. A nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása esetén a Kaspersky Endpoint Security engedélyezi a hálózati kapcsolatot. A nem megbízható tanúsítvánnyal rendelkező tartomány böngészővel történő megnyitása esetén a Kaspersky Endpoint Security megjelenít egy HTML-oldalt, ami egy figyelmeztetést mutat, valamint az okot, amiért nem javasolt a tartomány meglátogatása. A felhasználó rákattinthat a hivatkozásra a HTML figyelmeztető oldalon, hogy hozzáférést kapjon a kért webes erőforráshoz. Ha egy harmadik féltől származó alkalmazás vagy szolgáltatás kapcsolatot létesít egy nem megbízható tanúsítványú tartománnyal, a Kaspersky Endpoint Security saját tanúsítványt hoz létre a forgalom vizsgálatához. Az új tanúsítvány *Nem megbízható* állapotot kap. Erre azért van szükség, hogy figyelmeztesse a harmadik féltől származó alkalmazást a nem megbízható kapcsolatra, mert a HTML-oldal ebben az esetben nem jeleníthető meg, és a kapcsolat létrejöhet háttérmódban. • **Blokkolás**. A nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása esetén a Kaspersky Endpoint Security blokkolja a hálózati kapcsolatot. A nem megbízható tanúsítvánnyal rendelkező tartomány böngészővel történő megnyitása esetén a Kaspersky Endpoint Security megjelenít egy HTML-oldalt, ami mutatja az okot, hogy miért van blokkolva a tartomány.
Titkosított kapcsolatok vizsgálati hibájával rendelkező tartomány meglátogatása	• **Blokkolás**. Ha titkosított kapcsolat vizsgálatakor hiba történik, a Kaspersky Endpoint Security blokkolja a hálózati kapcsolatot. • **Engedélyezés és tartomány hozzáadása a kizárásokhoz**. Ha titkosított kapcsolat vizsgálatakor hiba történik, a Kaspersky Endpoint Security hozzáadja a hibát okozó tartományt a vizsgálati hibákat mutató tartományok listájához, és nem figyeli a titkosított hálózati forgalmat, amikor ezt a tartományt meglátogatják. Azoknak a tartományoknak a listáját, amelyeknél a titkosított kapcsolatok vizsgálata során hiba jelentkezett, csak az alkalmazás helyi felületén lehet megtekinteni. A lista tartalmának törléséhez ki kell választania a **Blokkolás** lehetőséget. A Kaspersky Endpoint Security eseményt is generál a titkosított kapcsolat vizsgálati hibájához.
SSL 2.0 kapcsolatok blokkolása	Ha a jelölőnégyzet be van jelölve, akkor az alkalmazás figyeli és blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Az alkalmazás azonban nem figyeli a hálózati forgalmat ezen a protokollon keresztül.
SSL 3.0 kapcsolatok blokkolása	Ha a jelölőnégyzet be van jelölve, akkor az alkalmazás blokkolja az SSL 3.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem blokkolja az SSL 3.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Az alkalmazás ezen a protokollon keresztül figyeli a hálózati forgalmat. Az alkalmazás minden összetevője korlátozások nélkül működik.
TLS 1.0 kapcsolatok blokkolása	Ha a jelölőnégyzet be van jelölve, akkor az alkalmazás blokkolja az TLS 1.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem blokkolja az TLS 1.0 protokollon keresztül létrehozott hálózati kapcsolatokat. Az alkalmazás ezen a protokollon keresztül figyeli a hálózati forgalmat. Az alkalmazás minden összetevője korlátozások nélkül működik.
Titkosított kapcsolat visszafejtése EV-tanúsítványt használó webhelyeken	Az EV-tanúsítványok (Extended Validation Certificate) hitelesítik a weboldalakat és növelik a kapcsolat biztonságát. A Böngészők a zár ikont használják a címsávjukban, hogy jelezzék, hogy a weboldal EV-tanúsítvánnyal rendelkezik. A böngészők részben vagy egészben zöldre is színezhetik a címsávot. Ha ez a jelölőnégyzet be van jelölve, az alkalmazás visszafejti és figyeli az EV-tanúsítványt használó webhelyekkel történő titkosított kapcsolatokat. Ha a jelölőnégyzet nincs bejelölve, az alkalmazás nem fér hozzá a HTTPS-forgalom tartalmához. Ezen okokból az alkalmazás csak a webcím alapján figyeli meg a HTTPS-forgalmat, például: `https://bing.com`. Ha először nyit meg egy EV-tanúsítvánnyal rendelkező weboldalt, a titkosított kapcsolat attól függetlenül vissza lesz fejtve, hogy Ön kijelölte-e a jelölőnégyzetet.

Paraméter	Leírás
Megbízható címek konfigurálása	Olyan webcímeknek a listáját használja, amelyeknél a Kaspersky Endpoint Security nem vizsgálja a hálózati kapcsolatokat. Ebben az esetben a Kaspersky Endpoint Security nem vizsgálja a megbízható webcímek HTTPS-forgalmát, amikor a Web védelem, a Levelezés védelem és a Webfelügyelő összetevők végzik a munkájukat. Megadhat egy tartománynevet vagy egy IP-címet. A Kaspersky Endpoint Security támogatja a `*` karaktert maszk megadásához a tartománynévben. A Kaspersky Endpoint Security nem támogatja a `*` szimbólumot IP-címek esetén. Az IP-címek tartományát alhálózati maszk segítségével választhatja ki (például 198.51.100.0/24). Példák: • `domain.com` – a rekord a következő címeket tartalmazza: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. A rekord nem tartalmaz altartományt (pl. `subdomain.domain.com`). • `subdomain.domain.com` – a rekord a következő címeket tartalmazza: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt. • `*.domain.com` – a rekord a következő címeket tartalmazza: `https://movies.domain.com`, `https://images.domain.com/page123`. A rekord nem tartalmaz `domain.com` tartományt.
Megbízható alkalmazások konfigurálása	Azoknak az alkalmazásoknak a listája, amelyek tevékenységét a Kaspersky Endpoint Security nem figyeli a működése során. Kiválaszthatja azon alkalmazástevékenységek típusait, amiket a Kaspersky Endpoint Security nem fog megfigyelni (például: ne vizsgáljon hálózati forgalmat). A Kaspersky Endpoint Security támogatja a környezeti változókat, és a `*` és `?` karaktereket egy maszk megadásakor.
A saját tanúsítványtárolóval rendelkező alkalmazások titkosított kapcsolatainak vizsgálatához használja *(csak a Kaspersky Endpoint Security felületen érhető el)*	Ha ez a jelölőnégyzet be van jelölve, az alkalmazás megvizsgálja a titkosított forgalmat a Mozilla Firefox böngészőben és a Thunderbird levelezőprogramban. Néhány webhely HTTPS-protokollon keresztüli elérése blokkolva lehet. A Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmának vizsgálatához engedélyeznie kell a Titkosított kapcsolatok vizsgálatát. Ha a Titkosított kapcsolatok vizsgálata le van tiltva, az alkalmazás nem vizsgálja a Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmát. Az alkalmazás a Kaspersky főtanúsítványát használja a titkosított forgalom visszafejtésére és elemzésére. Kiválaszthatja azt a tanúsítványtárolót, amely a Kaspersky főtanúsítványt tartalmazza. • **Windows tanúsítványtároló (ajánlott)**. A Kaspersky főtanúsítvány bekerül ebbe a tárolóba a Kaspersky Endpoint Security telepítése során. • **Saját tanúsítványtároló**. A Mozilla Firefox és a Thunderbird saját tanúsítványtárolóját használja. Ha a Mozilla tanúsítványtároló van kiválasztva, manuálisan kell hozzáadnia a Kaspersky főtanúsítványt ehhez a tárolóhoz a böngésző beállításaiban.

Felület

Megadhatja az alkalmazás felületének beállításait.

Felület beállítások

Paraméter	Leírás
Interakció a felhasználóval *(csak a Kaspersky Security Center konzolon érhető el)*	**Egyszerűsített felület megjelenítése**. Az ügyfélszámítógépen a fő alkalmazásablak nem érhető el, csak a Windows értesítési sávon lévő ikon érhető el. Az ikon helyi menüjében a felhasználó korlátozott számú műveletet hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security csak azokat az értesítéseket jeleníti meg az alkalmazás ikonja felett, amelyek felhasználói beavatkozást igényelnek. **Felhasználói felület megjelenítése**. Ügyfélszámítógépeken a Kaspersky Endpoint Security fő ablaka és a Windows értesítési területén lévő ikon érhető el. Az ikon helyi menüjében a felhasználó műveleteket hajthat végre a Kaspersky Endpoint Security alkalmazással. A Kaspersky Endpoint Security értesítéseket is megjelenít az alkalmazásikon felett. **Az Alkalmazástevékenység-figyelő szakaszának elrejtése**. Az ügyfélszámítógépen a Kaspersky Endpoint Security főablakában az **Alkalmazástevékenység-figyelő** gombja nem érhető el. Az *Alkalmazástevékenység-figyelő* egy olyan eszköz, amellyel valós időben tekinthetők meg a felhasználó számítógépén futó alkalmazások tevékenységével kapcsolatos információk. **Ne jelenítse meg a felhasználói felületet**. Az ügyfélszámítógépen nincs jelen a Kaspersky Endpoint Security működésének. A Windows értesítési sávon lévő ikon és az értesítések nem érhetők el.

Paraméter	Leírás
Értesítések konfigurálása	Egy összetevő, feladat vagy a teljes alkalmazás működése során lehetségesen bekövetkező különböző fontossági szintű eseményekre vonatkozó értesítések beállításait tartalmazó táblázat. A Kaspersky Endpoint Security ezekről az eseményekről a képernyőn jelenít meg értesítéseket, elküldi e-mailben, illetve naplózza őket.
E-mail alapú értesítések konfigurálása	Az SMTP szerver beállításai az alkalmazás működése során regisztrált események értesítéseinek biztosításához. A Kaspersky Endpoint Security alapértelmezés szerint a Kaspersky Security Center e-mailes értesítési beállításait használja. Az e-mailes értesítések beállításaival kapcsolatos további részletekért lásd a Kaspersky Security Center súgóját. Ha egyéni e-mailes értesítést kell konfigurálnia, a következő beállításokat módosíthatja: • **Küldő címe**. A feladó e-mail-címe. Nem létező cím használata nem ajánlott. • **SMTP-kiszolgáló**. A vállalat e-mail kiszolgálóinak egy vagy több címe (például `mail.company.com`). Megadhat egy IP-címet (IPv4 vagy IPv6). A felhasználó hitelesítéséhez az SMTP-kiszolgálón adja meg a feladó hitelesítő adatait a megfelelő mezőkben. Az e-mailes értesítések teszteléséhez tesztüzenetet küldhet. • **Címzett címe**. Azon címzettek e-mail-címei, akiknek az alkalmazás értesítést küld. • **Küldési mód**. Az e-mail értesítések küldési módja. A Kaspersky Endpoint Security azonnal tud üzenetet küldeni egy esemény bekövetkeztekor; vagy követhet egy előre konfigurált ütemezést.
Az alkalmazás állapotának megjelenítése az értesítési területen	Alkalmazásesemények kategóriája, amik miatt a Kaspersky Endpoint Security ikon megváltozott a Microsoft Windows feladatsáv értesítési területén (vagy), előbukkanó értesítést eredményezve.
Helyi kártevőirtói adatbázis állapotáról szóló értesítések	Az alkalmazás által használt elavult antivírus adatbázisok értesítéseinek beállításai.
Jelszóvédelem	Ha a kapcsológomb be van kapcsolva, a Kaspersky Endpoint Security jelszót kér a felhasználótól, ha az olyan műveletet próbál meg végrehajtani, ami a Jelszóvédelem hatókörébe tartozik. A Jelszóvédelem hatókörébe tiltott műveletek (például a védelem összetevőinek letiltása) és a felhasználói fiókok (amikre a Jelszóvédelem vonatkozik) tartoznak. A Jelszóvédelem engedélyezése után a Kaspersky Endpoint Security egy jelszó megadását kéri a KLAdmin fiókhoz.
Felhasználói támogatás / Hivatkozások webes erőforrásokra *(csak a Kaspersky Security Center konzolon érhető el)*	Hivatkozások listája a webes erőforrásokról, amelyek a Kaspersky Endpoint Security terméktámogatására vonatkozó információkat tartalmaznak. Hozzáadott hivatkozások jelennek meg a Kaspersky Endpoint Security helyi felületének **Támogatás** ablakában az alapértelmezett hivatkozások helyett.
Felhasználói támogatás / Leírás *(csak a Kaspersky Security Center konzolon érhető el)*	Az üzenet, ami a Kaspersky Endpoint Security **Támogatás** ablakában jelenik meg.

Beállítások kezelése

A Kaspersky Endpoint Security jelenlegi beállításait elmentheti egy fájlba, és használhatja azokat az alkalmazás gyors konfigurálásához egy másik számítógépen. Akkor is használhat egy konfigurációs fájlt, ha az alkalmazást a Kaspersky Security Centeren keresztül telepíti egy telepítőcsomaggal. Az alapértelmezett beállításokat bármikor visszaállíthatja.

Az alkalmazáskonfigurációs kezelési beállítások csak a Kaspersky Endpoint Security felületen érhetők el.

Alkalmazáskonfiguráció kezelési beállítások

Beállítások	Leírás
Importálás	Az alkalmazásbeállítások kicsomagolása CFG formátumú fájlból, majd azok alkalmazása.
Exportálás	A jelenlegi alkalmazásbeállítások mentése CFG formátumú fájlba.
Visszaállítás	Az Kaspersky által ajánlott alkalmazás beállításokat bármikor visszaállíthatja. A beállítások visszaállítása után minden védelmi összetevőnél az **Ajánlott** biztonsági szint lesz beállítva.

Adatbázisok és alkalmazás-szoftvermodulok frissítése

A Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítése biztosítja a számítógép védelmének naprakész állapotát. Nap mint nap jelentős számú új vírus és más típusú rosszindulatú program jelenik meg világszerte. A fenyegetésekről és a semlegesítésük módjáról a Kaspersky Endpoint Security adatbázisai tartalmaznak információkat. A fenyegetések gyors észlelése érdekében javasoljuk, hogy rendszeresen frissítse az adatbázisokat és az alkalmazásmodulokat.

Elképzelhető, hogy a frissítési funkciók (beleértve a vírusirtó aláírások és a kódbázis frissítéseit) nem lesznek elérhetők a szoftverben az Egyesült Államok területén.

A rendszeres frissítéshez működő licenc szükséges. Ha nincs aktuális licence, csak egyetlen alkalommal végezhet frissítést.

A frissítési csomagoknak a Kaspersky frissítési kiszolgálóiról való sikeres letöltéséhez a számítógépnek csatlakoznia kell az internethez. Alapértelmezés szerint az alkalmazás automatikusan észleli az internetkapcsolat beállításait. Ha proxykiszolgálót használ, konfigurálnia kell a proxykiszolgáló beállításait.

A frissítések HTTPS protokollon keresztül töltődnek le. HTTP protokollon is le lehet tölteni őket, ha nem lehet HTTPS protokollon frissítéseket letölteni.

Frissítés végrehajtásakor az alkalmazás letölti és telepíti az alábbi objektumokat a számítógépre:

- A Kaspersky Endpoint Security adatbázisai. A számítógép védelme olyan adatbázisokra épül, amelyek tartalmazzák a vírusok és egyéb fenyegetések aláírásait, valamint a semlegesítésükre vonatkozó információkat. A védelmi összetevők ezen információk segítségével keresik meg és semlegesítik a számítógépen található fertőzött fájlokat. Az adatbázisok folyamatosan kiegészülnek az új fenyegetések adataival és hatástalanításuk módszereivel. Emiatt javasoljuk, hogy rendszeresen frissítse az adatbázisokat.

  A Kaspersky Endpoint Security adatbázisai mellett frissülnek azok a hálózati illesztőprogramok is, amelyek segítségével az alkalmazás összetevői elfoghatják a hálózati forgalmat.

- Alkalmazásmodulok. A Kaspersky Endpoint Security adatbázisai mellett az alkalmazásmodulok is frissíthetők. Az alkalmazásmodulok frissítései kiküszöbölik a Kaspersky Endpoint Security sebezhetőségeit, új funkciókat adnak hozzá, illetve meglévő funkciókat bővítenek ki.

Frissítéskor az alkalmazás összehasonlítja a számítógépen található alkalmazásmodulokat és adatbázisokat a frissítési forráson található naprakész változatokkal. Ha az érvényes adatbázisok és alkalmazásmodulok eltérnek a naprakész verzióktól, a frissítés telepíti a hiányzó részeket a számítógépre.

Ha az adatbázisok elavultak, a frissítőcsomag nagy méretű lehet, és további internetforgalmat (több tucat MB) generálhat.

A Kaspersky Endpoint Security adatbázisok aktuális állapotával kapcsolatos információk az alkalmazás főablakában vagy az elemleírásban jelennek meg, amelyet akkor láthat, ha a kurzort az értesítési területen lévő alkalmazásikon fölé viszi.

A frissítés eredményeit és a frissítési feladat végrehajtása során történt eseményeket a Kaspersky Endpoint Security egy jelentésben naplózza.

Ha az alkalmazás Light Agent üzemmódban működik, az alkalmazás adatbázisainak és moduljainak frissítése különleges megfontolásokat igényel.

Alkalmazásmodul- és adatbázis-frissítési beállítások

Paraméter	Leírás
Adatbázis-frissítés ütemezése	**Automatikus**. Ebben a módban az alkalmazás a beállított gyakorisággal automatikusan ellenőrzi az új frissítési csomagok megjelenését a frissítési forráson. Vírusjárványok kirobbanásakor a frissítőcsomagok ellenőrzésének gyakorisága növekedhet, ezek elmúltával pedig újra lecsökkenhet. Miután a Kaspersky Endpoint Security új frissítési csomagot észlel, letölti és telepíti a számítógépen a frissítéseket. **Manually**. A frissítési feladatok ezen futásmódjában a frissítési feladatokat manuálisan lehet elindítani. **By schedule**. A frissítési feladatoknak ebben a futásmódjában a Kaspersky Endpoint Security a frissítési feladatot a megadott ütemtervnek megfelelően futtatja. Ha a frissítési feladatoknak ez a futásmódja van kiválasztva, akkor a Kaspersky Endpoint Security frissítési feladata kézileg is elindítható.
Run missed tasks	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott feladatot azonnal elindítja, amint lehetségessé válik. A feladat például akkor hagyható ki, ha a számítógép az ütemezett feladat indítási időpontjában ki volt kapcsolva. Amikor az alkalmazás lehetőséget kap a kihagyott feladatok végrehajtására, egy adott időintervallumon belül véletlenszerűen futtatja a feladatokat, hogy elossza a számítógép terhelését. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott feladatokat. Ehelyett a következő feladatot a jelenlegi ütemezésnek megfelelően futtatja.
Frissítésforrások	A *frissítésforrás* a Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítéseit tartalmazó erőforrás. A frissítési források közé a Kaspersky Security Center kiszolgálója, a Kaspersky frissítési kiszolgálói, valamint hálózati vagy helyi mappák tartoznak. Ha a Kaspersky frissítési kiszolgálói nem érhetők el, a Kaspersky Endpoint Security alternatív tartományokat használhat az adatbázisok és alkalmazásmodulok frissítéséhez. Részletes információkért tekintse meg a Terméktámogatási tudásbázist. A frissítésforrások alapértelmezett listáján a Kaspersky Security Center és a Kaspersky frissítéskiszolgálói szerepelnek. Felvehet más frissítésforrásokat is a listába. Frissítésforrásként megadhat HTTP-/FTP-kiszolgálókat és megosztott meghajtókat. A Kaspersky Endpoint Security csak akkor támogatja a frissítéseket HTTPS-kiszolgálókról, ha azok a Kaspersky saját frissítési kiszolgálói. Ha több forrás van kiválasztva frissítésforrásként, a Kaspersky Endpoint Security egymás után próbál kapcsolatot létesíteni azokkal a lista első elemétől kezdve, és úgy végzi el a frissítési feladatot, hogy az első elérhető forrásról letölti a frissítőcsomagot. Alapértelmezés szerint a Kaspersky Endpoint Security a Kaspersky Security Center kiszolgálóját használja első frissítési forrásként. Ez segít megőrizni az adatforgalmat a frissítés során. Ha a számítógépre nem vonatkozik házirend, az *Adatbázisok és alkalmazásmodulok frissítése* helyi feladat beállításaiban a Kaspersky-kiszolgálók kerülnek kiválasztásra első frissítési forrásként, mivel előfordulhat, hogy az alkalmazás nem fér hozzá a Kaspersky Security Center kiszolgálójához. Ha az alkalmazás Light Agent üzemmódban fut, az SVM egyik mappája lesz kiválasztva frissítésforrásként.
Adatbázis-frissítések futtatása mint	A Kaspersky Endpoint Security frissítési feladata alapértelmezés szerint ugyanannak a felhasználónak a nevében indul el, akinek a fiókjával bejelentkezett az operációs rendszerbe. A Kaspersky Endpoint Security azonban frissíthető olyan forrásból is, amelyhez a felhasználó a szükséges jogosultságok hiányában (például frissítési csomagot tartalmazó megosztott mappából), vagy egy olyan frissítésforrással, melyhez a proxykiszolgáló hitelesítése nincs konfigurálva, nem férhet hozzá. Az alkalmazás beállításaiban megadhat egy olyan felhasználót, aki rendelkezik ezekkel a jogosultságokkal, és a Kaspersky Endpoint Security frissítési feladatát elindíthatja ennek a felhasználói fióknak a nevében.

Paraméter	Leírás
Alkalmazásmodulok frissítéseinek letöltése	Alkalmazásmodulok frissítéseinek letöltése az alkalmazásadatbázis-frissítésekkel. Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security értesíti a felhasználót a rendelkezésre álló alkalmazásmodul-frissítésekről, és azokat is a frissítési csomagba helyezi a frissítési feladat futtatásakor. Az alkalmazásmodul-frissítések alkalmazásának módját az alábbi beállítások határozzák meg: • **Kritikus és jóváhagyott frissítések telepítése**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security automatikusan telepíti a létfontosságú frissítéseket, a többit pedig csak akkor, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről. • **Csak jóváhagyott frissítések telepítése**. Ha ennek a lehetőségnek a kiválasztása esetén alkalmazásmodul-frissítések válnak elérhetővé, a Kaspersky Endpoint Security csak akkor telepíti őket, ha a telepítés helyileg jóváhagyást kap az alkalmazás felületén vagy a Kaspersky Security Center részéről. Alapértelmezésben ez a lehetőség van kiválasztva. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem értesíti a felhasználót a rendelkezésre álló alkalmazásmodul-frissítésekről, és azokat nem helyezi a frissítési csomagba a frissítési feladat futtatásakor. Ha az alkalmazásmodul-frissítésekhez át kell tekinteni és el kell fogadni a Végfelhasználói licencszerződés feltételeit, akkor az alkalmazás csak ennek megtörténte után telepíti a frissítéseket. Alapértelmezésben a négyzet be van jelölve.
Frissítések másolása mappába	Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a frissítési csomagot a jelölőnégyzet alatt megadott mappába másolja. Ezt követően a helyi hálózaton lévő többi számítógép a frissítési csomagot a megosztott mappából megkaphatja. Ezzel csökken az internetes forgalom, mivel a frissítési csomag letöltésére csak egyszer kerül sor. A következő mappa van megadva alapértelmezés szerint: `C:\ProgramData\Kaspersky Lab\KES.14.1\Update distribution\`.
Frissítési proxykiszolgáló *(csak a Kaspersky Endpoint Security felületen érhető el)*	A kliensszámítógépek felhasználóinak internet-hozzáférésére vonatkozó proxykiszolgáló-beállítások az alkalmazásmodulok és adatbázisok frissítéséhez. A proxykiszolgáló automatikus beállításához a Kaspersky Endpoint Security a WPAD protokollt használja (Web Proxy Auto-Discovery Protocol). Ha a proxykiszolgáló IP-címe a protokoll segítségével nem állapítható meg, a Kaspersky Endpoint Security a Microsoft Internet Explorer böngészőbeállításaiban megadott proxykiszolgáló címét használja fel.
Proxykiszolgáló kihagyása helyi címek esetén *(csak a Kaspersky Endpoint Security felületen érhető el)*	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem használ proxykiszolgálót megosztott mappából történő frissítéshez.

2. melléklet Alkalmazások megbízható csoportjai

A Kaspersky Endpoint Security a számítógépen elindított összes alkalmazást megbízhatósági csoportokba sorolja. Az alkalmazások megbízhatósági csoportokba sorolása az operációs rendszerre jelentett fenyegetési szint alapján történik.

Az alábbi megbízhatósági csoportok léteznek:

- **Megbízható**. Ebbe a csoportba tartoznak azok az alkalmazások, amelyeknél az alábbi feltételek közül egy vagy több teljesül:
  - Az alkalmazásokat megbízható forgalmazók digitálisan aláírták.
  - Az alkalmazások szerepelnek a Kaspersky Security Network megbízható alkalmazásokról készült adatbázisában.
  - A felhasználó az alkalmazást a *Megbízható* csoportba helyezte.

  Az ilyen alkalmazások műveletei nincsenek tiltva.

- **Alacsony korlátozás**. Ebbe a csoportba tartoznak azok az alkalmazások, amelyeknél az alábbi feltételek teljesülnek:
  - Az alkalmazásokat nem írták alá digitálisan megbízható forgalmazók,
  - Az alkalmazások nem szerepelnek a Kaspersky Security Network megbízható alkalmazásokról készült adatbázisában,
  - A felhasználó az alkalmazást az *Alacsony korlátozás* csoportba helyezte.

  Az ilyen alkalmazások minimális korlátozások mellett férhetnek hozzá az operációs rendszer erőforrásaihoz.
- **Magas korlátozás**. Ebbe a csoportba tartoznak azok az alkalmazások, amelyeknél az alábbi feltételek teljesülnek:
  - Az alkalmazásokat nem írták alá digitálisan megbízható forgalmazók,
  - Az alkalmazások nem szerepelnek a Kaspersky Security Network megbízható alkalmazásokról készült adatbázisában,
  - A felhasználó az alkalmazást a *Magas korlátozás* csoportba helyezte.

  Az ilyen alkalmazások nagyfokú korlátozások mellett férhetnek hozzá az operációs rendszer erőforrásaihoz.
- **Nem megbízható**. Ebbe a csoportba tartoznak azok az alkalmazások, amelyeknél az alábbi feltételek teljesülnek:
  - Az alkalmazásokat nem írták alá digitálisan megbízható forgalmazók,
  - Az alkalmazások nem szerepelnek a Kaspersky Security Network megbízható alkalmazásokról készült adatbázisában,
  - A felhasználó az alkalmazást a *Nem megbízható* csoportba helyezte.

  Ezeknek az alkalmazásoknak minden művelete le van tiltva.

3. melléklet Fájlkiterjesztések a cserélhető meghajtók gyors vizsgálatához

com – 64 KB-nál nem nagyobb az alkalmazás végrehajtható fájlja

exe – futtatható fájl vagy önkicsomagoló archívum

sys – Microsoft Windows rendszerfájl

prg – dBase™, Clipper vagy Microsoft Visual FoxPro® programszöveg, illetve WAVmaker program

bin – bináris fájl

bat – kötegfájl

cmd – Microsoft Windows NT (a DOS bat fájlhoz hasonló) vagy OS/2 parancsfájl

dpl – tömörített Borland Delphi könyvtár

dll – dinamikus csatolású könyvtár

scr – Microsoft Windows üdvözlő képernyő

cpl – Microsoft Windows vezérlőpult-modul

ocx – Microsoft OLE (Object Linking and Embedding) objektum

tsp – felosztott idejű módban futó program

drv – eszköz illesztőprogramja

vxd – Microsoft Windows virtuális eszközillesztő

pif – programinformációs fájl

lnk – Microsoft Windows hivatkozásfájl

reg – Microsoft Windows beállításkulcsfájl

ini – Microsoft Windows, Windows NT és egyes alkalmazások konfigurációs adatait tartalmazó konfigurációs fájl

cla – Java osztály

vbs – Visual Basic® szkript

vbe – BIOS videokiterjesztés

js, jse – JavaScript forrásszöveg

htm – hiperszöveg dokumentum

htt – Microsoft Windows hiperszöveg fejléc

hta – hiperszöveg program a Microsoft Internet Explorer® részére

asp – Active Server Pages szkript

chm – lefordított HTML fájl

pht – beépített PHP szkripteket tartalmazó HTML fájl

php – HTML fájlokba beépített szkript

wsh – Microsoft Windows Script Host fájl

wsf – Microsoft Windows szkript

the – Microsoft Windows 95 asztali háttérkép-fájl

hlp – Win súgófájl

msg – Microsoft Mail e-mail üzenet

plg – e-mail üzenet

mbx – elmentett Microsoft Office Outlook e-mail üzenet

doc* – Microsoft Office Word dokumentumok, például: doc Microsoft Office Word dokumentumoknál, docx Microsoft Office Word 2007 dokumentumoknál, melyek XML támogatást tartalmaznak, és docm Microsoft Office Word 2007 dokumentumoknál, melyek makrótámogatást tartalmaznak

dot* – Microsoft Office Word dokumentumsablonok, például: dot Microsoft Office Word dokumentumsablonoknál, dotx Microsoft Office Word 2007 dokumentumsablonoknál, dotm Microsoft Office Word 2007 dokumentumsablonoknál, melyek makrótámogatást tartalmaznak

fpm – adatbázisprogram, Microsoft Visual FoxPro indítófájl

rtf – Rich Text Format dokumentum

shs – Windows Shell Scrap Object Handler töredék

dwg – AutoCAD® rajz adatbázisa

msi – Microsoft Windows Installer csomag

otm – VBA projekt Microsoft Office Outlook részére

pdf – Adobe Acrobat dokumentum

swf – Shockwave® Flash csomagobjektum

jpg, jpeg – tömörített képformátum

emf – Enhanced Metafile formátumú fájl.

ico – objektum ikonfájlja

Ov? – Microsoft Office Word végrehajtható fájlok

xl* – Microsoft Office Excel dokumentumok és fájlok, például: xla, a Microsoft Office Excel kiterjesztése, xlc grafikonoknál, xlt dokumentumsablonoknál, xlsx Microsoft Office Excel 2007 munkafüzeteknél, xltm Microsoft Office Excel 2007 munkafüzeteknél makrótámogatással, xlsb Microsoft Office Excel 2007 bináris (nem XML) formátumú munkafüzeteknél, xltx Microsoft Office Excel 2007 sablonoknál, xlsm Microsoft Office Excel 2007 sablonoknál makrótámogatással, és xlam Microsoft Office Excel 2007 bővítményeknél makrótámogatással

pp* – Microsoft Office PowerPoint® dokumentumok és fájlok, például: pps Microsoft Office PowerPoint diáknál, ppt bemutatóknál, pptx Microsoft Office PowerPoint 2007 bemutatóknál, pptm Microsoft Office PowerPoint 2007 bemutatóknál makrótámogatással, potx Microsoft Office PowerPoint 2007 bemutatósablonoknál, potm Microsoft Office PowerPoint 2007 bemutatósablonoknál makrótámogatással, ppsx Microsoft Office PowerPoint 2007 diavetítéseknél, ppsm Microsoft Office PowerPoint 2007 diavetítéseknél makrótámogatással, és ppam Microsoft Office PowerPoint 2007 bővítményeknél makrótámogatással

md* – Microsoft Office Access® dokumentumok és fájlok, például: mda Microsoft Office Access munkacsoportoknál és mdb adatbázisoknál

sldx – Microsoft PowerPoint 2007 dia

sldm – Microsoft PowerPoint 2007 dia makrótámogatással

thmx – Microsoft Office 2007 téma

4. melléklet A Levelezés védelem mellékletszűrőhöz tartozó fájltípusok

Megjegyzés: előfordulhat, hogy egy fájl tényleges formátuma nem egyezik a fájlnév kiterjesztésével.

Ha bekapcsolta az e-mailekhez csatolt mellékletek szűrését, a Levelezés védelem összetevő az alábbi kiterjesztéssel rendelkező fájlokat átnevezheti vagy törölheti:

com – 64 KB-nál nem nagyobb az alkalmazás végrehajtható fájlja

exe – futtatható fájl vagy önkicsomagoló archívum

sys – Microsoft Windows rendszerfájl

prg – dBase™, Clipper vagy Microsoft Visual FoxPro® programszöveg, illetve WAVmaker program

bin – bináris fájl

bat – kötegfájl

cmd – Microsoft Windows NT (a DOS bat fájlhoz hasonló) vagy OS/2 parancsfájl

dpl – tömörített Borland Delphi könyvtár

dll – dinamikus csatolású könyvtár

scr – Microsoft Windows üdvözlő képernyő

cpl – Microsoft Windows vezérlőpult-modul

ocx – Microsoft OLE (Object Linking and Embedding) objektum

tsp – felosztott idejű módban futó program

drv – eszköz illesztőprogramja

vxd – Microsoft Windows virtuális eszközillesztő

pif – programinformációs fájl

lnk – Microsoft Windows hivatkozásfájl

reg – Microsoft Windows beállításkulcsfájl

ini – Microsoft Windows, Windows NT és egyes alkalmazások konfigurációs adatait tartalmazó konfigurációs fájl

cla – Java osztály

vbs – Visual Basic® szkript

vbe – BIOS videokiterjesztés

js, jse – JavaScript forrásszöveg

htm – hiperszöveg dokumentum

htt – Microsoft Windows hiperszöveg fejléc

hta – hiperszöveg program a Microsoft Internet Explorer® részére

asp – Active Server Pages szkript

chm – lefordított HTML fájl

pht – beépített PHP szkripteket tartalmazó HTML fájl

php – HTML fájlokba beépített szkript

wsh – Microsoft Windows Script Host fájl

wsf – Microsoft Windows szkript

the – Microsoft Windows 95 asztali háttérkép-fájl

hlp – Win súgófájl

msg – Microsoft Mail e-mail üzenet

plg – e-mail üzenet

mbx – elmentett Microsoft Office Outlook e-mail üzenet

doc* – Microsoft Office Word dokumentumok, például: doc Microsoft Office Word dokumentumoknál, docx Microsoft Office Word 2007 dokumentumoknál, melyek XML támogatást tartalmaznak, és docm Microsoft Office Word 2007 dokumentumoknál, melyek makrótámogatást tartalmaznak

dot* – Microsoft Office Word dokumentumsablonok, például: dot Microsoft Office Word dokumentumsablonoknál, dotx Microsoft Office Word 2007 dokumentumsablonoknál, dotm Microsoft Office Word 2007 dokumentumsablonoknál, melyek makrótámogatást tartalmaznak

fpm – adatbázisprogram, Microsoft Visual FoxPro indítófájl

rtf – Rich Text Format dokumentum

shs – Windows Shell Scrap Object Handler töredék

dwg – AutoCAD® rajz adatbázisa

msi – Microsoft Windows Installer csomag

otm – VBA projekt Microsoft Office Outlook részére

pdf – Adobe Acrobat dokumentum

swf – Shockwave® Flash csomagobjektum

jpg, jpeg – tömörített képformátum

emf – Enhanced Metafile formátumú fájl.

ico – objektum ikonfájlja

Ov? – Microsoft Office Word végrehajtható fájlok

xl* – Microsoft Office Excel dokumentumok és fájlok, például: xla, a Microsoft Office Excel kiterjesztése, xlc grafikonoknál, xlt dokumentumsablonoknál, xlsx Microsoft Office Excel 2007 munkafüzeteknél, xltm Microsoft Office Excel 2007 munkafüzeteknél makrótámogatással, xlsb Microsoft Office Excel 2007 bináris (nem XML) formátumú munkafüzeteknél, xltx Microsoft Office Excel 2007 sablonoknál, xlsm Microsoft Office Excel 2007 sablonoknál makrótámogatással, és xlam Microsoft Office Excel 2007 bővítményeknél makrótámogatással

pp* – Microsoft Office PowerPoint® dokumentumok és fájlok, például: pps Microsoft Office PowerPoint diáknál, ppt bemutatóknál, pptx Microsoft Office PowerPoint 2007 bemutatóknál, pptm Microsoft Office PowerPoint 2007 bemutatóknál makrótámogatással, potx Microsoft Office PowerPoint 2007 bemutatósablonoknál, potm Microsoft Office PowerPoint 2007 bemutatósablonoknál makrótámogatással, ppsx Microsoft Office PowerPoint 2007 diavetítéseknél, ppsm Microsoft Office PowerPoint 2007 diavetítéseknél makrótámogatással, és ppam Microsoft Office PowerPoint 2007 bővítményeknél makrótámogatással

md* – Microsoft Office Access® dokumentumok és fájlok, például: mda Microsoft Office Access munkacsoportoknál és mdb adatbázisoknál

sldx – Microsoft PowerPoint 2007 dia

sldm – Microsoft PowerPoint 2007 dia makrótámogatással

thmx – Microsoft Office 2007 téma

5. melléklet A külső szolgáltatásokkal való interakció hálózati beállításai

A Kaspersky Endpoint Security és a Kaspersky Security Center titkosított kommunikációs csatornát használ TLS-sel (átviteli réteg biztonsága) a Kaspersky külső szolgáltatásaival való együttműködéshez.

A Kaspersky Endpoint Security a következő hálózati beállításokat használja a külső szolgáltatásokkal való interakcióhoz.

Cím	Leírás
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokoll: `HTTPS` Port: `443`	Alkalmazás aktiválása.

Cím	Leírás

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protokoll: `HTTPS`
Port: `443`
	Adatbázisok és alkalmazás-szoftvermodulok frissítése.

`downloads.upd.kaspersky.com` Protokoll: `HTTPS` Port: `443`	• Adatbázisok és alkalmazás-szoftvermodulok frissítése. • A Kaspersky kiszolgálókhoz való hozzáférés ellenőrzése. Ha a kiszolgálókhoz a rendszer DNS használatával nem lehet hozzáférni, az alkalmazás a nyilvános DNS-t használja. Erre azért van szükség, hogy a vírusadatbázisok frissítve legyenek, és a számítógép biztonsági szintje megmaradjon. A Kaspersky Endpoint Security a nyilvános DNS-kiszolgálók alábbi listáját használja ebben a sorrendben: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Az alkalmazás által kibocsátott kérések tartalmazhatnak tartománycímeket és a felhasználó nyilvános IP-címét, mivel az alkalmazás TCP/UDP-kapcsolatot létesít a DNS-kiszolgálóval. Ez az információ például egy webes erőforrás tanúsítványának érvényesítéséhez szükséges HTTPS használatakor. Ha a Kaspersky Endpoint Security nyilvános DNS-kiszolgálót használ, az adatfeldolgozásra az adott szolgáltatás adatvédelmi irányelvei vonatkoznak. Ha meg szeretné akadályozni, hogy a Kaspersky Endpoint Security nyilvános DNS-kiszolgálót használjon, forduljon a Terméktámogatáshoz privát hibajavításért.
`touch.kaspersky.com` Protokoll: `HTTP`	• Megbízható idő fogadása a tanúsítvány érvényességi idejének ellenőrzéséhez (TLS-kapcsolat). • Figyelmeztetés webes erőforráshoz való hozzáférés megtagadásáról a böngészőben, amikor a Web védelem fut.

Cím	Leírás

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protokoll: `HTTP`
Port: `80`
	Adatbázisok és alkalmazás-szoftvermodulok frissítése.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protokoll: `HTTPS`
Port: `443`
	A Kaspersky Security Network használata.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protokoll: `KSN`
Port: `443`, `1443`
	A Kaspersky Security Network használata.

`click.kaspersky.com`
`redirect.kaspersky.com`
Protokoll: `HTTPS`
Port: `443`
	Kövesse a felület hivatkozásait.

Titkosításhoz használt beállítások

Cím	Leírás

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protokoll: `HTTP`
Port: `80`
	Public Key Infrastructure (PKI).

6. melléklet Alkalmazás eseményei

A Kaspersky Endpoint Security egyes összetevőinek működésére, az adattitkosítási eseményekre, az egyes kártevővizsgálati feladatok, frissítési feladatok és integritás-ellenőrzési feladatok befejezésére, valamint az alkalmazás általános működésére vonatkozó információk bekerülnek a Kaspersky Security Center eseménynaplójába és a Windows eseménynaplóba.

A Kaspersky Endpoint Security a következő típusú eseményeket állítja elő: általános események és specifikus események. Specifikus eseményeket csak a Kaspersky Endpoint Security for Windows állít elő. A specifikus események egyszerű azonosítóval rendelkeznek, például: `000000cb`. A specifikus események az alábbi szükséges paramétereket tartalmazzák:

- `GNRL_EA_DESCRIPTION`: az esemény tartalma.
- `GNRL_EA_ID`: az esemény szolgáltatásazonosítója.
- `GNRL_EA_SEVERITY`: az esemény állapota. `1` – *Info*, `2` – *Warning*, `3` – *Functional failure*, `4` – *Critical*.
- `EVENT_TYPE_DISPLAY_NAME`: az esemény címe.
- `TASK_DISPLAY_NAME`: az eseményt kiváltó alkalmazásösszetevő neve.

Általános események a Kaspersky Endpoint Security for Windows, illetve más Kaspersky-alkalmazások (például a Kaspersky Security for Windows Server) révén is létrehozhatók. Az általános események azonosítói összetettebbek, például: `GNRL_EV_VIRUS_FOUND`. Az általános események a szükséges beállításokon túl speciális beállításokat is tartalmaznak.

Mennyi ideig tárolódnak az események a kiszolgálón

Kritikus

License expired

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	`201`
Kaspersky Security Center eseményazonosító	`GNRL_EV_LICENSE_EXPIRATION`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

License has almost expired

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	`203`

Kaspersky Security Center eseményazonosító	000000cb
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Databases are missing or corrupted

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	206
Kaspersky Security Center eseményazonosító	000000ce
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Databases are extremely out of date

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	207
Kaspersky Security Center eseményazonosító	000000cf
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application autorun is disabled

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	209
Kaspersky Security Center eseményazonosító	000000d1
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Activation error

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	229
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Active threat detected. Advanced Disinfection should be started

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	231
Kaspersky Security Center eseményazonosító	000000e7

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

KSN servers unavailable

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2023
Kaspersky Security Center eseményazonosító	000007e7
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Not enough space in Quarantine storage

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	343
Kaspersky Security Center eseményazonosító	00000157
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object not restored from Quarantine

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	346
Kaspersky Security Center eseményazonosító	0000015a
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object not deleted from Quarantine

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	348
Kaspersky Security Center eseményazonosító	0000015c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The application established a connection to a website with an untrusted certificate

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	57
Kaspersky Security Center eseményazonosító	00000039

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Failed to verify an encrypted connection. The domain is added to the list of exclusions

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	`60`
Kaspersky Security Center eseményazonosító	`0000003c`
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Malicious object detected (local bases)

Státusz	!
Összetevő	Fájl védelem Web védelem Levelezés védelem AMSI védelem Behatolásmegelőző rendszer Viselkedésészlelés Anti-Cryptor Biztonsági rések kihasználásának megelőzése Kártevő vizsgálata
Windows eseményazonosító	`302`
Kaspersky Security Center eseményazonosító	`GNRL_EV_VIRUS_FOUND`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. A megosztott mappák külső titkosításának észlelésekor az alkalmazás megjeleníti a célfájl elérési útját. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`). • `GNRL_EA_PARAM_9` további információ az észlelt objektumról: Alkalmazásösszetevő (`engine`). Fenyegetésészlelő technológia (`method`). A Kaspersky Private Security Network által észlelt fenyegetés (`blacklist`): `true` vagy `false`. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Malicious object detected (KSN)

Státusz	ⓘ
Összetevő	Fájl védelem Web védelem Levelezés védelem AMSI védelem Behatolásmegelőző rendszer Viselkedésészlelés Anti-Cryptor Biztonsági rések kihasználásának megelőzése Kártevő vizsgálata
Windows eseményazonosító	`302`
Kaspersky Security Center eseményazonosító	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`). • `GNRL_EA_PARAM_9` további információ az észlelt objektumról: Alkalmazásösszetevő (`engine`). Fenyegetésészlelő technológia (`method`). A Kaspersky Private Security Network által észlelt fenyegetés (`blacklist`): `true` vagy `false`. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Disinfection impossible

Státusz	ⓘ
Összetevő	Fájl védelem Levelezés védelem Behatolásmegelőző rendszer Viselkedésészlelés Anti-Cryptor Kártevő vizsgálata
Windows eseményazonosító	`312`
Kaspersky Security Center eseményazonosító	`GNRL_EV_OBJECT_NOTCURED`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`). • `GNRL_EA_PARAM_9` további információ az észlelt objektumról: Alkalmazásösszetevő (`engine`). Fenyegetésészlelő technológia (`method`). A Kaspersky Private Security Network által észlelt fenyegetés (`blacklist`): `true` vagy `false`. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Cannot be deleted

Státusz	!
Összetevő	Fájl védelem Behatolásmegelőző rendszer Viselkedésészlelés Anti-Cryptor Kártevő vizsgálata
Windows eseményazonosító	313
Kaspersky Security Center eseményazonosító	00000139
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Processing error

Státusz	!
Összetevő	Fájl védelem Web védelem Levelezés védelem Behatolásmegelőző rendszer AMSI védelem Kártevő vizsgálata
Windows eseményazonosító	317
Kaspersky Security Center eseményazonosító	0000013d
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Process terminated

Státusz	!
Összetevő	Fájl védelem Behatolásmegelőző rendszer Viselkedésészlelés Kártevő vizsgálata
Windows eseményazonosító	452
Kaspersky Security Center eseményazonosító	000001c4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Unable to terminate process

Státusz	!
Összetevő	Fájl védelem Behatolásmegelőző rendszer Viselkedésészlelés Kártevő vizsgálata
Windows eseményazonosító	453
Kaspersky Security Center eseményazonosító	000001c5
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Dangerous link blocked

Státusz	!
Összetevő	Web védelem
Windows eseményazonosító	362
Kaspersky Security Center eseményazonosító	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Esemény paraméterei	• GNRL_EA_PARAM_2: az objektum elérési útja. • GNRL_EA_PARAM_5 az objektum neve a Kaspersky besorolása szerint. • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_8: a fenyegetés típusa (típus). • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Privát KSN által észlelt fenyegetés (blacklist): true vagy false.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Dangerous link opened

Státusz	!
Összetevő	Web védelem
Windows eseményazonosító	363
Kaspersky Security Center eseményazonosító	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Esemény paraméterei	• GNRL_EA_PARAM_2: az objektum elérési útja. • GNRL_EA_PARAM_5 az objektum neve a Kaspersky besorolása szerint. • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_8: a fenyegetés típusa (típus). • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Privát KSN által észlelt fenyegetés (blacklist): true vagy false.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Previously opened dangerous link detected

Státusz	!
Összetevő	Web védelem
Windows eseményazonosító	1201
Kaspersky Security Center eseményazonosító	GNRL_EV_VIRUS_FOUND_AND_PASSED
Esemény paraméterei	• GNRL_EA_PARAM_2: az objektum elérési útja. • GNRL_EA_PARAM_5 az objektum neve a Kaspersky besorolása szerint. • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_8: a fenyegetés típusa (típus). • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Privát KSN által észlelt fenyegetés (blacklist): true vagy false.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Process action blocked

Státusz	ⓘ
Összetevő	Adaptív Anomáliafelügyelő
Windows eseményazonosító	`2200`
Kaspersky Security Center eseményazonosító	`GNRL_EV_ADSEC_DETECT`
Esemény paraméterei	• `GNRL_EA_PARAM_1`: az Adaptív Anomáliafelügyeleti szabály neve. • `GNRL_EA_PARAM_2`: a heurisztikai szabály azonosítója. • `GNRL_EA_PARAM_3` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_4`: a forrásfolyamat. • `GNRL_EA_PARAM_5`: a forrásobjektum. • `GNRL_EA_PARAM_6`: a célfolyamat. • `GNRL_EA_PARAM_7`: a célobjektum. • `GNRL_EA_PARAM_8` további információ az észlelt objektumról: A forrásfolyamat/-objektum és a célfolyamat/-objektum ellenőrzőösszegei. Folyamat blokkolva (`verdict_type`): `true` vagy `false`. Felhasználó biztonsági azonosítója (SID).
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Keyboard not authorized

Státusz	ⓘ
Összetevő	BadUSB védelem
Windows eseményazonosító	`2051`
Kaspersky Security Center eseményazonosító	`00000803`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

AMSI request was blocked

Státusz	ⓘ
Összetevő	AMSI védelem
Windows eseményazonosító	`2200`
Kaspersky Security Center eseményazonosító	`00000898`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network activity blocked

Státusz	ⓘ
Összetevő	Tűzfal
Windows eseményazonosító	`602`
Kaspersky Security Center eseményazonosító	`00000329`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network attack detected

Státusz	!
Összetevő	Hálózati védelem
Windows eseményazonosító	651
Kaspersky Security Center eseményazonosító	GNRL_EV_ATTACK_DETECTED
Esemény paraméterei	• GNRL_EA_PARAM_1 a támadás neve. • GNRL_EA_PARAM_2 a protokoll. • GNRL_EA_PARAM_3 a hálózati támadás forrásaként szolgáló számítógép IP-címe. Az IP-cím a gazdagép bájtsorrendjében van megadva. Például 2886729929 172.16.0.201 esetén. • GNRL_EA_PARAM_4 a port száma. • GNRL_EA_PARAM_5 egy IPv6 -cím, például 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 a hálózati támadás célpontjának számító számítógép IP-címe. Az IP-cím a gazdagép bájtsorrendjében van megadva. Például 2886729929 172.16.0.201 esetén.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application startup prohibited

Státusz	!
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	702
Kaspersky Security Center eseményazonosító	GNRL_EV_APPLICATION_LAUNCH_DENIED
Esemény paraméterei	• GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a kategória manuálisan létrehozott azonosítója. • GNRL_EA_PARAM_4 az alkalmazáskategória azonosítója. • GNRL_EA_PARAM_5 az alkalmazás digitális aláírására vonatkozó információ. • GNRL_EA_PARAM_6 az alkalmazás futtatható fájljának neve (például chrome.exe). • GNRL_EA_PARAM_7 a futtatható fájl elérési útja. • GNRL_EA_PARAM_8 az objektum kivonata (SHA256). • GNRL_EA_PARAM_9 a felhasználó által futtatni kívánt alkalmazás verziója.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Prohibited process was started before Kaspersky Endpoint Security startup

Státusz	!
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	710
Kaspersky Security Center eseményazonosító	000002c6
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Access denied (local bases)

Státusz	!
Összetevő	Webfelügyelő

Windows eseményazonosító	752
Kaspersky Security Center eseményazonosító	GNRL_EV_WEB_URL_BLOCKED
Esemény paraméterei	• GNRL_EA_PARAM_1 az URL. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a Web Control szabály neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Access denied (KSN)

Státusz	ⓘ
Összetevő	Webfelügyelő
Windows eseményazonosító	752
Kaspersky Security Center eseményazonosító	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Esemény paraméterei	• GNRL_EA_PARAM_1 az URL. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a Web Control szabály neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Operation with the device prohibited

Státusz	ⓘ
Összetevő	Eszközfelügyelő
Windows eseményazonosító	802
Kaspersky Security Center eseményazonosító	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Esemény paraméterei	• GNRL_EA_PARAM_1 a hardverazonosító (HWID). • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network connection blocked

Státusz	ⓘ
Összetevő	Eszközfelügyelő
Windows eseményazonosító	809
Kaspersky Security Center eseményazonosító	00000329
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error updating component

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1011
Kaspersky Security Center eseményazonosító	000003f3

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error distributing component updates

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1012
Kaspersky Security Center eseményazonosító	000003f4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Local update error

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1014
Kaspersky Security Center eseményazonosító	000003f6
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Network update error

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1015
Kaspersky Security Center eseményazonosító	000003f7
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Cannot start two tasks at the same time

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1017
Kaspersky Security Center eseményazonosító	000003f9
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error verifying application databases and modules

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1018
Kaspersky Security Center eseményazonosító	000003fa

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error in interaction with Kaspersky Security Center

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1019
Kaspersky Security Center eseményazonosító	000003fb
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Not all components were updated

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1021
Kaspersky Security Center eseményazonosító	000003fd
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Update completed successfully, update distribution failed

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1023
Kaspersky Security Center eseményazonosító	000003ff
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Internal task error

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	101
Kaspersky Security Center eseményazonosító	00000065
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Patch installation failed

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2153
Kaspersky Security Center eseményazonosító	00000869

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Patch rollback failed

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2156
Kaspersky Security Center eseményazonosító	0000086C
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error applying file encryption / decryption rules

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	904
Kaspersky Security Center eseményazonosító	00000388
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File encryption / decryption error

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	912
Kaspersky Security Center eseményazonosító	GNRL_EV_ENCRYPTION_ERROR
Esemény paraméterei	• GNRL_EA_PARAM_1: a fájl elérési útja. • GNRL_EA_PARAM_2: a hiba oka. • GNRL_EA_PARAM_3: az eszköz típusa.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File access blocked

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	940
Kaspersky Security Center eseményazonosító	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Esemény paraméterei	• GNRL_EA_PARAM_1: a célobjektum. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3: azon alkalmazás futtatható fájljának neve (például chrome.exe), amely megpróbál hozzáférni a fájlhoz.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Error enabling portable mode

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	951
Kaspersky Security Center eseményazonosító	000003b7
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error disabling portable mode

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	953
Kaspersky Security Center eseményazonosító	000003b9
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error creating encrypted package

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	931
Kaspersky Security Center eseményazonosító	000003a3
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error encrypting / decrypting device

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1305
Kaspersky Security Center eseményazonosító	00000519
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Could not load encryption module

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1311
Kaspersky Security Center eseményazonosító	0000051f
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The task for managing Authentication Agent accounts ended with an error

Státusz	!
Összetevő	Adattitkosítás
Windows eseményazonosító	1340
Kaspersky Security Center eseményazonosító	0000053c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Policy cannot be applied

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	1312
Kaspersky Security Center eseményazonosító	00000520
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

FDE upgrade failed

Státusz	!
Összetevő	Adattitkosítás
Windows eseményazonosító	1342
Kaspersky Security Center eseményazonosító	0000053e
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

FDE upgrade rollback failed (for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help)

Státusz	!
Összetevő	Adattitkosítás
Windows eseményazonosító	1344
Kaspersky Security Center eseményazonosító	00000540
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Kaspersky Anti Targeted Attack Platform server unavailable

Státusz	!
Összetevő	Végponti szenzor
Windows eseményazonosító	2100
Kaspersky Security Center eseményazonosító	00000834
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Failed to delete object

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2252
Kaspersky Security Center eseményazonosító	000008cc
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object not quarantined (Sandbox)

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2603
Kaspersky Security Center eseményazonosító	00000a2b
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

An internal error occurred

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2607
Kaspersky Security Center eseményazonosító	00000a2f
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Invalid Sandbox server certificate

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2613
Kaspersky Security Center eseményazonosító	00000a35
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The Sandbox node is unavailable

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2614
Kaspersky Security Center eseményazonosító	00000a36
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Failed to process the object in Sandbox

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2617
Kaspersky Security Center eseményazonosító	00000a39
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Maximum load to Sandbox is exceeded

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2618
Kaspersky Security Center eseményazonosító	00000a3a
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

IOC found

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2651
Kaspersky Security Center eseményazonosító	00000a5b
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Sandbox license verification failed

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2620
Kaspersky Security Center eseményazonosító	00000a3c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

A felhasználónak nem sikerült elküldenie a vizsgálati feladatot a Sandbox számára

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2623
Kaspersky Security Center eseményazonosító	00000a3e
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Hiba történt a Sandbox-feladat létrehozásakor

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2621
Kaspersky Security Center eseményazonosító	00000a3d
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object startup blocked

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2553
Kaspersky Security Center eseményazonosító	000009f9
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Process startup blocked

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2551
Kaspersky Security Center eseményazonosító	000009f7
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Script execution blocked

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2559
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object not quarantined (Endpoint Detection and Response)

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2556
Kaspersky Security Center eseményazonosító	000009fc
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Process startup is not blocked

Státusz	!
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2561
Kaspersky Security Center eseményazonosító	00000a01
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object is not blocked

Státusz	!
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2562
Kaspersky Security Center eseményazonosító	00000a02
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Script execution is not blocked

Státusz	!
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2563
Kaspersky Security Center eseményazonosító	00000a03
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error changing application components

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	1401
Kaspersky Security Center eseményazonosító	00000579
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

There are patterns of a possible brute-force attack in the system

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2800
Kaspersky Security Center eseményazonosító	00000af0
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

There are patterns of a possible Windows Event Log abuse

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2801
Kaspersky Security Center eseményazonosító	00000af1
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Atypical actions detected on behalf of a new service installed

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2802
Kaspersky Security Center eseményazonosító	00000af2
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Atypical logon that uses explicit credentials detected

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2803
Kaspersky Security Center eseményazonosító	00000af3
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2804
Kaspersky Security Center eseményazonosító	00000af4
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Suspicious changes detected in the privileged built-in Administrators group

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2805
Kaspersky Security Center eseményazonosító	00000af5
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

There is an atypical activity detected during a network logon session

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2806
Kaspersky Security Center eseményazonosító	00000af6
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Log Inspection rule triggered

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2807
Kaspersky Security Center eseményazonosító	00000af7
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Atypical event occurs too often. Event aggregation started

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2808
Kaspersky Security Center eseményazonosító	00000af8
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Report on an atypical event for the aggregation period

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2809
Kaspersky Security Center eseményazonosító	00000af9
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error connecting to the EDR Expert server

Státusz	!
Összetevő	Endpoint Detection and Response Expert (on-premises)
Windows eseményazonosító	2850
Kaspersky Security Center eseményazonosító	00000b22
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Invalid certificate of the EDR Expert server

Státusz	!
Összetevő	Endpoint Detection and Response Expert (on-premises)
Windows eseményazonosító	2851
Kaspersky Security Center eseményazonosító	00000b23
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Invalid certificate of the agent on the EDR Expert server

Státusz	!
Összetevő	Endpoint Detection and Response Expert (on-premises)
Windows eseményazonosító	2852
Kaspersky Security Center eseményazonosító	00000b24
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Hiba történt az EDR Expert-válaszkiszolgálóhoz való csatlakozáskor

Státusz	!
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	2858
Kaspersky Security Center eseményazonosító	00000b22
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az EDR Expert válaszkiszolgáló tanúsítványa érvénytelen

Státusz	!
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	2859
Kaspersky Security Center eseményazonosító	00000b23
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az ügynök tanúsítványa érvénytelen az EDR Expert válaszkiszolgálón

Státusz	!
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	2860
Kaspersky Security Center eseményazonosító	00000b24

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

EDR Expert telemetriai adatgyűjtői kiszolgáló csatlakozási hiba

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	`2854`
Kaspersky Security Center eseményazonosító	`00000b22`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az EDR Expert telemetriai adatgyűjtő kiszolgáló tanúsítványa érvénytelen

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	`2855`
Kaspersky Security Center eseményazonosító	`00000b23`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az ügynök tanúsítványa érvénytelen az EDR Expert telemetriai adatgyűjtő kiszolgálón

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	`2856`
Kaspersky Security Center eseményazonosító	`00000b24`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Hiba történt az NDR-kiszolgálóhoz való csatlakozásban

Státusz	ⓘ
Összetevő	Network Detection and Response (KATA)
Windows eseményazonosító	`3080`
Kaspersky Security Center eseményazonosító	`00000c08`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az NDR-kiszolgáló érvénytelen tanúsítványa

Státusz	ⓘ
Összetevő	Network Detection and Response (KATA)
Windows eseményazonosító	`3081`

Kaspersky Security Center eseményazonosító	00000c09
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Érvénytelen az ügynök tanúsítványa az NDR kiszolgálón

Státusz	!
Összetevő	Network Detection and Response (KATA)
Windows eseményazonosító	3082
Kaspersky Security Center eseményazonosító	00000c0a
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az eszköz egy nem megbízható felügyeleti kiszolgálóhoz csatlakozik. Lépjen kapcsolatba a rendszergazdával

Státusz	!
Összetevő	Felügyeleti kiszolgálói kapcsolat védelme
Windows eseményazonosító	3301
Kaspersky Security Center eseményazonosító	00000ce5
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File or folder change was detected

Státusz	i / ⚠ / !
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2950
Kaspersky Security Center eseményazonosító	00000b86
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Object changes too often. Event aggregation started

Státusz	i / ⚠ / !
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2955
Kaspersky Security Center eseményazonosító	00000b8b
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Report on object modification for the aggregation period

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2956
Kaspersky Security Center eseményazonosító	00000b8c
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Monitoring scope includes incorrect objects

Státusz	ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2953
Kaspersky Security Center eseményazonosító	00000b89
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Registry change was detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2951
Kaspersky Security Center eseményazonosító	00000b87
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Device connection / disconnection is detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2952
Kaspersky Security Center eseményazonosító	00000b88
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

A figyelési hatókör helytelen objektumokat tartalmaz

Státusz	/ /
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2903
Kaspersky Security Center eseményazonosító	00000b89
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Attempts to perform the restricted operations with the object is too many. Event aggregation started

Státusz	
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2963
Kaspersky Security Center eseményazonosító	00000b93
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

An operation with the files of the monitoring scope was blocked

Státusz	
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2959
Kaspersky Security Center eseményazonosító	00000b8f
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Registry modification blocked

Státusz	
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2960
Kaspersky Security Center eseményazonosító	00000b90
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Processing error

Státusz	!
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2954
Kaspersky Security Center eseményazonosító	00000b8a
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

Státusz	!
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2964
Kaspersky Security Center eseményazonosító	00000b94
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

Státusz	!
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	711
Kaspersky Security Center eseményazonosító	000002c7
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

Státusz	!
Összetevő	Eszközfelügyelő
Windows eseményazonosító	810
Kaspersky Security Center eseményazonosító	0000032a
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

Státusz	!
Összetevő	Webfelügyelő
Windows eseményazonosító	757
Kaspersky Security Center eseményazonosító	000002f5
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

Státusz	!
Összetevő	Adaptív Anomáliafelügyelő
Windows eseményazonosító	504
Kaspersky Security Center eseményazonosító	000001f8
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

Státusz	!
Összetevő	Naplóvizsgálat
Windows eseményazonosító	2810
Kaspersky Security Center eseményazonosító	00000afa
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Unable to connect to the Integration Server for more than 6 hours. Check Integration Server status and network settings

Státusz	!
Összetevő	Light Agent
Windows eseményazonosító	3103
Kaspersky Security Center eseményazonosító	00000c1f
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

SVM is unavailable

Státusz	!
Összetevő	Light Agent
Windows eseményazonosító	3151
Kaspersky Security Center eseményazonosító	00000c4f
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Malicious object detected. Advanced Disinfection should be started on a virtual machine template

Státusz	!
Összetevő	Light Agent
Windows eseményazonosító	3182
Kaspersky Security Center eseményazonosító	00000c6e
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az elavult protokollal létrehozott hálózati kapcsolat blokkolva lett

Státusz	!
Összetevő	Védelem
Windows eseményazonosító	75
Kaspersky Security Center eseményazonosító	0000004b
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

KUMA kiszolgáló kapcsolódási hibája

Státusz	!
Összetevő	KUMA integráció
Windows eseményazonosító	2854
Kaspersky Security Center eseményazonosító	00000b26
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az KUMA-kiszolgáló érvénytelen tanúsítványa

Státusz	!
Összetevő	KUMA integráció
Windows eseményazonosító	2855
Kaspersky Security Center eseményazonosító	00000b27
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Érvénytelen az ügynök tanúsítványa az KUMA kiszolgálón

Státusz	!
Összetevő	KUMA integráció
Windows eseményazonosító	2856
Kaspersky Security Center eseményazonosító	00000b28
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Működési hiba

Task cannot be performed

Státusz	!
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	212
Kaspersky Security Center eseményazonosító	000000d4

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Invalid task settings. Settings not applied

Státusz	⊗
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	707
Kaspersky Security Center eseményazonosító	000002c3
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Figyelmeztet

Application crashed during previous session

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	237
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

License expires soon

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	204
Kaspersky Security Center eseményazonosító	000000cc
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Databases are out of date

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	208
Kaspersky Security Center eseményazonosító	000000d0
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Automatic updates are disabled

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	210
Kaspersky Security Center eseményazonosító	000000d2
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Self-Defense is disabled

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	211
Kaspersky Security Center eseményazonosító	000000d3
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Protection components are disabled

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	214
Kaspersky Security Center eseményazonosító	000000d6
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Computer is running in safe mode

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	215
Kaspersky Security Center eseményazonosító	000000d7
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

There are unprocessed files

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	216
Kaspersky Security Center eseményazonosító	000000d8
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Group policy applied

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	219
Kaspersky Security Center eseményazonosító	000000db
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Task stopped

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	222
Kaspersky Security Center eseményazonosító	000000de
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Quit and reopen the application to complete updating

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	224
Kaspersky Security Center eseményazonosító	0000057b
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Computer restart required

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	225
Kaspersky Security Center eseményazonosító	000000e1
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The license allows the use of components that have not been installed

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	226
Kaspersky Security Center eseményazonosító	000000e2
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Advanced Disinfection started

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	232
Kaspersky Security Center eseményazonosító	000000e8
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Advanced Disinfection completed

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	233
Kaspersky Security Center eseményazonosító	000000e9
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Incorrect reserve key

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	230
Kaspersky Security Center eseményazonosító	000000e6
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Subscription expires soon

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	240
Kaspersky Security Center eseményazonosító	000000f0
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Blokkolt

Státusz	⚠
Összetevő	Viselkedésészlelés Anti-Cryptor Biztonsági rések kihasználásának megelőzése Web védelem
Windows eseményazonosító	331

Kaspersky Security Center eseményazonosító	GNRL_EV_OBJECT_BLOCKED
Esemény paraméterei	• GNRL_EA_PARAM_1 az objektum kivonata (SHA256). • GNRL_EA_PARAM_2 az objektum neve. A megosztott mappák külső titkosításának észlelésekor az alkalmazás megjeleníti a célfájl elérési útját. • GNRL_EA_PARAM_5: a fenyegetés neve a Kaspersky besorolása szerint, pl. EICAR-Test-File. • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_8: a fenyegetés típusa (típus). • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Kaspersky Private Security Network által észlelt fenyegetés (blacklist): true vagy false. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

The operating system settings do not allow to control access to Wi-Fi networks

Státusz	⚠
Összetevő	Eszközfelügyelő
Windows eseményazonosító	249
Kaspersky Security Center eseményazonosító	000000f9
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Object not restored from Backup

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	336
Kaspersky Security Center eseményazonosító	00000150
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Suspicious network activity detected

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2001
Kaspersky Security Center eseményazonosító	000007d1
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Encrypted connection terminated

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	250
Kaspersky Security Center eseményazonosító	000007d3
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Participation in KSN disabled

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2021
Kaspersky Security Center eseményazonosító	000007e5
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Processing of some OS functions is disabled

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	245
Kaspersky Security Center eseményazonosító	000000f5
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Quarantine storage is almost out of space

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	344
Kaspersky Security Center eseményazonosító	00000158
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network connection blocked

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	809
Kaspersky Security Center eseményazonosító	00000abe
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Cannot create a backup copy

Státusz	⚠
Összetevő	Fájl védelem Levelezés védelem Behatolásmegelőző rendszer AMSI védelem Kártevő vizsgálata
Windows eseményazonosító	`314`
Kaspersky Security Center eseményazonosító	`GNRL_EV_OBJECT_REPORTED`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`). • `GNRL_EA_PARAM_9` további információ az észlelt objektumról: Alkalmazásösszetevő (`engine`). Fenyegetésészlelő technológia (`method`). A Kaspersky Private Security Network által észlelt fenyegetés (`blacklist`): `true` vagy `false`. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Státusz	⚠
Összetevő	Fájl védelem Viselkedésészlelés Anti-Cryptor Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	`310`
Kaspersky Security Center eseményazonosító	`00000136`
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object encrypted

Státusz	⚠
Összetevő	Behatolásmegelőző rendszer
Windows eseményazonosító	`320`
Kaspersky Security Center eseményazonosító	`00000140`
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Object corrupted

Státusz	⚠
Összetevő	Fájl védelem Web védelem Levelezés védelem AMSI védelem Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	`321`
Kaspersky Security Center eseményazonosító	`00000141`
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)

Státusz	⚠
Összetevő	Fájl védelem Web védelem Levelezés védelem Behatolásmegelőző rendszer AMSI védelem Viselkedésészlelés Anti-Cryptor Anti-Cryptor Kártevő vizsgálata
Windows eseményazonosító	`303`
Kaspersky Security Center eseményazonosító	`GNRL_EV_VIRUS_FOUND`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`).
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Legitimate software that can be used by intruders to damage your computer or personal data was detected (KSN)

Státusz	⚠
Összetevő	Fájl védelem Web védelem Levelezés védelem Behatolásmegelőző rendszer AMSI védelem Viselkedésészlelés Anti-Cryptor Anti-Cryptor Kártevő vizsgálata
Windows eseményazonosító	`303`

Kaspersky Security Center eseményazonosító	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`).
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object deleted

Státusz	⚠
Összetevő	Fájl védelem Levelezés védelem Behatolásmegelőző rendszer Biztonsági rések kihasználásának megelőzése Viselkedéselemzés Anti-Cryptor Kártevő vizsgálata
Windows eseményazonosító	`307`
Kaspersky Security Center eseményazonosító	`GNRL_EV_OBJECT_DELETED`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`). • `GNRL_EA_PARAM_9` további információ az észlelt objektumról: Alkalmazásösszetevő (`engine`). Fenyegetéselemző technológia (`method`). A Kaspersky Private Security Network által észlelt fenyegetés (`blacklist`): `true` vagy `false`. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object disinfected

Státusz	⚠
Összetevő	Fájl védelem Levelezés védelem Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	`306`

Kaspersky Security Center eseményazonosító	GNRL_EV_OBJECT_CURED
Esemény paraméterei	• GNRL_EA_PARAM_1 az objektum kivonata (SHA256). • GNRL_EA_PARAM_2 az objektum neve. • GNRL_EA_PARAM_5: a fenyegetés neve a Kaspersky besorolása szerint, pl. EICAR-Test-File. • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_8: a fenyegetés típusa (típus). • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Kaspersky Private Security Network által észlelt fenyegetés (blacklist): true vagy false. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object will be disinfected on restart

Státusz	⚠
Összetevő	Behatolásmegelőző rendszer Fájl védelem Kártevő vizsgálata
Windows eseményazonosító	324
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Object will be deleted on restart

Státusz	⚠
Összetevő	Viselkedésészlelés Anti-Cryptor Biztonsági rések kihasználásának megelőzése Behatolásmegelőző rendszer Fájl védelem Kártevő vizsgálata
Windows eseményazonosító	323
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Object deleted according to settings

Státusz	⚠
Összetevő	Levelezés védelem
Windows eseményazonosító	342
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Rollback completed

Státusz	⚠
Összetevő	Fájl védelem Viselkedésészlelés Anti-Cryptor Biztonsági rések kihasználásának megelőzése Kártevő vizsgálata
Windows eseményazonosító	`455`
Kaspersky Security Center eseményazonosító	`000001c7`
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object download was blocked

Státusz	⚠
Összetevő	Web védelem
Windows eseményazonosító	`341`
Kaspersky Security Center eseményazonosító	`GNRL_EV_OBJECT_BLOCKED`
Esemény paraméterei	• `GNRL_EA_PARAM_1` az objektum kivonata (SHA256). • `GNRL_EA_PARAM_2` az objektum neve. • `GNRL_EA_PARAM_5`: a fenyegetés neve a Kaspersky besorolása szerint, pl. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` a munkamenet felhasználójának neve. • `GNRL_EA_PARAM_8`: a fenyegetés típusa (`típus`). • `GNRL_EA_PARAM_9` további információ az észlelt objektumról: Alkalmazásösszetevő (`engine`). Fenyegetésészlelő technológia (`method`). A Kaspersky Private Security Network által észlelt fenyegetés (`blacklist`): `true` vagy `false`. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Keyboard authorization error

Státusz	⚠
Összetevő	BadUSB védelem
Windows eseményazonosító	`2052`
Kaspersky Security Center eseményazonosító	`00000804`
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The object scan result has been sent to a third-party application

Státusz	⚠
Összetevő	AMSI védelem
Windows eseményazonosító	`1512`

Kaspersky Security Center eseményazonosító	GNRL_EV_OBJECT_REPORTED
Esemény paraméterei	• GNRL_EA_PARAM_1 az objektum kivonata (SHA256). • GNRL_EA_PARAM_2 az objektum neve. • GNRL_EA_PARAM_5: a fenyegetés neve a Kaspersky besorolása szerint, pl. EICAR-Test-File. • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_8: a fenyegetés típusa (típus). • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Kaspersky Private Security Network által észlelt fenyegetés (blacklist): true vagy false. EDR verzió. Fenyegetés azonosítója az EDR-ben. Az objektum MD5-üzenetkivonata.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Task settings applied successfully

Státusz	⚠
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	708
Kaspersky Security Center eseményazonosító	000002c4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Warning about undesirable content (local bases)

Státusz	⚠
Összetevő	Webfelügyelő
Windows eseményazonosító	708
Kaspersky Security Center eseményazonosító	GNRL_EV_WEB_URL_WARNING
Esemény paraméterei	• GNRL_EA_PARAM_1 az URL. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a Web Control szabály neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Warning about undesirable content (KSN)

Státusz	⚠
Összetevő	Webfelügyelő
Windows eseményazonosító	708
Kaspersky Security Center eseményazonosító	GNRL_EV_WEB_URL_WARNING
Esemény paraméterei	• GNRL_EA_PARAM_1 az URL. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a Web Control szabály neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Undesirable content was accessed after a warning

Státusz	⚠
Összetevő	Webfelügyelő
Windows eseményazonosító	754
Kaspersky Security Center eseményazonosító	000002f2
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Temporary access to the device activated

Státusz	⚠
Összetevő	Eszközfelügyelő
Windows eseményazonosító	803
Kaspersky Security Center eseményazonosító	000002f2
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Operation canceled by the user

Státusz	⚠
Összetevő	Frissítés
Windows eseményazonosító	1016
Kaspersky Security Center eseményazonosító	000003f8
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

User has opted out of the encryption policy

Státusz	⚠
Összetevő	Adattitkosítás
Windows eseményazonosító	1306
Kaspersky Security Center eseményazonosító	0000051a
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Interrupted applying file encryption / decryption rules

Státusz	⚠
Összetevő	Adattitkosítás
Windows eseményazonosító	903
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File encryption / decryption interrupted

Státusz	⚠
Összetevő	Adattitkosítás
Windows eseményazonosító	914
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device encryption / decryption interrupted

Státusz	⚠
Összetevő	Adattitkosítás
Windows eseményazonosító	1303
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image

Státusz	⚠
Összetevő	Adattitkosítás
Windows eseményazonosító	1345
Kaspersky Security Center eseményazonosító	00000541
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Module signature check failed

Státusz	⚠
Összetevő	Rendszerintegritás ellenőrzése
Windows eseményazonosító	2002
Kaspersky Security Center eseményazonosító	000007d2
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application startup was blocked

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2105
Kaspersky Security Center eseményazonosító	00000839
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Document opening was blocked

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2106
Kaspersky Security Center eseményazonosító	0000083a
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2112
Kaspersky Security Center eseményazonosító	00000840
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2113
Kaspersky Security Center eseményazonosító	00000841
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2111
Kaspersky Security Center eseményazonosító	0000083f
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2110
Kaspersky Security Center eseményazonosító	0000083e
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by the administrator

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2109
Kaspersky Security Center eseményazonosító	0000083d
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network activity of all third-party applications is blocked

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2107
Kaspersky Security Center eseményazonosító	0000083b
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network activity of all third-party applications is unblocked

Státusz	⚠
Összetevő	Végponti szenzor
Windows eseményazonosító	2108
Kaspersky Security Center eseményazonosító	0000083c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object will be deleted after restart (Sandbox)

Státusz	⚠
Összetevő	Sandbox
Windows eseményazonosító	2605
Kaspersky Security Center eseményazonosító	00000a2d
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Total size of scan tasks exceeded the limit

Státusz	⚠
Összetevő	Sandbox
Windows eseményazonosító	2612
Kaspersky Security Center eseményazonosító	00000a34
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object startup allowed, event logged

Státusz	⚠
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2553
Kaspersky Security Center eseményazonosító	000009fa
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Process startup allowed, event logged

Státusz	⚠
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2554
Kaspersky Security Center eseményazonosító	000009f8
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object will be deleted after restart (Endpoint Detection and Response)

Státusz	⚠
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2558
Kaspersky Security Center eseményazonosító	000009fe
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network isolation

Státusz	⚠
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2700
Kaspersky Security Center eseményazonosító	00000a8c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Termination of network isolation

Státusz	⚠
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2701
Kaspersky Security Center eseményazonosító	00000a8d
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Restart required to complete the task

Státusz	⚠
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	225
Kaspersky Security Center eseményazonosító	0000057b
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application startup blockage message to administrator

Státusz	⚠
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	503
Kaspersky Security Center eseményazonosító	GNRL_EV_AC_USER_REQUEST
Esemény paraméterei	• GNRL_EA_DESCRIPTION: az üzenet a felhasználónak. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_6 az alkalmazás futtatható fájljának neve (például chrome.exe). • GNRL_EA_PARAM_7 a futtatható fájl elérési útja. • GNRL_EA_PARAM_8 az objektum kivonata (SHA256). • GNRL_EA_PARAM_9 a felhasználó által futtatni kívánt alkalmazás verziója.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Device access blockage message to administrator

Státusz	⚠
Összetevő	Eszközfelügyelő
Windows eseményazonosító	804
Kaspersky Security Center eseményazonosító	GNRL_EV_DC_USER_REQUEST
Esemény paraméterei	• c_er_descr: az üzenet a felhasználónak. • GNRL_EA_PARAM_1 a hardverazonosító (HWID). • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Web page access blockage message to administrator

Státusz	⚠
Összetevő	Webfelügyelő
Windows eseményazonosító	755
Kaspersky Security Center eseményazonosító	GNRL_EV_WC_USER_REQUEST
Esemény paraméterei	• GNRL_EA_DESCRIPTION: az üzenet a felhasználónak. • GNRL_EA_PARAM_1 az URL. • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Device connection blocked

Státusz	⚠
Összetevő	Eszközfelügyelő
Windows eseményazonosító	807
Kaspersky Security Center eseményazonosító	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Esemény paraméterei	• GNRL_EA_PARAM_1 a hardverazonosító (HWID). • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application activity blockage message to administrator

Státusz	⚠
Összetevő	Fájlintegritás-figyelő
Windows eseményazonosító	2901
Kaspersky Security Center eseményazonosító	00000b55
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Státusz	⚠
Összetevő	Fájlintegritás-figyelő
Windows eseményazonosító	2900
Kaspersky Security Center eseményazonosító	00000b54
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Státusz	⚠
Összetevő	Adaptív Anomáliafelügyelő
Windows eseményazonosító	503
Kaspersky Security Center eseményazonosító	GNRL_EV_ADSEC_USER_REQUEST
Esemény paraméterei	• GNRL_EA_DESCRIPTION: az üzenet a felhasználónak. • GNRL_EA_PARAM_1: az Adaptív Anomáliafelügyeleti szabály neve. • GNRL_EA_PARAM_2: a heurisztikai szabály azonosítója. • GNRL_EA_PARAM_3 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_4: a forrásfolyamat. • GNRL_EA_PARAM_5: a forrásobjektum. • GNRL_EA_PARAM_6: a célfolyamat. • GNRL_EA_PARAM_7: a célobjektum. • GNRL_EA_PARAM_8 további információ az észlelt objektumról: A forrásfolyamat/-objektum és a célfolyamat/-objektum ellenőrző összegei. Folyamat blokkolva (verdict_type): true vagy false. Felhasználó biztonsági azonosítója (SID).
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Starting the cloud service client application is blocked

Státusz	⚠
Összetevő	Cloud Discovery
Windows eseményazonosító	2212
Kaspersky Security Center eseményazonosító	000008a4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Access to the cloud service is blocked

Státusz	⚠
Összetevő	Cloud Discovery
Windows eseményazonosító	2213
Kaspersky Security Center eseményazonosító	000008a5
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File or folder change was detected

Státusz	ⓘ / ⚠ / ⓔ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2950
Kaspersky Security Center eseményazonosító	00000b86
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Object changes too often. Event aggregation started

Státusz	ⓘ / ⚠ / ⓔ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2955
Kaspersky Security Center eseményazonosító	00000b8b
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Report on object modification for the aggregation period

Státusz	ⓘ / ⚠ / ⓔ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2956
Kaspersky Security Center eseményazonosító	00000b8c
Windows eseménynapló (alapértelmezett)	–

Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Registry change was detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2951
Kaspersky Security Center eseményazonosító	00000b87
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Device connection / disconnection is detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2952
Kaspersky Security Center eseményazonosító	00000b88
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

A figyelési hatókör helytelen objektumokat tartalmaz

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2903
Kaspersky Security Center eseményazonosító	00000b89
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

The prohibited operation was allowed in test mode

Státusz	⚠
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2961
Kaspersky Security Center eseményazonosító	00000b91
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Nem lehet csatlakozni az integrációs kiszolgálóhoz több mint 30 perce. Ellenőrizze az integrációs kiszolgáló állapotát és hálózati beállításait

Státusz	⚠
Összetevő	Light Agent
Windows eseményazonosító	3102
Kaspersky Security Center eseményazonosító	00000c1e
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Nem lehet csatlakozni az integrációs kiszolgálóhoz. Ellenőrizze az integrációs kiszolgáló állapotát és hálózati beállításait

Státusz	⚠
Összetevő	Light Agent
Windows eseményazonosító	3101
Kaspersky Security Center eseményazonosító	00000c1d
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

A virtuális gép sablonja frissítést igényel

Státusz	⚠
Összetevő	Light Agent
Windows eseményazonosító	3181
Kaspersky Security Center eseményazonosító	00000c6d
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The Standard license is terminated. The application is running under the Enterprise license

Státusz	⚠
Összetevő	Light Agent
Windows eseményazonosító	3171
Kaspersky Security Center eseményazonosító	00000c64
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Információs üzenet

Application started

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	235
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Application stopped

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	236
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Self-Defense restricted access to the protected resource

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	213
Kaspersky Security Center eseményazonosító	000000d5
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Report cleared

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	217
Kaspersky Security Center eseményazonosító	000000d9
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Group policy disabled

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	220

Kaspersky Security Center eseményazonosító	000000dc
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Application settings changed

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	218
Kaspersky Security Center eseményazonosító	000000da
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Task started

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	221
Kaspersky Security Center eseményazonosító	000000dd
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Task completed

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	223
Kaspersky Security Center eseményazonosító	000000df
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

All application components that are defined by the license have been installed and run in normal mode

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	227
Kaspersky Security Center eseményazonosító	000000e3
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Subscription settings have changed

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	238

Kaspersky Security Center eseményazonosító	000000ee
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Subscription has been renewed

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	239
Kaspersky Security Center eseményazonosító	000000ef
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object restored from Backup

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	335
Kaspersky Security Center eseményazonosító	0000014f
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

User name and password input

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2000
Kaspersky Security Center eseményazonosító	000007d0
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Participation in KSN enabled

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2020
Kaspersky Security Center eseményazonosító	000007e4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

KSN servers available

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2022

Kaspersky Security Center eseményazonosító	000007e6
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The application works and processes data under relevant laws and uses the appropriate infrastructure

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2024
Kaspersky Security Center eseményazonosító	000007e8
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object restored from Quarantine

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	345
Kaspersky Security Center eseményazonosító	00000159
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object deleted from Quarantine

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	347
Kaspersky Security Center eseményazonosító	0000015b
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

A backup copy of the object was created

Státusz	ⓘ
Összetevő	Fájl védelem Levelezés védelem Viselkedésészlelés Anti-Cryptor Behatolásmegelőző rendszer Sandbox Kártevő vizsgálata
Windows eseményazonosító	308
Kaspersky Security Center eseményazonosító	00000134
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Overwritten by a copy that was disinfected earlier

Státusz	
Összetevő	Fájl védelem Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	327
Kaspersky Security Center eseményazonosító	00000147
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Password-protected archive detected

Státusz	
Összetevő	Fájl védelem Web védelem Levelezés védelem AMSI védelem Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	322
Kaspersky Security Center eseményazonosító	GNRL_EV_PASSWD_ARCHIVE_FOUND
Esemény paraméterei	• GNRL_EA_PARAM_2 az objektum neve. • GNRL_EA_PARAM_3 az objektum létrehozásának dátuma (nem kötelező). • GNRL_EA_PARAM_7 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_9 további információ az észlelt objektumról: Alkalmazásösszetevő (engine). Fenyegetésészlelő technológia (method). A Privát KSN által észlelt fenyegetés (tiltólista): true vagy false.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Information about detected object

Státusz	
Összetevő	Fájl védelem Web védelem Levelezés védelem AMSI védelem Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	332
Kaspersky Security Center eseményazonosító	0000014c
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The object is in the Kaspersky Private Security Network allowlist

Státusz	
Összetevő	Fájl védelem Web védelem Levelezés védelem AMSI védelem Behatolásmegelőző rendszer Kártevő vizsgálata
Windows eseményazonosító	340

Kaspersky Security Center eseményazonosító	00000154
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object renamed

Státusz	ⓘ
Összetevő	Levelezés védelem Biztonsági rések kihasználásának megelőzése Viselkedéselemzés Anti-Cryptor Kártevő vizsgálata
Windows eseményazonosító	329
Kaspersky Security Center eseményazonosító	00000149
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object processed

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer Fájl védelem Web védelem Levelezés védelem Kártevő vizsgálata
Windows eseményazonosító	301
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Object skipped

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer Fájl védelem AMSI védelem Kártevő vizsgálata
Windows eseményazonosító	315
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Archive detected

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer Fájl védelem Web védelem Levelezés védelem AMSI védelem Kártevő vizsgálata
Windows eseményazonosító	318

Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Packed object detected

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer Fájl védelem Web védelem Levelezés védelem AMSI védelem Kártevő vizsgálata
Windows eseményazonosító	319
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Link processed

Státusz	ⓘ
Összetevő	Web védelem
Windows eseményazonosító	361
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Application startup allowed

Státusz	ⓘ
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	701
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Update source is selected

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1001
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Proxykiszolgáló kijelölve

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1002
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

The link is in the Kaspersky Private Security Network allowlist

Státusz	ⓘ
Összetevő	Web védelem
Windows eseményazonosító	370
Kaspersky Security Center eseményazonosító	00000172
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application placed in the trusted group

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer
Windows eseményazonosító	401
Kaspersky Security Center eseményazonosító	00000191
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application placed in restricted group

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer
Windows eseményazonosító	402
Kaspersky Security Center eseményazonosító	00000192
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Host Intrusion Prevention was triggered

Státusz	ⓘ
Összetevő	Behatolásmegelőző rendszer
Windows eseményazonosító	403
Kaspersky Security Center eseményazonosító	00000193
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File restored

Státusz	ⓘ
Összetevő	Viselkedésészlelés Anti-Cryptor Biztonsági rések kihasználásának megelőzése Behatolásmegelőző rendszer
Windows eseményazonosító	457
Kaspersky Security Center eseményazonosító	000001c9
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Registry value restored

Státusz	ⓘ
Összetevő	Viselkedésészlelés Biztonsági rések kihasználásának megelőzése
Windows eseményazonosító	458
Kaspersky Security Center eseményazonosító	000001ca
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Registry value deleted

Státusz	ⓘ
Összetevő	Viselkedésészlelés Biztonsági rések kihasználásának megelőzése
Windows eseményazonosító	459
Kaspersky Security Center eseményazonosító	000001cb
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Process action skipped

Státusz	ⓘ
Összetevő	Adaptív Anomáliafelügyelő
Windows eseményazonosító	2201
Kaspersky Security Center eseményazonosító	GNRL_EV_ADSEC_DETECT
Esemény paraméterei	• GNRL_EA_PARAM_1: az Adaptív Anomáliafelügyeleti szabály neve. • GNRL_EA_PARAM_2: a heurisztikai szabály azonosítója. • GNRL_EA_PARAM_3 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_4: a forrásfolyamat. • GNRL_EA_PARAM_5: a forrásobjektum. • GNRL_EA_PARAM_6: a célfolyamat. • GNRL_EA_PARAM_7: a célobjektum. • GNRL_EA_PARAM_8 további információ az észlelt objektumról: A forrásfolyamat/-objektum és a célfolyamat/-objektum ellenőrző összegei. Folyamat blokkolva (verdict_type): true vagy false. Felhasználó biztonsági azonosítója (SID).
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Keyboard authorized

Státusz	ⓘ
Összetevő	BadUSB védelem
Windows eseményazonosító	2050
Kaspersky Security Center eseményazonosító	00000802
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Network activity allowed

Státusz	ⓘ
Összetevő	Tűzfal
Windows eseményazonosító	601
Kaspersky Security Center eseményazonosító	00000259
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Application startup prohibited in test mode

Státusz	ⓘ
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	703
Kaspersky Security Center eseményazonosító	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Esemény paraméterei	• GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a kategória manuálisan létrehozott azonosítója. • GNRL_EA_PARAM_4 a fiók biztonsági azonosítója (SID). • GNRL_EA_PARAM_5 az alkalmazás digitális aláírására vonatkozó információ. • GNRL_EA_PARAM_6 az alkalmazás futtatható fájljának neve (például chrome.exe). • GNRL_EA_PARAM_7 a futtatható fájl elérési útja. • GNRL_EA_PARAM_8 az objektum kivonata (SHA256). • GNRL_EA_PARAM_9 a felhasználó által futtatni kívánt alkalmazás verziója.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application startup allowed in test mode

Státusz	ⓘ
Összetevő	Alkalmazásfelügyelő
Windows eseményazonosító	704
Kaspersky Security Center eseményazonosító	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Esemény paraméterei	• GNRL_EA_PARAM_2 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_3 a kategória manuálisan létrehozott azonosítója. • GNRL_EA_PARAM_4 a fiók biztonsági azonosítója (SID). • GNRL_EA_PARAM_5 az alkalmazás digitális aláírására vonatkozó információ.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

A page that is allowed was opened

Státusz	ⓘ
Összetevő	Webfelügyelő
Windows eseményazonosító	751
Kaspersky Security Center eseményazonosító	000002f4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Operation with the device allowed

Státusz	ⓘ
Összetevő	Eszközfelügyelő
Windows eseményazonosító	801
Kaspersky Security Center eseményazonosító	00000321
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File operation performed

Státusz	ⓘ
Összetevő	Eszközfelügyelő
Windows eseményazonosító	808
Kaspersky Security Center eseményazonosító	GNRL_EV_USB_FILE_OPERATION
Esemény paraméterei	• GNRL_EA_PARAM_1: a fájlművelet (írás vagy törlés). • GNRL_EA_PARAM_2: a fájl elérési útja. • GNRL_EA_PARAM_3: az eszköz neve. • GNRL_EA_PARAM_4 a munkamenet felhasználójának neve. • GNRL_EA_PARAM_5 a hardverazonosító (HWID).
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

No available updates

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1020
Kaspersky Security Center eseményazonosító	000003fc
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Update distribution completed successfully

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1022
Kaspersky Security Center eseményazonosító	000003fe

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Downloading files

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1003
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File downloaded

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1004
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File installed

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1005
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File updated

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1006
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File rolled back due to update error

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1007
Kaspersky Security Center eseményazonosító	–

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Updating files

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1008
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Distributing updates

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1009
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Rolling back files

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1010
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Creating the list of files to download

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	1013
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Downloading patches

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2150
Kaspersky Security Center eseményazonosító	–

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Installing patch

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2151
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Patch installed

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2152
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Rolling back patch

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2154
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Patch rolled back

Státusz	ⓘ
Összetevő	Frissítés
Windows eseményazonosító	2155
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Started applying file encryption / decryption rules

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	901
Kaspersky Security Center eseményazonosító	00000385

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Finished applying file encryption / decryption rules

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	902
Kaspersky Security Center eseményazonosító	00000386
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Resumed applying file encryption / decryption rules

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	905
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File encryption / decryption started

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	910
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File encryption / decryption completed

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	911
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

File has not been encrypted because it is an exclusion

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	913
Kaspersky Security Center eseményazonosító	–

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Portable mode enabled

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	950
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Portable mode disabled

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	952
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device encryption / decryption started

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1301
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device encryption / decryption completed

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1302
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device encryption / decryption resumed

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1304
Kaspersky Security Center eseményazonosító	–

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device is not encrypted

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1307
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device encryption / decryption process has been switched to active mode

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1308
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Device encryption / decryption process has been switched to passive mode

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1309
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Encryption module loaded

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1310
Kaspersky Security Center eseményazonosító	0000051e
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

New Authentication Agent account created

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1330
Kaspersky Security Center eseményazonosító	00000532

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Authentication Agent account deleted

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1331
Kaspersky Security Center eseményazonosító	00000533
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Authentication Agent account password changed

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1332
Kaspersky Security Center eseményazonosító	00000534
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Successful Authentication Agent login

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1333
Kaspersky Security Center eseményazonosító	00000535
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Failed Authentication Agent login attempt

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1334
Kaspersky Security Center eseményazonosító	00000536
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Hard drive accessed using the procedure of requesting access to encrypted devices

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1335
Kaspersky Security Center eseményazonosító	00000537

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1336
Kaspersky Security Center eseményazonosító	00000538
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Account was not added. This account already exists

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1337
Kaspersky Security Center eseményazonosító	00000539
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Account was not modified. This account does not exist

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1338
Kaspersky Security Center eseményazonosító	0000053a
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Account was not deleted. This account does not exist

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1339
Kaspersky Security Center eseményazonosító	0000053b
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

FDE upgrade successful

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1341
Kaspersky Security Center eseményazonosító	0000053d

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

FDE upgrade rollback successful

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1343
Kaspersky Security Center eseményazonosító	0000053f
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1346
Kaspersky Security Center eseményazonosító	00000542
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

BitLocker recovery key was changed

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1370
Kaspersky Security Center eseményazonosító	0000055a
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

BitLocker password / PIN was changed

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1371
Kaspersky Security Center eseményazonosító	0000055b
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

BitLocker recovery key was saved to a removable drive

Státusz	ⓘ
Összetevő	Adattitkosítás
Windows eseményazonosító	1372
Kaspersky Security Center eseményazonosító	0000055c

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive

Státusz	ⓘ
Összetevő	Végponti szenzor
Windows eseményazonosító	2103
Kaspersky Security Center eseményazonosító	00000837
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Endpoint Sensor connected to server

Státusz	ⓘ
Összetevő	Végponti szenzor
Windows eseményazonosító	2101
Kaspersky Security Center eseményazonosító	00000835
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Connection to the Kaspersky Anti Targeted Attack Platform server restored

Státusz	ⓘ
Összetevő	Végponti szenzor
Windows eseményazonosító	2102
Kaspersky Security Center eseményazonosító	00000836
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed

Státusz	ⓘ
Összetevő	Végponti szenzor
Windows eseményazonosító	2104
Kaspersky Security Center eseményazonosító	00000838
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object deleted

Státusz	ⓘ
Összetevő	Adatok törlése
Windows eseményazonosító	2251
Kaspersky Security Center eseményazonosító	000008cb

Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Wipe task statistics

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises)
Windows eseményazonosító	2853
Kaspersky Security Center eseményazonosító	00000b25
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Státusz	ⓘ
Összetevő	Adatok törlése
Windows eseményazonosító	2253
Kaspersky Security Center eseményazonosító	000008cd
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object quarantined (Sandbox)

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2602
Kaspersky Security Center eseményazonosító	00000a2a
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object deleted (Sandbox)

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2604
Kaspersky Security Center eseményazonosító	00000a2c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

IOC Scan started

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2652
Kaspersky Security Center eseményazonosító	00000a5c
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

IOC Scan completed

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2653
Kaspersky Security Center eseményazonosító	00000a5d
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object quarantined (Endpoint Detection and Response)

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2555
Kaspersky Security Center eseményazonosító	000009fb
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Object deleted (Endpoint Detection and Response)

Státusz	ⓘ
Összetevő	Endpoint Detection and Response
Windows eseményazonosító	2557
Kaspersky Security Center eseményazonosító	000009fd
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Application components successfully changed

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	1402
Kaspersky Security Center eseményazonosító	0000057a
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2606
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2609
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2610
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2616
Kaspersky Security Center eseményazonosító	–
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	–

A felügyeleti kiszolgáló, amelyhez az eszköz csatlakozik, megbízhatónak van beállítva

Státusz	ⓘ
Összetevő	Felügyeleti kiszolgálói kapcsolat védelme
Windows eseményazonosító	3300
Kaspersky Security Center eseményazonosító	00000ce4
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az eszköz egy új, megbízható felügyeleti kiszolgálóhoz csatlakozik

Státusz	ⓘ
Összetevő	Felügyeleti kiszolgálói kapcsolat védelme
Windows eseményazonosító	3302
Kaspersky Security Center eseményazonosító	00000ce6
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

A felügyeleti kiszolgáló, amelyhez az eszköz csatlakozik, már nem megbízhatónak van beállítva

Státusz	ⓘ
Összetevő	Felügyeleti kiszolgálói kapcsolat védelme
Windows eseményazonosító	3303

Kaspersky Security Center eseményazonosító	00000ce7
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Asynchronous Sandbox detection

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2619
Kaspersky Security Center eseményazonosító	GNRL_EV_APP_INCIDENT_OCCURED
Esemény paraméterei	• GNRL_EA_PARAM_1 a Sandbox összetevőinek paraméterei. • GNRL_EA_PARAM_2: az objektum elérési útja. • GNRL_EA_PARAM_3: az incidens azonosítója. • GNRL_EA_PARAM_4 az objektum kivonata (SHA256).
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

The scan task has been successfully sent to Sandbox by a user

Státusz	ⓘ
Összetevő	Sandbox
Windows eseményazonosító	2622
Kaspersky Security Center eseményazonosító	00000a3e
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Device is connected

Státusz	ⓘ
Összetevő	Eszközfelügyelő
Windows eseményazonosító	805
Kaspersky Security Center eseményazonosító	GNRL_EV_DEVCTRL_DEV_PLUGGED
Esemény paraméterei	• GNRL_EA_PARAM_1 a hardverazonosító (HWID). • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Device is disconnected

Státusz	ⓘ
Összetevő	Eszközfelügyelő
Windows eseményazonosító	806
Kaspersky Security Center eseményazonosító	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Esemény paraméterei	• GNRL_EA_PARAM_1 a hardverazonosító (HWID). • GNRL_EA_PARAM_2 a munkamenet felhasználójának neve.
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Error removing the previous version of the application

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	246
Kaspersky Security Center eseményazonosító	000000f6
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Successful connection to the EDR Expert server

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises)
Windows eseményazonosító	2853
Kaspersky Security Center eseményazonosító	00000b25
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Sikeres csatlakozás az EDR Expert válaszkiszolgálóhoz

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	2853
Kaspersky Security Center eseményazonosító	00000b25
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Sikeres csatlakozás az EDR Expert telemetriai adatgyűjtő kiszolgálóhoz

Státusz	ⓘ
Összetevő	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows eseményazonosító	2857
Kaspersky Security Center eseményazonosító	00000b26
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Sikeres kapcsolat az NDR-kiszolgálóval

Státusz	ⓘ
Összetevő	Network Detection and Response (KATA)
Windows eseményazonosító	3083
Kaspersky Security Center eseményazonosító	00000c0b

Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Starting the cloud service client application is allowed

Státusz	ⓘ
Összetevő	Cloud Discovery
Windows eseményazonosító	2210
Kaspersky Security Center eseményazonosító	000008a2
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Access to the cloud service is allowed

Státusz	ⓘ
Összetevő	Cloud Discovery
Windows eseményazonosító	2211
Kaspersky Security Center eseményazonosító	000008a3
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Hozzáférés a védett területhez

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	2004
Kaspersky Security Center eseményazonosító	000007d4
Windows eseménynapló (alapértelmezett)	✓
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

File or folder change was detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2950
Kaspersky Security Center eseményazonosító	00000b86
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Object changes too often. Event aggregation started

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2955
Kaspersky Security Center eseményazonosító	00000b8b
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Report on object modification for the aggregation period

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2956
Kaspersky Security Center eseményazonosító	00000b8c
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Registry change was detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2951
Kaspersky Security Center eseményazonosító	00000b87
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Device connection / disconnection is detected

Státusz	ⓘ / ⚠ / ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2952
Kaspersky Security Center eseményazonosító	00000b88
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

A figyelési hatókör helytelen objektumokat tartalmaz

Státusz	ⓘ / ⚠ / !
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2903
Kaspersky Security Center eseményazonosító	00000b89
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Baseline created

Státusz	ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2957
Kaspersky Security Center eseményazonosító	00000b8d
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Baseline updated

Státusz	ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2958
Kaspersky Security Center eseményazonosító	00000b8e
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

An operation is performed by the trusted user

Státusz	ⓘ
Összetevő	Rendszerintegritás-figyelő
Windows eseményazonosító	2962
Kaspersky Security Center eseményazonosító	00000b92
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Az esemény megőrzési idejének konfigurálásához nyissa meg a házirend **Event configuration** szakaszát, és állítsa be az általános rendszerintegritás-felügyeleti esemény – *File or folder change was detected*.

Connected to SVM

Státusz	ⓘ
Összetevő	Light Agent

Windows eseményazonosító	3152
Kaspersky Security Center eseményazonosító	00000c50
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

A new temporary password was created

Státusz	ⓘ
Összetevő	Rendszer-felülvizsgálat
Windows eseményazonosító	265
Kaspersky Security Center eseményazonosító	00000109
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Connected to the Integration Server

Státusz	ⓘ
Összetevő	Light Agent
Windows eseményazonosító	3105
Kaspersky Security Center eseményazonosító	00000c21
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Restoring connection to the Integration Server

Státusz	ⓘ
Összetevő	Light Agent
Windows eseményazonosító	3104
Kaspersky Security Center eseményazonosító	00000c20
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

Sikeres kapcsolat az KUMA-kiszolgálóval

Státusz	ⓘ
Összetevő	KUMA integráció
Windows eseményazonosító	2857
Kaspersky Security Center eseményazonosító	00000b29
Windows eseménynapló (alapértelmezett)	–
Kaspersky Security Center eseménynapló (alapértelmezett)	✓

7. melléklet Támogatott fájlkiterjesztések a végrehajtás megelőzéséhez

A Kaspersky Endpoint Security támogatja az Office-formátumú fájlok megnyitásának megakadályozását bizonyos alkalmazásokban. A támogatott fájlkiterjesztésekkel és alkalmazásokkal kapcsolatos információkat a következő táblázat tartalmazza.

Támogatott fájlkiterjesztések a végrehajtás megelőzéséhez

Alkalmazásnév	Futtatható fájl	Fájlkiterjesztés
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Alkalmazásnév	Futtatható fájl	Fájlkiterjesztés
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

8. melléklet Támogatott szkript értelmezők a végrehajtás megelőzéséhez

A végrehajtás megelőzése a következő szkriptértelmezőket támogatja:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

A végrehajtás megakadályozása támogatja a Java-alkalmazásokkal való munkát a Java-futtatókörnyezetben (java.exe és javaw.exe folyamatok).

9. melléklet IOC vizsgálat hatóköre a rendszerleíró adatbázisban (RegistryItem)

Amikor hozzáadja a **Windows registry - RegistryItem** adattípust az IOC vizsgálat hatóköréhez, a Kaspersky Endpoint Security a következő beállításkulcsokat vizsgálja alapértelmezés szerint:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

10. melléklet IOC-fájl követelményei

Az IOC vizsgálati feladatok létrehozásakor vegye figyelembe az IOC-fájlra vonatkozó alábbi követelményeket és korlátozásokat:

- Az alkalmazás támogatja az IOC és XML kiterjesztésű, illetve a nyílt szabványú OpenIOC 1.0 és 1.1 verzióinak megfelelő IOC-fájlokat a biztonsági sérülési indikátorok leírására.
- Az IOC-fájlok feltöltése után manuálisan szerkesztheti a fájlokat a beépített szerkesztőben közvetlenül a feladat tulajdonságaiban. A Kaspersky Endpoint Security az OpenIOC 1.1 szabványnak megfelelő IOC-fájlok szerkesztését támogatja. Az OpenIOC 1.0 verziójával kompatibilis IOC fájlok tartalma nem módosítható.
- Ha az *IOC Scan* feladat parancssori létrehozása során olyan IOC-fájlokat tölt fel, amelyek közül néhány nem támogatott, a feladat futtatásakor az alkalmazás csak a támogatott IOC-fájlokat használja. Ha az *IOC Scan* feladat parancssori létrehozása során a feltöltött IOC-fájlok mindegyike nem támogatottnak bizonyul, a feladat továbbra is futtatható, de nem fogja észlelni a biztonsági sérülési indikátorokat. Nem támogatott IOC-fájlok feltöltése a Web Console vagy a Cloud Console segítségével nem lehetséges.

- A szemantikai hibák és a nem támogatott IOC-kifejezések és -címkék az IOC-fájlokban nem okoznak sikertelen feladatvégrehajtást. Az IOC-fájlok ilyen szakaszaiban az alkalmazás nem észlel egyezést.
- Az egy IOC vizsgálati feladatban használt összes IOC-fájl azonosítójának egyedinek kell lennie. Ha ugyanolyan azonosítóval rendelkező IOC-fájlok vannak, az befolyásolhatja a feladatvégrehajtás eredményeit.
- Egy IOC-fájl mérete nem haladhatja meg a 2 MB-ot. Nagyobb fájlok használata az IOC vizsgálati feladatok hibával történő leállását okozza. Az IOC-gyűjteményhez hozzáadott összes fájl teljes mérete nem haladhatja meg a 10 MB-ot. Ha az összes fájl teljes mérete meghaladja a 10 MB-ot, akkor fel kell osztania az IOC-gyűjteményt, és több *IOC Scan* feladatot kell létrehoznia.
- Fenyegetésenként egy IOC-fájlt ajánlott létrehozni. Ez megkönnyíti az *IOC Scan* feladat eredményeinek elemzését.

Az alábbi hivatkozásra kattintva letölthető fájl egy táblázatot tartalmaz az OpenIOC szabvány IOC-feltételeinek teljes listájával.

TÖLTSE LE AZ IOC_TERMS.XLSX FÁJLT

Az alkalmazás OpenIOC szabványt támogató jellemzőit és korlátait az alábbi táblázat mutatja be.

Az OpenIOC 1.0 és 1.1 verzió támogatási jellemzői és korlátai.

Támogatott feltételek	OpenIOC 1.0:
	
	`is`
	`isnot` (kivétel a halmazból)
	`contains`
	`containsnot` (kivétel a halmazból)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Az E-mail/* feltételek esetén csak a `contains` és `is` feltételek támogatottak. Ahhoz, hogy a Visszamenőleges IOC vizsgálat megfelelően működjön a `is` feltétellel, az IOC-fájlokban lévő e-mail-címeket a következő formátumban kell megadni: `"name@example.org" <SMTP:name@example.org>`. Az *IOC vizsgálat* feladat rendes futtatásához elegendő az e-mail-címet a következő formátumban megadni: `name@example.org`.

Támogatott feltételattribútumok	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Támogatott operátorok	`AND` `OR`
Támogatott adattípusok	`"date"`: dátum (alkalmazható feltételek: `is`, `greater-than`, `less-than`) `"int"`: egész szám (alkalmazható feltételek: `is`, `greater-than`, `less-than`) `"string"`: karakterlánc (alkalmazható feltételek: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: időtartam másodpercben (alkalmazható feltételek: `is`, `greater-than`, `less-than`)

Az adattípusok értelmezésének jellemzői	A `"boolean string"`, a `"restricted string"`, az `"md5"`, az `"IP"`, az `"sha256"` és a `"base64Binary"` adattípusok értelmezése karakterláncként történik.
	
	Az alkalmazás támogatja az `int` és a `date` adattípusokhoz tartozó `Content` beállítás értelmezését, ha az intervallum formájában van megadva:
	
	OpenIOC 1.0:
	A `TO` operátor használata a `Content` mezőben:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	A `greater-than` és a `less-than` feltételek
	A `TO` operátor használata a `Content` mezőben
	Az alkalmazás támogatja a `date` és a `duration` adattípusokat, ha a jelölők `ISO 8601, Zulu time zone, UTC` formátumban vannak beállítva.

Melléklet 11. Az EDR fenyegetésre adott válasz API-ja

A Kaspersky Endpoint Security 12.9 for Windows támogatja az EDR fenyegetésekre adott válaszműveleteket (EDR responses) a Kaspersky Security Center OpenAPI segítségével. Ez azt jelenti, hogy OpenAPI metódusokat hívhat az EDR fenyegetésekre adott válasz automatizálására Python használatával. Ezeket a metódusokat SIEM-megoldásokba integrálva hívhatja meg. A *Kaspersky Unified Monitoring and Analysis Platform* a Kaspersky SIEM megoldásaként támogatja az EDR Threat Response OpenAPI-ját a 3.4.1-es verziótól kezdődően. Például szkripteket, további információkat a KUMA dokumentációban talál.

Az EDR fenyegetésekre vonatkozó válaszműveletek végrehajtásához létre kell hoznia egy kérést, és el kell küldenie azt a KSC Open API (`AddIncident`) használatával. A kérés feldolgozása után egy speciális feladat jön létre a Kaspersky Security Center konzolon.

Ha az EDR fenyegetésekre reagálva szeretne feladatokat létrehozni, létre kell hoznia egy háttérkapcsolatot a felügyeleti kiszolgáló és a Kaspersky Security Center Web Console között. A háttérkapcsolati szolgáltatás a Kaspersky Security Center Windows 14.2 vagy újabb és a Kaspersky Security Center Linux 15.2 vagy újabb verziókban érhető el. Más konzolok, beleértve a Kaspersky Detection and Response megoldások konzoljait, nem támogatottak.

Az EDR fenyegetésre adott válaszhoz meg kell adnia az alapvető kérés paramétereit, például JSON formátumban:

- A `task` a feladat típusa (lásd alább).
- A `targetHost` annak a számítógépnek az azonosítója, amelyen a parancsfájlt futtatni kell. Szükséges argumentum. A szkript ezt az argumentumot az eseményből kapja.
- A `responseEventIncidentArea` a szkriptet futtató alkalmazás neve (például `KUMA`). Ez a paraméter hozzáadódik a létrehozott feladat nevéhez.

Az EDR fenyegetésre adott válasz konfigurálásához meg kell adnia a feladat beállításait JSON formátumban a `"KLINCDT_BODY": json.dumps(data)` paraméterben. Ennek eredményeként az alkalmazás létrehozza a `[Response][KUMA] <task type> - <Date> <Time> - <ID>` elemet a Kaspersky Security Center konzolon.

Kapcsolódás a Kaspersky Security Center OpenAPI-hoz

Az EDR fenyegetésre adott válasz részeként az alkalmazás speciális feladatokat hoz létre a Kaspersky Security Center konzolon. E feladatok végrehajtásához kapcsolatot kell létesíteni a számítógép és a Kaspersky Security Center között. Ehhez a Kaspersky Security Center kapcsolódási paramétereit meg kell adni a kérésben.

A Kaspersky XDR 2.1-es verziójában a kérések engedélyezési módja megváltozott. A Kaspersky XDR PAT tokeneket használ a felhasználónév és jelszó hitelesítése helyett. Ezért nem lehet parancsfájlokat futtatni a Kaspersky XDR alkalmazásban. Az engedélyezési kéréssel kapcsolatos további információkért tekintse meg a Kaspersky XDR súgóját.

A Kaspersky Security Center kapcsolódási paraméterei

Paraméter	Típus	Leírás
`kscHost`	`string`	A Kaspersky Security Center Administration Server címe. Szükséges paraméter.
`kscPort`	`int`	A Felügyeleti kiszolgálói kapcsolódási portja. Szükséges paraméter.
`kscCert`	`string`	A Kaspersky Security Center Administration Serverhez való csatlakozáshoz szükséges tanúsítványfájl elérési útja. Alapértelmezés szerint a paraméter `False` értékre van beállítva.
`kscUser`	`string`	Felhasználói fiók neve. Szükséges paraméter.
`kscPassword`	`string`	Felhasználói fiók jelszava. Szükséges paraméter.

Példa

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

A felhasználói fiókok adatai nem védettek, ezért külön felhasználót kell kijelölnie, amely csak ezeket a műveleteket végzi.

Fájl lekérése – getFile

A Fájl lekérése feladat beállításai

Paraméter	Típus	Leírás
`md5hash`	`string`	A lekérendő fájl MD5 kivonata.
`sha256hash`	`string`	A lekérendő fájl SHA256 kivonata.
`path`	`string`	A lekérendő fájl elérési útja.

Példa

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Fájl törlése– deleteFile

A Fájl törlése feladat beállításai

Paraméter	Típus	Leírás
`md5hash`	`string`	A törlendő fájl MD5 kivonata.
`sha256hash`	`string`	A törlendő fájl SHA256 kivonata.
`path`	`string`	A törlendő fájl elérési útja.
`searchInSubfolders?`	`boolean`	Keresse meg a törlendő fájlt az almappákban.

Példa

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Fájl áthelyezése a Karanténba – quarantineFile

A Fájl áthelyezése a Karanténba feladat beállításai

Paraméter	Típus	Leírás
`md5hash`	`string`	A karanténba helyezendő fájl MD5 kivonata.
`sha256hash`	`string`	A karanténba helyezendő fájl SHA256 kivonata.
`path`	`string`	A karanténba helyezendő fájl elérési útja.

Példa

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

IOC vizsgálat – iocScan

Az IOC vizsgálati feladat beállításai

Paraméter	Típus	Leírás
`ioc`	`string`	A vizsgálathoz használni kívánt IOC-fájlt tartalmazó ZIP-archívum elérési útja.
`isolateHost`	`boolean`	A fenyegetés továbbterjedésének megelőzéséhez válassza le a számítógépet a hálózatról, ha fertőzöttségi mutatót észlel.
`scanCriticalAreas`	`boolean`	Futtassa a *Kritikus területek vizsgálata* feladatot, ha fertőzöttségi mutatót észlel.
`quarantineObject`	`boolean`	Törölje a rosszindulatú objektumot, ha fertőzöttségi mutatót észlel. Az objektum törlése előtt a Kaspersky Endpoint Security biztonsági másolatot készít arra az esetre, ha az objektumot később vissza kell állítani. A Kaspersky Endpoint Security a biztonsági másolatot karanténba helyezi.

Példa

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Folyamat indítása – startProcess

A Folyamat indítása feladat beállításai

Paraméter	Típus	Leírás
executablePath	string	A folyamat indításához használandó futtatható fájl elérési útja.
arguments?	string	További parancssori argumentumok a folyamat indításához.
workingFolder?	string	A folyamat munkamappájának elérési útja.

Példa

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Folyamat megszakítása – terminateProcess

A Folyamat megszakítása feladat beállításai

Paraméter	Típus	Leírás
md5hash	string	Annak a fájlnak az MD5 kivonata, amelynek folyamatát meg akarja szakítani.
sha256hash	string	Annak a fájlnak az SHA256 kivonata, amelynek folyamatát meg akarja szakítani.
path	string	A törlendő fájl elérési útja.
caseSensitive	boolean	A kis- és nagybetűk különbözőek fájl keresésekor.

Példa

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Számítógép hálózatelkülönítése – isolateHost

A számítógép hálózatelkülönítési beállításai

Paraméter	Típus	Leírás
`action`	`string`	A Hálózatelkülönítés működési módja.

Példa

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Végrehajtás megelőzése – preventExecution

Végrehajtás-megelőzési beállítások

Paraméter	Típus	Leírás
`hash`	`string`	Annak a fájlnak az MD5 kivonata, amelynek futtatását meg akarja akadályozni.
`path`	`string`	Annak a fájlnak az elérési útja, amelynek futtatását meg akarja akadályozni.
`caseSensitive`	`boolean`	A kis- és nagybetűk különbözőek fájl keresésekor.

Példa

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Kártevő vizsgálata– onDemandScan

A Kártevő vizsgálata feladat beállításai

Paraméter	Típus	Leírás
`path`	`string`	A fájlok és mappák szóközzel tagolt listája az Egyéni vizsgálathoz.
`recursive`	`boolean`	Rekurzív vizsgálati mód.

Paraméter	Típus	Leírás
type	number	Vizsgálat hatóköre.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Példa

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Melléklet 12. Felhasználói fiókok az alkalmazásösszetevői szabályokban

Egyes alkalmazásösszetevők konfigurálásához speciális szabályokat kell megadni. Például a Webfelügyelő esetében hozzá kell adnia egy szabályt, amely tartalmazza azoknak a webcímeknek a listáját, amelyeket az alkalmazásnak blokkolnia kell. Az alkalmazásösszetevő szabályaiban ütemezést is beállíthat az összetevőhöz, vagy kiválaszthatja azokat a felhasználókat, akikre az alkalmazásnak alkalmaznia kell a szabályt.

Az alábbi alkalmazásösszetevők konfigurálásához szabályokat kell megadni:

- Alkalmazásfelügyelő.
- Webfelügyelő.
- Eszközfelügyelő.
- Naplóvizsgálat.
- Adaptív Anomáliafelügyelő.
- Rendszerintegritás-figyelő.

A Kaspersky Endpoint Security for Windows 12.5-től kezdve nemcsak az Active Directoryból, hanem a Kaspersky Security Center felhasználói listájából is kiválaszthatja a felhasználókat. A helyi felhasználói fiókok adatait manuálisan is megadhatja. Ez azt jelenti, hogy a következő módokon adhat hozzá felhasználókat:

- Active Directory (ajánlott)
- A Kaspersky Security Center felhasználóinak listája
- Helyi felhasználói fiók

Az összes felhasználókiválasztási módszer helyes használatához frissítenie kell a Kaspersky Endpoint Security alkalmazást és az adminisztrációs bővítményt a 12.5-ös vagy újabb verzióra.

A Kaspersky csak olyan különleges esetekben javasolja a helyi felhasználói fiókok használatát, amikor nem lehetséges tartományi felhasználói fiókok használata. A helyi fiókok használatának biztonsági kockázataival kapcsolatos részleteket a Microsoft Tudásbázisban találja. Ön viseli a teljes felelősséget a számítógép biztonságáért, ha helyi felhasználói fiókokat használ; ez különösen magában foglalja a Kaspersky Endpoint Security beállításaihoz való hozzáférés ellenőrzését és korlátozását.

Az alkalmazás a felhasználó SID-jét (biztonsági azonosítóját) használja a felhasználók azonosítására. Ha az Active Directoryból vagy a Kaspersky Security Center felhasználói listájáról származó felhasználói fiókokat használ, az alkalmazás meghatározza a SID azonosítót a felügyeleti kiszolgálón. Ez azt jelenti, hogy az alkalmazás nem terheli külön a számítógépet a felhasználó azonosításával. Ha 1000-nél több helyi felhasználói fiókot adott hozzá egy alkalmazásszabályhoz, az alkalmazások kapcsolatba lépnek a tartományvezérlővel a felhasználó azonosítása érdekében. Ez azt jelenti, hogy a számítógép terhelése megnő. A számítógép teljesítményére gyakorolt hatás optimalizálása céljából javasoljuk az Active Directoryból vagy a Kaspersky Security Center felhasználói listájából származó felhasználói fiókok használatát.

Az alkalmazás NetBIOS-neveket használ a manuálisan hozzáadott felhasználói fiókok azonosítására a `<username>` és `<hostname>\<username>` formátumokban. A NetBIOS-név legfeljebb 16 bájt (15 karakter) hosszú lehet. Ha a számítógép neve 15 karakternél hosszabb, az alkalmazás nem tudja azonosítani a felhasználót. Ekkor az alkalmazás letiltja a szabályt, és hibát generál, például *Web Control: rule triggering disabled for user accounts without matching security identifier (SID)*. A szabály működéséhez manuálisan kell lerövidítenie a számítógép nevét. Felhasználói fiókokat az Active Directoryból vagy a Kaspersky Security Centerből adhat hozzá. Ebben az esetben az alkalmazás automatikusan lerövidíti a számítógép nevét.

A Kaspersky Endpoint Security támogatja a szabályokba beépített felhasználókat és csoportokat is (például az „Összes” csoportot). A felhasználói SID meghatározási módja miatt az alkalmazás csak az Active Directoryból vagy a Kaspersky Security Center felhasználói listájából hozzáadott beépített felhasználói fiókok használatát teszi lehetővé. Nem működnek azok a szabályok, amelyekben a beépített felhasználói fiók helyileg van hozzáadva.

Jogi információk

Adatok feletti rendelkezés

Ez a rész információkat tartalmaz azokról az adatokról, amelyeket a Kaspersky Endpoint Security alkalmazás tárolhat az eszközön, és működése során automatikusan továbbíthat a Kaspersky-nek.

A kapott adatokat a Kaspersky a törvénynek és a Kaspersky vonatkozó követelményeinek és előírásainak megfelelően védi. Az adatok továbbítása titkosított kommunikációs csatornákon keresztül zajlik.

Az adatok feletti rendelkezés a Végfelhasználói licencszerződés szerint

Ha egy aktiváló kód használatával aktiválja a Kaspersky Endpoint Security-t, beleegyezik a következő információk automatikus továbbításába a Kaspersky számára, az alkalmazás megfelelő használatának hitelesítése céljából:

- Kaspersky Endpoint Security típus, verzió és változat;
- Kaspersky Endpoint Security feltelepített frissítéseinek verziói;
- A számítógép- és a számítógépre feltelepített Kaspersky Endpoint Security azonosítója;
- Sorozatszám és aktív kulcs-azonosító;
- Az operációs rendszer típusa, verziója és bitrátája, valamint a virtuális környezet neve (ha a Kaspersky Endpoint Security virtuális környezetbe van feltelepítve);
- egyedi kérésazonosító a Jogtulajdonos szolgáltatásainál;
- Az információ továbbítása közben aktív Kaspersky Endpoint Security összetevők azonosítói.

A Kaspersky is használhatja ezeket az információkat a Kaspersky szoftverek használatáról és terjesztéséről szóló statisztikák előállítása érdekében.

Aktiváló kód használatával beleegyezik a fent felsorolt adatok automatikus továbbításába. Ha nem egyezik bele ezen információ továbbításába a Kaspersky felé, kulcsfájlt kell használnia a Kaspersky Endpoint Security aktiválásához.

A Végfelhasználói licencszerződés elfogadásával beleegyez a következő információk automatikus továbbításába:

- Kaspersky Endpoint Security frissítése közben:
  - A Kaspersky Endpoint Security verziója;
  - A Kaspersky Endpoint Security azonosítója;
  - Aktív kulcs;

- A frissítés indításának egyedi azonosítója;
- A Kaspersky Endpoint Security telepítés egyedi azonosítója.

- Ha a Kaspersky Endpoint Security felületen lévő következő hivatkozások:
  - A Kaspersky Endpoint Security verziója;
  - Az operációs rendszer verziója;
  - A Kaspersky Endpoint Security aktiválásának dátuma;
  - licenc lejáratának dátuma;
  - A kulcs létrehozásának dátuma;
  - A Kaspersky Endpoint Security telepítésének dátuma;
  - A Kaspersky Endpoint Security azonosítója;
  - Az operációs rendszerben észlelt sebezhetőség azonosítója;
  - A Kaspersky Endpoint Security utolsó feltelepített frissítésének azonosítója;
  - Az észlelt fájl fenyegetésének ellenőrzőösszeg kódja, és neve a Kaspersky osztályozás alapján;
  - Kaspersky Endpoint Security aktiválási hibakategóriája;
  - Kaspersky Endpoint Security aktiválási hibakód;
  - A kulcs lejártáig hátralévő napok száma;
  - A kulcs hozzáadása óta eltelt napok száma;
  - A licenc lejárta óta eltelt napok száma;
  - Azon számítógépek száma, amelyeken az aktuális licenc alkalmazva van;
  - Aktív kulcs;
  - Kaspersky Endpoint Security licencfeltétel;
  - A licenc jelenlegi állapota;
  - Az aktuális licenc típusa;
  - Alkalmazástípus;
  - A frissítés indításának egyedi azonosítója;
  - A Kaspersky Endpoint Security számítógépre telepített példányának egyedi azonosítója;
  - A Kaspersky Endpoint Security felületének nyelve.

A kapott adatokat a Kaspersky a törvénynek és a Kaspersky vonatkozó követelményeinek és előírásainak megfelelően védi. Az adatok továbbítása titkosított kommunikációs csatornákon keresztül zajlik.

Olvassa el a Végfelhasználói licencszerződést és keresse fel a Kaspersky webhelyet, ha szeretné bővebben megismerni, hogyan kapjuk meg, dolgozzuk fel, tároljuk és semmisítjük meg az alkalmazás használatára vonatkozó adatokat, miután elfogadta a Végfelhasználói licencszerződést és beleegyezik a Kaspersky Security Network nyilatkozatba. A license.txt és ksn_<language ID>.txt fájlok tartalmazzák a Végfelhasználói licencszerződés és a Kaspersky Security Network nyilatkozat szövegét, valamint megtalálhatóak az alkalmazás terjesztőkészletben.

Az adatok feletti rendelkezés a Kaspersky Security Network használatakor

A Kaspersky Endpoint Security által a Kaspersky-nek küldött adatkészlet a licenc típusától és a Kaspersky Security Network használati beállításaitól függ.

A KSN használata licenc alapján legfeljebb 4 számítógépen

A Kaspersky Security Network nyilatkozat elfogadásával beleegyezik, a következő információk automatikus továbbításába:

- a KSN konfigurációs fájljainak frissítésére vonatkozó információk: az aktív konfiguráció azonosítója, a kapott konfiguráció azonosítója, a konfigurációs frissítés hibakódja;
- az ellenőrizendő fájlokkal és URL-címekkel kapcsolatos információk: az ellenőrzött fájl ellenőrzőösszegei (MD5, SHA2-256, SHA1) és a fájlminták (MD5), a minta mérete, az észlelt fenyegetés típusa és a Jogbirtokos besorolása szerinti megnevezése, a vírusadatbázisok azonosítója, az URL-cím, amelyhez a megbízhatóság ellenőrzését kérelmezték, illetve a hivatkozó URL-cím, a kapcsolat protokollazonosítója és a használt portok száma;
- a vizsgálati feladat azonosítója, amely a fenyegetést észlelte;
- a használt digitális tanúsítványok hitelességének ellenőrzéséhez szükséges információk: az ellenőrzött objektum megjelöléséhez használt tanúsítvány ellenőrzőösszegei (SHA256) és a tanúsítvány nyilvános kulcsa;
- A vizsgálatot végző szoftverösszetevő azonosítója;
- Az antivírus adatbázisok és ezen antivírus adatbázisok jelentéseinek azonosítói;
- a számítógépen lévő szoftver aktiválásának információi: az aktiválási szolgáltatástól kapott jegy aláírt fejléce (a regionális aktiválási központ azonosítója, az aktiválási kód ellenőrzőösszege, a jegy ellenőrzőösszege, a jegy létrehozási dátuma, a jegy egyedi azonosítója, a jegy verziója, a licenc állapota, a jegy érvényességének kezdési/befejezési dátuma és időpontja, a licenc egyedi azonosítója, a licenc verziója), a jegy fejlécének aláírására használt tanúsítvány azonosítója és a kulcsfájl ellenőrzőösszege (MD5);
- A jogtulajdonos szoftverének információi: teljes verzió, típus, a Kaspersky szolgáltatáshoz történő csatlakozáshoz használt protokoll verziója.

A KSN használata licenc alapján 5 vagy több számítógépen

A Kaspersky Security Network nyilatkozat elfogadásával beleegyezik, a következő információk automatikus továbbításába:

Ha a **Kaspersky Security Network** jelölőnégyzet be van jelölve, a **Kiterjesztett KSN mód engedélyezése** jelölőnégyzet pedig törölve van, az alkalmazás a következő információkat továbbítja:

- a KSN konfigurációs fájljainak frissítésére vonatkozó információk: az aktív konfiguráció azonosítója, a kapott konfiguráció azonosítója, a konfigurációs frissítés hibakódja;
- az ellenőrizendő fájlokkal és URL-címekkel kapcsolatos információk: az ellenőrzött fájl ellenőrzőösszegei (MD5, SHA2-256, SHA1) és a fájlminták (MD5), a minta mérete, az észlelt fenyegetés típusa és a Jogbirtokos besorolása szerinti megnevezése, a vírusadatbázisok azonosítója, az URL-cím, amelyhez a megbízhatóság ellenőrzését kérelmezték, illetve a hivatkozó URL-cím, a kapcsolat protokollazonosítója és a használt portok száma;
- a vizsgálati feladat azonosítója, amely a fenyegetést észlelte;
- a használt digitális tanúsítványok hitelességének ellenőrzéséhez szükséges információk: az ellenőrzött objektum megjelöléséhez használt tanúsítvány ellenőrzőösszegei (SHA256) és a tanúsítvány nyilvános kulcsa;
- A vizsgálatot végző szoftverösszetevő azonosítója;
- Az antivírus adatbázisok és ezen antivírus adatbázisok jelentéseinek azonosítói;
- a számítógépen lévő szoftver aktiválásának információi: az aktiválási szolgáltatástól kapott jegy aláírt fejléce (a regionális aktiválási központ azonosítója, az aktiválási kód ellenőrzőösszege, a jegy ellenőrzőösszege, a jegy létrehozási dátuma, a jegy egyedi azonosítója, a jegy verziója, a licenc állapota, a jegy érvényességének kezdési/befejezési dátuma és időpontja, a licenc egyedi azonosítója, a licenc verziója), a jegy fejlécének aláírására használt tanúsítvány azonosítója és a kulcsfájl ellenőrzőösszege (MD5);
- A jogtulajdonos szoftverének információi: teljes verzió, típus, a Kaspersky szolgáltatáshoz történő csatlakozáshoz használt protokoll verziója.

Ha a **Kiterjesztett KSN mód engedélyezése** és a **Kaspersky Security Network** jelölőnégyzet egyaránt be van jelölve, a fentiek mellett az alkalmazás a következő információkat is továbbítja:

- információk a kért webes erőforrások kategorizálásának eredményeiről, amelyek tartalmazzák a gazdagép feldolgozott URL- és IP-címét, a Szoftverösszetevő verzióját, amely a kategorizálást végezte, a kategorizálás módszerét és a webes erőforrás számára meghatározott kategóriák halmazát;
- a számítógépre telepített szoftverre vonatkozó információ: a szoftveres alkalmazások és szoftverszállítók neve, regisztrációs kulcsok és azok értéke, a telepített szoftverösszetevők fájljaira vonatkozó információk (ellenőrzőösszeg (MD5, SHA2-256, SHA1), a Számítógépen lévő fájl neve, elérési útja, mérete, verziója és digitális aláírása);
- a számítógép vírusvédelmi állapotára vonatkozó információk: a használt vírusadatbázisok verziói és kiadási időbélyegei, a feladat azonosítója és a vizsgálatot végző szoftver azonosítója;
- a Végfelhasználó által letöltött fájlokkal kapcsolatos információk: a letöltés URL- és IP-címe és a letöltési oldalak, a letöltés protokollazonosítója és a kapcsolódási port száma, hogy az URL-címek kártékonyak vagy sem, a fájl jellemzői, mérete és az ellenőrzőösszegek (MD5, SHA2-256, SHA1), a fájl letöltésének folyamatával kapcsolatos információ (ellenőrzőösszegek (MD5, SHA2-256, SHA1), létrehozás/build dátuma és ideje, automatikus lejátszás státusza, jellemzői, a csomagolók neve, információ az aláírásokkal kapcsolatban, futtatható fájl jelzője, formátumazonosító és entrópia), a folyamatfájlra vonatkozó adatok (név, fájl elérési útja és mérete), a fájl neve és elérési útja a Számítógépen, a fájl digitális aláírása és létrehozásának időbélyegzője, az URL-cím, ahol az észlelés történt, a parancsfájlszám a gyanúsnak vagy kártékonynak tűnő oldalon;

- a futó alkalmazásokkal és azok moduljaival kapcsolatos információk: a rendszeren futó folyamatokkal kapcsolatos adatok (folyamatazonosító (PID)), a folyamat neve, azon felhasználói fiókkal kapcsolatos információk, ahonnan a folyamat elindult, a folyamatot elindító alkalmazás és parancs, a megbízható program vagy folyamat jele, a folyamat fájljaihoz vezető teljes útvonal és az ellenőrzőösszegeik (MD5, SHA2-256, SHA1), a kezdő parancssor, a folyamat integritásának szintje, azon termék leírása, amelyhez a folyamat tartozik (a termék neve és a kiadóval kapcsolatos információk), valamint a felhasznált digitális tanúsítványok és a hitelességük ellenőrzéséhez szükséges információk, illetve egy fájl digitális aláírásának hiányával kapcsolatos információk, valamint a folyamatokba töltött modulokkal kapcsolatos információk (nevük, méretük, típusaik, létrehozásuk dátuma, attribútumok, ellenőrző összegek (MD5, SHA2-256, SHA1), a hozzájuk vezető útvonalak a Számítógépen, a PE-fájl fejlécadatai, a tömörítők neve (ha a fájl be volt csomagolva);

- az összes potenciálisan rosszindulatú objektum és tevékenység adatai: az észlelt objektum neve és a teljes elérési útvonala a számítógépen, a feldolgozott fájlok ellenőrzőösszegei (MD5, SHA2-256, SHA1), az észlelés dátuma és időpontja, a fertőzött fájlok neve, mérete, elérési útvonala és az elérési útvonal sablonkódja, a végrehajtható fájl jelölése, a jelzés, hogy az objektum egy tároló-e, a tömörítő neve (ha a fájl tömörítve volt), a fájl típuskódja, a fájl formátumazonosítója, a rosszindulatú program által végrehajtott tevékenységek, továbbá a szoftver és a felhasználó válaszként meghozott döntése, a döntés meghozatalára használt antivírus adatbázisok azonosítója és a jelentésük, a potenciálisan rosszindulatú objektum jelzője, az észlelt fenyegetés neve a Jogbirtokos osztályozása szerint, a fenyegetési szint, az észlelés állapota és módszere, az elemzett kontextusba való belefoglalás oka, valamint a kontextusban lévő fájl sorozatszáma, azon alkalmazás végrehajtható fájljának neve, attribútumai és ellenőrzőösszegei (MD5, SHA2-256, SHA1), melyen keresztül a fertőzött üzenet vagy hivatkozás továbbítva lett, a blokkolt objektum gazdagépének személytelenített IP-címei (IPv4 és IPv6), a fájl entrópia, fájl automatikus futtatás jelző, a fájl első észlelésének időpontja a rendszerben, a fájl futtatási alkalmainak száma az utolsó statisztikák elküldése óta, a levelezőprogram nevének, méretének és ellenőrzőösszegeinek (MD5, SHA2-256, SHA1) adatai, melyről a rosszindulatú objektum érkezett, a vizsgálatot végző szoftverfeladat azonosítója, jelzés, hogy a fájl hírneve vagy aláírása ellenőrizve volt-e, a fájl feldolgozásának eredménye, az objektumhoz összegyűjtött minta ellenőrzőösszege (MD5), a minta mérete bájtban, valamint a használt észlelő technológiák műszaki adatai;

- a vizsgált objektumokkal kapcsolatos információk: a hozzárendelt megbízhatósági csoport, amelyikbe és/vagy amelyikből a fájl áthelyezése történt, a fájl adott kategóriába helyezésének oka, a kategória azonosítója, a kategóriák forrására és a kategória-adatbázis verziójára vonatkozó információk, a fájl megbízható tanúsítványjelzése, a fájl forgalmazójának neve, a fájl verziója, a fájlt tartalmazó szoftveralkalmazás neve és verziója;

- az észlelt biztonsági résekre vonatkozó információk: a biztonsági rés azonosítója a biztonsági rések adatbázisában és a biztonsági rés veszélyességi osztálya;

- a futtatható fájl emulációjával kapcsolatos információ: a fájl mérete és az ellenőrzőösszegek (MD5, SHA2-256, SHA1), az emulációs komponens verziója, a emuláció mértéke, a logikai blokkok tulajdonságai és az emuláció során megszerzett logikai blokkok funkciói, a futtatható fájl PE fejléceiből származó adatok;

- a támadó számítógép IP-címe (IPv4 és IPv6), annak a portnak a száma a Számítógépen, amely ellen a hálózati támadás irányul, a támadást tartalmazó IP-csomag protokolljának azonosítója, a támadás célpontja (szervezet neve, webhelye), a támadásra adott válasz jelzője, a támadás súlya, a megbízhatóság szintje;

- a hamisított hálózati erőforrásokkal összefüggésbe hozható támadásokkal kapcsolatos információk, valamint a meglátogatott webhelyek DNS- és IP-címei (IPv4 és IPv6);

- a kért webes erőforrás DNS- és IP-címe (IPv4 vagy IPv6), a fájllal és a webes erőforráshoz hozzáférő webügyféllel kapcsolatos információk, a fájl neve, mérete, ellenőrzőösszegek (MD5, SHA2-256, SHA1), a fájl teljes útvonala, az útvonal sablonjának kódja, a digitális aláírás ellenőrzésének eredménye és a KSN szerinti állapota;

- a rosszindulatú tevékenységek visszagörgetésének adatai: a fájl adatai, melynek tevékenységei vissza lettek görgetve (a fájl neve, teljes elérési út a fájlhoz, a mérete és ellenőrzőösszegei (MD5, SHA2-256, SHA1)), a sikeresen / sikertelenül törölt tevékenységek adatai, a fájlok átnevezése és másolása és a beállításjegyzék értékeinek visszaállítása (a beállításkulcsok nevei és értékei), valamint a rosszindulatú program által módosított rendszerfájlok, a visszagörgetés előtt és után.

- Az Adaptív anomália-ellenőrzési összetevő kizárási készletére vonatkozó információ: az aktivált szabály azonosítója és állapota, a Szoftver által a szabály aktiválásakor végrehajtott művelet, annak a felhasználói fióknak a típusa, amely alatt a folyamat vagy a szál gyanús tevékenységet végez, információ a folyamatról amely végrehajtotta vagy a gyanús tevékenység tárgya volt (szkriptazonosító vagy a folyamat fájlneve, a folyamat fájljának teljes elérési útja, a sablonkód elérési útja, a folyamatfájl ellenőrzőösszegei (MD5, SHA2-256, SHA1)); arra az objektumra vonatkozó információ, amely a gyanús tevékenységeket végezte, és amely a gyanús tevékenységek tárgya volt (a beállításkulcs neve vagy fájlneve, a fájl teljes elérési útja, az elérési út sablonkódja és a fájl ellenőrzőösszegei (MD5, SHA2-256, SHA1)).

- a betöltött szoftver modulok adatai: a modul fájl neve, mérete és ellenőrzőösszegei (MD5, SHA2-256, SHA1), teljes elérési útvonal és az elérési út sablonkódja, a modul fájl digitális aláírásának beállításai, az aláírás létrehozásának dátuma és időpontja, a modulfájlt aláírt alany vagy szervezet neve, a modult betöltő folyamat azonosítója, a modult szállító neve, valamint a modul sorszáma a betöltési sorban.

- a Szoftver KSN szolgáltatással végzett interakciójának minőségére vonatkozó információ: a statisztikák generálásának kezdési és befejezési dátuma és ideje, a használt KSN szolgáltatásokba irányuló kérelmek és kapcsolatok minőségére vonatkozó információ (KSN szolgáltatási azonosítója, sikeres kérelmek száma, a gyorsítótárból kapott válaszokkal rendelkező kérelmek száma, sikeres kérelmek száma (hálózati problémák, a KSN le van tiltva a Szoftver beállításaiban, helytelen útválasztás), a sikeres kérelmek időbeli eloszlása, a megszakított kérelmek időbeli eloszlása, a túllépett időkorláttal rendelkező kérelmek időbeli eloszlása, a KSN-nel a gyorsítótárból létrehozott kapcsolatok száma, a KSN-nel sikeresen létrehozott kapcsolatok száma, a KSN-hez történő sikertelen kapcsolódások száma, a sikeres tranzakciók száma, a sikertelen tranzakciók száma, a KSN-nel létrehozott sikeres kapcsolatok időbeli eloszlása, a KSN-hez történő sikertelen kapcsolódások időbeli eloszlása, a sikeres kapcsolatok időbeli eloszlása, a sikertelen kapcsolatok időbeli eloszlása);

- potenciálisan rosszindulatú objektum észlelésekor információt kell biztosítani az eljárások által használt memóriákban található adatokról: a rendszerobjektum-hierarchiában (ObjectManager) lévő elemekről, az UEFI BIOS memóriában tárolt adatokról, a rendszerleíró kulcsok nevéről és értékéről;

- rendszernaplókban lévő eseményekkel kapcsolatos információk: az esemény időbélyege, a napló neve, amelyben az esemény található, az esemény típusa és kategóriája, az esemény forrásának neve, valamint az esemény leírása;

- hálózati kapcsolatokra vonatkozó információk: annak a fájlnak a verziója és ellenőrzőösszegei (MD5, SHA2-256, SHA1), amelyből a portot megnyitó eljárást elindították, az eljárás fájljának útvonala és digitális aláírása, a helyi és a távoli IP-címek, a helyi és a távoli csatlakozási portok száma, a csatlakozási állapot, a port nyitásának időbélyege;

- információ a szoftver számítógépen történő telepítésének és aktiválásának dátumáról: a licencet értékesítő partner azonosítója, a licenc sorozatszáma, az aktiválási szolgáltatástól kapott jegy aláírt fejléce (a regionális aktiválási központ azonosítója, az aktiválási kód ellenőrzőösszege, a jegy ellenőrzőösszege, a jegy létrehozási dátuma, a jegy egyedi azonosítója, a jegy verziója, a licenc állapota, a jegy érvényességének kezdési/befejezési dátuma és időpontja, a licenc egyedi azonosítója, a licenc verziója), a jegy fejlécének aláírására használt tanúsítvány azonosítója és a kulcsfájl ellenőrzőösszege (MD5), a számítógépen lévő szoftvertelepítés egyedi azonosítója, a frissítésre kerülő alkalmazás azonosítója és típusa, a frissítési feladat azonosítója;

- információk az összes telepített frissítés halmazáról és a legújabban telepített/eltávolított frissítések halmazáról, az eseménytípusról, amely a frissítésinformációk elküldését kezdeményezte, a legutolsó frissítés telepítése óta eltelt időtartamról, információk bármely jelenleg telepített vírusadatbázisról;

- a számítógépen lévő szoftver működésének adatai: CPU használat adatai, memóriahasználat adatai (Private Bytes, Non-Paged Pool, Paged Pool), a szoftverfolyamat aktív szálainak és függőben lévő szálainak száma, a szoftver működési ideje a hiba előtt.

- a szoftverrel és a rendszerrel kapcsolatos memóriaképek (BSOD) száma a Szoftver telepítése és az utolsó frissítés óta, annak a Szoftvermodulnak az azonosítója és verziója, ahol az összeomlás történt, a Szoftverfolyamat memóriaverme, valamint vírusadatbázisokkal kapcsolatos információk az összeomlás előtt;

- a kékképernyős összeomlásra (BSOD) vonatkozó adatok: a Számítógép kékképernyős összeomlást jelző jelölője, a kékképernyős összeomlást okozó illesztőprogram neve, a cím és a memóriaverem az illesztőprogramban, az operációs rendszer munkamenetének hosszát jelző jelölő a kékképernyős összeomlás előtt, az összeomlott meghajtó memóriaverme, a tárolt memóriakép típusa, az operációs rendszer azon munkamenetének jelölése, amely a BSOD előtt 10 percnél tovább tartott, a memóriakép egyéni azonosítója, a BSOD időbélyegzője;

- információk a Szoftverösszetevők működése közben felmerült hibákról vagy teljesítményproblémákról: a Szoftver állapotazonosítója, a hiba típusa, kódja, valamint előfordulásának időpontja, az összetevő azonosítói, a termék modulja és folyamata, amelyben a hiba felmerült, a feladat vagy frissítési kategória azonosítója, amely során a hiba felmerült, a Szoftver által használt illesztőprogramok naplói (hibakód, modul neve, a forrásfájl neve és a sor, ahol a hiba felmerült);

- a víruskereső adatbázisok és Szoftverösszetevők frissítéseire vonatkozó információk: a legutóbbi frissítéskor és a jelenlegi frissítés során letöltött indexfájlok neve, letöltésük dátuma és időpontja;

- a Szoftverműködés rendellenes leállására vonatkozó információk: a memóriakép létrehozásának időbélyege, típusa, az esemény típusa, amely a Szoftverműködés rendellenes leállását idézte elő (váratlan kikapcsolás, harmadik fél alkalmazásának összeomlása), a váratlan kikapcsolás dátuma és ideje;

- a Szoftver illesztőprogramjainak a hardverrel és a szoftverrel való kompatibilitására vonatkozó információ: a Szoftver összetevőinek működését korlátozó operációsrendszer-tulajdonságokra vonatkozó információ (biztonságos rendszerindítás, KPTI, WHQL, Enforce, BitLocker, kis- és nagybetűk megkülönböztetése), a telepített letöltött Szoftver típusa (UEFI, BIOS), platformmegbízhatósági modul (TPM) azonosítója, TPM specifikációjának verziója, a számítógépbe telepített CPU-ra vonatkozó információ, működési mód és a kódintegritás és eszközvédelem paraméterei, az illesztőprogramok működési módja és a jelenlegi mód használatának oka, a Szoftver-illesztőprogramok verziója, a szoftver- és hardvervirtualizálás támogatási verziója a számítógépen;

- a hibát okozó, külső gyártóktól származó alkalmazásokkal kapcsolatos információk: azok neve, verziója és honosítása, a hibakód és a hiba adatai az alkalmazások rendszernaplójából, a külső gyártótól származó alkalmazás hibájának címe és memóriaverme, a Szoftverösszetevő hibájának előfordulását jelző jelölő, a külső gyártótól származó alkalmazás működésének időtartama a hiba előfordulása előtt, az alkalmazás folyamatképének ellenőrzőösszegei (MD5, SHA2-256, SHA1), amelyben a hiba kialakult, az alkalmazás folyamatképének elérési útja és az elérési út sablonkódja, információ a rendszernaplóról az alkalmazáshoz kapcsolt hibának a leírásával, információ az alkalmazásmodulról, amelyben a hiba keletkezett (kivételazonosító, az összeomlás-memória címe ofszetként az alkalmazásmodulban, a modul neve és verziója, az alkalmazás összeomlásának azonosítója a Jogbirtokos beépülő moduljában és az összeomlás memóriaverme, az alkalmazás munkafolyamatának időtartama az összeomlás előtt);

- a Szoftverfrissítő összetevő verziója, a frissítő összetevő összeomlásainak száma frissítési feladatok futtatása közben az összetevő élettartama alatt, a frissítési feladattípus azonosítója, a frissítő összetevő meghiúsult kísérleteinek száma a frissítési feladatok befejezésére;

- a Szoftver rendszerfigyelő összetevőinek működésével kapcsolatos információk: az összetevők teljes verziója és azok elindításának dátuma és időpontja, annak az eseménynek a kódja, amelynek köszönhetően túlcsordult az eseménysor és ezen események száma, az eseménysor túlcsordulásához vezető események száma összesen, információ az eseményt kiváltó folyamat fájljáról (a fájl neve és elérési útja a Számítógépen, a fájl elérési útjának sablonkódja, a fájlhoz kapcsolt folyamat ellenőrzőösszegei (MD5, SHA2-256, SHA1), a fájl verziója), az esemény bekövetkezett megszakadásának azonosítója, a megszakítás szűrőjének teljes verziója, a megszakított esemény típusának azonosítója, az eseménysor mérete és az események száma a sorban szereplő első és az aktuális esemény között, a lejárt események száma a sorban, információk az aktuális esemény kiváltó folyamatának fájljáról (a fájl neve és elérési útja a Számítógépen, a fájl elérési útjának sablonkódja, a fájlhoz kapcsolt folyamat ellenőrzőösszegei (MD5, SHA2-256, SHA1)), az esemény feldolgozásának időtartama, az esemény feldolgozásának maximális időtartama, a statisztikák küldésének valószínűsége, az időkorlátot meghaladó operációsrendszer-eseményekre vonatkozó információ (az esemény dátuma és ideje, a víruskereső adatbázisok legutóbbi ismételt inicializálásának dátuma és ideje a frissítésüket követően, az egyes rendszerfigyelési összetevők eseményfeldolgozási késleltetési ideje, a sorba állított események száma, a feldolgozott események száma, a jelenlegi típusú késleltetett események száma, a jelenlegi típusú események teljes késleltetési ideje, az összes esemény teljes késleltetési ideje);

- a windowsos esemény-nyomkövetési eszköz adatai (Windows esemény-nyomkövetés, ETW) Szoftverteljesítménnyel kapcsolatos problémák esetén, a Microsoft SysConfig / SysConfigEx / WinSATAssessment eseményei esetén: a számítógépre vonatkozó információ (modell, gyártó, a ház méretformátuma, verzió), a Windows teljesítménymetrikáira vonatkozó információ (WinSAT-értékelések, Windows-teljesítményindex), tartománynév, a fizikai és logikai feldolgozókra vonatkozó információ (a fizikai és logikai feldolgozók száma, gyártó, modell, stepping szintje, magok száma, órafrekvencia, CPUID, gyorsítótár jellemzői, logikai processzor jellemzői, a támogatott utasítási módok jelzői), RAM-modulokra vonatkozó információ (típus, méretformátum, gyártól, modell, kapacitás, a memóriakiosztás granularitása), a hálózati csatolófelületek adatai (a hálózat csatolófelület IP- és MAC-címe, neve, leírása és konfigurációja, a hálózati csomagok, a hálózati csomagok számának és méretének részletezése típus, szerint, hálózati forgalom sebessége, a hálózati hibák számának részletezése típus szerint), az IDE-vezérlő konfigurációja, a DNS-kiszolgálók IP-címei, a videokártyára vonatkozó információ (modell, leírás, gyártó, kompatibilitás, videomemória mérete, képernyőengedély, a bitek száma képpontonként, a BIOS verziója), információ a plug-and-play működésű eszközökről (név, leírás, eszközazonosító [PnP, ACPI], lemezekre és tárolóeszközökre vonatkozó információ (lemezek vagy flash-meghajtók száma, gyártója, modellje, lemezkapacitása, cilinderek száma, cilinderenkénti sávok száma, sávonkénti szektorok száma, szektorkapacitás, gyorsítótárazási jellemzők, sorozatszám, partíciók száma, az SCSI-vezérlő konfigurációja), logikai lemezekre vonatkozó információ (sorozatszám, partíciós kapacitás, kötetkapacitás, kötet betűjele, partíciós típus, fájlrendszertípus, fürtök száma, fürtméret, fürtönkénti szektorok száma, üres és foglalt fürtök száma, rendszerindító kötet betűjele, a partíció eltolási címe a lemez kezdetéhez képest), a BIOS-alaplapra vonatkozó információ (gyártó, kiadási dátum, verzió), az alaplapra vonatkozó információ (gyártó, modell, típus), a fizikai memóriára vonatkozó információ (megosztott és szabad kapacitás), az operációs rendszer szolgáltatásaira vonatkozó információ (név, leírás, állapot, címke, a folyamatokra vonatkozó információ [név és PID]), a számítógép energiafogyasztási paraméterei, a megszakításvezérlő konfigurációja, a Windows rendszermappáinak elérési útja (Windows és System32), az operációs rendszerre vonatkozó információ (verzió, build, kiadási dátum, név, típus, telepítési dátum), lapozófájl mérete, monitorokra vonatkozó információ (számuk, gyártójuk, képernyőengedélyük, felbontási kapacitás, típus), videokártya illesztőprogramjára vonatkozó információ (gyártó, kiadási dátum, verzió);

- az ETW-ből az EventTrace/EventMetadataiból származó információ a Microsofttól: a rendszeresemények sorrendjére vonatkozó információ (típus, időpont, dátum, időzóna), a nyomkövetési eredményekkel rendelkező fájl metaadatai (név, struktúra, nyomkövetési paraméterek, a nyomonkövetési műveletek számának részletezése típus szerint), az operációs rendszerre vonatkozó információ (név, típus, verzió, build, kiadási dátum, kezdési idő);

- az ETW-ből, a folyamatszolgáltatókból / a Microsoft Windows kernelfolyamatából / a Microsoft Windows kernelének processzorenergia-eseményeiből származó információ a Microsofttól: (név, PID, kezdési paraméterek, parancssor, visszaadott kód, energiakezelési paraméterek, kezdési és befejezési idő, hozzáférési token típusa, SID, munkamenet-azonosító, telepített leírók száma), a szálprioritások változásainak száma (TID, prioritás, idő), a folyamat lemezműveleteire vonatkozó információ (típus, idő, kapacitás, szám), a felhasználható memóriafolyamatok struktúrájának és kapacitásának változási előzményei;

- a ETW-ből, a StackWalk szolgáltatóitól / Perfinfoból származó eseményekre vonatkozó információ a Microsofttól: teljesítményszámlálókra vonatkozó információ (egyedi kódszakaszok teljesítménye, funkcióhívások sorrendje, PID, TID, ISR-ek és DPC-k címei és attribútumai);

- az ETW-ből, a KernelTraceControl-ImageID esemény szolgáltatójától származó információ a Microsofttól: végrehajtható fájlokra és dinamikus könyvtárakra vonatkozó információ (név, képméret, teljes elérési út), PDB-fájlokra vonatkozó információ (név, azonosító), VERSIONINFO erőforrásadatok végrehajtható fájlokhoz (név, leírás, létrehozó, lokalizáció, alkalmazás verziója és azonosítója, fájl verziója és azonosítója);

- az ETW-ből származó információ FileIo- / DiskIo- / rendszerkép- / Windows kernel lemezre vonatkozó események a Microsofttól: fájl- és lemezműveletekre vonatkozó információ (típus, kapacitás, kezdési idő, befejezési idő, időtartam, befejezés állapot, PID, TID, illesztőprogram függvényhívási címei, I/O-kérelmi csomag (IRP), windowsos fájlobjektum-attribútumok), a fájl- és lemezműveletekben érintett fájlokra vonatkozó információ (név, verzió, méret, teljes elérési út, attribútumok, eltolás, rendszerkép ellenőrzőösszege, megnyitási és hozzáférési beállítások);

- az ETW-ből származó információ, laphibaesemények szolgáltatója a Microsofttól: a memória lapelérési hibáira vonatkozó információ (cím, idő, kapacitás, PID, TID, Windows-fájlobjektum attribútumai, memóriakiosztási paraméterek);

- az ETW-ből származó információ, szálesemények szolgáltatója a Microsofttól: szálak létrehozására/befejezésére vonatkozó információ (PID, TID, köteg mérete, CPU-erőforrások prioritása és kiosztása, I/O-erőforrások, szálak közötti memórialapok, kötegcím, inicializálási funkció címe, szálkörnyezeti blokk (TEB) címe, Windows-szolgáltatáscímke);

- az ETW-ből származó információ, a Microsoft Windows kernelmemória-eseményeinek szolgáltatója a Microsofttól: a memóriakezelési műveletekre vonatkozó információ (befejezési állapot, idő, mennyiség, PID), memóriakiosztási struktúra (típus, kapacitás, munkamenet-azonosító, PID);

- Szoftverműveletre vonatkozó információ teljesítményproblémák esetén: Szoftvertelepítési azonosító, teljesítmény csökkenésének típusa és értéke, események sorozatára vonatkozó információ a Szoftverben (idő, időzóna, típus, befejezési állapot, a Szoftverösszetevő azonosítója, Szoftverműködtetési forgatókönyv azonosítója, TID, PID, függvényhívási címek), az ellenőrizendő hálózati kapcsolatokra vonatkozó információ (URL, kapcsolat iránya, hálózati csomag mérete), PDB-fájlokra vonatkozó információ (név, azonosító, végrehajtható fájl rendszerképének mérete), az ellenőrizendő fájlokra vonatkozó információ (név, teljes elérési út, ellenőrzőösszeg), Szoftverteljesítmény-figyelési paraméterek;

- az operációs rendszer legutolsó sikertelen indításának adatai: sikertelen indítások száma az operációs rendszer telepítése óta, a rendszerrel kapcsolatos memóriakép adatai (a hiba kódja és paraméterei, név, verzió és azon modul ellenőrzőösszege (CRC32), amely a hibát okozta az operációs rendszerben, a hiba címe ofszetként a modulban, a rendszerrel kapcsolatos memóriakép ellenőrzőösszegei (MD5, SHA2-256, SHA1));

- a fájlok aláírására használt digitális tanúsítványok hitelességének ellenőrzésére szolgáló információk: a tanúsítványon lévő ujjlenyomat, az ellenőrzőösszeg algoritmusa, a tanúsítvány nyilvános kulcsa és sorozatszáma, a tanúsítvány kibocsátójának neve, a tanúsítvány érvényesítésének eredménye, valamint a tanúsítvány adatbázisbeli azonosítója;

- a Szoftver önvédelmét megtámadó folyamattal kapcsolatos információk: a folyamat fájljának neve és mérete, ellenőrzőösszegei (MD5, SHA2-256, SHA1), a folyamat fájljának teljes elérési útja és a fájlútvonal sablonkódja, a létrehozási/build időbélyegzők, a futtatható fájl jelölése, a folyamat fájljának attribútumai, a folyamatot elindításához használt fiók kódja, a folyamat eléréséhez végrehajtott műveletek azonosítója, a művelet elvégzéséhez használt erőforrás típusa (folyamat, fájl, beállításjegyzékbeli objektum, FindWindow keresési funkció), a művelet elvégzéséhez használt erőforrás neve, a művelet sikerességét jelző jelölő, a folyamat fájljának állapota, valamint a KSN szerinti aláírása;

- Információ a Jogbirtokos szoftverrel kapcsolatban: a használt Szoftver teljes verziója, típusa, lokalizációja és működési állapota, a telepített Szoftverösszetevők verziója és működési állapota, információk a telepített frissítésekről, a TARGET szűrő értéke, a jogtulajdonos szolgáltatásaihoz való csatlakozáshoz használt protokoll verziója;

- a Számítógépre telepített hardverrel kapcsolatos információk: típus, név, modellnév, a firmware verziója, a beépített és a csatlakoztatott eszközök paraméterei, azon Számítógép egyedi azonosítója, amelyre a Szoftvert telepítették;

- információk az operációs rendszer és a telepített frissítések verzióival, az operációs rendszer futási módjának szóméretével, kiadásával és paramétereivel, az operációs rendszer kernelfájljának verziójával és ellenőrzőösszegeivel (MD5, SHA2-256, SHA1), valamint az operációs rendszer elindítási dátumával és idejével kapcsolatban;

- végrehajtható és nem végrehajtható fájlok, részben vagy egészben;

- a számítógép RAM-jának részei;

- az operációs rendszer indításában résztvevő szektorok;

- hálózati forgalmi adatok;

- weboldalak és a gyanús és rosszindulatú objektumokat tartalmazó weboldalak és e-mailek;

- az osztályok leírása és példák a WMI könyvtárban szereplő osztályokra;

- alkalmazástevékenységre vonatkozó jelentések:

    - a küldött fájl neve, mérete és verziója, leírása és ellenőrzőösszegei (MD5, SHA2-256, SHA1), fájlformátum azonosító, fájl forgalmazójának neve, a termék neve, melyhez a fájl tartozik, a fájl teljes elérési útja a számítógépen, az elérési út sablonkódja, a fájl időbélyegeinek létrehozása és módosítása;

    - a tanúsítvány érvényességi időtartamának kezdeti időpontja és vége (ha a fájl rendelkezik digitális aláírással), az aláírás dátuma és időpontja, a tanúsítvány kiadójának neve, a tanúsítvány birtokosának információi, az ujjlenyomat, a tanúsítvány nyilvános kulcsa és a megfelelő algoritmusok, illetve a tanúsítvány sorozatszáma;

    - a felhasználói fiók neve, amely alatt a folyamat fut;

    - a számítógép nevének ellenőrzőösszegei (MD5, SHA2-256, SHA1), melyről a folyamat fut;

    - a folyamatablakok neve;

    - A vírusadatbázisok azonosítója, az észlelt fenyegetés neve a Jogtulajdonos besorolása szerint;

    - a telepített licenc adatai, azonosítója, típusa és lejárati dátuma;

    - a számítógép helyi ideje az információk megadásakor;

    - a folyamat során elért fájlok nevei és elérési útjai;

    - a folyamat során elért beállítási kulcsok nevei és értékük;

    - a folyamat által elért URL-ek és IP-címek;

    - az URL-ek és IP-címek, melyekről a futtatott fájl le lett töltve.

Az adatok feletti rendelkezés a Detection and Response-megoldások használatakor

Azokon a számítógépeken, amelyeken a Kaspersky Endpoint Security telepítve van, a rendszer tárolja a Kaspersky Endpoint Detection and Response, a Kaspersky Sandbox és a Kaspersky Anti Targeted Attack Platform kiszolgálóinak történő automatikus küldésre előkészített adatokat. A fájlok tárolása a számítógépeken egyszerű, nem titkosított formában történik.

A konkrét adattartalom attól a megoldástól függ, amelynek részeként a Kaspersky Endpoint Securityt alkalmazzák.

Kaspersky Endpoint Detection and Response

A Kaspersky Endpoint Security eltávolításakor az alkalmazás által a számítógépen helyileg tárolt összes adat törlődik a számítógépről.

Az IOC Scan feladat végrehajtásának eredményeképpen kapott adatok (standard feladat)

A Kaspersky Endpoint Security automatikusan elküldi az *IOC vizsgálat* feladat végrehajtási eredményadatait a Kaspersky Security Centernek.

Az *IOC vizsgálat* feladat végrehajtási eredményadatai a következő információkat tartalmazhatják:

- IP-cím az ARP-tábláról
- Fizikai cím az ARP-tábláról
- DNS-rekord típusa és neve
- A védett számítógép IP-címe
- A védett számítógép fizikai címe (MAC-címe)
- Azonosító az eseménynapló-bejegyzésben
- Adatforrás neve a naplóban
- Napló neve
- Esemény ideje
- A fájl MD5 és SHA256 hash kivonatai
- A fájl teljes neve (az elérési úttal együtt)
- Fájlméret

- A távoli IP-cím és port, amellyel kapcsolat létesült a vizsgálat során
- Helyi adapter IP-címe
- Nyitott port a helyi adapteren
- Protokoll számként (az IANA szabványnak megfelelően)
- Folyamatnév
- Folyamat argumentumai
- A folyamatfájl elérési útja
- A folyamat Windows-azonosítója (PID)
- A szülőfolyamat Windows-azonosítója (PID)
- A folyamatot elindító felhasználói fiók
- A folyamat elindításának dátuma és időpontja
- A szolgáltatás neve
- A szolgáltatás leírása
- A DLL-szolgáltatás elérési útja és neve (svchost-hoz)
- A szolgáltatás futtatható fájljának elérési útja és neve
- A szolgáltatás Windows-azonosítója (PID)
- A szolgáltatás típusa (például kernel-illesztőprogram vagy adapter)
- A szolgáltatás állapota
- A szolgáltatás indítási módja
- Felhasználói fiók neve
- Kötet neve
- Kötet betűjele
- Kötet típusa
- Windows-beállításazonosító
- Rendszerleíró adatbázis értéke
- A beállításkulcs elérési útja (struktúra és értéknév nélkül)
- Rendszerleíró adatbázis beállítása
- Rendszer (környezet)

- A számítógépre telepített operációs rendszer neve és verziója
- A védett számítógép hálózatneve
- Tartomány vagy csoport, amelyhez a védett számítógép tartozik
- Böngésző neve
- Böngésző verziója
- A webes erőforráshoz való legutóbbi hozzáférés időpontja
- URL-cím a HTTP-kérésből
- A HTTP-kéréshez használt fiók neve
- A HTTP-kérést létrehozó folyamat fájlneve
- A HTTP-kérést létrehozó folyamat fájljának teljes elérési útja
- A HTTP-kérést létrehozó folyamat Windows-azonosítója (PID)
- HTTP hivatkozója (HTTP-kérés forrás URL-je)
- A HTTP-n keresztül kért erőforrás URI-ja
- A HTTP felhasználói ügynökre (a HTTP-kérést létrehozó alkalmazásra) vonatkozó információk
- A HTTP-kérés végrehajtási ideje
- A HTTP-kérést létrehozó folyamat egyedi azonosítója

Adatok egy fenyegetésfejlődési lánc létrehozásához

A fenyegetésfejlődési lánc létrehozásához felhasználható adatokat a rendszer alapértelmezés szerint hét napig tárolja. Az adatokat a rendszer automatikusan elküldi a Kaspersky Security Centernek.

A fenyegetésfejlődési lánc létrehozásához használható adatok a következő információkat tartalmazhatják:

- Incidens dátuma és időpontja
- Észlelés neve
- Vizsgálat módja
- Az észleléssel összefüggésben lévő utolsó művelet állapota
- Az észlelésfeldolgozás meghiúsulásának oka
- Észlelt objektum típusa
- Észlelt objektum neve

- Fenyegetés állapota az objektum feldolgozását követően
- Az ok, amiért a műveletek végrehajtása az objektumon meghiúsult
- A rosszindulatú műveletek visszaállítása céljából elvégzett műveletek
- Információk a feldolgozott objektumról:
  - A folyamat egyedi azonosítója
  - A szülőfolyamat egyedi azonosítója
  - A folyamatfájl egyedi azonosítója
  - Windows-folyamatazonosító (PID)
  - Folyamat parancssora
  - A folyamatot elindító felhasználói fiók
  - A bejelentkezési munkamenet kódja, amelyben a folyamat fut
  - A munkamenet típusa, amelyben a folyamat fut
  - A feldolgozás alatt álló folyamat integritási szintje
  - A folyamatot a jogosultsággal rendelkező helyi és tartománycsoportokban elindító felhasználói fiók tagsága
  - A feldolgozott objektum azonosítója
  - A feldolgozott objektum teljes neve
  - A védett eszköz azonosítója
  - Az objektum teljes neve (helyi fájlnév vagy a letöltött fájl webcíme)
  - A feldolgozott objektum MD5 vagy SHA256 hash kivonata
  - A feldolgozott objektum típusa
  - A feldolgozott objektum létrehozásának dátuma
  - A feldolgozott objektum legutóbbi módosításának dátuma
  - A feldolgozott objektum mérete
  - A feldolgozott objektum attribútumai
  - A feldolgozott objektumot aláíró szervezet
  - A feldolgozott objektumhoz tartozó digitális tanúsítvány ellenőrzésének eredménye
  - A feldolgozott objektum biztonsági azonosítója (SID)
  - A feldolgozott objektum időzóna-azonosítója

- A feldolgozott objektum letöltési webcíme (csak lemezre mentett fájlok esetében)
- A fájlt letöltő alkalmazás neve
- A fájlt letöltő alkalmazás MD5 és SHA256 hash kivonata
- A fájlt legutóbb módosító alkalmazás neve
- A fájlt legutóbb módosító alkalmazás MD5 és SHA256 hash kivonata
- A feldolgozott objektumindítások száma
- A feldolgozott objektum első indításának dátuma és időpontja
- A fájl egyedi azonosítói
- A fájl teljes neve (helyi fájlnév vagy a letöltött fájl webcíme)
- A Windows beállításjegyzék feldolgozott változójának elérési útja
- A Windows beállításjegyzék feldolgozott változójának neve
- A Windows beállításjegyzék feldolgozott változójának értéke
- A Windows beállításjegyzék feldolgozott változójának típusa
- A feldolgozott beállításkulcs tagságának jelzése az automatikus futtatási ponton
- A feldolgozott webes kérés webcíme
- A feldolgozott webes kérés hivatkozási forrása
- A feldolgozott webes kérés felhasználói ügynöke
- A feldolgozott webes kérés típusa (`GET` vagy `POST`)
- A feldolgozott webes kérés helyi IP-portja
- A feldolgozott webes kérés távoli IP-portja
- A feldolgozott webes kérés kapcsolatának iránya (bejövő vagy kimenő)
- Annak a folyamatnak az azonosítója, amelybe a rosszindulatú kód beágyazódott

Kaspersky Sandbox

A Kaspersky Endpoint Security eltávolításakor az alkalmazás által a számítógépen helyileg tárolt összes adat törlődik a számítógépről.

Szolgáltatási adatok

A Kaspersky Endpoint Security az automatikus válaszadás során feldolgozott alábbi adatokat tárolja:

- Feldolgozott fájlok és adatok, amelyeket a felhasználó ad meg a Kaspersky Endpoint Security beépített ügynökének konfigurálása során:
  - Karanténba helyezett fájlok
  - A Kaspersky Sandbox-integrációhoz használt tanúsítvány nyilvános kulcsa
- A Kaspersky Endpoint Security beépített ügynökének gyorsítótára:
  - Annak az időpontja, amikor a vizsgálati eredmények a gyorsítótárba kerültek
  - A vizsgálati feladat MD5 hash kivonata
  - A vizsgálati feladat azonosítója
  - Az objektum vizsgálati eredménye
- Objektumvizsgálati kérések várólistája:
  - A várólistán szereplő objektum azonosítója
  - Az objektum várólistára kerülésének időpontja
  - A várólistán szereplő objektum feldolgozottsági állapota
  - Azon felhasználói munkamenet azonosítója az operációs rendszerben, amely során az objektumvizsgálati feladat létrejött
  - Az operációs rendszer azon felhasználójának rendszer-azonosítója (SID), akinek a fiókjában a feladat létrejött
  - Az objektumvizsgálati feladat MD5 hash kivonata
- Azokra a feladatokra vonatkozó információk, amelyekkel kapcsolatban a Kaspersky Endpoint Security beépített ügynöke vizsgálati eredményekre vár a Kaspersky Sandboxtól:
  - Az objektumvizsgálati feladat beérkezésének időpontja
  - Az objektum feldolgozottsági állapota
  - Azon felhasználói munkamenet azonosítója az operációs rendszerben, amely során az objektumvizsgálati feladat létrejött
  - Az objektumvizsgálati feladat azonosítója
  - Az objektumvizsgálati feladat MD5 hash kivonata
  - Az operációs rendszer azon felhasználójának rendszer-azonosítója (SID), akinek a fiókjában a feladat létrejött
  - Az automatikusan létrehozott IOC XML-sémája

- A vizsgált objektum MD5 vagy SHA256 hash kivonata
- Feldolgozási hibák
- Azon objektumok neve, amelyekhez a feladatot létrehozták
- Az objektum vizsgálati eredménye

A Kaspersky Sandboxnak küldött kérésekben szereplő adatok

A Kaspersky Endpoint Security beépített ügynöke által a Kaspersky Sandboxhoz intézett kérésekből származó következő adatok helyileg tárolódnak a számítógépen:

- A vizsgálati feladat MD5 hash kivonata
- A vizsgálati feladat azonosítója
- Vizsgált objektum és minden kapcsolódó fájl

Az IOC Scan feladat végrehajtásának eredményeképpen kapott adatok (önálló feladat)

A Kaspersky Endpoint Security automatikusan elküldi az *IOC vizsgálat* feladat végrehajtási eredményadatait a Kaspersky Security Centernek.

Az *IOC vizsgálat* feladat végrehajtási eredményadatai a következő információkat tartalmazhatják:

- IP-cím az ARP-tábláról
- Fizikai cím az ARP-tábláról
- DNS-rekord típusa és neve
- A védett számítógép IP-címe
- A védett számítógép fizikai címe (MAC-címe)
- Azonosító az eseménynapló-bejegyzésben
- Adatforrás neve a naplóban
- Napló neve
- Esemény ideje
- A fájl MD5 és SHA256 hash kivonatai
- A fájl teljes neve (az elérési úttal együtt)
- Fájlméret

- A távoli IP-cím és port, amellyel kapcsolat létesült a vizsgálat során
- Helyi adapter IP-címe
- Nyitott port a helyi adapteren
- Protokoll számként (az IANA szabványnak megfelelően)
- Folyamatnév
- Folyamat argumentumai
- A folyamatfájl elérési útja
- A folyamat Windows-azonosítója (PID)
- A szülőfolyamat Windows-azonosítója (PID)
- A folyamatot elindító felhasználói fiók
- A folyamat elindításának dátuma és időpontja
- A szolgáltatás neve
- A szolgáltatás leírása
- A DLL-szolgáltatás elérési útja és neve (svchost-hoz)
- A szolgáltatás futtatható fájljának elérési útja és neve
- A szolgáltatás Windows-azonosítója (PID)
- A szolgáltatás típusa (például kernel-illesztőprogram vagy adapter)
- A szolgáltatás állapota
- A szolgáltatás indítási módja
- Felhasználói fiók neve
- Kötet neve
- Kötet betűjele
- Kötet típusa
- Windows-beállításazonosító
- Rendszerleíró adatbázis értéke
- A beállításkulcs elérési útja (struktúra és értéknév nélkül)
- Rendszerleíró adatbázis beállítása
- Rendszer (környezet)

- A számítógépre telepített operációs rendszer neve és verziója
- A védett számítógép hálózatneve
- Tartomány vagy csoport, amelyhez a védett számítógép tartozik
- Böngésző neve
- Böngésző verziója
- A webes erőforráshoz való legutóbbi hozzáférés időpontja
- URL-cím a HTTP-kérésből
- A HTTP-kéréshez használt fiók neve
- A HTTP-kérést létrehozó folyamat fájlneve
- A HTTP-kérést létrehozó folyamat fájljának teljes elérési útja
- A HTTP-kérést létrehozó folyamat Windows-azonosítója (PID)
- HTTP hivatkozója (HTTP-kérés forrás URL-je)
- A HTTP-n keresztül kért erőforrás URI-ja
- A HTTP felhasználói ügynökre (a HTTP-kérést létrehozó alkalmazásra) vonatkozó információk
- A HTTP-kérés végrehajtási ideje
- A HTTP-kérést létrehozó folyamat egyedi azonosítója

Kaspersky Endpoint Detection and Response Expert (on-premises)

A Kaspersky Endpoint Security eltávolításakor az alkalmazás által a számítógépen helyileg tárolt összes adat törlődik a számítógépről.

Szolgáltatási adatok

A Kaspersky Endpoint Security beépített ügynöke a következő adatokat tárolja helyileg:

- Az EDR Expert (on-premises) összetevővel való integrációhoz szükséges adatok:
  - A KATA központi csomóponti kiszolgálóhoz való csatlakozás címe és portja
  - A telemetriai adatátviteli kiszolgálóhoz való csatlakozás címe és portja
  - A válaszkiszolgálóhoz való csatlakozás címe és portja

- Információ a KATA központi csomóponttal való integrációhoz használt tanúsítványokról
- Információ a telemetriai átviteli kiszolgálóval való integrációhoz használt tanúsítványokról
- Információ a válaszkiszolgálóval való integrációhoz használt tanúsítványokról

- Karanténba helyezett fájlok

Továbbított telemetriai eseményekből származó adatok

- **Telemetriai adatok**
  - Fájlokkal kapcsolatos adatok:
    - A fájl egyedi azonosítói
    - Fájltípus
    - A fájl teljes elérési útja
    - Fájlméret
    - Fájlattribútumok
    - Zónaazonosító
    - A fájl létrehozásának dátuma és időpontja
    - A fájl legutóbbi módosításának dátuma és időpontja
    - Eredeti fájlnév
    - Alkalmazásnév
    - Alkalmazás verziója
    - Alkalmazás szállítója
    - Fájlleírás
    - Fájlverzió
    - Az objektum MD5 és SHA256 hash kivonatai
    - A fájlaláírás ellenőrzésének eredménye
    - A tanúsítvány kibocsátójának neve
    - A tanúsítvány tulajdonosának neve
    - A tanúsítvány sorozatszáma

- Az AMSI vizsgálat adatai:
  - A tevékenységet kezdeményező folyamat egyedi azonosítója
  - Az AMSI-nek átadott objektum tartalomtípusa
  - Az AMSI-nek átadott objektum tartalma
  - Objektum neve
  - Az objektum MD5 és SHA256 hash kivonatai
- Alkalmazásblokkolási adatok:
  - Az alkalmazásblokkolást kezdeményező folyamat egyedi azonosítója
  - A szülőfolyamat egyedi azonosítója
  - A folyamat egyedi rendszerazonosítója
  - A folyamat elindítására szolgáló parancs
  - Bejelentkezési munkamenet azonosítója
  - Folyamatintegritási szint
  - Folyamat állapota
  - A folyamatfájl egyedi azonosítója
  - Folyamat parancssora
  - Az értelmezett fájlok egyedi azonosítóinak listája
- Adatok a blokkolt fájlmegnyitásokról:
  - A fájl megnyitását kezdeményező folyamat egyedi azonosítója
  - A fájl egyedi azonosítói
- Adatok az illesztőprogram betöltésével kapcsolatban:
  - A betöltött illesztőprogram egyedi azonosítója
- Adatok az eseményekről:
  - Az esemény egyedi azonosítója
  - Esemény dátuma és időpontja
- Fájlmódosítási adatok:
  - A fájl megnyitását kezdeményező folyamat egyedi azonosítója
  - A fájl egyedi azonosítói

    - A módosítási művelet típusa
    - Jelölő, amely azt mutatja, hogy a fájl a számítógép újraindítása után törlődik
    - A módosított fájl egyedi azonosítója
    - A fájl egyedi azonosítója a módosítás előtt
    - A fájl megnyitásának módját meghatározó bitjelzők csoportja
    - Adatok a hozzáférés-vezérlési listán szereplő műveletekről
    - A fájl tulajdonjogának vagy szülőcsoportjának változásaira vonatkozó adatok
- A bejelentkezési munkamenet adatai:
    - Bejelentkezési munkamenet azonosítója
    - A bejelentkezett felhasználó neve
    - Felhasználói fiók típusa
    - Munkamenet típusa
- Adatok a hálózati kapcsolatokról:
    - A kapcsolatot kezdeményező folyamat egyedi azonosítója
    - A kapcsolat kezdeményezéséhez használt helyi IP-cím
    - A kapcsolat végpontjának távoli IP-címe
    - Csatlakozás iránya
    - Adatátviteli protokoll
    - HTTP módszer
    - Elérési út a gazdagépnév nélkül
    - Gazdagépnév
    - A folyamat dinamikus állapota a kapcsolódás pillanatában
    - Jelölő, amely azt mutatja, hogy a kapcsolat a nyers szoftvercsatorna szintjén nyitva van
    - A kapcsolati munkamenetben használt TLS-verzió
    - A TLS-kiszolgáló neve
    - A TLS kiszolgálótanúsítvány MD5 és SHA1 kivonatai
    - A tanúsítványtulajdonos alternatív neveinek listája (SAN)
    - A TLS tanúsítvány kibocsátójának neve

    - A tanúsítvány sorozatszáma
    - Használt titkosítási algoritmus
    - A tanúsítvány kezdő és záró dátuma
    - A TLS ügyfél JA3 ujjlenyomata
    - A kiszolgáló JA3S ujjlenyomata
- Hallgatás közben rögzített adatok a hálózati porton:
    - A kapcsolatot kezdeményező folyamat egyedi azonosítója
- Parancssori beviteli adatok:
    - A konzolbevitelt kezdeményező folyamat egyedi azonosítója
    - Konzolbevitel típusa
    - Felhasználó vagy folyamat által beírt szöveg
- A folyamat létrehozására vonatkozó adatok:
    - A folyamat egyedi azonosítója
    - A szülőfolyamat egyedi azonosítója
    - A folyamat egyedi rendszerazonosítója
    - A folyamat elindítására szolgáló parancs
    - Bejelentkezési munkamenet azonosítója
    - Folyamatintegritási szint
    - A folyamatfájl egyedi azonosítója
    - Az értelmezett fájlok egyedi azonosítóinak listája
    - A folyamat típusa
- A folyamat által betöltött adatok a modulról:
    - A letöltést kezdeményező folyamat egyedi azonosítója
    - A folyamatba feltöltött fájl teljes elérési útja
    - A modulfájl egyedi azonosítója
    - A .NET-szerelvény teljes tartományneve, ha a betöltött fájl .NET-modul
    - A szerelvényjegyzékfájlban definiált .NET-szerelvény jelölői

- A folyamat megszüntetésére vonatkozó adatok:
  - A megszakított folyamat egyedi azonosítója
- A beállításjegyzék-módosítással kapcsolatos adatok:
  - A beállításjegyzék-módosítást kezdeményező folyamat egyedi azonosítója
  - A beállításjegyzék-művelet típusa
  - A beállításkulcs teljes elérési útja
  - Az érték neve a beállításkulcsban
  - A beállításkulcs értékében tárolt adatok típusa
  - A beállításkulcs értékében megadott adatok
  - A kulcs neve átnevezés előtt
  - A kulcs vagy az elsődleges kulcscsoport tulajdonosának megváltozásával kapcsolatos információk
  - A kulcs hozzáférés-vezérlési listáján (ACL) végrehajtott módosítások listája
- Az észlelt fenyegetéssel és annak feldolgozásával kapcsolatos adatok:
  - Jelzölő, amely azt jelzi, hogy a fenyegetés-észlelés a háttérben futott
  - Fenyegetésről szóló döntés
  - A döntés neve
  - Az adatbázisrekord egyedi azonosítója
  - Az az időpont, amikor a fenyegetési rekord mentésre került az adatbázisban
  - A fenyegetés feldolgozási módja
  - Fertőzött objektum típusa
  - Fertőzött objektum neve
  - Az objektum MD5 és SHA256 hash kivonatai
  - A fertőzött objektum egyedi azonosítója
  - A fertőzött objektumot az internetről letöltő folyamat egyedi azonosítója
  - Az az URL, ahonnan a fertőzött objektumot letöltötték
  - A fertőzött objektumot küldő feladó e-mail-címe
  - Hálózati protokoll, amelyen keresztül a fertőzött objektum érkezett
  - Helyi cím, ahonnan a fertőzött objektum érkezett

    - Külső cím, ahonnan a fertőzött objektum érkezett
    - Objektumtartalom típusa
    - Objektumtartalom
- A folyamatokhoz való hozzáférésre vonatkozó adatok:
    - A hozzáférést megkísérlő folyamat egyedi azonosítója
    - Az elért célfolyamat egyedi azonosítója
    - A célfolyamattól kért jogosultságok készlete
    - Művelet típusa
    - Hívások készlete a folyamathoz való hozzáférés pillanatában
    - Forrásfolyamat leírása
    - Célfolyamat leírása
- DNS-adatok:
    - A DNS-lekérdezést kezdeményező folyamat egyedi azonosítója
    - DNS-kiszolgáló IP-címe
    - A DNS-lekérdezések működését kezelő jelölők
    - A kérés feldolgozásának állapota
    - A DNS-lekérdezésben megadott teljes tartománynév
    - Adattípus a DNS-lekérdezésben
    - DNS-kiszolgáló válaszai
- A kódbeszúrás adatai:
    - A kódbeszúrást megkísérlő folyamat egyedi azonosítója
    - Használt hozzáférési mód
    - Hívások készlete a beszúrt kód észlelésének időpontjában
    - A célfolyamat egyedi azonosítója, amelybe a kódot feltöltötték
    - Adatok a célfolyamat parancssorában bekövetkezett változásokról
    - Célfolyamat címe
    - A célfolyamatba feltöltött DLL-könyvtár neve
    - A DDL-fájl teljes elérési útja

- Adatok a megnevezett csatornákkal végzett műveletekről:
  - A csatornát létrehozó vagy ahhoz csatlakozó folyamat egyedi azonosítója
  - A megnevezett csatorna teljes neve
  - A művelet típusa (létrehozás vagy csatlakozás)
- Adatok a WMI-lekérdezésekről:
  - A WMI-műveletet kezdeményező folyamat egyedi azonosítója
  - A WMI-művelet típusa
  - A WMI-lekérdezés céleszközének neve
  - A WMI-lekérdezést kezdeményező felhasználói fiók
  - A WMI-lekérdezés szövege
  - Az a névtér, amelyben a WMI-lekérdezés végrehajtásra kerül
  - A WMI-szűrő neve
  - A feldolgozó objektum neve
  - A feldolgozó objektum műveletét leíró szöveg
- Adatok a LDAP-lekérdezésekről:
  - A LDAP-kérést létrehozó folyamat egyedi azonosítója
  - Az LDAP-lekérdezések keresési hatóköre
  - LDAP szűrő
  - Paraméter, amely azt az Active Directory-partíciót adja meg, amelyre a lekérdezés irányult
  - LDAP keresési attribútumok
- Adatok a csatlakoztatott USB-eszközökről:
  - USB-eszközművelet típusa
  - USB-eszköz típusa
  - Az USB-eszköz azonosítója
  - USB-eszköz neve
  - Az USB-eszköz elérési útja
  - Jelölő, amely azt mutatja, hogy az USB-eszköz rendszermeghajtó
- Ütemezett feladatok létrehozásával, törlésével és módosításával kapcsolatos adatok

- A szolgáltatások létrehozásával, törlésével és módosításával kapcsolatos adatok
- A fájlrendszer csatlakoztatásával és leválasztásával kapcsolatos adatok
- Adatok az EDR Expert (on-premise) összetevő működéséről:
  - Információ az ügynök indításával/leállításával kapcsolatban
  - Információ az ügynök telepítéséről/eltávolításáról
  - Az ügynökindítás egyedi azonosítója
  - Az ügynökfolyamat rendszerazonosítója
  - Az ügynökfolyamat egyedi azonosítója
  - Az ügynök megszűnésének oka
  - Ügynöki folyamat befejező kódja
- Az események szűrésének beállításai:
  - Modulnevek
  - Az objektumok teljes elérési útvonala
  - Az objektumok MD5 és SHA256 hash kivonatai
  - A Windows eseménynapló bejegyzéseinek azonosítói
  - Digitális tanúsítvány beállításai
  - Forgalom iránya, IP-címek, portok, protokollok, a futtatható fájlok teljes elérési útja
  - Felhasználónevek
  - Felhasználói bejelentkezési típusok
  - A kiszűrt telemetriai események típusai

A Kaspersky Endpoint Security beépített ügynökéhez intézett, az EDR Expert összetevőre vonatkozó kérések adatai

- Általános feladatbeállítások:
  - Feladattípus
  - Feladatütemezési beállítások
  - Azoknak a fiókoknak a neve és jelszava, amelyekkel a feladatok lefuttathatók
  - A beállítások verziói

- A karanténba helyezett objektumok azonosítói
- Az objektumok elérési útja
- Az objektumok MD5 és SHA256 hash kivonatai
- Parancssor a folyamat argumentumokkal való megkezdéséhez
- A feladatok elvégzésekor végrehajtott további műveletek jelölői
- A kiszolgálóról lekérdezni kívánt IOC-fájlazonosítók
- IOC-fájlok
- A szolgáltatás neve
- Szolgáltatás indítási típusa
- Mappák, amelyekre vonatkozóan a *Get forensic* feladat eredményeit meg kell kapni
- A *Get forensic* feladathoz kapcsolódó objektumnevek és bővítmények maszkjai

- Hálózatelkülönítési beállítások:
  - Beállítástípusok
  - A beállítások verziói
  - A hálózatelkülönítési kizárások és kizárási beállítások listái: forgalom iránya, IP-címek, portok, protokollok, a futtatható fájlok teljes elérési útja
  - A további műveletek jelölői
  - Az automatikus leválasztás letiltásának ideje
- Végrehajtás-megelőzési beállítások:
  - Beállítástípusok
  - A beállítások verziói
  - A futtatás megakadályozási szabályainak és a szabályok beállításainak listája: objektumok elérési útvonala, objektumok típusa, objektumok MD5 és SHA256 hash kivonatai
  - A további műveletek jelölői

A Kaspersky Endpoint Security által az EDR Expert összetevőnek küldött kérésekből származó adatok

Az EDR Expert (on-premises) megoldással való integráció során a következő adatok kerülnek helyi tárolásra a számítógépeken.

- Szinkronizálási kérésekben:
  - Egyedi azonosító
  - A kiszolgáló webcímének alapértelmezett része
  - Számítógép neve
  - Számítógép IP-címe
  - Számítógép MAC-címe
  - Helyi idő a számítógépen
  - A Kaspersky Endpoint Security önvédelmi állapota
  - A számítógépre telepített operációs rendszer neve és verziója
  - A Kaspersky Endpoint Security verziója
  - Az alkalmazásbeállítások és a feladatbeállítások verziói
  - Feladatállapotok: feladatok azonosítói, végrehajtási állapotok, hibakódok
- A fájlok kiszolgálóról való lekérésére irányuló kérésekben:
  - A fájlok egyedi azonosítói
  - Egyedi Kaspersky Endpoint Security-azonosító
  - A tanúsítványok egyedi azonosítói
  - A telepített Central Node összetevővel rendelkező kiszolgáló webcímének alapértelmezett része
  - Gazdagép IP-címe
- A feladatvégrehajtási eredményekről szóló jelentésekben:
  - Gazdagép IP-címe
  - Információk az IOC- vagy YARA-vizsgálat során észlelt objektumokról
  - A feladatok elvégzésekor végrehajtott további műveletek jelölői
  - Feladatvégrehajtási hibák és visszatérési kódok
  - Feladatok befejezési állapotai

- Feladatok befejezési ideje
- A feladatok végrehajtásához használt beállítások verziói
- A kiszolgálóra küldött, a karanténba áthelyezett és a karanténból visszaállított objektumokra vonatkozó információ: objektumok elérési útjai, MD5 és SHA256 hash kivonatok, a karanténba áthelyezett objektumok azonosítói
- A kiszolgáló kérésére a számítógépen elindított vagy leállított folyamatokra vonatkozó információk: PID és UniquePID, hibakód, az objektumok MD5 és SHA256 hash kivonatai
- A kiszolgáló kérésére a számítógépen elindított vagy leállított szolgáltatásokról szóló információk: szolgáltatás neve, indítási típus, hibakód, a szolgáltatásokhoz kapcsolódó fájlképek MD5 és SHA256 hash kivonatai
- Információ olyan objektumokkal kapcsolatban, amelyeknél a YARA-vizsgálat érdekében memóriakiíratásra került sor (útvonalak, memóriaképfájlok azonosítója)
- A kiszolgáló által kért fájlok

- Futó folyamatok adatai:
  - Futtatható fájl neve a teljes útvonalat és a kiterjesztést is beleértve
  - A folyamat automatikus futtatásával kapcsolatos paraméterek
  - Folyamatazonosító
  - Bejelentkezési munkamenet azonosítója
  - Bejelentkezési munkamenet neve
  - A folyamat elindításának dátuma és időpontja
  - Az objektum MD5 és SHA256 hash kivonatai
- Fájlokkal kapcsolatos adatok:
  - A fájl elérési útja
  - Fájlnév
  - Fájlméret
  - Fájlattribútumok
  - A fájl létrehozásának dátuma és időpontja
  - A fájl legutóbbi módosításának dátuma és időpontja
  - Fájlleírás
  - Vállalat neve

- Az objektum MD5 és SHA256 hash kivonatai
- Beállításkulcs (az automatikus futtatási pontokhoz)

- Az objektumok információinak fogadásakor felmerülő hibák adatai:
  - Annak az objektumnak a teljes neve, amelynek a feldolgozása során a hiba felmerült
  - Hibakód
- YARA-vizsgálati eredményekben szereplő adatok:

  A Kaspersky Endpoint Security beépített ügynöke automatikusan elküldi a YARA-vizsgálati eredményeket a Kaspersky Anti Targeted Attack Platform számára, fenyegetésfejlődési lánc felépítése céljából.

  Az adatokat a rendszer ideiglenesen helyben tárolja a feladatvégrehajtási eredmények elküldési várólistáján a Kaspersky Anti Targeted Attack Platform kiszolgálója számára. Az adatok az elküldés után törlődnek az ideiglenes tárból.
  - A fájl MD5 és SHA256 hash kivonatai
  - A fájl teljes neve
  - A fájl elérési útja
  - Fájlméret
  - Folyamatnév
  - Folyamat argumentumai
  - A folyamatfájl elérési útja
  - A folyamat Windows-azonosítója (PID)
  - A szülőfolyamat Windows-azonosítója (PID)
  - A folyamatot elindító felhasználói fiók
  - A folyamat elindításának dátuma és időpontja
- IOC-vizsgálati eredményekben szereplő adatok:
  - IP-cím az ARP-tábláról
  - Fizikai cím az ARP-tábláról
  - DNS-rekord neve
  - DNS-rekord típusa
  - Gazdagépnév
  - IP-cím
  - Eseményazonosító a naplóban

- Adatforrás neve a naplóban
- Napló neve
- Felhasználónév
- Az esemény generálásának dátuma és ideje ISO formátumban
- A fájl MD5 és SHA256 hash kivonatai
- A fájl teljes neve
- Fájlméret
- A távoli IP-cím és port, amellyel kapcsolat létesült a vizsgálat során
- A helyi adapter IP-címe és portja
- Protokoll
- Folyamatnév
- Folyamat argumentumai
- A folyamatfájl elérési útja
- A folyamat Windows-azonosítója (PID)
- A szülőfolyamat Windows-azonosítója (PID)
- A folyamatot elindító felhasználói fiók
- A folyamat elindításának dátuma és időpontja
- A beállításkulcs elérési útja
- A beállításkulcs neve
- A beállításkulcs szöveges értéke
- A szolgáltatás neve
- A szolgáltatás leírása
- A DLL-szolgáltatás elérési útja és neve
- A szolgáltatás futtatható fájljának elérési útja és neve
- A szolgáltatás Windows-azonosítója (PID)
- Szolgáltatás típusa
- A szolgáltatás állapota
- A szolgáltatás indítási módja

- Az operációs rendszer neve
- Az operációs rendszer verziója
- Számítógépes hálózat neve tartomány nélkül
- Tartomány vagy munkacsoport
- Felhasználónév
- Kötet neve
- Kötet betűjele
- Kötet típusa

Kaspersky Network Detection and Response (KATA)

A Kaspersky Endpoint Security eltávolításakor az alkalmazás által a számítógépen helyileg tárolt összes adat törlődik a számítógépről.

Telemetriai adatok

- **Fájlokkal kapcsolatos adatok**
  - A fájl egyedi azonosítói
  - Fájltípus
  - A fájl teljes elérési útja
  - Fájlméret
  - Fájlattribútumok
  - Zónaazonosító
  - A fájl létrehozásának dátuma és időpontja
  - A fájl legutóbbi módosításának dátuma és időpontja
  - Eredeti fájlnév
  - Alkalmazásnév
  - Alkalmazás verziója
  - Alkalmazás szállítója

- Fájlleírás
- Fájlverzió
- Az objektum MD5 és SHA256 hash kivonatai
- A fájlaláírás ellenőrzésének eredménye
- A fájlaláírás létrehozásának dátuma és időpontja
- Az aláírási fájlban használt tanúsítványláncok
- Tanúsítványlánc típusa
- Tanúsítványok a láncban
- A tanúsítvány kibocsátójának neve
- A tanúsítvány tulajdonosának neve
- A tanúsítvány sorozatszáma
- Tanúsítvány ujjlenyomat-algoritmusa
- Tanúsítvány ujjlenyomata
- A tanúsítvány érvényességi ideje

- **A bejelentkezési munkamenet adatai**
  - Bejelentkezési munkamenet azonosítója
  - A bejelentkezett felhasználó fiókneve
  - Felhasználói fiók típusa
  - Munkamenet típusa
  - Annak a számítógépnek az IP-címe, amelyről a bejelentkezési kísérlet történt
  - Annak a helyi számítógépnek az IP-címe, amelyre a bejelentkezési kísérlet történt
  - Jelölő, amely azt mutatja, hogy az esemény által képviselt munkamenet emelt szintű jogosultságokkal és rendszergazdai jogokkal rendelkezik
  - Paraméter, amely azt jelzi, hogy más munkamenetek kapcsolódnak-e ehhez a bejelentkezési munkamenethez
  - A terminál munkamenetében használt protokoll
  - A terminál munkamenetében használt IPv4 protokoll

- **A hálózati kommunikációra vonatkozó adatok**
  - Az adatgyűjtés időtartamának kezdete és vége
  - Kapcsolatok listája
  - A számítógép helyi IP-címe
  - A számítógép helyi MAC-címe
  - A számítógép távoli IP-címe
  - A számítógép távoli MAC-címe
  - Átjáró IP-címe
  - A továbbított adatcsomagok száma
  - Fogadott adatcsomagok száma
  - Az átvitt bájtok teljes száma
  - Adatátviteli protokoll
  - Ethernet-keret EtherType mezője
  - Az intervallum első csomagjának hasznos előtagja
  - Annak a hálózati interfésznek az IPv4-címe, amelyen keresztül a kommunikáció rögzítése történt
- **Adatok a hálózati kapcsolatról**
  - A kapcsolatot kezdeményező folyamat egyedi azonosítója
  - Adatátviteli protokoll
  - A kapcsolat kezdeményezéséhez használt helyi IP-cím
  - A kapcsolat végpontjának távoli IP-címe
  - HTTP módszer
  - Elérési út a gazdagépnév nélkül
  - Gazdagépnév
  - A folyamat dinamikus állapota a kapcsolódás pillanatában
  - Csatlakozás iránya
  - Dinamikus folyamatállapot
  - Ethernet-keret EtherType mezője

- **Hallgatás közben rögzített adatok a hálózati porton**
  - A kapcsolatot kezdeményező folyamat egyedi azonosítója
  - Adatátviteli protokoll
  - Helyi cím
  - A folyamat dinamikus állapota a kapcsolódás pillanatában
- **A kapcsolat ellenőrzésének eredménye**
  - A gazdagép hálózati beállításai
  - A hálózati interfész leírása
  - DNS-tartománynév
  - A számítógép helyi MAC-címe
  - Az IP-kapcsolat mérőszáma
  - IP-címek listája
  - IP-cím
  - Hálózati maszk
  - Átjáró IP-címe
  - Átjáró MAC-címe
  - A telepített javítások listája
  - Javítás száma
  - A javítás telepítésének dátuma
  - Eszközmodell
  - Eszköz szállítója
  - A gazdagép azonosítója a Kaspersky Security Centerben
  - A telepített Kaspersky vírusirtó leírása
  - A telepített Kaspersky vírusirtó összetevőjének neve
  - A telepített Kaspersky vírusirtó összetevőjének verziója
  - A telepített Kaspersky vírusirtó összetevőjének adatbázis-verziója
  - A telepített Kaspersky vírusirtó összetevőjének utolsó adatbázis-frissítési dátuma
  - A telepített Kaspersky vírusirtó összetevőjének állapota

- A licenckulcsok listája
- Kulcs sorozatszáma
- Kulcs típusa
- Kulcs lejáratának dátuma
- Kulcs állapota

- **A folyamat létrehozásának adatai a gazdagépen**
  - A folyamat egyedi azonosítója
  - A szülőfolyamat egyedi azonosítója
  - A folyamat egyedi rendszerazonosítója
  - A folyamat elindítására szolgáló parancs
  - Bejelentkezési munkamenet azonosítója
  - Terminál munkamenet-azonosítója
  - A folyamatfájl egyedi azonosítója
  - Folyamatintegritási szint
  - A folyamatjogok tokenjeinek listája
  - Attribútumjogok
  - Az értelmezett fájlok egyedi azonosítóinak listája
  - Folyamat állapota
  - A folyamat elindítására szolgáló parancs
- **A folyamat megszüntetésére vonatkozó adatok**
  - A folyamat egyedi azonosítója
- **Adatok az észlelt fenyegetésről**
  - Fenyegetési információk
  - Fenyegetésről szóló döntés
  - AMR rekordszám
  - Víruskereső adatbázis-verziója
  - Fenyegetés-észlelési mód
  - A fenyegetés egyedi azonosítója

- Védelmi technológia
- Információ a fertőzött objektumról
- Fertőzött objektum típusa
- Fertőzött objektum neve
- Az objektum MD5 és SHA256 hash kivonatai
- A fertőzött folyamat egyedi azonosítója
- A fertőzött objektum egyedi azonosítója
- A fertőzött objektumot az internetről letöltő folyamat egyedi azonosítója
- Az az URL, ahonnan a fertőzött objektumot letöltötték
- A fertőzött objektumot küldő feladó e-mail-címe
- Hálózati protokoll, amelyen keresztül a fertőzött objektum érkezett
- Helyi cím, ahonnan a fertőzött objektum érkezett
- Külső cím, ahonnan a fertőzött objektum érkezett
- Objektumtartalom típusa
- Az észlelt fenyegetés környezete
- Objektumtartalom
- Jelzölő, amely azt jelzi, hogy a fenyegetés-észlelés a háttérben futott

- **A fenyegetések feldolgozásával kapcsolatos adatok**
  - Fenyegetési információk
  - Fenyegetésről szóló döntés
  - AMR rekordszám
  - Víruskereső adatbázis-verziója
  - Fenyegetés-észlelési mód
  - Fertőzött objektum neve
  - Az objektum MD5 és SHA256 hash kivonatai
  - A fertőzött folyamat egyedi azonosítója
  - A fertőzött objektum egyedi azonosítója
  - Hálózati protokoll, amelyen keresztül a fertőzött objektum érkezett

- Helyi cím, ahonnan a fertőzött objektum érkezett
- Külső cím, ahonnan a fertőzött objektum érkezett
- A fenyegetés feldolgozottsági állapota
- Az ok, ami miatt a fenyegetés nem orvosolható
- Helyi fizikai cím

- **Adatok a felhasználókról**
  - Felhasználói SID
  - Felhasználói azonosító
  - Felhasználónév
  - A felhasználó teljes neve
  - Felhasználói leírás
  - A fiók aktív vagy blokkolt
  - Lejárt-e a jelszó
  - Szükséges-e a jelszó megváltoztatása
  - Megengedett-e a jelszó megváltoztatása
  - Felhasználói fiók típusa
  - Engedélyezve van-e az automatikus bejelentkezés ehhez a fiókhoz
  - A csoportok listája, amelyekhez a felhasználó tartozik

Integráció a Kaspersky Unified Monitoring and Analysis Platform (KUMA) megoldással

A Kaspersky Endpoint Security eltávolításakor az alkalmazás által a számítógépen helyileg tárolt összes adat törlődik a számítógépről.

A Kaspersky Unified Monitoring and Analysis Platform (KUMA) integrálásakor a kapcsolatbeállítások adatai, valamint a Windows-naplókban regisztrált összes esemény átvitelre kerül.

A fő Windows-eseménynaplók a Rendszer, a Biztonság, az Alkalmazás, a Továbbított események és a Hardveres események. A felhasználók egyedi naplófájlokat is létrehozhatnak és kezelhetnek, hogy azok megfeleljenek egyedi igényeiknek.

Az Európai Unió jogszabályainak való megfelelés (GDPR)

A Kaspersky Endpoint Security az alábbi esetekben továbbíthatja az adatokat a Kaspersky számára:

- A Kaspersky Security Network használata.
- Az alkalmazás aktiválása aktiváló kóddal.
- Alkalmazásmodulok és vírusadatbázisok frissítése.
- Hivatkozások követése az alkalmazás felületén.

Az adatok besorolásától és az adatok fogadásának területétől függetlenül a Kaspersky betartja az adatbiztonságra vonatkozó magas követelményeket, és különféle jogi, szervezési és technikai intézkedéseket alkalmaz a felhasználók adatainak védelme, az adatok biztonságának és titkosságának garantálása, valamint az adatok biztonságának biztosítása, valamint a vonatkozó jogszabályok által garantált felhasználói jogok biztosítása érdekében. Az adatvédelmi szabályzat szövege az alkalmazás forgalmazási készletében található, és elérhető a Kaspersky webhelyén.

A Kaspersky Endpoint Security használata előtt figyelmesen olvassa el a továbbított adatok leírását a Végfelhasználói licencszerződésben és a Kaspersky Security Network nyilatkozatban. Ha a Kaspersky Endpoint Security-től a leírt esetek bármelyikében továbbított konkrét adatok a helyi jogszabályok vagy szabványok szerint személyes adatoknak minősülnek, akkor biztosítania kell, hogy ezeket az adatokat törvényesen dolgozzák fel, és meg kell szereznie a végfelhasználók beleegyezését az ilyen adatok gyűjtésére és továbbítására.

Olvassa el a Végfelhasználói licencszerződést és keresse fel a Kaspersky webhelyet, ha szeretné bővebben megismerni, hogyan kapjuk meg, dolgozzuk fel, tároljuk és semmisítjük meg az alkalmazás használatára vonatkozó adatokat, miután elfogadta a Végfelhasználói licencszerződést és beleegyezik a Kaspersky Security Network nyilatkozatba. A license.txt és ksn_<language ID>.txt fájlok tartalmazzák a Végfelhasználói licencszerződés és a Kaspersky Security Network nyilatkozat szövegét, valamint megtalálhatóak az alkalmazás terjesztőkészletben.

Ha nem akarja az adatokat továbbítani a Kaspersky számára, letilthatja az adatok feletti rendelkezést.

Kaspersky Security Network használata

A Kaspersky Security Network használatával Ön hozzájárul, hogy automatikusan megadja a Kaspersky Security Network nyilatkozatban felsorolt adatokat. Ha nem járul hozzá ezen adatok megadásához a Kaspersky számára, használja a Privát Kaspersky Security Network (KPSN) szolgáltatást, vagy tiltsa le a KSN használatát. A KPSN-ről szóló további részletekért lásd a Kaspersky Private Security Network dokumentációját.

Az alkalmazás aktiválása aktiváló kóddal

Az aktiváló kód használatával hozzájárul, hogy automatikusan megadja a Végfelhasználói licencszerződésben felsorolt adatokat. Ha nem járul hozzá ezen adatok megadásához a Kaspersky számára, használjon kulcsfájlt a Kaspersky Endpoint Security aktiválásához.

Alkalmazásmodulok és vírusadatbázisok frissítése

A Kaspersky kiszolgáló használatával hozzájárul, hogy automatikusan megadja a Végfelhasználói licencszerződésben felsorolt adatokat. A Kaspersky-nek ezekre az információkra a Kaspersky Endpoint Security jogszerű felhasználásának ellenőrzéséhez van szüksége. Ha nem járul hozzá ezen adatok megadásához a Kaspersky számára, használja a Kaspersky Security Centert az adatbázis-frissítésekhez, vagy használja a Kaspersky Update Utility programot.

Hivatkozások követése az alkalmazás felületén

Az alkalmazás felületén lévő hivatkozások használatával hozzájárul, hogy automatikusan megadja a Végfelhasználói licencszerződésben felsorolt adatokat. Az egyes hivatkozásoknál továbbított adatok pontos listája attól függ, hogy a hivatkozás hol található az alkalmazás felületén, és milyen problémát próbál megoldani. Ha nem járul hozzá ezen adatok megadásához a Kaspersky számára, használja az egyszerűsített alkalmazásfelületet, vagy rejtse el az alkalmazásfelületet.

Memóriakiíratás

Ha engedélyezte a memóriakép írását, a Kaspersky Endpoint Security létrehoz egy memóriakiírási fájlt, amely a memóriának az alkalmazás folyamataiból a memóriakiírási fájl létrehozásának pillanatában származó összes adatát tartalmazza.

Védjegyekkel kapcsolatos megjegyzések

A bejegyzett védjegyek és szolgáltatási jegyek a megfelelő tulajdonosaik tulajdonát képezik.

Az Adobe, Acrobat, Flash, Reader és a Shockwave az Adobe bejegyzett védjegye vagy védjegye az Egyesült Államokban és/vagy más országokban.

Az Amazon, az Amazon Web Services és az AWS az Amazon.com, Inc. vagy leányvállalatainak védjegye.

Az Apple, a FireWire, az iTunes, a Mac és a Safari az Apple Inc. védjegyei.

Az Arm az Arm Limited (vagy leányvállalatainak) bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

Az AutoCAD az Autodesk, Inc. és/vagy leányvállalatai és/vagy társvállalatai védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Bluetooth szó, jel és logó a Bluetooth SIG, Inc. tulajdonát képezi.

A Borland a Borland Software Corporation védjegye vagy bejegyzett védjegye.

A Cisco, a Cisco AnyConnect, az IOS a Cisco Systems, Inc. és/vagy leányvállalatai bejegyzett védjegye vagy védjegye az Egyesült Államokban és bizonyos más országokban.

A Citrix, a Citrix Provisioning, a Citrix Provisioning Services, a Citrix Virtual Apps and Desktop, a XenDesktop és a XenServer a Cloud Software Group, Inc. és/vagy leányvállalatai bejegyzett védjegyei vagy védjegyei az Egyesült Államokban és/vagy más országokban.

A Cloudflare, a Cloudflare Workers és a Cloudflare logó a Cloudflare, Inc. védjegye és/vagy bejegyzett védjegye az Egyesült Államokban és más jogrendszerekben.

A Core az Intel Corporation vagy leányvállalatainak védjegye.

A dBase a dataBased Intelligence, Inc. védjegye.

A Dell Technologies, a Dell, az EMC és más védjegyek a Dell Inc. vagy leányvállalatainak védjegyei.

A Docker és a Docker logó a Docker, Inc. védjegye és/vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban. A Docker, Inc. és más felek védjegyjogokkal rendelkezhetnek az itt használt egyéb kifejezések tekintetében is.

Az ESET az ESET spol. s r.o. vagy az ESET megfelelő szervezeti egységének védjegye vagy bejegyzett védjegye.

A Foxit a Foxit Corporation bejegyzett védjegye.

A Radmin a Famatech bejegyzett védjegye.

A Google, az Android, a Google Public DNS, a Google Chrome és a Chrome a Google LLC védjegye.

A HUAWEI, a FusionCompute és a FusionSphere a Huawei Technologies Co., Ltd. védjegye.

Az ICQ az ICQ LLC védjegye és/vagy szolgáltatás-védjegye.

Az Intel az Intel Corporation vagy leányvállalatainak védjegye.

Az IBM az International Business Machines Corporation védjegye, mely a világ számos jogrendszerében be van jegyezve.

A Lenovo és a Lenovo ThinkPad a Lenovo védjegye az Egyesült Államokban és/vagy más országokban.

A Linux Linus Torvalds bejegyzett védjegye az Egyesült Államokban és más országokban.

A Logitech a Logitech bejegyzett védjegye vagy védjegye az Egyesült Államokban és/vagy más országokban.

A LogMeIn Pro és a Remotely Anywhere a LogMeIn, Inc. védjegye.

A Mail.ru a Mail.ru LLC védjegye.

A McAfee a McAfee LLC vagy leányvállalatainak védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft, az Access, az Active Directory, az ActiveSync, a Bing, a BitLocker, az Excel, a Hyper-V, az Internet Explorer, a JScript, a LifeCam Cinema, a Microsoft Edge, az MSDN, az MS-DOS, a MultiPoint, az Office 365, az Outlook, a PowerPoint, a PowerShell, a Skype, az SQL Server, a Surface, a Visual Basic, a Visual FoxPro, a Windows, a Windows Live, a Windows PowerShell, a Windows Server és a Windows Store a Microsoft vállalatcsoport védjegyei.

A Mozilla, a Firefox és a Thunderbird a Mozilla Foundation védjegyei az Egyesült Államokban és más országokban.

A NetApp a NetApp, Inc. védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

Az OpenSSL az OpenSSL Software Foundation védjegye.

Az OpenStack az OpenStack Foundation bejegyzett védjegye az Egyesült Államokban és más országokban.

Az Oracle, a Java és a JavaScript az Oracle és/vagy leányvállalatai bejegyzett védjegyei.

A Python a Python Software Foundation védjegye vagy bejegyzett védjegye.

A Realtek a Realtek Semiconductor Corporation védjegye.

SAMSUNG a SAMSUNG bejegyzett védjegye az Egyesült Államokban vagy más országokban.

A Thawte a Symantec Corporation vagy leányvállalatai védjegye vagy bejegyzett védjegye az Egyesült Államokban és más országokban.

A Trend Micro a Trend Micro Incorporated védjegye vagy bejegyzett védjegye.

A VERISIGN a VeriSign, Inc. és leányvállalatainak védjegye vagy bejegyzett védjegye az Egyesült Államokban és más országokban.

A VMware, a VMware ESXi, a VMware Horizon, a VMware Workstation, a VMware Tools és a VMware vSphere a VMware, Inc. bejegyzett védjegyei és/vagy védjegyei az Egyesült Államokban és más országokban.

A harmadik féltől származó kódra vonatkozó információk

A harmadik féltől származó kódra vonatkozó információkat az alkalmazás telepítési mappájában található legal_notices.txt fájl tartalmazza.