

kaspersky

Kaspersky Endpoint Security for Windows 11.8.0

© 2023 AO Kaspersky Lab

Tartalom

[Gyakori kérdések](#)

[Újdonságok](#)

[Kaspersky Endpoint Security for Windows](#)

[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](#)

[Frissítés az alkalmazás korábbi verziójáról](#)

[Alkalmazás eltávolítása](#)

[Eltávolítás a Kaspersky Security Centeren keresztül](#)

[Az alkalmazás eltávolítása a varázsló segítségével](#)

[Az alkalmazás licencelése](#)

[A végfelhasználói licencszerződésről](#)

[A licenc](#)

[A licenctanúsítvány](#)

[Az előfizetés](#)

[Tudnivalók a licenckulcsról](#)

[Az aktiváló kód](#)

[A kulcsfájl](#)

[Alkalmazások funkcionalitásának összehasonlítása a munkállomási licenctípustól függően](#)

[Alkalmazások funkcionalitásának összehasonlítása a kiszolgálói licenctípustól függően](#)

[Alkalmazás aktiválása](#)

[Az alkalmazás aktiválása a Kaspersky Security Centeren keresztül](#)

[Az Aktiválási varázslóval aktiválhatja az alkalmazást.](#)

[A licencadatok megtekintése](#)

[Licenc vásárlása](#)

[Előfizetés megújítása](#)

[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](#)

[Az Európai Unió jogszabályainak való megfelelés \(GDPR\)](#)

[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](#)

[Első lépések](#)

[A rendszabályok kezelése](#)

[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 számítógép vírusvizsgálata](#)

[Számítógép vizsgálata](#)

[Cserélhető meghajtók vizsgálata a számítógéphez történő csatlakoztatásukkor](#)

[Vizsgálat a háttérben](#)

[Vizsgálat a helyi menüből](#)

[Alkalmazás integritásának 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](#)

[Megosztott mappából való frissítések beállítása](#)

[Alkalmazásmodulok frissítése](#)

[Proxykiszolgáló használata a frissítésekhez](#)

[Utolsó frissítés visszagörgetése](#)

[Munkavégzés az aktív fenyegetésekkel](#)

[Aktív fenyegetések vírusmentesítése munkaállomásokon](#)

[Az aktív fenyegetések vírusmentesítése a kiszolgálókon](#)

[A Fejlett vírusmentesítő technológia be- és kikapcsolása](#)

[Aktív fenyegetések feldolgozása](#)

[Számítógépvédelem](#)

[Fájl védelem](#)

[A Fájl védelem engedélyezése és letiltása](#)

[A Fájl védelem automatikus szüneteltetése](#)

[A Fájlvédelem összetevő által fertőzött fájl észlelésekor elvégzett művelet módosítása](#)

[A Fájlvédelem összetevő védelmi hatókörének kialakítása](#)

[A vizsgálatmódok használata](#)

[Vizsgálati technológiák használata a Fájlvédelem összetevő működése során](#)

[A fájlvizsgálat optimalizálása](#)

[Az összetett fájlok vizsgálata](#)

[Vizsgálatmód megváltoztatása](#)

Web védelem

[A Web védelem engedélyezése és letiltása](#)

[A webes forgalomban észlelt rosszindulatú objektumokon végrehajtandó művelet módosítása](#)

[URL-címek vizsgálata adathalász és rosszindulatú webcímek adatbázisai ellen](#)

[Heurisztikus elemzés használata a Web védelem összetevő működése során](#)

[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](#)

Hálózati védelem

[A Hálózati védelem engedélyezése és letiltása](#)

[Támadó számítógép blokkolása](#)

[A blokkolásból kizárt címek beállítása](#)

[Blokkolásból való kizárások listájának exportálása és importálása](#)

[Hálózati támadások elleni védelem beállítása típus szerint](#)

Firewall

[A Tűzfal be- és kikapcsolása](#)

[A hálózati kapcsolat állapotának 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](#)

[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](#)

BadUSB védelem

[BadUSB védelem be- és kikapcsolása](#)

[Virtuális billentyűzet használata az USB-eszközök hitelesítésére](#)

AMSI védelem

[Az AMSI védelem engedélyezése és letiltása](#)

[Az AMSI védelem használata összetett fájlok vizsgálatához](#)

[Biztonsági rések kihasználásának megelőzése](#)

[A Biztonsági rések kihasználásának megelőzése összetevő be- és kikapcsolása](#)

[Sebezhetőség kihasználásának észlelésekor végzendő művelet kiválasztása](#)

[Rendszerfolyamatok memóriavédelme](#)

[Viselkedéselemzés](#)

[A Viselkedéselemzés be- és kikapcsolása](#)

[A rosszindulatú tevékenység észlelése esetén végrehajtandó művelet kiválasztása](#)

[A megosztott mappák védelme a külső titkosítás ellen](#)

[Megosztott mappák külső titkosítás elleni védelmének be- és kikapcsolása](#)

[Megosztott mappák külső titkosításának észlelése esetén végzendő művelet kiválasztása](#)

[Kizárás létrehozása a megosztott mappák külső titkosítás elleni védelmére](#)

[Megosztott mappák külső titkosítás elleni védelméből való kizárások címeinek beállítása](#)

[A megosztott mappák külső titkosítással szembeni védelméből származó kizárások listájának exportálása és importálása](#)

[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](#)

[Kármentesítő motor](#)

[Kaspersky Security Network](#)

[A Kaspersky Security Network használatának engedélyezése és letiltása](#)

[A privát KSN korlátozásai](#)

[Felhő mód be- és kikapcsolása a védelmi összetevőknél](#)

[KSN Proxy beállítások](#)

[Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével](#)

[Titkosított kapcsolatok vizsgálata](#)

[A titkosított kapcsolatok vizsgálata beállításainak konfigurálása](#)

[Titkosított kapcsolatok vizsgálata a Firefoxban és a Thunderbirdben](#)

[Titkosított kapcsolatok kizárása a vizsgálat alól](#)

[Adatok törlése](#)

[Számítógépvezérlés](#)

[Webfelügyelő](#)

[A Webfelügyelő be- és kikapcsolása](#)

[A webes erőforrások hozzáférési szabályainak műveletei](#)

[Webes erőforrás hozzáférési szabályainak megadása](#)

[Prioritás hozzárendelése webes erőforrások hozzáférési szabályaihoz](#)

[A webes erőforrások hozzáférési szabályainak engedélyezése és letiltása](#)

[Megbízható webcímek listájának exportálása és importálása](#)

[A webes erőforrások hozzáférési szabályainak tesztelése](#)

[Webes erőforrások címlistájának exportálása és importálása](#)

[A felhasználó internetes tevékenységének megfigyelése](#)

[A Webfelügyelő üzenetsablonjainak szerkesztése](#)

[Webes erőforrások címei maszkjainak használata](#)

[A webes erőforrások hozzáférési szabályainak áttelepítése az alkalmazás korábbi verzióiból](#)

Eszközfelügyelő

[Az Eszközfelügyelő be- és kikapcsolása](#)

[A hozzáférési szabályokról](#)

[Az eszközhozzáférési szabályok szerkesztése](#)

[A csatlakozóbuszok hozzáférési szabályainak szerkesztése](#)

[Wi-Fi-hálózat felvétele a megbízható listára](#)

[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 eszközhez 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 Anomáiafelügyelő

[Az Adaptív Anomáiafelügyelő engedélyezése és letiltása](#)

[Adaptív Anomáiafelügyeleti szabály engedélyezése és letiltása](#)

[Az Adaptív Anomáiafelügyeleti szabály kiváltásakor végrehajtott művelet módosítása](#)

[Kizárás létrehozása Adaptív Anomáiafelügyeleti szabályhoz](#)

[Kizárások exportálása és importálása az Adaptív Anomáiafelügyeleti szabályokhoz](#)

[Az Adaptív Anomáiafelügyeleti szabályok frissítéseinek alkalmazása](#)

[Adaptív Anomáiafelügyelő üzenetsablonok szerkesztése](#)

[Az Adaptív Anomáiafelügyelő jelentéseinek megtekintése](#)

Alkalmazásfelügyelő

[Az Alkalmazásfelügyelő funkcióinak korlátozásai](#)

[Az Alkalmazásfelügyelő engedélyezése és letiltása](#)

[Az Alkalmazásfelügyelő módjának kiválasztása](#)

[Munka az Alkalmazásfelügyeleti szabályokkal az alkalmazás felületén](#)

[Alkalmazásfelügyeleti szabály hozzáadása](#)

[Alkalmazásfelügyeleti szabályt kiváltó feltétel hozzáadása](#)

[Alkalmazásfelügyeleti szabály állapotának módosítása](#)

[Az Alkalmazásfelügyeleti szabályok kezelése a Kaspersky Security Centerben](#)

[A felhasználói számítógépeken telepített alkalmazásokra vonatkozó információk fogadása](#)

[Alkalmazáskategóriák létrehozása](#)

[Futtatható fájlok hozzáadása a Futtatható fájlok mappából az alkalmazáskategóriákba](#)

[Eseményhez kapcsolódó végrehajtható fájlok hozzáadása az alkalmazáskategóriához](#)

[Alkalmazásfelügyeleti szabály hozzáadása vagy módosítása a Kaspersky Security Center használatával](#)

[Az Alkalmazásfelügyeleti szabályok állapotának módosítása a Kaspersky Security Center segítségével](#)

[Alkalmazásfelügyeleti szabályok exportálása és importálása](#)

[Az Alkalmazásfelügyeleti szabályok tesztelése a Kaspersky Security Center segítségével](#)

[Az Alkalmazásfelügyelő összetevő tesztműködéséből eredő események megtekintése](#)

[A teszt módban blokkolt alkalmazások jelentéseinek megtekintése](#)

[Az Alkalmazásfelügyelő összetevő működéséből eredő események megtekintése](#)

[A blokkolt alkalmazásokra vonatkozó jelentés megtekintése](#)

[Az Alkalmazásfelügyeleti szabályok tesztelése](#)

[Alkalmazástevékenység-figyelő](#)

[Fájlok vagy mappák névmaszkjainak létrehozási szabályai](#)

[Az Alkalmazásfelügyelő üzenetsablonjainak szerkesztése](#)

[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](#)

[Jelszóvédelem](#)

[Jelszóvédelem engedélyezése](#)

[Jogosultságok megadása egyéni felhasználóknak vagy csoportoknak](#)

[Ideiglenes jelszó használata a jogosultságok megadásához](#)

[A Jelszóvédelem jogosultságok speciális szempontjai](#)

[Megbízható zóna](#)

[Kizárás a vizsgálatból létrehozása](#)

[A vizsgálatból való kizárás be- és kikapcsolása](#)

[Az észlelhető objektumok típusának kiválasztása](#)

[A megbízható alkalmazások listájának szerkesztése](#)

[Megbízható zónaszabályok engedélyezése és letiltása a megbízható alkalmazások listáján szereplő alkalmazásnál](#)

[Megbízható rendszertanúsítványok tárolójának használata](#)

[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](#)

[A külső kezelésvédelem be- és kikapcsolása](#)

[A távoli adminisztrációs alkalmazások támogatása](#)

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](#)

Adattitkosítás

[A titkosítási funkció korlátozásai](#)

[A titkosítási kulcs hosszának módosítása \(AES56 / AES256\)](#)

Kaspersky lemeztitkosítás

[Az SSD-meghajtó titkosításának speciális jellemzői](#)

[Teljes lemeztitkosítás a Kaspersky lemeztitkosítás technológiával](#)

[A titkosításból kizárt merevlemez listájának létrehozása](#)

[A titkosításból kizárt merevlemez 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](#)

[Az operációs rendszer frissítése](#)

[A titkosítás funkció hibáinak elhárításával kapcsolatos frissítés](#)

[A Hitelesítési ügynök nyomkövetési szintjének kiválasztása](#)

[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 fájl hozzáférési szabályainak kialakítása az alkalmazások számára](#)

[Adott alkalmazások által létrehozott és módosított fájl titkosítása](#)

[Visszafejtési szabály előállítása](#)

[A számítógép helyi meghajtóin lévő fájl visszafejtése](#)

[Titkosított csomagok létrehozása](#)

[Titkosított fájl hozzáféréseinek helyreállítása](#)

[Titkosított adatokhoz való hozzáférés visszaállítása az operációs rendszer hibáját követően](#)

[A titkosított fájlhoz 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 fájl 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

Kaspersky Endpoint Agent

Szabályzatok és feladatok áttelepítése a Kaspersky Endpoint Agent számára

A [KES+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra

Managed Detection and Response

Integráció az MDR-re

Áttelepítés a Kaspersky Endpoint Agentből

Endpoint Detection and Response

Integráció a Kaspersky Endpoint Detection and Response szolgáltatással

Áttelepítés a Kaspersky Endpoint Agentből

Biztonsági sérülési indikátorok vizsgálata (szabványos feladat)

Fájláthelyezése a Karanténba

Fájl lekérése

Fájl törlése

Folyamat indítása

Folyamat megszakítása

Végrehajtás megelőzése

Számítógép hálózatalkülönítése

1. melléklet Támogatott fájlkiterjesztések a végrehajtás megelőzéséhez

2. melléklet Támogatott szkriptértelmezők

3. melléklet IOC vizsgálat hatóköre a rendszerleíró adatbázisban (RegistryItem)

4. melléklet IOC-fájl követelményei

Kaspersky Sandbox

Integráció a Kaspersky Sandbox szolgáltatással

Áttelepítés a Kaspersky Endpoint Agentből

TLS-tanúsítvány hozzáadása

Kaspersky Sandbox-kiszolgálók hozzáadása

Biztonsági sérülési indikátorok vizsgálata (önálló feladat)

Karantén kezelése

A karantén maximális méretének konfigurálása

A karanténba helyezett fájlok adatainak küldése a Kaspersky Security Centernek

Kaspersky Security for Windows Server

A KES telepítése a KSWs-re

A KES aktiválása egy KSWs-kulccsal

Az alkalmazás kezelése a parancssorból

Az alkalmazás telepítése

Alkalmazás aktiválása

Alkalmazás eltávolítása

AVP parancsok

SCAN. Vírusvizsgálat

[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](#)

[EXPORTÁLÁS. Alkalmazásbeállítások exportálása](#)

[IMPORT. Alkalmazásbeállítások importálása](#)

[ADDKEY. Kulcsfájl alkalmazása](#)

[LICENSE. Licencelés](#)

[RENEW. Licenc vásárlása](#)

[PBATESTRESET. 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. Globális/privát KSN átmenet](#)

[KESCLI parancsok](#)

[Scan. Vírusvizsgálat](#)

[GetScanState. Vizsgálat befejezési állapota](#)

[GetLastScanTime. A vizsgálat befejezési időpontjának meghatározása](#)

[GetThreats. Az észlelt fenyegetésekre vonatkozó adatok beszerzése](#)

[UpdateDefinitions. Adatbázisok és alkalmazás-szoftvermodulok frissítése](#)

[GetDefinitionState. A frissítés befejezési időpontjának meghatározása](#)

[EnableRTP. Védelem engedélyezése](#)

[GetRealTimeProtectionState. Fájl védelem állapota](#)

[Version. Az alkalmazás verziójának azonosítása](#)

[Detection and Response felügyeleti parancsok](#)

[SANDBOX. A Kaspersky Sandbox felügyelete](#)

[MEGELŐZÉS. A végrehajtás megakadályozásának kezelése](#)

[ELKÜLÖNÍTÉS. A hálózatelkülönítés kezelése](#)

[RESTORE. Fájlok visszaállítása a Karanténból](#)

[IOCSKAN. Biztonsági sérülési indikátorok \(IOC\) vizsgálata](#)

[MDRLICENSE. MDR aktiválás](#)

[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](#)

[Memóriakiírás](#)

Memóriakiíratási fájlok és nyomkövetési fájlok védelme

Korlátozások és figyelmeztetések

Szójegyzék

Adathalász webcímek adatbázisa

Adminisztrációs csoport

Aktív kulcs

Archívum

Feladat

Fertőzhető fájl

Fertőzött fájl

Hálózati Ügynök

Hitelesítési ügynök

Hordozható fájlkezelő

IOC

IOC-fájl

Kártékony webcímek adatbázisa

Licenctanúsítvány

Maszk

OLE objektum

OpenIOC

Tanúsítvány kibocsátója

Téves riasztás

További kulcs

Trusted Platform Module (TPM)

Védelem hatóköre

Vírusadatbázisok

Vírusmentesítés

Vizsgálat hatóköre

Webes erőforrás címének normalizált formája

Függelékek

1. melléklet Alkalmazásbeállítások

Fájl védelem

Web védelem

Levelezés védelem

Hálózati védelem

Firewall

BadUSB védelem

AMSI védelem

Biztonsági rések kihasználásának megelőzése

Viselkedéselemzés

Behatolásmegelőző rendszer

Kármentesítő motor

Kaspersky Security Network

Webfelügyelő

Eszközfelügyelő

Alkalmazásfelügyelő

Adaptív Anomálfelügyelő

Végponti szenzor

[Kaspersky Sandbox](#)
[Endpoint Detection and Response](#)
[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 fájl típusok](#)
[5. melléklet A külső szolgáltatásokkal való interakció hálózati beállításai](#)
[6. melléklet Alkalmazásesemények a Windows eseménynaplójában](#)
[7. melléklet Alkalmazásesemények a Kaspersky Security Center eseménynaplójában](#)
[A harmadik féltől származó kódra vonatkozó információk](#)
[Védjegyekkel kapcsolatos megjegyzések](#)

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 számítógémem a pendrive-okról érkező vírusok ellen?](#)

[Hogyan futtathatók vírusvizsgálatot, ami rejtve van 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 \(letár\)?](#)

[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 számítógémem operációs rendszere hibás, de az adat titkosítva marad?](#)



TÁMOGATÁS

[Hol van tárolva a jelentésfájl?](#)

[Hogyan hozhatok létre nyomkövetési fájlt?](#)

[Hogyan engedélyezhetem a kiíratást?](#)

Újdonságok

11.8.0 frissítés

A Kaspersky Endpoint Security 11.8.0 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. [Új beépített ügynök a Kaspersky Endpoint Detection and Response Expert megoldás működésének támogatásához](#). A *Kaspersky Endpoint Detection and Response Expert* 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. 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](#).
2. Ezentúl könnyebb navigálni a [Hálózatfigyelő](#) felületén. A Hálózatfigyelő mostantól a TCP mellett az UDP protokollt is megjeleníti.
3. Javult a [Vírusvizsgálat](#) feladat. Ha a vizsgálat során újraindította a számítógépet, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol a vizsgálat megszakadt.
4. Mostantól beállíthatja a feladat végrehajtási idejének korlátját. Korlátozhatja a végrehajtási időt a *Vírusvizsgálat* és az *IOC vizsgálat* feladatoknál. A megadott idő elteltével a Kaspersky Endpoint Security leállítja a feladatot. A *Vírusvizsgálat* feladat végrehajtási idejének csökkentéséhez pl. [konfigurálhatja a vizsgálat hatókörét](#) vagy [optimalizálhatja a vizsgálatot](#).
5. A kiszolgálói platformok korlátozásai megszűnnek a több munkamenetes Windows 10 Enterprise rendszerre telepített alkalmazás esetén. A Kaspersky Endpoint Security a több munkamenetes Windows 10 Enterprise rendszert mostantól munkaállomásos operációs rendszernek tekinti, nem pedig kiszolgálói operációs rendszernek. Ennek megfelelően a [kiszolgálói platformok korlátozásai](#) többé nem vonatkoznak a több munkamenetes Windows 10 Enterprise rendszerre telepített alkalmazásra. Ezenkívül az alkalmazás munkaállomásos licenckulcsot használ az aktiváláshoz kiszolgálói licenckulcs helyett.

11.7.0 frissítés

A Kaspersky Endpoint Security for Windows 11.7.0 a következő új funkciókat és fejlesztéseket kínálja:

1. Frissült a [Kaspersky Endpoint Security for Windows kezelőfelülete](#).
2. [A Windows 11, a Windows 10 21H2 és a Windows Server 2022 támogatása](#).
3. Bekerült új összetevők:
 - A [Kaspersky Sandbox-szal való integráció céljából](#) egy beépített ügynök kerül hozzáadásra. A *Kaspersky Sandbox megoldás* észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Kaspersky Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Kaspersky Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (Kaspersky Sandbox-kiszolgálók). A megoldás részleteit a [Kaspersky Sandbox súgóban](#) találja.

A Kaspersky Sandbox használatához már nincs szükség a Kaspersky Endpoint Agentre. A Kaspersky Endpoint Security képes a Kaspersky Endpoint Agent összes funkcióját elvégezni. A Kaspersky Endpoint Agent házirendjeinek áttelepítéséhez használja az [áttelepítési varázslót](#). A Kaspersky Security Center 13.2 verzióra van szükség a Kaspersky Sandbox összes funkciójának működéséhez. A Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security for Windows szolgáltatásra történő áttéréssel kapcsolatos részletekért olvassa el az [alkalmazás súgóját](#).

- [Új beépített ügynök a Kaspersky Endpoint Detection and Response Optimum megoldás működésének támogatásához](#). A Kaspersky Endpoint Detection and Response Optimum 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](#).

A Kaspersky Endpoint Detection and Response használatához már nincs szükség a Kaspersky Endpoint Agent megoldásra. A Kaspersky Endpoint Security képes a Kaspersky Endpoint Agent összes funkcióját elvégezni. A Kaspersky Endpoint Agent házirendjeinek és feladatainak áttelepítéséhez használja az [áttelepítési varázslót](#). A Kaspersky Endpoint Detection and Response Optimum összes funkciójának használatához a Kaspersky Security Center 13.2 szükséges. A Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security for Windows szolgáltatásra történő áttéréssel kapcsolatos részletekért olvassa el az [alkalmazás súgóját](#).

4. Új [áttelepítési varázsló](#) a Kaspersky Endpoint Agent házirendjeinek és feladatainak áttelepítéséhez. Az áttelepítési varázsló új egyesített házirendeket és feladatokat hoz létre a Kaspersky Endpoint Security for Windows számára. A varázsló lehetővé teszi a Detection and Response megoldások Kaspersky Endpoint Agent szolgáltatásról Kaspersky Endpoint Security szolgáltatásra váltását. A Detection and Response megoldások közé tartozik a Kaspersky Sandbox, a Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) és a Kaspersky Managed Detection and Response (MDR).

5. A terjesztőkészletben is szereplő [Kaspersky Endpoint Agent](#) frissült a 3.11-es verzióra.

A Kaspersky Endpoint Security frissítések az alkalmazás felismeri a Kaspersky Endpoint Agent verzióját és rendeltetését. Ha a Kaspersky Endpoint Agent a Kaspersky Sandbox, a Kaspersky Managed Detection and Response (MDR) és a Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) használatára szolgál, a Kaspersky Endpoint Security átadja ezen megoldások használatát az alkalmazás beépített ügynökének. A Kaspersky Sandbox és az EDR Optimum esetében az alkalmazás automatikusan eltávolítja a Kaspersky Endpoint Agentet. Az MDR esetében a Kaspersky Endpoint Agentet manuálisan is eltávolíthatja. Ha az alkalmazás a Kaspersky Endpoint Detection and Response Expert (EDR Expert) használatára szolgál, a Kaspersky Endpoint Security frissíti a Kaspersky Endpoint Agent verzióját. Az alkalmazással kapcsolatos további információért olvassa el a Kaspersky Endpoint Agent szolgáltatást támogató Kaspersky megoldások dokumentációját.

6. Javult a BitLocker titkosítási funkciója:

- A bővített PIN-kód mostantól használható [BitLocker meghajtótitkosítással](#). A bővített PIN-kód lehetővé teszi a számokon kívül más karakterek használatát is: latin nagy- és kisbetűket, speciális karaktereket és szöközőket.
- Új funkció [a BitLocker-hitelesítés letiltására az operációs rendszer frissítésekor vagy a frissítőcsomagok telepítésekor](#). A frissítések telepítéséhez szükség lehet a számítógép többszöri újraindítására. A frissítések helyes telepítéséhez ideiglenesen kikapcsolhatja a BitLocker hitelesítést, és a frissítések telepítése után újra engedélyezheti a hitelesítést.
- Most már [leállíthatja a BitLocker titkosítási jelszó vagy a PIN-kód lejáratát dátumát](#). Amikor a jelszó vagy a PIN-kód lejár, a Kaspersky Endpoint Security új jelszót kér a felhasználatól.

7. Most már beállíthatja a BadUSB támadások megelőzéséhez szükséges billentyűzethitelesítési kísérletek maximális számát. Amikor eléri [a hitelesítési kód beírásához megadott sikertelen kísérletek számát](#), az USB-eszköz ideiglenesen zárolva lesz.

8. Javult a tűzfal funkciója:

- Most már beállíthat IP-címtartományt a [tűzfal csomagszabályaihoz](#). A címtartományt IPv4 vagy IPv6 formátumban adhatja meg. Például 192.168.1.1-192.168.1.100 vagy 12:34::2-12:34::99.
- Most már megadhat DNS-neveket [a tűzfal csomagszabályainál](#) IP-címek 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.

9. Javult a [Web Control szabály](#) keresése. Egy webes erőforrás hozzáférési szabályának kereséséhez a szabály nevén kívül használhatja a webhely URL-jét, felhasználónevet, tartalomkategóriát vagy adattípust.

10. Továbbfejlesztettük a *Vírusvizsgálat* feladatot:

- Továbbfejlesztettük a [Vírusvizsgálat](#) feladatot inaktív módban. Ha a vizsgálat során újraindította a számítógépet, a Kaspersky Endpoint Security automatikusan futtatja a feladatot onnan folytatva, ahol a vizsgálat megszakadt.
- Optimalizáltuk a [Vírusvizsgálat](#) feladatot. Alapértelmezés szerint a Kaspersky Endpoint Security csak akkor futtatja a vizsgálatot, ha a számítógép tétlen. A feladattulajdonságokban konfigurálhatja a számítógép vizsgálatának futtatási időpontját.

11. Most már korlátozhatja a felhasználók hozzáférését az [Alkalmazástevékenység-figyelő](#) által szolgáltatott adatokhoz. Az Alkalmazástevékenység-figyelő egy olyan eszköz, amellyel valós időben tekinthetők meg a felhasználó számítógépén futó alkalmazások tevékenységével kapcsolatos információk. A rendszergazda elrejtheti az Alkalmazástevékenység-figyelőt a felhasználótól az alkalmazás házirendjének tulajdonságaiban.

12. [Javult az alkalmazás REST API-n keresztüli felügyeletének biztonsága](#). A Kaspersky Endpoint Security mostantól érvényesíti a REST API-n keresztül küldött kérések aláírását. A program felügyeletéhez telepítenie kell egy kérésazonosító tanúsítványt.

[11.6.0 frissítés](#)

A Kaspersky Endpoint Security 11.6.0 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. [Windows 10 21H1 támogatás](#). A Microsoft Windows 10 operációs rendszer támogatásának részleteiért lásd a [Terméktámogatási Tudásbázist](#).
2. [Hozzá lett adva a Managed Detection and Response összetevő](#). Ez az összetevő megkönnyíti az interakciót a Kaspersky Managed Detection and Response néven ismert megoldással. A Kaspersky Managed Detection and Response (MDR) éjjel-nappal védelmet nyújt az egyre növekvő számú fenyegetésekkel szemben, amelyek képesek megkerülni az automatizált védelmi mechanizmusokat olyan cégek esetében, amelyek nehezen találnak magasan képzett szakértőket, vagy korlátozott belső erőforrásokkal rendelkeznek. A megoldás működéséről részletes információt a Kaspersky Managed Detection and Response súgójában talál.
3. A terjesztőkészletben is szereplő [Kaspersky Endpoint Agent](#) frissült a 3.10-es verzióra. A Kaspersky Endpoint Agent 3.10 új funkciókat kínál, megold néhány korábbi problémát, és javítja a stabilitást. Az alkalmazással kapcsolatos további információért olvassa el a Kaspersky Endpoint Agent szolgáltatást támogató Kaspersky megoldások dokumentációját.
4. A [Hálózati védelem beállításai](#)ban mostantól képes kezelni az olyan támadások elleni védelmet, mint a hálózati elárastás és a portkeresés.
5. Új módszer hálózati szabályok létrehozására a tűzfalhoz. Hozzáadhat [csomagszabályokat](#) és [alkalmazásszabályokat](#) a [Hálózatfigyelő](#) ablakban megjelenő kapcsolatokhoz. Azonban a hálózati szabályok csatlakozási beállításainak konfigurálása automatikusan megtörténik.
6. Ezentúl könnyebb navigálni a [Hálózatfigyelő](#) felületén. Új információk a hálózati tevékenységről: a hálózati tevékenységet kezdeményező folyamatazonosító; hálózat típusa (helyi hálózat vagy Internet); helyi portok. Alapértelmezés szerint a hálózat típusára vonatkozó információk rejtettek.
7. Mostantól lehetőség van Hitelesítési ügynöki fiókok automatikus létrehozására új Windows-felhasználóknak. Az Ügynök lehetővé teszi a felhasználónak a hitelesítés végrehajtását [Kaspersky lemeztitkosítási technológiával titkosított](#) meghajtók elérésekor és az operációs rendszer betöltésekor. Az alkalmazás 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. Ez azt jelenti, hogy a már titkosított meghajtókkal rendelkező számítógépek esetében nem kell [manuálisan hozzáadnia hitelesítési ügynöki fiókokat](#).
8. Mostantól lehetőség van a lemeztitkosítási folyamat figyelemmel kísérésére a felhasználó számítógépének felhasználói felületén (Kaspersky lemeztitkosítás és BitLocker). A Titkosítási figyelő eszközt a [fő alkalmazásablakból](#) futtathatja.

[11.5.0 frissítés](#)






A Kaspersky Endpoint Security 11.5.0 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. [Windows 10 20H2 támogatás](#). A Microsoft Windows 10 operációs rendszer támogatásának részleteiért lásd a [Terméktámogatási Tudásbázist](#).
2. Frissített [alkalmazásfelület](#). Ezenkívül frissítettük az [alkalmazás ikonját az értesítési területen](#), az alkalmazás értesítéseit és a párbeszédpaneleket.
3. Fejlesztve lett a Kaspersky Endpoint Security webes bővítmény felülete az Alkalmazásfelügyelő, az Eszközfelügyelő és az Adaptív anomálfelügyelő összetevőkhöz.
4. Bekerült egy funkció a szabályok és kizárások listájának importálására és exportálására XML-formátumban. Az XML-formátum lehetővé teszi a listák szerkesztését az exportálás után. A listákat csak a Kaspersky Security Center konzolban kezelheti. A következő listák érhetők el exportálásra/importálásra:
 - [Viselkedéselemzés \(kizárások listája\)](#).
 - [Web védelem \(megbízható webcímek listája\)](#).
 - [Levelezés védelem \(mellékletszűrő bővítmények listája\)](#).
 - [Hálózati védelem \(kizárások listája\)](#).
 - [Tűzfal \(hálózati csomagszabályok listája\)](#).
 - [Alkalmazásfelügyelő \(szabályok listája\)](#).
 - [Web felügyelő \(szabályok listája\)](#).
 - [Hálózati port figyelése \(a Kaspersky Endpoint Security által figyelt portok és alkalmazások listája\)](#).
 - [Kaspersky lemeztitkosítás \(kizárások listája\)](#).
 - [Cserélhető meghajtók titkosítása \(szabályok listája\)](#).
5. Az MD5 objektuminformáció hozzá lett adva a [fenyegetésészlelési jelentéshez](#). Az alkalmazás korábbi verzióiban a Kaspersky Endpoint Security csak az objektum SHA256 értékét mutatta.
6. Bekerült egy funkció az [eszközhozzáférési szabályok prioritásának hozzárendeléséhez](#) az Eszközfelügyelő beállításában. A prioritás hozzárendelése az eszközökhöz való felhasználói hozzáférés még rugalmasabb konfigurálását teszi lehetővé. Ha egy felhasználót több csoporthoz adtak hozzá, a Kaspersky Endpoint Security a legmagasabb prioritású szabály alapján szabályozza az eszközhozzáférést. Például csak olvasható jogosultságokat adhat a Mindenki csoportnak, és olvasási/írási jogosultságokat adhat a rendszergazdák csoportnak. Ehhez rendeljen 0-s prioritást a rendszergazdák csoporthoz, és rendeljen 1-es prioritást a Mindenki csoporthoz. A prioritást csak azokhoz az eszközökhöz konfigurálhatja, amelyek rendelkeznek fájlrendszerrel. Ide tartoznak a merevlemezek, cserélhető meghajtók, hajlékonylemezes-meghajtók, CD/DVD-meghajtók és hordozható eszközök (MTP).
7. Bekerült új funkció:
 - [Hangos értesítések kezelése](#).
 - Költségtudatos hálózati figyelés: A Kaspersky Endpoint Security korlátozza saját hálózati forgalmát, ha az internetkapcsolat korlátozott (például mobilkapcsolaton keresztül).

- [A Kaspersky Endpoint Security beállításainak kezelése megbízható távoli adminisztrációs alkalmazásokon keresztül](#) (például TeamViewer, LogMeIn vagy Remotely Anywhere). Távoli adminisztrációs alkalmazások segítségével elindíthatja a Kaspersky Endpoint Security alkalmazást, és kezelheti a beállításokat az alkalmazás felületén.
 - [Kezelheti a biztonságos forgalom vizsgálatának beállításait a Firefox és a Thunderbird alkalmazásban](#). Kiválaszthatja a Mozilla által használt tanúsítványtárolót: Windows vagy Mozilla tanúsítványtároló. Ez a funkció csak azoknál a számítógépeknél érhető el, amelyek nem rendelkeznek alkalmazott házirenddel. Ha egy számítógépen van érvényes házirend, a Kaspersky Endpoint Security automatikusan engedélyezi a Windows tanúsítványtároló használatát a Firefox és a Thunderbird alkalmazásokban.
8. Bekerült egy funkció a [biztonságos forgalmi vizsgálati mód konfigurálására](#): mindig ellenőrzi a forgalmat, még akkor is, ha védelmi összetevők vannak letiltva, vagy csak akkor ellenőrzi a forgalmat, ha a védelmi összetevők kéri.
 9. Átdolgozásra került az információk a [jelentésből való törlésére](#) szolgáló eljárás. A felhasználó csak az összes jelentést törölheti. Az alkalmazás korábbi verzióiban a felhasználó kiválaszthatta azokat az alkalmazás-összetevőket, amelyek információi törlésre kerülnek a jelentésekből.
 10. Átdolgozásra került a [Kaspersky Endpoint Security beállításait tartalmazó konfigurációs fájl importálására](#) szolgáló eljárás és az [alkalmazás beállításainak visszaállítására](#) szolgáló eljárás. Importálás vagy visszaállítás előtt a Kaspersky Endpoint Security csak figyelmeztetést jelenít meg. Az alkalmazás korábbi verzióiban az új beállítások értékét még az alkalmazásuk előtt megtekinthette.
 11. Egyszerűsítve lett a [BitLocker által titkosított meghajtóhoz való hozzáférés visszaállítására](#) szolgáló eljárás. A hozzáférés visszaállítására szolgáló eljárás befejezése után a Kaspersky Endpoint Security felkéri a felhasználót, hogy állítson be új jelszót vagy PIN kódot. Az új jelszó beállítása után a BitLocker titkosítja a meghajtót. Az alkalmazás előző verziójában a felhasználónak manuálisan kellett visszaállítania a jelszót a BitLocker beállításaiiban.
 12. A felhasználóknak most lehetőségük van létrehozni saját helyi [megbízható zónájukat](#) egy adott számítógép számára. Így a felhasználók a házirendben található általános megbízható zóna mellett létrehozhatják a [kizárásokra](#) és [megbízható alkalmazásokra](#) vonatkozó saját listájukat is. A rendszergazda engedélyezheti vagy blokkolhatja a helyi kizárások vagy helyi megbízható alkalmazások használatát. A rendszergazda a Kaspersky Security Center használatával megtekintheti, hozzáadhatja, szerkesztheti vagy törölheti a számítógép tulajdonságaiban szereplő listaelemeket.
 13. Bekerült egy [megjegyzések hozzáadása szolgáló funkció a megbízható alkalmazások tulajdonságainál](#). A megjegyzések megkönnyítik a megbízható alkalmazások keresését és rendezését.
 14. [Az alkalmazás kezelése a REST API-n keresztül](#):
 - Mostantól lehetőség van az Outlook Levelezés védelem bővítménye beállításainak konfigurálására.
 - Tilos letiltani a vírusok, férgek és trójai programok észlelését.

11.4.0 frissítés

A Kaspersky Endpoint Security 11.4.0 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Új tervezésű [alkalmazásikon a tálca értesítési területén](#). Mostantól az új  ikon jelenik meg a régi  ikon helyett. Ha a felhasználónak műveletet kell végrehajtania (például az alkalmazás frissítése után a számítógép újraindítását), az ikon a következőre módosul: . Ha az alkalmazás védelmi összetevői le vannak tiltva vagy hibásan működnek, az ikon a következőre módosul:  vagy . Ha a mutatót az ikon fölé húzza, a Kaspersky Endpoint Security megjeleníti a számítógépes védelemben fellépő probléma leírását.
2. A terjesztőkészletben is szereplő Kaspersky Endpoint Agent frissült a 3.9-es verzióra. A Kaspersky Endpoint Agent 3.9 támogatja az új Kaspersky megoldásokkal történő integrációt. Az alkalmazással kapcsolatos további információért olvassa el a Kaspersky Endpoint Agent szolgáltatást támogató Kaspersky megoldások dokumentációját.
3. A *Nincs támogatva a licenc által* állapot hozzá lett adva a Kaspersky Endpoint Security összetevőkhöz. Az összetevők állapotát megtekintheti a [fő alkalmazásablak](#) összetevőlistájában.
4. A [Biztonsági rések kihasználásának megelőzése](#) új eseményei [lettek hozzáadva a jelentésekhez](#).
5. A [Kaspersky lemeztitkosítás technológiánál](#) a meghajtók mostantól automatikusan hozzá lesznek adva a Windows visszaállítási környezethez (WinRE), amikor elindítja a meghajtótitkosítást. A Kaspersky Endpoint Security előző verziója hozzáadta a meghajtókat az alkalmazás telepítésekor. Ha hozzáad meghajtókat a WinRE környezethez, azzal nagyban növelheti az alkalmazás stabilitását, ha olyan számítógépeken állítja vissza az operációs rendszert, melyek a Kaspersky Lemeztitkosítás technológiával vannak védve.

A Végponti szenzor összetevő sikeresen el lett távolítva a Kaspersky Endpoint Security alkalmazásból. Továbbra is 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.

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.

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 víruskezelő által hozzáadott fenyegetési adatokat használja. A víruskezelők értékelik az objektumokat, ha azok megbízhatósága nem határozható meg automatikusan.



Viselkedésvizsgálat

A Kaspersky Endpoint Security valós időben elemzi az objektumok tevékenységét.



Automatikus elemzés

A Kaspersky Endpoint Security adatokat kap az automatikus objektumvizsgáló rendszertől. A rendszer feldolgozza a Kasperskynek 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 víruskezelőinek véleményét.




Kaspersky 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](#).

Összetevők kiválasztása

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

Összetevők kiválasztása

Rész	Összetevő
Fenyegetések elleni alapvető védelem 	Fájl védelem A Fájl védelem összetevő lehetővé teszi a számítógép fájlrendszere fertőzéseinek megelőzését. Alapértelmezés szerint a „Fájl védelem” összetevő folyamatosan jelen van a számítógép memóriájában. Az összetevő vizsgálja a fájlokat a számítógép összes meghajtóján, valamint a csatlakoztatott meghajtókon. 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 egyúttal azt is vizsgálja, hogy az üzenetekben szerepel-e kártékony vagy adathalászatra szolgáló hivatkozás. Alapértelmezés szerint a „Levelezés védelem” összetevő folyamatosan jelen van a számítógép memóriájában, és megvizsgál minden olyan érkező és elküldött üzenetet, amely a POP3, az SMTP, az IMAP vagy az NNTP protokollt, vagy a Microsoft Office Outlook levelezési ügyfélprogramot (MAPI) használja. Az összetevő antivírus adatbázisok, a [Kaspersky Security Network felhőszolgáltatás](#) és heurisztikus elemzés segítségével biztosít védelmet a számítógépnek.

Hálózati védelem

A „Hálózati védelem” összetevő a hálózati támadásokra jellemző bejövő hálózati forgalmat vizsgálja. Ha a Kaspersky Endpoint Security hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában. A Kaspersky Endpoint Security adatbázisai 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.

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 részt vesz a Kaspersky Security Networkben, a KSN szolgáltatás megadja a Kaspersky Endpoint Security számára a vizsgált fájlok kategóriáját és hírnevét, valamint a vizsgált webcímek hírnevét.

Viselkedéselemzés

A Viselkedéselemzés összetevő a számítógépen futó alkalmazások műveleteiről fogad adatokat, és a teljesítmény növelése érdekében átadja ezeket az információkat a többi védelmem összetevőinek. A Viselkedéselemzés 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 viselkedésfolyam-aláíráson alapuló funkciói a számítógép számára proaktív védelmet nyújtanak.

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.

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 révén a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben elvégzett műveleteket visszagörgetni.

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 Eszkőfelügyelő felügyeli az olyan eszközökhöz történő felhasználói elérést, amik csatlakoztatva vannak a számítógéphez (például merevlemez, kamerák vagy Wi-Fi modulok). Ez lehetővé teszi, hogy védje számítógépét a fertőzésektől, ha ilyen eszközök vannak csatlakoztatva, valamint megelőzi az adatvesztéséget- vagy szivárgást.

Webfelügyelő

A Webfelügyelő kezeli a felhasználók hozzáférést 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 Anomálfelügyelő

Az Adaptív Anomálfelügyelő összetevő megfigyeli és letiltja azokat a tevékenységeket, amelyek nem megszokottak a cég hálózatán található számítógépeken. Az Adaptív Anomálfelügyelő egy szabálycsoport alapján követi nyomon a nem megszokott viselkedést (például a *Microsoft PowerShell indítása egy Office-alkalmazásból szabályt*). A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján. Konfigurálhatja, hogy az Adaptív Anomálfelügyelő 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.

Feladatok



Vírusvizsgálat

A Kaspersky Endpoint Security megvizsgálja a számítógépet vírusok és egyéb fenyegetések szempontjából. A vírusvizsgálat segít megelőzni a rosszindulatú programok terjedését, amiket például az alacsony biztonsági szint miatt nem észleltek a védelmi összetevők.

Frissítés

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 kézzel 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.

Integritás ellenőrzés

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 fájl szintű titkosítást.

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 Expert 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](#).

Kaspersky Sandbox

Beépített ügynök a Kaspersky Sandbox megoldáshoz. A *Kaspersky Sandbox megoldás* észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Kaspersky Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Kaspersky Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (Kaspersky Sandbox-kiszolgálók). A megoldás részleteit a [Kaspersky Sandbox 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 alkalmazás szervizfunkciói

A Kaspersky Endpoint Security számos szervizfunkcióval rendelkezik. A szervizfunkciók az alkalmazás naprakészen tartása érdekében működnek, képességeinek bővítése és a felhasználó segítése az alkalmazás használata során.

- **Jelentések.** Működése során az alkalmazás jelentést készít az egyes alkalmazásösszetevőkről. A jelentések használatával a befejezett feladatok eredményeit is megtekintheti. A jelentés tartalmazza azon események listáját, amik a Kaspersky Endpoint Security működése alatt történtek, valamint minden olyan műveletet, amit az alkalmazás végrehajt. Incidens esetén jelentéseket küldhet a Kaspersky részére, ahol a Terméktámogatás szakemberei részletesebben megvizsgálhatják az ügyet.
- **Biztonsági mentés.** Ha az alkalmazás fertőzött fájlokat észlel, miközben a számítógépen vírusokat és egyéb fenyegetéseket keres, blokkolja ezeket a fájlokat. A Kaspersky Endpoint Security a vírusmentesített és törölt fájlok másolatait a *Biztonsági mentés* területen tárolja. A Kaspersky Endpoint Security a bármilyen okból fel nem dolgozott fájlokat az *aktív fenyegetések listájára* helyezi. Megvizsgálhatja a fájlokat, visszaállíthatja a fájlokat eredeti mappájukba, illetve ürítheti az adattárhelyet.
- **Értesítések.** Az értesítési szolgáltatással a felhasználó következi az eseményeket, amik hatással vannak a számítógép védelmi állapotára és a Kaspersky Endpoint Security működésére. Az értesítések megjeleníthetők a képernyőn, illetve elküldhetők e-mailben.
- **Kaspersky Security Network.** A felhasználók Kaspersky Security Network való részvétele a számítógép védelmének hatékonyságát a fájlok hírnevére, a webes erőforrásokra és a szoftverekre vonatkozó információk valós idejű használata, a világ minden tájáról történő gyűjtése révén fokozza.
- **Licenc.** Licenc vásárlásával használatba veheti az alkalmazás összes funkcióját, hozzáférhet az adatbázis- és alkalmazásmodul-frissítésekhez, és telefonos vagy e-mailes támogatást vehet igénybe alkalmazás telepítésével, beállításával és használatával kapcsolatos ügyekben.
- **Támogatás.** A Kaspersky Endpoint Security minden regisztrált felhasználója segítséget kérhet a Terméktámogatás szakembereitől. Küldhet egy kérelmet a Kaspersky Terméktámogatásnak a Kaspersky CompanyAccount portálon vagy telefonon keresztül.

Forgalmazási készlet

A terjesztőkészlet a következő terjesztőcsomagokat tartalmazza:

- **Erős titkosítás (AES256)**

Ez a terjesztőcsomag kriptográfiai eszközöket tartalmaz az AES (Advanced Encryption Standard) 256 bites hatásos kulchosszúságú titkosítási algoritmus elvégzésére.

- **Egyszerű titkosítás (AES56)**

Ez a terjesztőcsomag kriptográfiai eszközöket tartalmaz az AES 56 bites hatásos kulchosszúságú titkosítási algoritmus elvégzésére.

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	Kaspersky Endpoint Security Adminisztrációs bővítmény telepítőcsomag a Kaspersky Security Centerhez.
bases.cab	Frissítse a telepítés során használt csomagfájlokat.
cleaner.cab	Fájlok az inkompatibilis szoftver eltávolításához.
incompatible.txt	A fájl, melyben inkompatibilis szoftverek listája látható.
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.
endpointagent.msi	A Kaspersky Endpoint Agent telepítőcsomagja, amely szükséges a más Kaspersky-megoldásokkal való integrációhoz (például Kaspersky Sandbox).
NDP<version>-<package properties>	Microsoft .NET-keretrendszer telepítőcsomag.
keswin_web_plugin.zip	Az archívum a Kaspersky Endpoint Security webes bővítmény telepítéséhez szükséges fájlokat tartalmazza.

E beállítások értékeinek módosítása nem javasolt. Ha módosítani szeretné a telepítési lehetőségeket, használja a [setup.ini](#) fájlt.

Hardveres és szoftveres rendszerkövetelmények

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

Minimális általános követelmények:

- 2 GB szabad lemezterület a merevlemezen;
- CPU:
 - Munkaállomás: 1 GHz;
 - Kiszolgáló: 1,4 GHz;
 - SSE2 utasításkészlet támogatása.
- RAM:
 - Munkaállomás (x86): 1 GB;
 - Munkaállomás (x64): 2 GB;
 - Kiszolgáló: 2 GB.

Munkaállomások

Támogatott operációs rendszerek a munkaállomások esetében:

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

Az SHA-1 modul aláírási algoritmus a Microsoft szerint elavult. A Kaspersky Endpoint Security sikeres telepítéséhez a Microsoft Windows 7 operációs rendszert futtató számítógépen a KB4474419 frissítés szükséges. A frissítéssel kapcsolatos további információkért keresse fel a [Microsoft Terméktámogatás webhelyét](#).

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 11.8.0 támogatja az alkalmazás alapvető összetevőit a Windows operációs rendszert futtató számítógépeken kiszolgálók esetében. Mostantól használhatja a Kaspersky Endpoint Security for Windows szolgáltatást a Kaspersky Security for Windows Server helyett a cége kiszolgálóin és fűrtjein. A Core Mode [korlátozásokkal](#) támogatott.

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 vagy frissebb;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Az SHA-1 modul aláírási algoritmus a Microsoft szerint elavult. A Kaspersky Endpoint Security sikeres telepítéséhez a Microsoft Windows Server 2008 R2 operációs rendszert futtató számítógépen a KB4474419 frissítés szükséges. A frissítéssel kapcsolatos további információkért keresse fel a [Microsoft Terméktámogatás webhelyét](#).

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](#).

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 Távolsi asztali szolgáltatások Windows Server 2019 rendszeren alapulva.

Virtuális platformok

Támogatott virtuális platformok:

- VMware Workstation 16.1.2;
- VMware ESXi 7.0 Update 3;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2106;
- Citrix Provisioning 2109;
- Citrix Hypervisor 8.2 (XS82E033 gyorsjavítás).

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

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2.

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 funkcióinak összehasonlítása

Funkció	Workstation	Kiszolgáló
Fenyegetések elleni fejlett védelem		
Kaspersky Security Network	✓	✓
Viselkedéselemzés	✓	✓
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		
Alkalmazásfelügyelő	✓	✓
Eszközfelügyelő	✓	✓
Webfelügyelő	✓	✓
Adaptív Anomáliafelügyelő	✓	–
Adattitkosítás		
Kaspersky lemeztitkosítás	✓	–
BitLocker meghajtótitkosítás	✓	✓
Fájl szintű titkosítás	✓	–
Cserélhető meghajtók titkosítása	✓	–
Detection and Response		
Kaspersky Endpoint Agent	✓	✓
Endpoint Detection and Response Optimum	✓	✓
Endpoint Detection and Response Expert	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response	✓	✓

Az alkalmazásfunkciók összehasonlítása a kezelőeszközök alapján.

A Kaspersky Endpoint Security elérhető funkciói a kezelőeszközöktől függenek (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 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	✓	✓	–
Viselkedéselemzés	✓	✓	✓
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			
Alkalmazásfelügyelő	✓	✓	✓
Eszközfelügyelő	✓	✓	✓
Webfelügyelő	✓	✓	✓
Adaptív Anomáliafelügyelő	✓	✓	✓
Adattitkosítás			
Kaspersky lemeztitkosítás	✓	✓	–
BitLocker meghajtótitkosítás	✓	✓	✓
Fájl szintű titkosítás	✓	✓	–
Cserélhető meghajtók titkosítása	✓	✓	–
Detection and Response			
Kaspersky Endpoint Agent	✓	✓	✓
Endpoint Detection and Response Optimum	–	✓	✓

Endpoint Detection and Response Expert	-	-	✓
Kaspersky Sandbox	-	✓	-
Managed Detection and Response (MDR)	✓	✓	✓
Feladatok			
Kulcs hozzáadása	✓	✓	✓
Alkalmazásösszetevők módosítása	✓	✓	✓
Leltár	✓	✓	✓
Frissítés	✓	✓	✓
Frissítés visszaállítása	✓	✓	✓
Vírusvizsgálat	✓	✓	✓
Integritás ellenőrzés	✓	✓	-
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 telepítést megelőzően a Kaspersky Endpoint Security ellenőrzi a számítógépen megtalálható Kaspersky alkalmazásokat. Az alkalmazás ellenőrzi a számítógépen az inkompatibilis szoftvereket is. Azon inkompatibilis szoftverek listája, amik elérhetőek a [terjesztőkészletben](#) lévő incompatible.txt fájlban.



[TÖLTSE LE AZ INCOMPATIBLE.TXT FÁJLT](#)

A Kaspersky Endpoint Security az alábbi Kaspersky alkalmazásokkal nem kompatibilis:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.

- Kaspersky Anti-Ransomware Tool.
- A Kaspersky Célzott Támadások Elleni Platform (a Végponti szenzor összetevővel).
- Kaspersky Sandbox (beleértve a Kaspersky Endpoint Agent alkalmazást).
- A Kaspersky végponti észlelés és válasz (beleértve a Végponti szenzor összetevőt).

Ha az Endpoint Agent összetevő telepítése egyéb Kaspersky alkalmazások távoli telepítési eszközeivel történt, a rendszer automatikusan eltávolítja az összetevőt a Kaspersky Endpoint Security telepítése során. A Kaspersky Endpoint Security a Végponti szenzor/Kaspersky Endpoint Agent összetevőt is tartalmazhatja, ha az Endpoint Agent lehetőséget választotta az alkalmazás-összetevők listájában.

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

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.

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

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. 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 beállításával, 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 tudnivalóért lásd a [Kaspersky Security Center súgót](#).

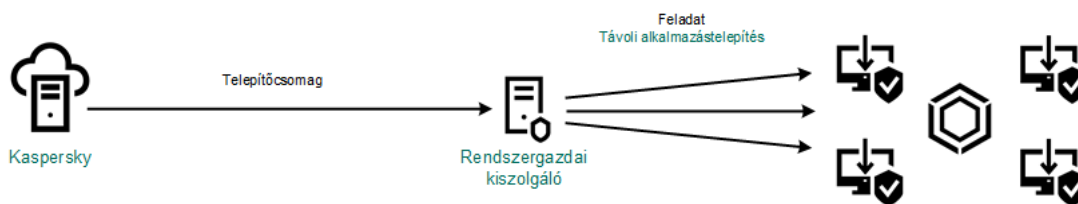
Az alkalmazás normál telepítése

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. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Additional** → **Remote installation** lehetőséget.

2. 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 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 eszközcímekeket kézzel, vagy importálja a címekeket a listáról. Megadhat NetBIOS neveket, IP-címekeket és az eszközök IP-alhálózatait, amihez hozzá kívánja rendelni a feladatot.

3. 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.** Ha nem volt Hálózati ügynök telepítve a számítógépre, akkor először a Hálózati ügynök lesz telepítve az operációs rendszer eszközeinek 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 Sűgőt](#).

- **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 jogossalggal kell futtatni a távoli telepítés feladatot.

4. 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. Később [activate the application](#) az *Add key* feladat használatával.

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 eltávolítani a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.

6. 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.

7. 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.

8. lépés A telepítés elindítása

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Feladat futtatása, ha a varázsló végzett** 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 webkonzol főablakában válassza a **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. Később [activate the application](#) az *Add key* feladat használatával.

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 kézzel, 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.** Az alkalmazástelepítés módszerének kiválasztása:
 - **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 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 kéziként, az Active Directory segítségével van telepítve. A Hálózati ügynök telepítéséhez tartomány adminisztrációs jogosultsággal kell futtatni a távoli telepítés feladatát.

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 eltávolítani 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 [rendszer szabályokat](#) és [csoportfeladatokat](#). Ha egy számítógép már tagja adminisztrációs csoportnak, a számítógépet nem lehet áthelyezni. Ha nem választ ki adminisztrációs csoportot, a számítógép a **Hozzá nem rendelt eszközök** 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 **Feladat futtatása, ha a varázsló végzett** 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** → **Additional** → **Remote installation** → **Installation packages** mappát.

Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.

2. Kattintson a **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 11.8.0*.

3. lépés A terjesztőcsomag kiválasztása telepítéshez

Kattintson a **Tallózás** gombra, és válassza ki a `kes_win.kud` fájlt a [terjesztési készletben](#).

Szükség esetén frissítse a telepítőcsomagban elérhető víruskeresési adatbázist a **Copy updates from repository to installation package** jelölőnégyzet 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 beállításai között kiválaszthatja az alkalmazás összetevőit, és megadhatja az alkalmazástelepítés beállításait (lásd az alábbi táblázatot). A telepítőcsomag az Adminisztrációs kiszolgáló tárhelyének antivírus adatbázisait tartalmazza. Ön [update the databases in the installation package](#), hogy csökkentse a fogyasztást, miután a Kaspersky Endpoint Security telepítése után frissíti az adatbázisokat.

[Telepítőcsomag létrehozásának menete a Web Console-ban és a Cloud Console-ban](#) 

1. A webkonzol főablakában válassza a **Discovery & Deployment** → **Deployment & Assignment** → **Installation packages** lehetőséget.

Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.

2. Kattintson a **Add** 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.

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.

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 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 beállításai között kiválaszthatja az alkalmazás összetevőit, és megadhatja az alkalmazástelepítés beállításait (lásd az alábbi táblázatot). A telepítőcsomag az Adminisztrációs kiszolgáló tárhelyének antivírus adatbázisait tartalmazza. Ön [update the databases in the installation package](#), hogy csökkentse a fogyasztást, miután a Kaspersky Endpoint Security telepítése után frissíti az adatbázisokat.

Telepítőcsomag beállítások

Rész	Leírás
Védelmi összetevők	<p>Ebben a részben kiválaszthatja az alkalmazás összetevőket, amik elérhetőek lesznek. Ön később módosíthatja az alkalmazásösszetevők készletét a <i>Change application components</i> feladattal. A BadUSB védelem összetevő, a Detection and Response összetevő és az adattitkosítási összetevők alapértelmezetten nincsenek telepítve. Ezek az összetevők a telepítőcsomag beállításai között adhatók hozzá.</p> <p>Ha telepítenie kell a Detection and Response összetevőket, a Kaspersky Endpoint Security a következő konfigurációkat támogatja:</p> <ul style="list-style-type: none">• Csak Endpoint Agent• Csak Endpoint Detection and Response Optimum• Csak Endpoint Detection and Response Expert• Csak Kaspersky Sandbox• Endpoint Detection and Response Optimum és Kaspersky Sandbox

	<ul style="list-style-type: none"> Endpoint Detection and Response Expert és Kaspersky Sandbox. <p>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.</p>
Licenckulcs	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 .
Inkompatibilis alkalmazások	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.
Telepítési beállítások	<p>Add application location to environment variable %PATH%. A parancssori felület kényelmes használata érdekében hozzáadhatja a telepítés elérési útvonalát a %PATH% változóhoz.</p> <p>Ne legyen védett a telepítési folyamat. 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.</p> <p>Biztosítsa a Citrix PVS szolgáltatásokkal való kompatibilitást (csak Citrix PVS-szel való munkavégzés esetén szükséges). Engedélyezheti a Citrix Provisioning Services támogatását, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre telepítse.</p> <p>Az alkalmazás telepítési mappájának elérési útja. Megváltoztathatja a Kaspersky Endpoint Security telepítési útvonalát egy ügyfélszámítógépen. Alapértelmezés szerint az alkalmazás telepítési mappája a %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.</p> <p>Konfigurációs fájl. Feltölthet egy fájlt, ami megszabja a Kaspersky Endpoint Security beállításait. Létrehozhat egy konfigurációs fájlt az alkalmazás helyi felületén.</p>

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 *Frissítések letöltése az Adminisztrációs kiszolgáló tárhelyére* 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. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Additional** → **Remote installation** → **Installation packages** mappát.

Ezzel megnyitja a Kaspersky Security Centerre letöltött telepítőcsomagok listáját.

2. Nyissa meg a telepítőcsomag tulajdonságait.
3. Az **General** részben kattintson az **Update databases** gombra.

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 webkonzol főablakában válassza a **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. Az **General information** fülön kattintson az **Update databases** linkre.

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 *Alkalmazás távoli telepítése* feladat a Kaspersky Endpoint Security távoli telepítésére szolgál. Az *Alkalmazás távoli telepítése* 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 alkalmazás-összetevőket a telepítőcsomag tulajdonságai között.

[Távoli telepítési feladat létrehozása az Adminisztrációs Konzolban \(MMC\)](#)

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 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.** 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 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 számítógépre. 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 számítógépre 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 eltávolítani 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 kézzel, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-hálózatait, 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 11.8.0 telepítése*.

10. lépés. A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Feladat futtatása, ha a varázsló végzett** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Az alkalmazás csendes módban lesz telepítve. A telepítés után az **k** ikon lesz hozzáadva a felhasználó számítógépének értesítési területéhez. Az ikon a következőképp 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 ki a **Devices** → **Tasks** lehetőséget.

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** listában válassza ki a **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 olyat, hogy *Installation of Kaspersky Endpoint Security for Managers*.

4. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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 (11.8.0) 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** szakaszban válassza ki az alkalmazás telepítési 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 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 állítson be egy korlátot az alkalmazás telepítésének megpróbálásához. Ha a Kaspersky Endpoint Security telepítése hibával ér véget, a feladat automatikusan elindítja újra a telepítést.
6. Ha szükséges, törölje a **Do not re-install application if it is already installed** jelölőnégyzetet. Például engedélyezi az alkalmazás egyik előző verziójának telepítését.
7. Ha szükséges, törölje a **Verify operating system type before downloading** jelölőnégyzetet. 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. Szükség esetén jelölje be a **Assign package installation in Active Directory group policies** jelölőnégyzetet. A Kaspersky Endpoint Security a Hálózati Ügynökkel vagy kézilég, az Active Directory segítségével van telepítve. A Hálózati ügynök telepítéséhez tartomány adminisztrációs jogosultsággal kell futtatni a távoli telepítés feladatot.
9. Szükség esetén jelölje be a **Prompt users to close running applications** jelölőnégyzetet. 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. Az **Behavior for devices managed through other Administration Servers** részben válassza ki a Kaspersky Endpoint Security telepítési 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 **Indítás** gombra. Az alkalmazás csendes módban lesz telepítve. A telepítés után az **k** 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.

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:

- A telepített inkompatibilis szoftverek jelenléte (azon inkompatibilis szoftverek listája, amik elérhetőek a [terjesztőkészletben](#) lévő incompatible.txt fájlban).
- Teljesülnek-e a [hardver- és szoftverkövetelmények](#).
- A felhasználó jogosult-e a szoftvertermék telepítésére.

Ha a fenti feltételek közül bármelyik nem teljesül, a képernyőn ezt jelző értesítés jelenik meg.

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 kézzel.

Ha az észlelt alkalmazások között megtalálhatók a Kaspersky Endpoint Security korábbi verziói, akkor minden áttelepíthető adat a Kaspersky Endpoint Security 11.8.0 for Windows telepítése során megőrződik 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 10 Service Pack 2 Maintenance Release 3 for Windows (10.3.3.275 számú build).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (10.3.3.304 számú build).
- Kaspersky Endpoint Security 11.0.0 for Windows (build 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (build 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (11.0.1.90 számú build).
- Kaspersky Endpoint Security 11.1.0 for Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (11.1.1.126 számú build).
- Kaspersky Endpoint Security 11.2.0 for Windows (11.2.0.2254 számú build).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (11.2.0.2254 számú build).
- Kaspersky Endpoint Security 11.3.0 for Windows (11.3.0.773 számú build).
- Kaspersky Endpoint Security 11.4.0 for Windows (11.4.0.233 számú build).
- Kaspersky Endpoint Security 11.5.0 for Windows (11.5.0.590 számú build).

- Kaspersky Endpoint Security 11.6.0 for Windows (11.6.0.394 számú build).
- Kaspersky Endpoint Security 11.7.0 for Windows (11.7.0.669 számú build).

Kaspersky Endpoint Security összetevők

A telepítés során kiválaszthatja a Kaspersky Endpoint Security telepíteni kívánt összetevőit. A Fájlvédelem egy kötelezően telepítendő összetevő. Telepítését nem lehet törölni.

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 alkalmazás-összetevőket](#). 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 Agent
- Csak Endpoint Detection and Response Optimum
- Csak Endpoint Detection and Response Expert
- Csak Kaspersky Sandbox
- Endpoint Detection and Response Optimum és Kaspersky Sandbox
- Endpoint Detection and Response Expert és Kaspersky Sandbox.

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.

Speciális beállítások

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.

Biztosítsa a Citrix PVS szolgáltatásokkal való kompatibilitást (csak Citrix PVS-szel való munkavégzés esetén szükséges). Engedélyezheti a Citrix Provisioning Services támogatását, hogy a Kaspersky Endpoint Security alkalmazást egy virtuális gépre telepítse.

Add application location to environment variable %PATH%. 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 **Frissítés** 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 **Application type** 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 **Command line** 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 megadott 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 telepítési beállításainak leírása

A setup.ini fájlt a rendszer az alkalmazás parancssori telepítései, 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.



[TÖLTSE LE A SETUP.INI FÁJLT](#)

A setup.ini fájl a következő részekből áll:

- **[Setup]** – az alkalmazástelepítés általános beállításai.
- **[Components]** – a telepíteni kívánt 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. A Managed Detection and Response összetevő szintén hiányzik ebből a részből. Az összetevő telepítéséhez [aktiválnia kell a Managed Detection and Response szolgáltatást a Kaspersky Security Center konzolban](#).
- **[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.


Az 1 érték alternatívái a `yes`, `on`, `enable` és `enabled` értékek.

A 0 érték alternatívái a no, off, disable és disabled értékek.

A setup.ini fájl beállításai

Rész	Paraméter	Leírás
[Setup]	InstallDir	Az alkalmazás telepítési mappájának elérési útja.
	ActivationCode	Kaspersky Endpoint Security aktiváló kód.
	EULA=1	<p>A Végfelhasználói licencszerződés feltételeinek elfogadása. A Licencszerződés szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>A Végfelhasználói licencszerződés feltételeit az alkalmazás telepítéséhez, illetve verziójának frissítéséhez kötelező elfogadni.</p> </div>
	PrivacyPolicy=1	<p>Az Adatvédelmi szabályzat elfogadása. Az Adatvédelmi szabályzat szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Az alkalmazás telepítéséhez, vagy a verziója frissítéséhez el kell fogadnia az Adatvédelmi szabályzatot.</p> </div>
	KSN	<p>A Kaspersky Security Network 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:</p> <ul style="list-style-type: none"> • 1 – a KSN-ben való részvétel elfogadása. • 0 – a KSN-ben való részvétel elutasítása (alapértelmezett érték). <p>A Kaspersky Endpoint Security terjesztőcsomag a with Kaspersky Security Networktel 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.</p>
	Login	<p>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.</p>
	Jelszó	<p>A Kaspersky Endpoint Security funkcióihoz és beállításaihoz való hozzáférés jelszavának megadása (a jelszót a Login és a PasswordArea paraméterekkel együtt kell megadni).</p>

		Ha a Bejelentkezés paraméternél jelszót megadott, de felhasználónevet nem, alapértelmezés szerint a rendszer a KLAdmin felhasználónevet használja.
	PasswordArea	<p>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.</p> <p>Választható értékek:</p> <ul style="list-style-type: none"> • 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. • REMOVE LIC – a kulcs eltávolítása. • REPORTS – a jelentések megtekintése.
	SelfProtection	<p>Az alkalmazástelepítés védelmi mechanizmusának engedélyezése és letiltása. Választható értékek:</p> <ul style="list-style-type: none"> • 1 – az alkalmazástelepítés védelmi mechanizmusa engedélyezve van (alapértelmezett érték). • 0 – az alkalmazástelepítés védelmi mechanizmusa nincs engedélyezve. <p>A telepítési védelemben 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.</p>
	Reboot=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 eltávolítani 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
	SetupReg	Engedélyezi a beállításkulcsok írását a setup.reg fájlból a beállításjegyzékbe. SetupReg: setup.reg paraméter értéke.
	EnableTraces	Az alkalmazások nyomkövetésének engedélyezése vagy kikapcsolása. Indulása után a Kaspersky Endpoint Security elmenti a nyomkövetési fájlokat a %ProgramData%\Kaspersky Lab\KES\Traces mappába. Választható értékek: <ul style="list-style-type: none"> • 1 – a nyomkövetés engedélyezve van. • 0 – a nyomkövetés ki van kapcsolva (alapértelmezett érték).
	TracesLevel	A nyomkövetések részleteinek szintje. Választható értékek: <ul style="list-style-type: none"> • 100 (kritikus). Csak a súlyos hibákról szóló üzenetek. • 200 (magas). Minden hibáról szóló üzenet, köztük a súlyos hibáké.

		<ul style="list-style-type: none"> • 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	<p>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).</p> <p>Választható értékek:</p> <ul style="list-style-type: none"> • 1 – a REST API felületen keresztül történő kezelés engedélyezve van. • 0 – a REST API felületen keresztül történő kezelés blokkolva van (alapértelmezett érték). <p>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.</p>
	RESTAPI_User	<p>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>\<Felhasználónév> (például RESTAPI_User=COMPANY\Administrator). A REST API-val történő munkálatokhoz csak egy felhasználót választhat ki.</p> <p>Egy felhasználónév megadása szükséges ahhoz, hogy az alkalmazást a REST API felületen keresztül kezelhesse.</p>
	RESTAPI_Port	<p>Az alkalmazás REST API felületen keresztül történő kezeléséhez használt port. A 6782 az alapértelmezett port.</p>
	RESTAPI_Certificate	<p>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.</p>
[Components]	ALL	<p>Az összes összetevő telepítése. Az 1 paraméterérték megadása esetén minden összetevő telepítésére sor</p>

		<p>kerül, függetlenül az egyedi összetevők telepítési beállításaitól.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>A Detection and Response megoldások támogatási módja miatt az Endpoint Detection and Response Optimum és a Kaspersky Sandbox összetevői is telepítve kerülnek a számítógépen. Az Endpoint Detection and Response Expert és a Endpoint Agent összetevők nem kompatibilisek ezzel a konfigurációval.</p> </div>
	MailThreatProtection	Levelezés védelem.
	WebThreatProtection	Web védelem.
	AMSI	AMSI védelem.
	HostIntrusionPrevention	Behatolásmegelőző rendszer.
	BehaviorDetection	Viselkedéselemzés.
	ExploitPrevention	Biztonsági rések kihasználásának megelőzése.
	RemediationEngine	Kármentesítő motor.
	Tűzfal	Tűzfal.
	NetworkThreatProtection	Hálózati védelem.
	WebControl	Webfelügyelő.
	DeviceControl	Eszközfelügyelő.
	ApplicationControl	Alkalmazásfelügyelő.
	AdaptiveAnomaliesControl	Adaptív Anomálfelügyelő.
	FileEncryption	Fájlszintű titkosítás könyvtárak.
	DiskEncryption	Teljes lemeztitkosítás rész.
	BadUSBAttackPrevention	BadUSB védelem.
	AntiAPT	<p>Endpoint Agent. Az Endpoint Agent telepíti a Kaspersky Endpoint Agent megoldást. A Kaspersky Endpoint Agent támogatja a speciális fenyegetések észlelésére szolgáló Detection and Response megoldásokat (például Kaspersky Sandbox).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Az összetevő nem kompatibilis az EDR Optimum (EDR), az EDR Expert (EDRCloud) és a Kaspersky Sandbox (SB) összetevőkkel.</p> </div>
	EDR	Endpoint Detection and Response Optimum (EDR Optimum).

		<p>Az összetevő nem kompatibilis az Endpoint Agent (AntiAPT) és az EDR Expert (EDRCloud) összetevőkkel.</p>
	EDRCloud	<p>Endpoint Detection and Response Expert (EDR Expert).</p> <p>Az összetevő nem kompatibilis az Endpoint Agent (AntiAPT) és az EDR Optimum (EDR) összetevőkkel.</p>
	SB	<p>Kaspersky Sandbox.</p> <p>Az összetevő nem kompatibilis az Endpoint Agent összetevővel (AntiAPT).</p>
	AdminKitConnector	<p>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.</p> <p>Választható értékek:</p> <ul style="list-style-type: none"> • 1 – az adminisztrációs rendszerekkel történő alkalmazáskezelés engedélyezve van (alapértelmezett érték). • 0 – az alkalmazáskezelés csak a helyi felületen keresztül van engedélyezve.
[Tasks]	ScanMyComputer	<p>Teljes vizsgálat feladat. Választható értékek:</p> <ul style="list-style-type: none"> • 1 – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • 0 – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.
	ScanCritical	<p>Kritikus területek vizsgálata feladat. Választható értékek:</p> <ul style="list-style-type: none"> • 1 – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • 0 – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.
	Updater	<p>Frissítési feladat. Választható értékek:</p> <ul style="list-style-type: none"> • 1 – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára.

- | | | |
|--|--|---|
| | | <ul style="list-style-type: none">• 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 alkalmazás-összetevőket:

- Helyben, a Telepítővarázsló segítségével.

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

- 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 található [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.

[Alkalmazás-összetevők hozzáadásának és eltávolításának menete az Adminisztrációs Konzolon \(MMC\) !\[\]\(8bba887393ca45b761e5cb49e755e762_img.jpg\)](#)

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 (11.8.0)** → **Change application components** lehetőséget.

2. lépés Feladatbeállítások az alkalmazás-összetevők módosításához

Válassza ki, hogy mely alkalmazás-összetevők lesznek elérhetők a felhasználó számítógépén.

Tegyen jelölést a **Harmadik féltől származó, nem kompatibilis alkalmazások eltávolítása** jelölőnégyzetbe. A nem kompatibilis alkalmazások listája megtekinthető az `incompatible.txt` fájlban, amely megtalálható a [terjesztési készletben](#). Ha a számítógépre inkompatibilis alkalmazások vannak telepítve, a Kaspersky Endpoint Security telepítése hibával ér véget.

Szükség esetén engedélyezze a [jelszóvédelem](#) lehetőséget a feladat teljesítménye érdekében:

1. Kattintson a **További** gombra.

2. Jelölje be a **Jelszó használata az alkalmazás összetevőkészletének módosításához** jelölőnégyzetet.

3. Adja meg a KLAdmin felhasználói fiókjának bejelentkezési adatait.

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 eszközcímetek kéziké, vagy importálja a címetek a listáról. Megadhat NetBIOS neveket, IP-címeteket 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: *Az Alkalmazásfelügyelő összetevő hozzáadása.*

6. lépés A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Feladat futtatása, ha a varázsló végzett** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

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.

[Alkalmazás-összetevő hozzáadásának, illetve eltávolításának menete a Web Console-ban és a Cloud Console-ban](#)



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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** 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 olyat, hogy *Add the Application Control component*.

4. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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 **Open task details when creation is complete** jelölőnégyzetbe, és zárja be a varázslót. A feladat tulajdonságainak ablakában válassza az **Alkalmazásbeállítások** lapfület, és jelölje ki a később elérhető alkalmazás-összetevőket.

Szükség esetén engedélyezze a [jelszóvédelem](#) lehetőséget a feladat teljesítménye érdekében:

1. A **Speciális beállítások** területen tegyen jelölést az **Jelszó használata az alkalmazás összetevőkészletének módosításához** jelölőnégyzetbe.

2. Adja meg a KAdmin felhasználói fiókjának bejelentkezési adatait.

Mentse a változtatásokat, és futtassa a feladatot.

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.

Frissítés az alkalmazás korábbi verziójáról

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

- Ajánlott kilépni minden aktívan futó alkalmazásból, mielőtt megkezdje a frissítést.
- Amennyiben a számítógép olyan merevlemezekkel rendelkezik, amelyek a [Teljes lemeztitkosítás \(FDE\)](#) használatával lettek titkosítva, vissza kell fejteni a titkosított merevlemezeket ahhoz, hogy frissítse a Kaspersky Endpoint Security verzióját 10-esről 11.0.0-ás vagy újabb verzióra.

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 10 Service Pack 2 Maintenance Release 3 for Windows (10.3.3.275 számú build).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (10.3.3.304 számú build).
- Kaspersky Endpoint Security 11.0.0 for Windows (build 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (build 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (11.0.1.90 számú build).
- Kaspersky Endpoint Security 11.1.0 for Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (11.1.1.126 számú build).
- Kaspersky Endpoint Security 11.2.0 for Windows (11.2.0.2254 számú build).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (11.2.0.2254 számú build).
- Kaspersky Endpoint Security 11.3.0 for Windows (build 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (11.4.0.233 számú build).
- Kaspersky Endpoint Security 11.5.0 for Windows (11.5.0.590 számú build).
- Kaspersky Endpoint Security 11.6.0 for Windows (11.6.0.394 számú build).
- Kaspersky Endpoint Security 11.7.0 for Windows (11.7.0.669 számú build).

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows Kaspersky Endpoint Security 11.8.0 for Windows verzióra történő frissítése esetén a rendszer az alkalmazás korábbi verziójának Biztonsági mentésébe vagy Karanténjába helyezett fájlokat az alkalmazás új verziójának Biztonsági mentésébe helyezi át. A Kaspersky Endpoint Security 10 Service Pack 2 for Windowsnál régebbi verziók esetén a fájlok, melyeket az előző verzióban a Biztonsági mentésbe és a Karanténba helyezett, nem kerülnek át az új verzióba.

A Kaspersky Endpoint Security több módon frissíthető 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](#).

Ha a vállalati hálózatra telepített alkalmazás az alapértelmezettekben 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 beállításában](#).

Alkalmazás eltávolítása

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

A Kaspersky Endpoint Security több módszerrel távolítható el a számítógépről:

- helyileg, a [Telepítővarázsló](#) használatával;
- helyileg, a [parancssorból](#);
- távolról, a Kaspersky Security Center segítségével (további részletek: [Kaspersky Security Center Súgó](#));
- távolról, a Microsoft Windows csoportos rendszabálykezelő szerkesztőben (további információért keresse fel a [Microsoft Terméktámogatás weboldalát](#)).

Ha az alkalmazás telepítése során kiválasztotta az Endpoint Agent összetevőt, akkor a következő két alkalmazást lesz telepítve a számítógépre: Kaspersky Endpoint Security és Kaspersky Endpoint Agent. Miután törli a Kaspersky Endpoint Security alkalmazást, a Kaspersky Endpoint Agent is automatikusan törölve lesz.

Eltávolítás a Kaspersky Security Centeren keresztül

Távolról is eltávolíthatja az alkalmazást az *Alkalmazás eltávolítása távolról* 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 !\[\]\(1d3a1175dd4902218e694b9c098adb83_img.jpg\)](#)

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 Security Center Administration Server** → **Additional** → **Uninstall application remotely** lehetőséget.

2. lépés Az eltávolítani kívánt alkalmazás kiválasztása

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

3. lépés Feladatbeállítások az alkalmazás eltávolításához

Válassza ki a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

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](#).
- **Az operációs rendszer verziójának ellenőrzése a letöltés előtt.** 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. Jelölje be az **Use uninstallation password** jelölőnégyzetet.
2. Nyomja meg a **Szerkesztés** gombot.

3. Adja meg a KAdmin 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 kézzel, vagy importálja a címeket a listáról. Megadhat NetBIOS neveket, IP-címeket és az eszközök IP-hálózatait, 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 11.8.0 eltávolítása*.

10. lépés. A feladat létrehozásának befejezése

Lépjen ki a varázslóból. Ha szükséges, tegyen jelölést a **Feladat futtatása, ha a varázsló végzett** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

Az alkalmazás csendes módban lesz eltávolítva.

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** listában válassza ki a **Kaspersky Security Center** lehetőséget.

2. A **Feladat típusa** legördülő listából válassza ki az **Alkalmazás eltávolítása távolról** lehetőséget.

3. A **Task name** mezőben adjon meg egy rövid leírást, például olyat, hogy *A Kaspersky Endpoint Security eltávolítása a Terméktámogatás számítógépekről.*

4. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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 a **Uninstall managed application** lehetőséget.

2. Válassza ki a **Kaspersky Endpoint Security for Windows (11.8.0)** 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 Súlyót](#).

4. Az **Egyidejű letöltések maximális száma** 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. Az **Maximum number of uninstallation attempts** mezőben állítson be egy korlátot az alkalmazás eltávolításának megpróbálásához. Ha a Kaspersky Endpoint Security telepítése hibával ér véget, a feladat automatikusan elindítja újra az eltávolítást.

6. Ha szükséges, törölje a **Verify operating system type before downloading** jelölőnégyzetet. 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 **Indítás** 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 *Alkalmazás távoli eltávolítása* feladat tulajdonságaiban. Jelszó nélkül a feladat nem lesz végrehajtva.

Ahhoz, hogy használja a KLAdmin fiók jelszavát az Alkalmazás távoli eltávolítása feladatban:

1. A Web Console fő ablakában válassza ki a **Devices** → **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** fület.
4. Jelölje be az **Use uninstallation password** jelölőnégyzetet.
5. Adja meg a KLAdmin fiók jelszavát.
6. Mentse el a módosításokat.

Az alkalmazás eltávolítása a varázsló 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.

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, az alkalmazás teljes mértékben törlődik.

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 érhetőek 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 újraterlepi a Kaspersky Endpoint Security alkalmazást. Nincs szükség további műveletre a korábban titkosított fájlok és meghajtók eléréséhez.

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\Kaspersky Endpoint Security for Windows\Doc\\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 lejáratá 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.
- *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 licenctanúsítvány

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

A licenctanúsítvány az alábbi licencadatokat tartalmazza:

- Licenckulcs vagy sorrendszám.
- 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 lejárat dátuma vagy licencidőszak.
- Licenctípus.

Az előfizetés

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

Az előfizetés lehet korlátozott (például egy éves) vagy korlátlan (lejárat 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 [kulcsfájllal](#) 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](#).

Licenckulcsot felvehet az alkalmazáshoz akár kulcsfájl segítségével, akár aktiválási 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 elérhetőek, amelyek a licenc lejáratá után hozzáférhetőek maradnak. A védelmi és felügyeleti összetevőket használhatja, és a licenc lejáratá előtt telepített alkalmazás-adatbázisokkal vizsgálatot végezhet. Az alkalmazás továbbra is titkosítja az olyan fájlokat, amelyek módosultak, és a titkosításuk a licenc lejáratá 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. Kulcsfájllra például Kaspersky CompanyAccount fiók regisztrálásához lehet szüksége.

Kulcsfájl visszaállításához tegye az alábbiak valamelyikét:

- Lépjen kapcsolatba a licenc eladóival.
- Kulcsfájl beszerzése a [Kaspersky webhelyen](#) a meglévő aktiváló kód alapján.

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 munkállomási licenctípustól függően

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

[Lásd még az alkalmazásfunkciók összehasonlítását a kiszolgálók esetében](#)

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
Fenyegetések elleni fejlett védelem						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Viselkedéselemzés	✓	✓	✓	✓	✓	✓
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						
Alkalmazásfelügyelő	✓	✓	✓	✓	✓	✓
Eszközfelügyelő	✓	✓	✓	✓	✓	✓
Webfelügyelő	✓	✓	✓	✓	✓	✓
Adaptív Anomáiafelügyelő	–	✓	✓	✓	✓	✓
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 <i>(A Kaspersky Sandbox-licencet külön kell megvásárolni)</i>	✓	✓	✓	✓	✓	✓

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](#)

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
Fenyegetések elleni fejlett védelem						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Viselkedéselemzés	✓	✓	✓	✓	✓	✓
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						
Alkalmazásfelügyelő	–	✓	✓	✓	✓	✓
Eszközfelügyelő	–	✓	✓	✓	✓	✓
Webfelügyelő	–	✓	✓	✓	✓	✓
Adaptív Anomáiafelügyelő	–	–	–	–	–	–
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 <i>(A Kaspersky Sandbox-licencet külön kell megvásárolni)</i>	✓	✓	✓	✓	✓	✓

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:

- Helyben, az alkalmazás kezelőfelületén, az [Aktiválási varázsló](#) segítségével. Így az aktív és a tartalék kulcsot is megadhatja.
- Távolról a [Kaspersky Security Center szoftvercsomaggal licenckulcs hozzáadási feladat létrehozásával](#), majd elindításával. Így az aktív és a tartalék kulcsot is megadhatja.
- A Kaspersky Security Center felügyeleti kiszolgálójának kulcstárhelyén tárolt kulcsfájlok aktiválási kódok távoli megosztásával az ügyfélszámítógépek felé. A kulcsok megosztásával kapcsolatos további részletekről [tájékozódjon a Kaspersky Security Center súgójában](#). Így az aktív és a tartalék kulcsot is megadhatja.

Elsőként az előfizetés alapján vásárolt aktiváló kód terjesztésére kerül sor.

- 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 terheléelosztás miatt. Ha az alkalmazást azonnal aktiválni szeretné, megszakíthatja a folyamatban lévő aktiválási eljárást, és elkezdheti az aktiválást az Aktiválási varázslóval.

Az alkalmazás aktiválása a Kaspersky Security Centeren keresztül

Az alkalmazást távolról is aktiválhatja a Kaspersky Security Centeren keresztül a következő módokon:

- A *Kulcs hozzáadása* feladat használata.

Ezzel a módszerrel hozzáadhat egy kulcsot egy megadott számítógéphez vagy számítógépekhez, amik az adminisztrációs csoport tagjai.

- 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 Sűgőt](#).
- 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 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 próbalicencia alatt, köztük a Kaspersky Endpoint Security is. Azonban nem fogja tudni aktiválni a Kaspersky Endpoint Security alkalmazást a saját próbalicencia alatt, miután a Kaspersky Security Center Cloud Console próbalicencia 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 próbalicencia nem teszi lehetővé, hogy egymás után váltson kereskedelmi verzióra. 30 nappal a próbaidőszak lejártá után a munkafelület összes tartalma törlődik.

A licencek használatát a következő módokon figyelheti meg:

- Tekintse meg a *Kulcshasználat jelentést* a szervezet felépítéséhez (**Monitoring and reporting** → **Reports**).
- A számítógép állapotának megtekintésével az **Devices** → **Managed devices** fülön. Ha az alkalmazás nincs aktiválva, a számítógép állapota ▲ *Az alkalmazás nincs aktiválva* lesz.
- Tekintse meg a licencadatokat a számítógép tulajdonságaiban.
- Tekintse meg a kulcstulajdonságokat (**Műveletek** → **Licencelés**).

[Az alkalmazás aktiválásának menete az Adminisztrációs Konzolon \(MMC\)](#)

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 (11.8.0)** → **Kulcs hozzáadása** lehetőséget.

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 kézzel, 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 **Feladat futtatása, ha a varázsló végzett** 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 ki a **Devices** → **Tasks** lehetőséget.

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

2. A **Task type** legördülő listából válassza ki az **Add key** lehetőséget.

3. A **Task name** mezőben adjon meg egy rövid leírást, például olyat, hogy *A Kaspersky Endpoint Security for Windows aktiválása*.

4. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét. 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 kézzel, 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 (**Műveletek** → **Licencelés**).

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 **Indítás** gombra. Ennek eredményeképpen a rendszer csendes módban aktiválja a Kaspersky Endpoint Security alkalmazást minden felhasználói számítógépen.

A *Kulcs hozzáadása* feladat tulajdonságaiban megadhat egy tartalék kulcsot a számítógéphez. A *tartalék kulcs* akkor válik aktívvá, ha az aktív kulcs lejár vagy törlődik. A rendelkezésre álló tartalék kulcs segítségével elkerülheti, hogy az alkalmazás funkciói csak korlátozottan legyenek elérhetők a licenc lejáratára esetén.

Licenckulcs automatikus hozzáadása az Adminisztrációs Konzolon keresztül (MMC)

1. Az Adminisztrációs Konzolon nyissa meg a mappát: **Administration Server** → **Kaspersky licenses**.
Megnyílik a licencek listája.
2. Nyissa meg a licenckulcs tulajdonságait.
3. Az **General** területen tegyen jelölést az **Automatically distributed license key** jelölőnégyzetbe.
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) licenclési korlát van érvényben. A licenclési 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 főablakában válassza az **Operations** → **Licensing** → **Kaspersky Licenses** lehetőséget.
Megnyílik a licencek listája.
2. Nyissa meg a licenckulcs tulajdonságait.
3. Az **General** fülön kapcsolja be a **Deploy license key automatically** kapcsológombot.
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) licenclési korlát van érvényben. A licenclési 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.

Az Aktiválási varázslóval aktiválhatja az alkalmazást.

A Kaspersky Endpoint Security aktiválása az Aktiválási varázsló segítségével:

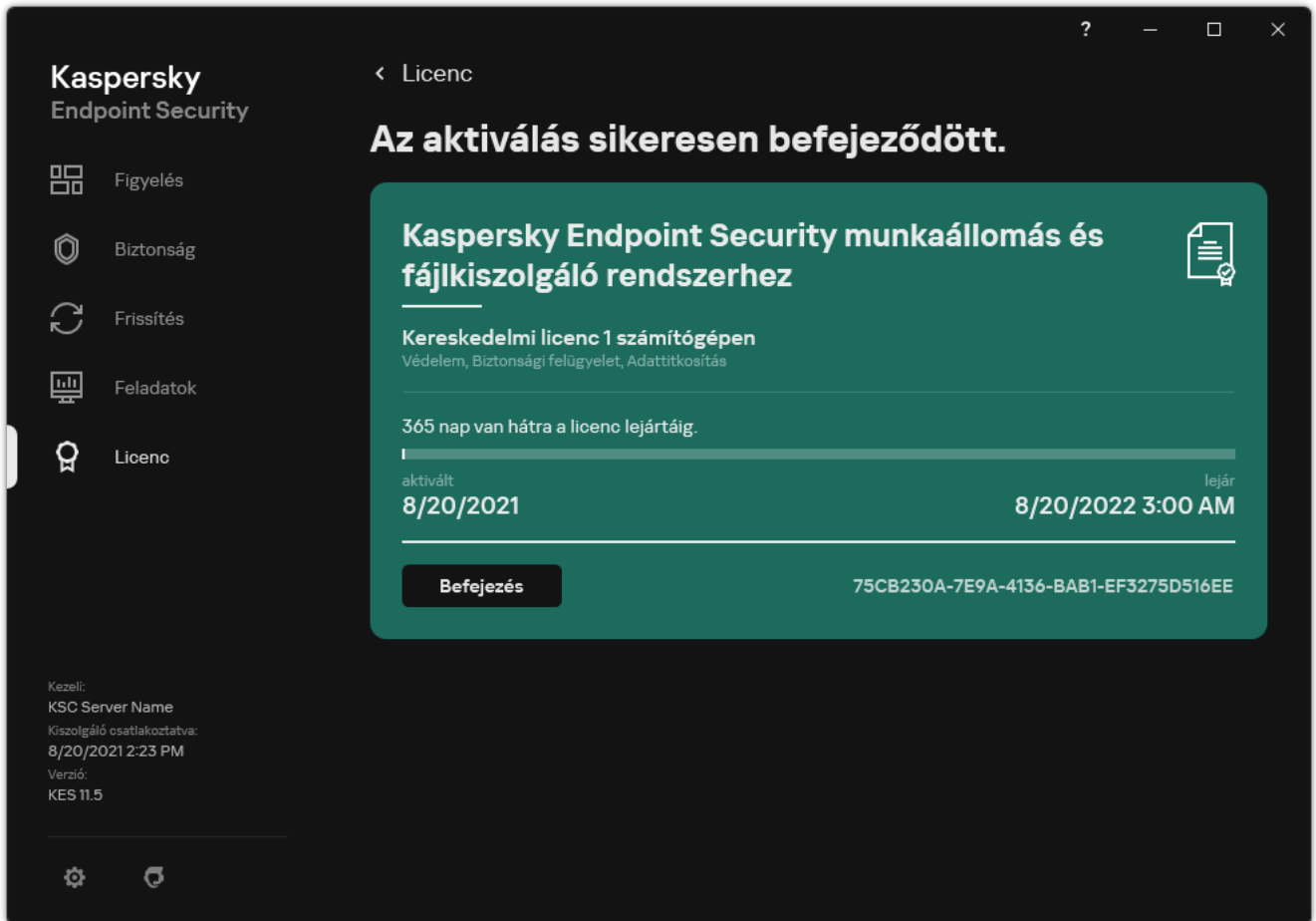
1. Nyissa meg a fő alkalmazásablakban a **Licenc** részt.
2. Kattintson **Az alkalmazás aktiválása új licenc használatával** gombra.

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

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.
- **Licenc típus.** 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 egyéb. 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 lejárat 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 licenccel 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 **Lépjén kapcsolatba az előfizetési szolgáltatójával** gombra.

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.

Adatok feletti rendelkezés

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);
- 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 előállítására 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 beleegyezik 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 lejártá óta eltelt napok száma;
- Azon számítógépek száma, amelyeken az aktív licenc alkalmazva van;
- Aktív kulcs;
- Kaspersky Endpoint Security licencfeltétel;
- A licenc jelenlegi állapota;
- Az aktív 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 Kasperskynek 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 csomagoló neve, információ az aláírásokkal kapcsolatban, futtatható fájl jelzője, formátumazonosító és entrópia), a folyamatfájllra 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 gyanús vagy kártékony 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 fejléceadatai, 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 fájl 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 sorozatszám, 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 and 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 fájljal 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 beállítástábla 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 beállításában, 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 nevééről 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 eseménnytípusról, 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 azonosítója, 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 leállítására vonatkozó információk: a memóriakép létrehozásának időbélyege, típusa, az esemény típusa, amely a Szoftverműködés rendellenes leállítását 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 folyamatképeinek ellenőrzőösszegei (MD5, SHA2-256, SHA1), amelyben a hiba kialakult, az alkalmazás folyamatképeinek 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 megghiúsult 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 túlcsoordult az eseménysor és ezen események száma, az eseménysor túlcsoordulásához 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, gyártó, 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, cylinderenkénti 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, fűrtök száma, fűrtméret, fűrtönkénti szektorok száma, üres és foglalt fűrtök 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 esemény-nyomkövetésből/események metaadataiból származó információ a Microsofttól: a rendszeresemények sorrendjére vonatkozó információ (típus, időpont, dátum, időzóna), a nyomkövetési eredményekkel rendelkező fájl metaadatai (név, struktúra, nyomkövetési paraméterek, a nyomkövetési 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, priorítás, idő), a folyamat lemezműveleteire vonatkozó információ (típus, idő, kapacitás, szám), a felhasználható memóriafolyamatok struktúrájának és kapacitásának változási előzményei;
- a ETW-ből, a StackWalk szolgáltatótól / 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 Filelo- / Disklo- / 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-szolgáltatóscímke);
- 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 algoritmus, a tanúsítvány nyilvános kulcsa és sorozatszám, 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 fájlút vonal 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 sorozatszám;
 - 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 lejárat dátuma;
- a számítógép helyi ideje az információk megadásakor;
- a folyamat során elért fájlok nevei és elérési útvjai;
- 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](#) és a [Kaspersky Sandbox](#) 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 vizsgálat 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 megghiúsulásának oka
- Észlelt objektum típusa
- Észlelt objektum neve
- Fenyegetés állapota az objektum feldolgozását követően
- Az ok, amiért a műveletek végrehajtása az objektumon megghiúsult
- 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 fájlnev 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 azonosító
- A fájl teljes neve (helyi fájlnev 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 or 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

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 vizsgálat 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)
- Fájl méret

- 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 beállítás kulcs 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

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.
- Memóriakiíratás.

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](#) ².

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 Securitytől a leírt esetek bármelyikében továbbított konkrét adatok a helyi jogszabályok vagy szabványok szerint személyes adatoknak minősülnek, akkor biztosítani 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 KSN szolgáltatást, vagy [tiltsa le a KSN használatát](#). A Privát KSN-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 Kasperskynek 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](#).

Memóriakiírás

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.

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 Súgót](#)*.

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: [rendszerbeállítások](#), [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 Kaspersky Security Center Adminisztrációs Konzol Adminisztrációs bővítményével ellentétben, ami egy adminisztrációs munkaállomásra van telepítve, a webes bővítményt egy olyan számítógépre kell telepíteni, amire telepítve van a Kaspersky Security Center Web Console. A webes bővítmény funkciója minden rendszergazdának elérhető, akik hozzáférnek a Webfelügyelőhöz egy böngészőben. A telepített webes bővítmények listáját megtekintheti 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](#).

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 hozzá a terjesztőcsomag ZIP-archívumát a Kaspersky Endpoint Security webes bővítményhez a Web Console felületében **Console settings** → **Web plug-ins**. A webes bővítmény terjesztőcsomagja például a Kaspersky webhelyéről tölthető le.

Az Adminisztrációs bővítmény frissítése

A Kaspersky Endpoint Security for Windows Adminisztrációs bővítmény frissítéséhez töltsen 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 érhetőek el a felhasznált bővítményekhez* értesítést. A Webfelügyelő értesítéseiből frissítheti a webes bővítmény verzióját. A Web Console 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 terjesztőcsomag ZIP-archívumát a Kaspersky Endpoint Security webes bővítményéhez 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.

A Kaspersky Endpoint Security 10 for Windows adminisztrációs bővítmény frissítése

Ha a Kaspersky Endpoint Security 10 for Windows adminisztrációs bővítmény az Adminisztrációs konzolban van telepítve, akkor a Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény telepítése előtt vegye figyelembe a következőket:

- A Kaspersky Endpoint Security 10 for Windows adminisztrációs bővítmény nem kerül eltávolításra, elérhető lesz a műveletek számára. Ezért két felügyeleti bővítményhez lesz hozzáférése a 10-es és 11-es alkalmazásverzióval való használathoz.


- A Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény nem támogatja a Kaspersky Endpoint Security 10 for Windows felhasználói számítógépeken történő telepítését.
- A Kaspersky Endpoint Security 11 for Windows Adminisztrációs bővítmény nem támogatja az olyan összetevőket (például szabályzatok vagy feladatok), amik a Kaspersky Endpoint Security 10 for Windows Adminisztrációs bővítménnyel lettek létrehozva.

Használhatja a Házirendek és feladatok kötegelt átalakítása varázslót a házirendek és feladatok konvertálására a 10-es verzióról a 11-es verzióra. A házirendek és feladatok konvertálásának további részleteiről a [Kaspersky Security Center súgójából](#) ² tájékozódhat.



A Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény frissítése

Ha a Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény az Adminisztrációs konzolban van telepítve, akkor a Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény új verziójának telepítése előtt vegye figyelembe a következőket:

- A Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény korábbi verziói el lettek távolítva.
- A Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény új verziója támogatja a Kaspersky Endpoint Security 11 for Windows adminisztrációs bővítmény előző verzióinak felhasználói számítógépeken történő kezelését.
- 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 [alkalmazásúgót](#).

- Ha az adminisztrációs bővítmény új verziójának csoportbeállításaihoz új paraméter lett hozzáadva, a csoportbeállítás  /  tulajdonsága korábban meghatározott állapota nem változik meg.
- Az adminisztrációs bővítmény 11.2.0 verzióra történő frissítésekor meg kell nyitnia egy házirendet annak automatikus konvertálásához. Ennek során a Kaspersky Endpoint Security megerősítést kér a KSN-ben való részvételhez. Ha a vállalat számítógépein már frissítette az alkalmazást a 11.2.0 verzióra, a KSN-ben való részvétel le lesz tiltva, amíg el nem fogadja a KSN-ben való részvétel feltételeit.

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 (átviteli réteg biztonsága) 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.

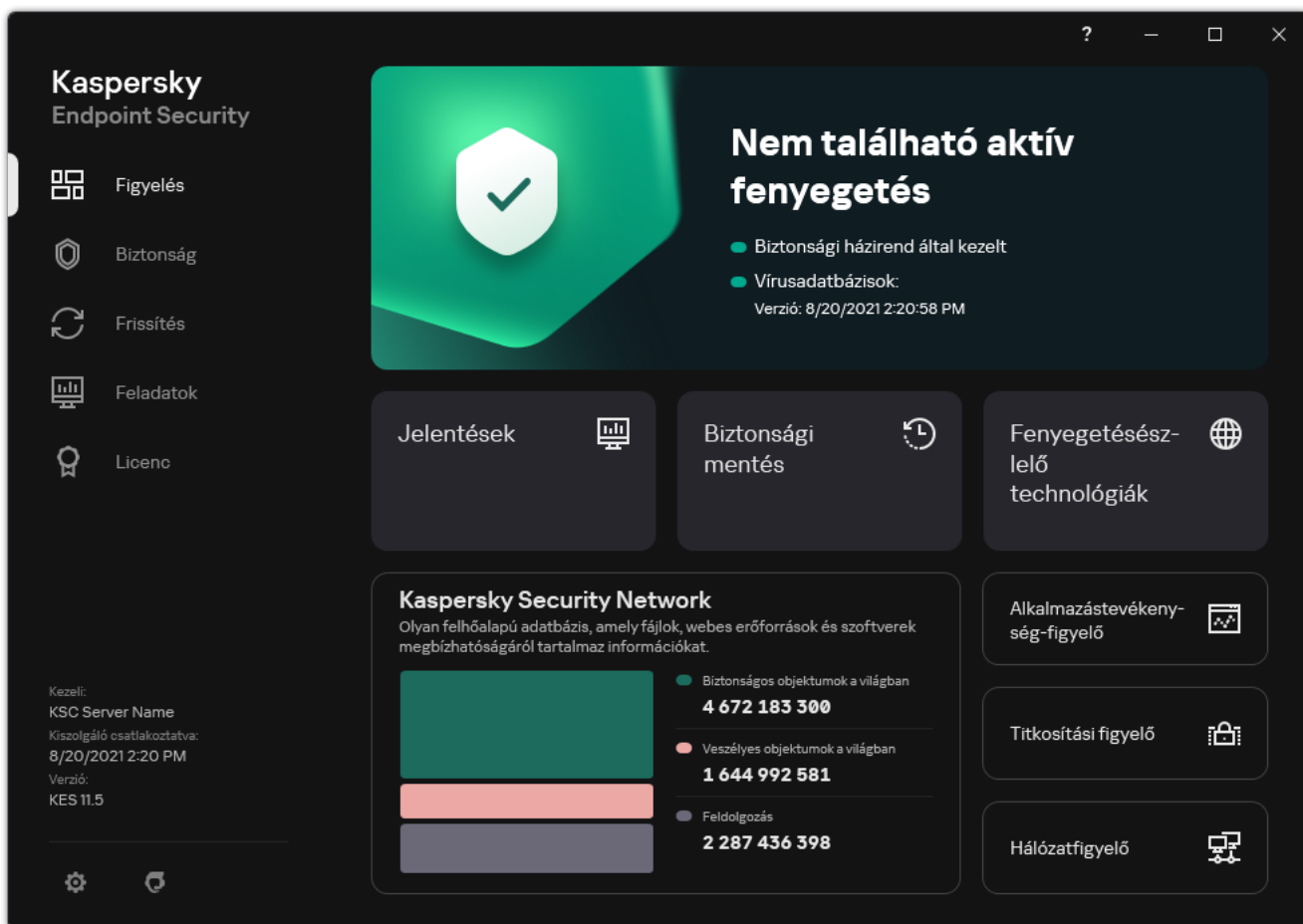
A TLS használata a következő funkciókkal növeli az alkalmazás biztonságát:

- 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 nyilvános kulcsú infrastruktúra (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 ön aláírt tanúsítványok 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 részt vesz a Kaspersky Security Networkben, a KSN szolgáltatás megadja a Kaspersky Endpoint Security számára a vizsgált fájlok kategóriáját és hírnevét, valamint a vizsgált webcímek hírnevét.
- **Alkalmazástevékenység-figyelő.** Információk megtekintése a telepített alkalmazások működéséről. A Rendszerfigyelő az alkalmazással kapcsolatos fájl-, beállításjegyzék-, illetve operációsrendszer-eseményeket követi nyomon.
- **Hálózatfigyelő.** [Információk megtekintése valós időben a számítógép hálózati tevékenységéről.](#)

	<ul style="list-style-type: none"> • Titkosítási figyelő. Valós időben figyeli a lemez titkosítási vagy visszafejtési folyamatát. A Titkosítási figyelő akkor érhető el, ha a Kaspersky lemeztitkosítás vagy a BitLocker meghajótitkosítás 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 vírusvizsgálatot és az alkalmazásintegritás ellenőrzését . A rendszergazda elrejtheti a feladatokat egy felhasználó elől , vagy korlátozhatja a feladatok kezelését .
Licenc	Az alkalmazás licencléle. 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.

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.

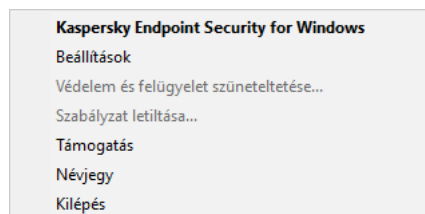
- **Védelem felfüggesztése / Védelem folytatása.** Szünetelteti a védelmi és felügyeleti összetevők műveleteit, amik nincsenek zárva a (☐) rendszabályban. Mielőtt elvégezné ezt a műveletet, javasolt kikapcsolni a Kaspersky Security Center rendszabályt.

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 vizsgálati feladatok teljesítményére. Az alkalmazás folytatja a Kaspersky Security Network használatát.

- **Szabályzat letiltása / Szabályzat engedélyezése.** Letiltja a Kaspersky Security Center szabályzatot 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.



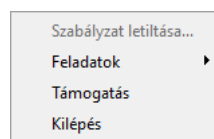
Az alkalmazás ikonjának helyi menüje

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.** Letiltja a Kaspersky Security Center szabályzatot 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:

- Integritás-ellenőrzés.
- 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 törölődik 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:

- **With simplified interface.** 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 értesítéseket is megjelenít az alkalmazásikon felett.
- **Teljes felületen.** 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.
- **No interface.** 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.
6. Az **Interakció a felhasználóval** részen hajtsa végre a következő műveletek valamelyikét:
 - Jelölje be a **Felhasználói felület megjelenítése** jelölőnégyzetet, ha azt szeretné, hogy a felület következő elemei megjelenjenek az ügyfélszámítógépen:
 - Az alkalmazás nevét tartalmazó mappa a **Start** menüben
 - A Microsoft Windows tálca értesítési területén lévő [Kaspersky Endpoint Security ikon](#)
 - Előbukkanó értesítések

Ha be van jelölve ez a jelölőnégyzet, a felhasználó az alkalmazás felületén megtekintheti, és amennyiben a rendelkezésre álló jogok megengedik, megváltoztathatja az alkalmazás beállításait.

 - Törölje a **Felhasználói felület megjelenítése** jelölőnégyzet jelölését, ha a Kaspersky Endpoint Security minden jelét el szeretné rejteni az ügyfélszámítógépen.
7. Jelölje be az **Interakció a felhasználóval** részben az **Egyszerűsített alkalmazásfelület megjelenítése** jelölőnégyzetet, ha azt szeretné, hogy az [egyszerűsített alkalmazásfelület](#) megjelenjen az olyan számítógépen, amelyre fel van telepítve a Kaspersky Endpoint Security.

[Az alkalmazásfelület megjelenítési módja konfigurálásának menete a Web Console-ban, illetve a Cloud Console-ban](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Felület** helyre.
5. Az **Interaction with user** részben konfigurálja az alkalmazásfelület megjelenésének módját:
 - **With simplified interface.** 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 értesítéseket is megjelenít az alkalmazásikon felett.
 - **Teljes felületen.** 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.
 - **No interface.** Az ügyfélszámítógépen nincs jelen a Kaspersky Endpoint Security működésének. A [Windows értesítési sávon lévő ikon](#) és az értesítések nem érhetők el.
6. Mentse el a módosításokat.

Első lépések

Miután telepíti az alkalmazást az ügyfélszámítógépekre, ahhoz, hogy a Kaspersky Endpoint Security from Kaspersky Security Center Web Console 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 a *Frissítés* és *Vírusvizsgálat* feladatokat.

A *Frissítés* feladat ahhoz szükséges, hogy a számítógép védelme naprakész legyen. A feladat végrehajtásakor a Kaspersky Endpoint Security [frissíti az antivírus adatbázisokat és az alkalmazásmodulokat](#). A *Update* feladatot a Kaspersky Security Center Kezdeti beállító varázslója hozza létre automatikusan. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows webes bővítményt, miközben futtatja a Varázslót.

A *Vírusvizsgálat* feladattal időben észlelni lehet a vírusokat, és egyéb rosszindulatú programok keresésére szükséges. Kézzel kell létrehoznia a *Vírusvizsgálat* feladatot.

[Vírusvizsgálati feladat létrehozásának menete az Adminisztrációs Konzolban \(MMC\)](#) 

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 (11.8.0)** → **Virus Scan** lehetőséget.

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 a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security törli a fájlokat.
- **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 lehetséges, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.
- **Értesítés.** 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, amittől a többi alkalmazás lelassulhat. A fejlett vírusmentesítés elvégzését követően a Kaspersky Endpoint Security anélkül újraindítja a számítógépet, hogy ehhez a felhasználó megerősítését kérné.

Konfigurálja a feladatfuttatási módot a **Csak akkor fusson, ha a számítógép üresjáratban van** jelölőnégyzettel. Ez a jelölőnégyzet ki- és bekapcsolja a *Vírusvizsgálatot* felfüggesztő funkciót, ha a számítógép erőforrásai korlátozottak. A Kaspersky Endpoint Security a képernyőkímélő kikapcsolásakor és a számítógép feloldásakor szünetelteti a *Vírusvizsgálatot*.

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 kézzel, 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 *Vírusvizsgálat* 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 kézzel 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 **Feladat futtatása, ha a varázsló végzett** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni. Ennek eredményeképpen a Vírusvizsgálat feladat végre lesz hajtva a felhasználói számítógépeken, a megadott ütemterv alapján.

[Vírusvizsgálati feladat létrehozásának menete a Web Console-ban](#) 

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

b. A **Task type** legördülő listából válassza ki az **Virus scan** lehetőséget.

c. A **Task name** mezőben adjon meg egy rövid leírást, például olyat, hogy *Weekly scan*.

d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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

5. Lépjen ki a varázslóból.

Egy új feladat jelenik meg a feladatok listájában.

6. A feladat ütemtervének megadásához menjen a feladatok tulajdonságaiba.

Ajánlott ütemezni a feladat futtatását legalább heti egy alkalomra.

7. Válassza ki a feladat melletti jelölőnégyzetet.

8. Kattintson a **Futtatás** gombra.

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

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

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.

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.

Aktív és inaktív rendszabály

A rendszabály a kezelt számítógépek egy csoportjának van megszabva, lehet aktív és inaktív is. 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.



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.

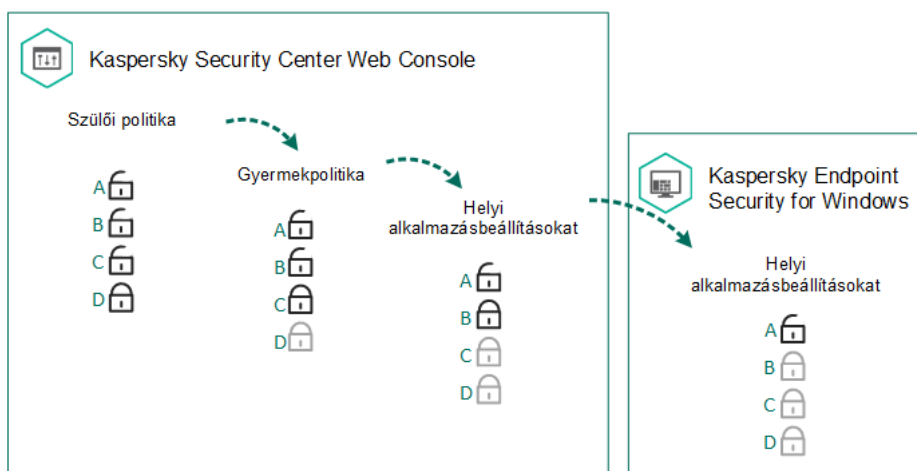
Házon kívüli rendszabály

A házon kívüli rendszabály akkor aktiválódik, ha a számítógép elhagyja a szervezet hálózatának területét.

A beállítások öröklődése

A rendszabályok, például az adminisztrációs csoportok hierarchiával rendelkeznek. Alapértelmezés szerint a gyermek rendszabályok öröklik a szülő rendszabályok beállításait. A *Gyermekrendszabály* egy rendszabály a beágyazott hierarchiaszintekhez, vagyis egy rendszabály a beágyazott adminisztrációs csoportokhoz és a másodlagos adminisztrációs kiszolgálókhoz. A szülő rendszabályokban kikapcsolhatja az öröklési beállításokat.

Minden egyes rendszabály-beállításnak van  tulajdonsága, amely jelzi, hogy módosítható-e a gyermekrendszabályokban vagy a [helyi alkalmazásbeállításokban](#). A  tulajdonság csak akkor alkalmazható, ha a szülőrendszabály-beállítások engedélyezve vannak a gyermekrendszabályokhoz. 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 hatóköréinél. A rendszabályok beállításaihoz való hozzáférés beállításához lépjen a Kaspersky Security Center felügyeleti kiszolgáló tulajdonságok ablakában a **Biztonság** részhez.



Rendszabály létrehozása

[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. A munkaterületen válassza ki a **Policies** lapot.
4. Kattintson az **New policy** gombra.
Elindul a Rendszabályvarázsló.
5. Kövesse a Rendszabályvarázsló utasításait.

[Rendszabály létrehozásának menete a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a **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. Az **General** fülön a következő műveleteket végezheti el:
 - A rendszabály nevének megváltoztatása.
 - A rendszabály állapotának kiválasztása:
 - **Aktív.** A következő szinkronizáció után a rendszabály aktív rendszabályként lesz használva a számítógépen.
 - **Inaktív.** Biztonsági mentési rendszabály. Szükség esetén az inaktív rendszabály átváltható aktív állapotra.
 - **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 örököve. 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 **Szülőrendszabály beállításainak öröklése** 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.
6. Az **Application settings** fülön beállíthatja a [Kaspersky Endpoint Security rendszabály beállításait](#).
7. Mentse el a módosításokat.

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 beállításaiiban engedélyeznie kell a bővített rendszabályadatok fogadását. A Hálózati ügynök rendszabály további részleteiről a [Kaspersky Security Center súgójából](#)  tájékozódhat.

Biztonságiszint-jelző

A biztonsági szint jelzése a **Tulajdonságok: <Rendszabály neve>** 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.
 - Viselkedéselemzés.
 - Biztonsági rések kihasználásának megelőzése.
 - Kármentesítő motor.
 - **Fontos.** Ez a kategória a következő összetevőket foglalja magába:
 - Kaspersky Security Network.
 - Web védelem.
 - Levelezés védelem.
 - Behatolásmegelőző rendszer.
- **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 **Közepes védelmi szint** vagy **Alacsony védelmi szint** érték jelenik meg, az **Ajánlott védelmi összetevők** hivatkozás elérhető lesz a jelzéstől jobbra. Ebben az ablakban engedélyezheti az ajánlott védelmi összetevők bármelyikét.

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 tudnivalóért lásd a [Kaspersky Security Center Sűgőt](#).

A Kaspersky Endpoint Security az alábbi feladatokat támogatja:

- **Vírusvizsgálat.** A Kaspersky Endpoint Security megvizsgálja a számítógép feladatbeállításokban megadott területein a vírusok és egyéb fenyegetések jelenlétét. A *Vírusvizsgálat* feladat a Kaspersky Endpoint Security

működése érdekében szükséges, a Kezdeti beállító varázsló során van létrehozva. 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.
- **[Alkalmazásösszetevők módosítása](#)**. A Kaspersky Endpoint Security a feladat beállításaiiban 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.
- **[Frissítés](#)**. A Kaspersky Endpoint Security frissíti az adatbázisokat és alkalmazásmodulokat. A *Frissítés* 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 vizsgálja 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.
- **[Integritás ellenőrzés](#)**. 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.

A feladatok csak akkor futnak a számítógépen, ha a [Kaspersky Endpoint Security fut](#).

Új feladat hozzáadása

[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 **Feladatok** mappát.
3. Kattintson az **Új feladat** 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 ki a **Devices** → **Tasks** lehetőséget.

Megnyílik a feladatok listája.

2. Kattintson a **Hozzáadás** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** 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 **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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

5. Lépjen ki a varázslóból.

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 **Indítás** 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 and reporting** → **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.

Feladathozzáférés-felügyelet

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 a **Biztonság** 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. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakban válassza a **Helyi feladatok** → **Feladatkezelés** részt.
6. Feladatkezelési mód beállítása (lásd az alábbi ábrát).
7. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Alkalmazásbeállítások** fület.
4. Lépjen a **Helyi feladatok** → **Feladatkezelés** részre.
5. Feladatkezelési mód beállítása (lásd az alábbi ábrát).
6. Mentse el a módosításokat.

Feladatkezelés beállítások

Paraméter	Leírás
Helyi feladatok használatának engedélyezése	<p>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.</p> <p>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.</p> <p>A felhasználó ilyenkor is el tudja végezni fájl vagy mappa vírusvizsgálatát, ha az adott fájl vagy mappa helyi menüjében kiválasztja a Vírusok keresése lehetőséget. A vizsgálati feladat az egyéni vizsgálati feladatok alapértelmezett értékeivel indul el.</p>
Csoportfeladatok megjelenítésének engedélyezése	<p>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.</p>

	Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security egy üres feladatlistát jelenít meg.
Csoportfeladatok kezelésének engedélyezése	<p>Ha a jelölőnégyzet be van jelölve, a felhasználó elindíthat és leállíthat a Kaspersky Security Center alkalmazásban megadott csoportfeladatokat. A felhasználók az alkalmazás felületén vagy az egyszerűsített alkalmazásfelületen indíthatnak el vagy állíthatnak le feladatokat.</p> <p>A jelölőnégyzet törlése után a Kaspersky Endpoint Security automatikusan elindítja az ütemezett feladatot vagy a rendszergazda manuálisan elindítja a feladatokat a Kaspersky Security Center alkalmazásban.</p>

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 [rendszerbeállítások 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 ügyfélszámítógép tartozik.
 3. Válassza ki a munkaterületen a **Devices** lapot.
 4. Válassza ki azt a számítógépet, amelyen meg szeretné adni a Kaspersky Endpoint Security beállításait.
 5. Az ügyfélszámítógép helyi menüjében válassza ki a **Properties** elemet.
Megnyílik az ügyfélszámítógép tulajdonságainak ablaka.
 6. Válassza ki az ügyfélszámítógép tulajdonságainak ablakában az **Applications** részt.
Megjelenik az ügyfélszámítógépen telepített Kaspersky applications listája az ügyfélszámítógép tulajdonságainak ablakában a jobb oldalon.
 7. Válassza a Kaspersky Endpoint Security alkalmazást.
 8. Kattintson a Kaspersky alkalmazások listája alatti **Tulajdonságok** gombra.
Ezzel megnyílik a **Kaspersky Endpoint Security for Windows application settings** ablak.
 9. Konfigurálja az **General settings** részen a Kaspersky Endpoint Security és a Jelentések és tároló beállításait.
A **Kaspersky Endpoint Security for Windows alkalmazás beállításai** ablak többi része megegyezik a Kaspersky Security Center szokásos részeivel. E részek ismertetése a Kaspersky Security Center Súlyó 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.
10. 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 ki a **Devices** → **Managed devices** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.
Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki a **Applications** lapot.
4. Kattintson a **Kaspersky Endpoint Security for Windows** lehetőségre.
Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** fület.
6. Adja meg a helyi alkalmazásbeállításokat.
7. A helyi alkalmazásbeállítások megegyeznek a [rendszerbeállításokkal](#), 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
6. Használja **A Kaspersky Endpoint Security for Windows indítása a számítógép bekapcsolásával egy időben** jelölőnégyzetet, hogy konfigurálja az alkalmazás indítását.
7. Mentse el a módosításokat.

[A Kaspersky Endpoint Security elindításának konfigurálási menete a Web Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Alkalmazásbeállítások** elemhez.
5. Használja **A Kaspersky Endpoint Security indítása a számítógép bekapcsolásával egy időben (ajánlott)** jelölőnégyzetet az alkalmazás indításának beállításához.
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.
3. Használja **A Kaspersky Endpoint Security for Windows indítása a számítógép bekapcsolásával egy időben** jelölőnégyzetet, hogy konfigurálja az alkalmazás indítását.
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 **Védelmi állapot** eszközzel 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 ügyfélszámítógép tartozik.
3. Válassza ki a munkaterületen a **Devices** lapot.
4. Válassza ki azt a számítógépet, amelyen az alkalmazást elindítani vagy leállítani szeretné.
5. Az ügyfélszámítógép helyi menüjének megjelenítéséhez kattintson a jobb egérgombbal, és válassza a **Tulajdonságok** parancsot.
6. Válassza ki az ügyfélszámítógép tulajdonságainak ablakában az **Applications** részt.
Megjelenik az ügyfélszámítógépen telepített Kaspersky applications listája az ügyfélszámítógép tulajdonságainak ablakában a jobb oldalon.
7. Válassza a Kaspersky Endpoint Security alkalmazást.
8. Végezze el az alábbiakat:
 - 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 ki a **Devices** → **Managed 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 a **Applications** lapot.
4. Tegyen jelölést a **Kaspersky Endpoint Security for Windows** lehetőséggel szembeni jelölőnégyzetbe.
5. Kattintson az **Indítás** vagy **Leállítás** gombra.

[A Kaspersky Endpoint Security alkalmazás elindítása vagy leállítása a parancssorból](#)

Ahhoz, hogy leállítsa az alkalmazást a parancssorból, [be kell kapcsolnia a rendszerszolgáltatások külső kezelését](#).



A klpsm.exe fájl, ami megtalálható a Kaspersky Endpoint Security terjesztőkészletben, elindíthat vagy leállíthat alkalmazást 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. 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`.

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 jelenti, hogy a számítógép védelme és felügyelete szünetel.
- A  ikon azt jelenti, hogy a számítógép védelme és felügyelete engedélyezve van.

A számítógép védelmének és felügyeletének szüneteltetése és újraindítása a vizsgálati és frissítési feladatokra nincsnek hatással.

Ha a számítógép védelmének és felügyeletének felfüggesztése, illetve újraindítása idején hálózati kapcsolatok létesülnek, értesítés jelenik meg ezen kapcsolatok megszakításáról.

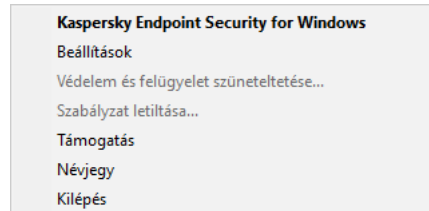
A számítógép védelmének és felügyeletének szüneteltetése és folytatása:

1. Kattintson a jobb egérgombbal a tálcá 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. Ehhez a konfigurációs fájlt a terjesztőcsomaggal megegyező mappában kell menteni.
- A Kaspersky Endpoint Security távoli telepítésének elvégzése a Kaspersky Security Centeren keresztül előre megadott beállításokkal.
- A Kaspersky Endpoint Security beállításainak áttelepítése egyik számítógépről a másikra.


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 fájl a Kaspersky Endpoint Security helyi, illetve távoli telepítéséhez használhassa, az install.cfg nevet kell adnia.

5. Mentse a fájlt.

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 **Importálás** 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 alapértelmezett alkalmazásbeállítások visszaállítása

Bármikor visszatérhet az Endpoint Security alkalmazás Kaspersky által ajánlott beállításaihoz. 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.

A számítógép vírusvizsgálata

A víruskeresés a számítógép biztonsága szempontjából létfontosságú. A rendszeresen elvégzett vírusvizsgálatok kizárják 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

- Microsoft Outlook postaláda
- 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 háttérvizsgálat 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.

Integritás ellenőrzés

A Kaspersky Endpoint Security ellenőrzi, hogy az alkalmazásmodulok nem sérültek vagy módosultak-e.

Számítógép vizsgálata

A víruskeresés a számítógép biztonsága szempontjából létfontosságú. A rendszeresen elvégzett vírusvizsgálatok kizárják 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 szabványos feladatai előre meghatározottak: *Teljes vizsgálat*, *Kritikus területek vizsgálata*, *Egyéni vizsgálat*. Ha a vállalata telepítette a Kaspersky Security Center adminisztrációs rendszerét, akkor [létrehozhat egy Vírusvizsgálat feladatot](#), és konfigurálhatja a vizsgálatot. A [Vizsgálat a háttérben feladat](#) a Kaspersky Security Centerben is elérhető. A háttérben végzett vizsgálat nem konfigurálható.

[Vírusvizsgálat futtatása 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.
Ha szükséges, [hozzon létre egy vírusvizsgálati](#) feladatot.
5. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.
6. Konfigurálja a vizsgálati feladatot (lásd az alábbi táblázatot).
Ha szükséges, [konfigurálja a vizsgálati feladat ütemezését](#).
7. Mentse el a módosításokat.
8. 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.

[Vírusvizsgálat futtatása a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a vizsgálati feladatra.
Megnyílik a feladatok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
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.

[Vírusvizsgálat 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 házi rendben](#).

Vizsgálati beállítások

Paraméter	Leírás
Biztonsági szint	<p>A Kaspersky Endpoint Security különböző beállítás csoportokat használhat a vizsgálat futtatásához. Ezek az alkalmazásban tárolt beállítás csoportokat <i>biztonsági szinteknek</i> nevezzük:</p> <ul style="list-style-type: none"> • Magas. A Kaspersky Endpoint Security minden típusú fájlt megvizsgál. Összetett fájlok vizsgálata esetén a Kaspersky Endpoint Security a levél formátumú fájlokat is megvizsgálja. • Ajánlott. A Kaspersky Endpoint Security a merevlemezeken, a hálózati meghajtókon és a számítógép hordozható adattárolóin található fájl típusok közül csak a megadott formátumúakat vizsgálja, valamint a beágyazott OLE-objektumokat. A Kaspersky Endpoint Security nem vizsgálja az archívumokat és a telepítő csomagokat. • Alacsony. A Kaspersky Endpoint Security csak a megadott kiterjesztésű új és módosult fájlokat vizsgálja a számítógépen lévő összes merevlemezen, cserélhető meghajtón és hálózati meghajtón. A Kaspersky Endpoint Security nem vizsgál összetett fájlokat. <p>Kiválaszthatja az előre beállított biztonsági szintek egyikét, de kézzel is megadhatja a beállításokat. Ha módosítja a biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.</p>
Művelet fenyegetés észlelésekor	<p>Vírusmentesítés; törlés, 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 törli a fájlokat.</p> <p>Vírusmentesítés; blokkolás, 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 lehetséges, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.</p> <p>Értesítés. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.</p>

	<p>Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, a Kaspersky Endpoint Security létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.</p> <p>Windows Store-alkalmazás részét alkotó fertőzött fájlok észlelése esetén a Kaspersky Endpoint Security megkísérli törölni a fájlt.</p>
<p>Fejlett vírusmentesítés futtatása azonnal</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>A Fejlett vírusmentesítés csak akkor van alkalmazva a vírusvizsgálat alatt, ha a Fejlett vírusmentesítés funkció engedélyezve van a számítógépen alkalmazott irányelv tulajdonságaiban.</p> <p>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.</p> <p>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.</p>
<p>Vizsgálat hatóköre</p>	<p>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 másolatáról, a levelezési adatbázisok, a merevlemez, a cserélhető meghajtó vagy a hálózati meghajtó, egy-egy mappa, illetve fájl.</p>
<p>Vizsgálat ütemezése</p>	<p>Manually. A futásmód, amelyben manuálisan elindíthatja a vizsgálatot, amikor az Önnek kényelmes.</p> <p>By schedule. A vizsgálati feladatoknak ebben a futásmódjában a Kaspersky Endpoint Security a feladatot a létrehozott ütemtervnek megfelelően futtatja. A vizsgálati feladat ezen futásmódjának kiválasztása esetén a vizsgálati feladat elindítható kézzel is.</p>
<p>Futtatás elhalasztása az alkalmazásindítás után N percre</p>	<p>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.</p>
<p>Kihagyott vizsgálatok futtatása</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott vizsgálati feladatot azonnal elindítja, amint lehetségessé válik. A vizsgálati feladat például akkor hagyható ki, ha a számítógép a frissítési feladat indítási időpontjában ki volt kapcsolva. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott vizsgálati feladatokat. Ehelyett a következő vizsgálati feladatot a jelenlegi ütemezésnek megfelelően futtatja.</p>
<p>Csak akkor fusson, ha a számítógép üresjáratban van</p>	<p>A vizsgálati 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.</p>

Vizsgálat futtatása mint	<p>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. A Kaspersky Endpoint Security beállításában megadhat egy olyan felhasználót, aki rendelkezik a szükséges jogokkal, és a vizsgálati feladatot e felhasználói fiók alatt futtathatja.</p>
Fájltípusok	<div data-bbox="419 394 1493 555" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A Kaspersky Endpoint Security a kiterjesztés nélküli fájlokat végrehajthatónak tekinti. A Kaspersky Endpoint Security a végrehajtható fájlokat mindig megvizsgálja, függetlenül a vizsgálatra kiválasztott fájltypusoktól.</p> </div> <p>Minden fájl. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül).</p> <p>Formátum alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejléceket a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres.</p> <p>Kiterjesztés alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.</p> <p>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 fertőzötték listáján (pl. .123).</p>
Csak az új és módosult fájlok vizsgálata	<p>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.</p>
Vizsgált objektumok kihagyása, ha a vizsgálatuk hosszabb, mint N másodperc hosszabb idő szükséges	<p>Korlátozza egyetlen objektum vizsgálatának időtartamát. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.</p>
Archívumok vizsgálata	<p>ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb tömörített formátumok vizsgálata.</p>
Terjesztési csomagok vizsgálata	<p>Ez a jelölőnégyzet engedélyezi/letiltja a harmadik féltől származó terjesztőcsomagok vizsgálatát.</p>
Microsoft Office formátumú fájlok vizsgálata	<p>Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-objektumokat is magukban foglalják.</p>
E-mail formátumok vizsgálata	<p>Az e-mail formátumú fájlok és a levéladatbázis átvizsgálása. Az alkalmazás ellenőrzi az MS Outlook és a Windows Mail/Outlook Express levelezőprogramok által használt PST- és OST-fájlokat, valamint az EML-fájlokat.</p>

	<p>A Kaspersky Endpoint Security nem támogatja az MS Outlook e-mail kliens 64 bites verzióját. Ez azt jelenti, hogy a Kaspersky Endpoint Security akkor sem ellenőrzi a 64 bites verziójú MS Outlook-fájlokat (PST és OST), ha az e-mailek a vizsgálat hatókörébe tartoznak.</p> <p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security az e-mail formátumú fájlt egyetlen fájlként vizsgálja meg.</p>
<p>Jelszóvédett archívumok vizsgálata</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security megvizsgálja a jelszóval védett archívumokat. Mielőtt az archívumokban lévő fájlokat vizsgálatára sor kerülhetne, a rendszer felkéri a jelszó megadására.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security kihagyja a jelszóval védett archívumok vizsgálatát.</p>
<p>Ne csomagoljon ki nagy összetett fájlokat</p>	<p>Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket.</p> <p>Ha a négyzet nincs bejelölve, a Kaspersky Endpoint Security mindenfajta méretű összetett fájlt megvizsgál.</p> <p>A Kaspersky Endpoint Security megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.</p>
<p>Gépi tanulás és aláírás-elemzés</p>	<p>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.</p> <p>A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.</p>
<p>Heurisztikus elemzés</p>	<p>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.</p> <p>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 erőforrásainak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.</p>
<p>iSwift Technológia</p> <p><i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i></p>	<p>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.</p>
<p>iChecker Technológia</p>	<p>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</p>

(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)

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 (Fájl védelem összetevő). A vírusok és más rosszdindulató programok terjedésének megakadályozásához beállíthatja a cserélhető meghajtók automatikus vizsgálatát a számítógéphez történő csatlakoztatásukkor. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakban válassza a **Helyi feladatok** → **Cserélhető meghajtók vizsgálata** részt.
6. A **Cserélhető meghajtó csatlakoztatásukkor végzendő művelet** legördülő listából válassza a **Részletes vizsgálat** vagy a **Gyors vizsgálat** lehetőséget.
7. Konfigurálja a cserélhető meghajtók vizsgálatának speciális beállításait (lásd az alábbi táblázatot).
8. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Helyi feladatok** → **Cserélhető meghajtók vizsgálata** részt.
5. A **Cserélhető meghajtó csatlakoztatásakor végzendő művelet** legördülő listából válassza a **Részletes vizsgálat** vagy a **Gyors vizsgálat** lehetőséget.
6. Konfigurálja a cserélhető meghajtók vizsgálatának speciális beállításait (lásd az alábbi táblázatot).
7. 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
Cserélhető meghajtó csatlakoztatásakor végzendő művelet	<p>Részletes vizsgálat. Ha ez az elem van kiválasztva, akkor cserélhető meghajtó csatlakoztatásakor a Kaspersky Endpoint Security a cserélhető meghajtón lévő 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.</p> <p>Gyors vizsgálat. 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 sebezhetőek, és nem csomagolja ki az összetett objektumokat.</p>
Cserélhető meghajtó maximális mérete	Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security elvégzi a Cserélhető meghajtó csatlakoztatásakor végzendő művelet legördülő listából kiválasztott műveletet azokon a cserélhető meghajtókon, amelyek mérete nem haladja meg a megadott maximális meghajtóméretet.

	Ha ez a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security a Cserélhető meghajtó csatlakoztatásakor végzendő művelet legördülő listából kiválasztott műveletet bármilyen méretű cserélhető meghajtón elvégzi.
Vizsgálati folyamat megjelenítése	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.
A vizsgálati feladat leállításának tiltása	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 háttérvizsgálat 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. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakban válassza a **Helyi feladatok** → **Vizsgálat a háttérben** részt.
6. A **Háttérbeli vizsgálat engedélyezése** jelölőnégyzettel kapcsolhatja be vagy ki a vizsgálatot a háttérben.
7. Mentse el a módosításokat.

[A háttérvizsgálat engedélyezése a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Helyi feladatok** → **Vizsgálat a háttérben** részt.
5. A **Háttérbeli vizsgálat engedélyezése** jelölőnégyzettel kapcsolhatja be vagy ki a vizsgálatot a háttérben.
6. Mentse el a módosításokat.

[A háttérvizsgálat engedélyezése az alkalmazás felületén](#)

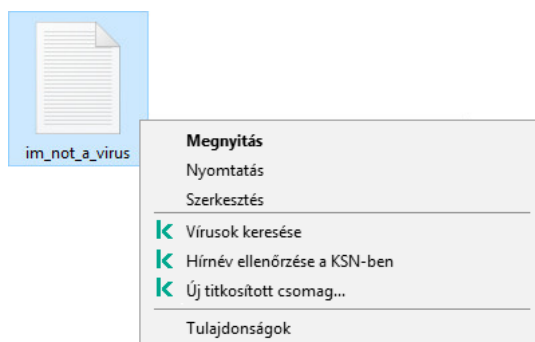
1. A fő alkalmazásablakban nyissa meg a **Feladatok** részt.
2. A feladatlistában válassza ki a vizsgálati feladatot, és kattintson a  elemre.
3. A **Vizsgálat a háttérben** kapcsolóval kapcsolhatja be vagy ki a háttérvizsgálatot.
4. Mentse el a módosításokat.

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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A házirend ablakban válassza a **Helyi feladatok** → **Vizsgálat a helyi menüből** lehetőséget.
6. A Vizsgálat a helyi menüből feladat konfigurálása (lásd az alábbi táblázatot).
7. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Helyi feladatok** → **Vizsgálat a helyi menüből** lehetőséget.
5. A Vizsgálat a helyi menüből feladat konfigurálása (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	<p>A Kaspersky Endpoint Security különböző beállításcsoportokat használhat a vizsgálat futtatásához. Ezek az alkalmazásban tárolt beállításcsoportokat <i>biztonsági szinteknek</i> nevezzük:</p> <ul style="list-style-type: none">• Magas. A Kaspersky Endpoint Security minden típusú fájlt megvizsgál. Összetett fájlok vizsgálata esetén a Kaspersky Endpoint Security a levél formátumú fájlokat is megvizsgálja.• Ajánlott. A Kaspersky Endpoint Security a merevlemezeken, a hálózati meghajtókon és a számítógép hordozható adattárolóin található fájlformátumok közül csak a megadott formátumúakat vizsgálja, valamint a beágyazott OLE-objektumokat. A Kaspersky Endpoint Security nem vizsgálja az archívumokat és a telepítő csomagokat.• Alacsony. A Kaspersky Endpoint Security csak a megadott kiterjesztésű új és módosult fájlokat vizsgálja a számítógépen lévő összes merevlemezen, cserélhető meghajtón és hálózati meghajtón. A Kaspersky Endpoint Security nem vizsgál összetett fájlokat.
Művelet fenyegetés észlelésekor	<p>Vírusmentesítés; törlés, 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 törli a fájlokat.</p> <p>Vírusmentesítés; blokkolás, 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 lehetséges, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.</p> <p>Értesítés. Ha ez a lehetőség van kiválasztva, a Kaspersky Endpoint Security hozzáadja a fertőzött fájlok információit az aktív fenyegetések listájához az ilyen fájlok észlelésekor.</p>
Fájltípusok	<div style="border: 1px solid #ccc; padding: 10px;"><p>A Kaspersky Endpoint Security a kiterjesztés nélküli fájlokat végrehajthatónak tekinti. A Kaspersky Endpoint Security a végrehajtható fájlokat mindig megvizsgálja, függetlenül a vizsgálatra kiválasztott fájlformátumoktól.</p></div> <p>Minden fájl. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül).</p>

	<p>Formátum alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejléceket a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres.</p> <p>Kiterjesztés alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.</p> <p>A Kaspersky Endpoint Security alapértelmezés szerint a formátumuk alapján vizsgálja a fájlokat. A fájl kiterjesztés szerinti vizsgálata kevésbé biztonságos, mert elképzelhető, hogy egy rosszindulatú fájl kiterjesztése nem szerepel a potenciálisan fertőzötték listáján (pl. .123).</p>
Csak az 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.
Vizsgált objektumok kihagyása, ha a vizsgálatuk hosszabb, mint N másodpercnél hosszabb idő szükséges	Korlátozza egyetlen objektum vizsgálatának időtartamát. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.
Archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb tömörített formátumok vizsgálata.
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.
E-mail formátumok vizsgálata	<p>Ez a jelölőnégyzet engedélyezi / letiltja a Kaspersky Endpoint Security azon lehetőségét, hogy e-mail formátumokban és e-mail adatbázisokban lévő fájlokat vizsgáljon.</p> <p>Az alkalmazás csak az MS Outlook, a Windows Mail/Microsoft Outlook Express és az EML levél fájlformátumokat vizsgálja teljes körűen, és csak akkor, ha a számítógép MS Outlook x86 levelezőprogrammal rendelkezik.</p> <p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security az e-mail formátumú fájlt egyetlen fájlként vizsgálja meg.</p>
Jelszóvédett archívumok vizsgálata	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security megvizsgálja a jelszóval védett archívumokat. Mielőtt az archívumokban lévő fájlokat vizsgálatára sor kerülhetne, a rendszer felkéri a jelszó megadására.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security kihagyja a jelszóval védett archívumok vizsgálatát.</p>
Ne	Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem vizsgálja az

<p>csomagoljon ki nagy összetett fájlokat</p>	<p>összetett fájlokat, ha méretük meghaladja a megadott értéket.</p> <p>Ha a négyzet nincs bejelölve, a Kaspersky Endpoint Security mindenfajta méretű összetett fájlt megvizsgál.</p> <p>A Kaspersky Endpoint Security megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.</p>
<p>Gépi tanulás és aláírás-elemzés</p>	<p>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.</p> <p>A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.</p>
<p>Heurisztikus elemzés</p>	<p>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.</p> <p>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 alaposága, az operációs rendszer erőforrásainak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.</p>
<p>iSwift Technológia</p>	<p>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.</p>
<p>iChecker Technológia</p>	<p>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).</p>

Alkalmazás integritásának 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 *Integritás-ellenőrzés* feladat az alkalmazásfájlok vizsgálatára való. Futtassa az *Integritás-ellenőrzés* feladatot, ha a Kaspersky Endpoint Security rosszindulatú objektumot észlelt, de nem hatástalanította azt.

Integritás-ellenőrzés 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 ismétlje 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. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 (11.8.0)** → **Integritás-ellenőrzés** lehetőséget.

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 kézzel, 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 **Feladat futtatása, ha a varázsló végzett** 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 ki a **Devices** → **Tasks** lehetőséget.

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

b. A **Task type** legördülő listából válassza ki az **Integrity check** lehetőséget.

c. A **Task name** mezőben adjon meg egy rövid leírást, például: *Check the integrity of the application after a computer infection.*

d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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

5. Lépjen ki a varázslóból.

Egy új feladat jelenik meg a feladatok listájában.

6. 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 **Integritás-ellenőrzés** feladatot, majd kattintson **Vizsgálat futtatása** 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 **Integritás-ellenőrzés** 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. By schedule. A vizsgálati feladatoknak ebben a futásmódjában a Kaspersky Endpoint Security a feladatot a létrehozott ütemtervnek megfelelően futtatja. A vizsgálati feladat ezen futásmódjának kiválasztása esetén a vizsgálati feladat elindítható kézzel is.
Kihagyott vizsgálatok	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott vizsgálati feladatot azonnal elindítja, amint lehetségessé válik. A vizsgálati feladat például akkor

futtatása	hagyható ki, ha a számítógép a frissítési feladat indítási időpontjában ki volt kapcsolva. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott vizsgálati feladatokat. Ehelyett a következő vizsgálati feladatot a jelenlegi ütemezésnek megfelelően futtatja.
Csak akkor fusson, ha a számítógép üresjáratban van	A vizsgálati feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárva 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.

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:

- **Saját e-mailek.**

Az Outlook levelezőprogramhoz tartozó fájlok: adatfájlok (PST), offline adatfájlok (OST).

- **Rendszermemória.**

- **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.**

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. 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 **Feladatok** lapot.
 4. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitására.
Ha szükséges, [hozzon létre egy vírusvizsgálati](#) feladatot.
 5. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.
 6. A **Vizsgálat hatóköre** részen kattintson a **Beállítások** elemre.
 7. A megnyílt ablakban válassza ki azokat az objektumokat, amelyeket hozzá kíván adni a vizsgálat hatóköréhez vagy ki szeretne zárni abból.
 8. Ha egy új objektumot szeretne hozzáadni a vizsgálat hatóköréhez:
 - a. Kattintson a **Add** 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a Mappa nevű mappában és az almappáiban található. 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 útját, aminek TXT-kiterjesztése van és három karakterből áll.
 9. Mentse el a módosításokat.
- Kizárhat egy objektumot a vizsgálatokból anélkül, hogy törölné azt a vizsgálati hatókörbe tartozó objektumok listájáról. Ehhez törölje az objektum melletti jelölőnégyzet jelölését.

[Vizsgálat hatókörének szerkesztése a Web Console-ban és a Cloud Console-ban](#) 

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

Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

Megnyílik a feladatok tulajdonságai ablak. Ha szükséges, [hozzon létre egy vírusvizsgálati](#) feladatot.

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

4. A **Vizsgálat hatóköre** 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 a **Add** gombra.

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 karakterhalmazzal helyettesíthet (az üres halmazzal 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a Mappa nevű mappában és az almappáiban található. 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.

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. A feladatlistában 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 megnyílt 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 házi rendben](#).

Ütemezett vizsgálat futtatása

A számítógép teljes vizsgálata némi időt és erőforrást igényel. Válassza ki az optimális időpontot a számítógép vizsgálatának futtatására, így elkerülheti más szoftverek teljesítményének csökkenését. A Kaspersky Endpoint Security lehetővé teszi a számítógép vizsgálatának normál ütemezés szerinti beállítását. Ez akkor kényelmes, ha a cége rendelkezik munkarenddel. Beállíthatja a számítógép vizsgálatát éjszakai vagy hétvégi futtatásra. Ha a vizsgálati 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.

Ha az optimális vizsgálati ütemezés konfigurálása nem lehetséges, a Kaspersky Endpoint Security lehetővé teszi a számítógép vizsgálatát az alábbi speciális feltételek teljesülésekor:

- Adatbázis-frissítés után.
A Kaspersky Endpoint Security frissített aláírási adatbázisokkal futtatja a számítógép vizsgálatát.
- Az alkalmazás elindulása után.
A Kaspersky Endpoint Security az alkalmazás indítása után meghatározott időtartam 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.
- Hálózati ébresztés.
A Kaspersky Endpoint Security ütemezetten futtatja a számítógép vizsgálatát, még akkor is, ha a számítógép ki van kapcsolva. Ehhez az alkalmazás az operációs rendszer Hálózati ébresztés funkcióját használja. A Hálózati ébresztés funkció lehetővé teszi a számítógép távoli bekapcsolását speciális jelet küldve annak a helyi hálózaton keresztül. A funkció használatához engedélyeznie kell a Hálózati ébresztés funkciót a BIOS beállításában.
A Hálózati ébresztés használatával történő vizsgálat futtatását csak a *Vírusvizsgálat* feladathoz konfigurálhatja a Kaspersky Security Centerben. Nem engedélyezheti a Hálózati ébresztés 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. Ez azt jelenti, hogy több napba is beletelhet, amíg az alkalmazás befejezi a számítógép teljes vizsgálatát.

[Vizsgálati ütemezés konfigurálása 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 **Feladatok** lapot.
4. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.
Ha szükséges, [hozzon létre egy vírusvizsgálati](#) feladatot.
5. Válassza ki a számítógép tulajdonságainak ablakában az **Ütemezés** részt.
6. Állítsa be a vizsgálati feladat ütemezését.
7. Adja meg a kiválasztott gyakoriság függvényében a feladatfutás ütemezését meghatározó speciális beállításokat (lásd az alábbi táblát).
8. Mentse el a módosításokat.

[A vizsgálat ütemezés konfigurálása a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a vizsgálati feladatra.
Megnyílik a feladatok tulajdonságai ablak.
3. Válassza ki az **Ütemezés** 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 *Vírusvizsgálat* 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 megnyitott ablakban konfigurálja a vizsgálati feladat futásának ütemezését.
5. Adja meg a kiválasztott gyakoriság függvényében a feladatfutas ütemezését meghatározó speciális beállításokat (lásd az alábbi táblát).
6. Mentse el a módosításokat.

Vizsgálati ütemezés beállításai

Paraméter	Leírás
Vizsgálat ütemezése	<p>Manually. A futásmód, amelyben manuálisan elindíthatja a vizsgálatot, amikor az Önnek kényelmes.</p> <p>By schedule. A vizsgálati feladatoknak ebben a futásmódjában a Kaspersky Endpoint Security a feladatot a létrehozott ütemtervnek megfelelően futtatja. A vizsgálati feladat ezen futásmódjának kiválasztása esetén a vizsgálati feladat elindítható kézzel is.</p>
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 vizsgálati feladatot azonnal elindítja, amint lehetségessé válik. A vizsgálati feladat például akkor hagyható ki, ha a számítógép a frissítési feladat indítási időpontjában ki volt kapcsolva. Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem futtatja a kihagyott vizsgálati feladatokat. Ehelyett a következő vizsgálati feladatot a jelenlegi ütemezésnek megfelelően futtatja.
Csak akkor fusson, ha a számítógép üresjáratban van	A vizsgálati feladat elhalasztott kezdése, ha a számítógép erőforrásai foglaltak. A Kaspersky Endpoint Security elindítja a vizsgálati feladatot, ha a számítógép zárva 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.
Use automatically randomized delay for task starts	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.

<p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a feladat pontosan az ütemezett időpontban fut.</p>
<p>Feladat leállítása, ha az N (perc) értéknél tovább fut</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>A megadott idő elteltével a feladat végrehajtási idejének korlátozásakor a Kaspersky Endpoint Security leállítja a feladatot. A feladat nincs befejeztként megjelölve. Amikor legközelebb a Kaspersky Endpoint Security futtatja a feladatot, az elejétől fog futni ütemezés szerint.</p> <p>A feladat végrehajtási idejének csökkentéséhez pl. konfigurálhatja a vizsgálat hatókörét vagy optimalizálhatja a vizsgálatot.</p>
<p>Activate the device before the task is started through Wake-on-LAN (min)</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>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.</p> <p>Jelölje be a jelölőnégyzetet, ha a feladatot minden számítógépen szeretné futtatni, beleértve a kikapcsolt számítógépeket is.</p>

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. A Kaspersky Endpoint Security beállításában 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 [Integrálás-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 **Feladatok** lapot.
4. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.
5. Válassza ki a feladat tulajdonságainak ablakában a **Fiók** 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 ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a vizsgálati feladatra.
Megnyílik a feladatok tulajdonságai ablak.
3. Válassza ki a **Beállítások** lapot.
4. A **Fiók** részen kattintson **Beállítások** elemre.
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 mint** 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

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 fájlalba, 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 fájl típusát, így felgyorsíthatja a vizsgálatot.

Bekapcsolhatja az iChecker és az iSwift technológiát is. Az iChecker és iSwift technológiák oly módon optimalizálják a fájl 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. 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 **Feladatok** lapot.
4. Válassza ki a vizsgálati feladatot, és kattintson duplán a feladat tulajdonságainak megnyitásához.
Ha szükséges, [hozzon létre egy vírusvizsgálati](#) feladatot.
5. Válassza ki a feladat tulajdonságainak ablakában a **Beállítások** részt.
6. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
Ezzel nyitható meg a vizsgálati feladat beállításainak ablaka.
7. A **Vizsgálatoptimalizáció** blokkban konfigurálja a vizsgálati beállításokat:
 - **Csak az 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.
Beállíthatja az új fájlok vizsgálatát is típus szerint. Például vizsgálhatja az összes terjesztőcsomagot, illetve csak az új archívumokat és az Office-formátumú fájlokat is.
 - **Azon fájlok kihagyása, amelyek vizsgálata tovább tart, mint N másodperc.** Ez időkorlátot határoz meg egyetlen objektum vizsgálatára. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.
8. Kattintson a **További** gombra.
Ez megnyitja az összetett fájlok vizsgálati beállításainak ablakát.
9. A **Méretkorlát** részben jelölje be a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet. Ez időkorlátot határoz meg egyetlen objektum vizsgálatára. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.

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.

10. Kattintson az **OK** gombra.
11. Válassza ki a **További** lapot.
12. 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).

13. Mentse el a módosításokat.

Vizsgálat optimalizálása a Web Console-ban és a Cloud Console-ban

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

Megnyílik a feladatok listája.

2. Kattintson a vizsgálati feladatra.

Megnyílik a feladatok tulajdonságai ablak. Ha szükséges, [hozzon létre egy vírusvizsgálati](#) feladatot.

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

4. A **Művelet fenyegetés észlelésekor** részben jelölje be a **Csak az új és módosult fájlok vizsgálata** 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. Jelölje be a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet. Ez időkorlátot határoz meg egyetlen objektum vizsgálatára. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.

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 **Speciális beállítások** részen jelölje be az **Azon fájlok kihagyása, amelyek vizsgálata tovább tart N másodpercnél** jelölőnégyzetet. Ez időkorlátot határoz meg egyetlen objektum vizsgálatára. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.

7. 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** gombra.
4. A **Vizsgálatoptimalizáció** blokkban konfigurálja a vizsgálati beállításokat:

- **Csak az 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.
Beállíthatja az új fájlok vizsgálatát is típus szerint. Például vizsgálhatja az összes terjesztőcsomagot, illetve csak az új archívumokat és az Office-formátumú fájlokat is.
- **Vizsgált objektumok kihagyása, ha a vizsgálatuk hosszabb, mint N másodpercnél** hosszabb idő szükséges. Ez időkorlátot határoz meg egyetlen objektum vizsgálatára. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.

5. A **Méretkorlát** részben jelölje be a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet. Ez időkorlátot határoz meg egyetlen objektum vizsgálatára. A megadott időtartam elteltével a Kaspersky Endpoint Security abbahagyja a fájl vizsgálatát. Ez csökkenti a vizsgálat idejét.

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.

A rendszeres frissítéshez működő licenc szükséges. Ha nincs aktuális licence, csak egyetlen alkalommal végezhet frissítést.

A Kaspersky Endpoint Security fő frissítésforrását a Kaspersky frissítéskiszolgálói jelentik.

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.

Az alkalmazásmodulok frissítéseivel együtt a helyi súgófájlok is frissülhetnek.

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.

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.

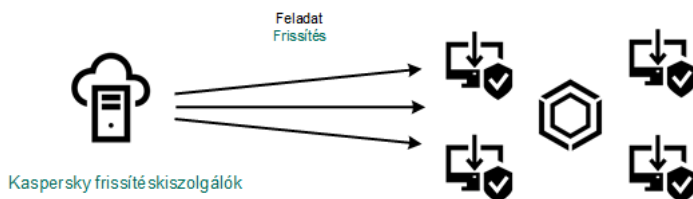
A következő objektumok frissülnek a felhasználói számítógépeken:

- 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 *Frissítések letöltése az Adminisztrációs kiszolgáló tárhelyére* nevű Adminisztrációs kiszolgáló feladat által.

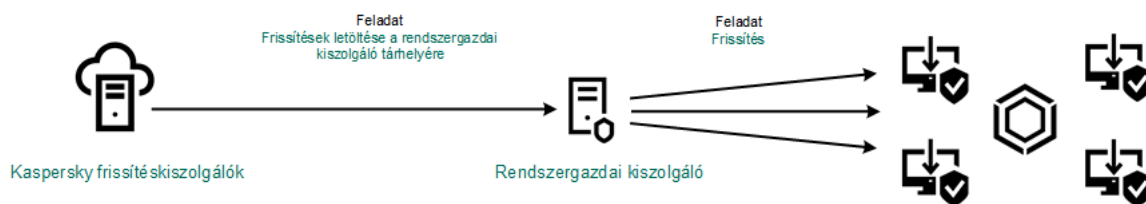
2. Töltse le a frissítési csomagot a megosztott mappába (opcionális).

A következő módszerekkel töltheti le a frissítési csomagot a megosztott mappába:

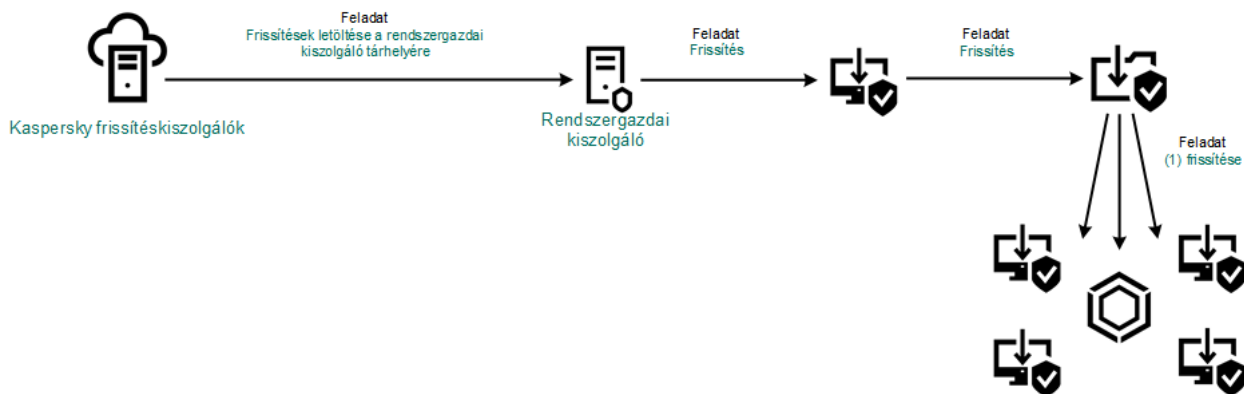
- A Kaspersky Endpoint Security *Frissítés* feladatának használata. A feladat a helyi vállalati hálózaton lévő egy számítógépre lett szánva.
- A Kaspersky Update Utility használata. A Kaspersky Update Utility használatával kapcsolatos további információkért lásd: [Kaspersky Tudásbázis](#).

3. A frissítési csomag megosztása az ügyfélszámítógépekkel.

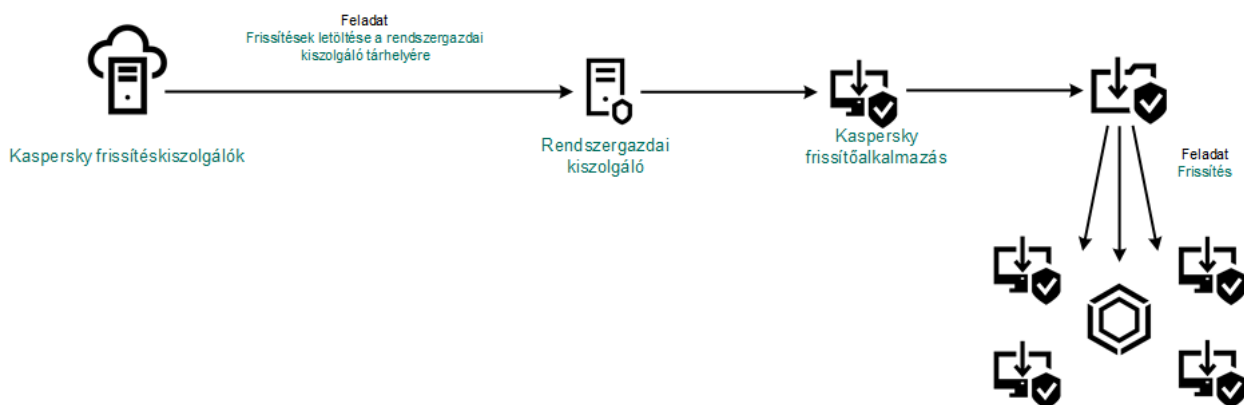
A frissítési csomagot a Kaspersky Endpoint Security *Frissítés* feladata megosztja az ügyfélszámítógépekkel. Korlátlan számú frissítési feladatot hozhat létre az adminisztrációs csoportokhoz.



Frissítés a kiszolgáló tárhelyéből



Megosztott mappából való frissítés



Frissítés a Kaspersky Update Utility használatával

A Web Console 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 Sútót](#). 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 beállításában](#).

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. Az Adminisztrációs kiszolgáló tárhelyén lévő frissítési csomag letöltési feladatának beállítása (*Frissítések letöltése az Adminisztrációs kiszolgáló tárhelyére*).
2. A megadott kiszolgáló tárhely adatbázisainak és alkalmazásmodul-frissítéseinek konfigurálása a helyi hálózat fennmaradó számítógépeire (*Frissítés feladat*).



A frissítési csomag kiszolgáló tárhelyére történő letöltésének a konfigurálásához:

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

Megnyílik a feladatok listája.

2. Válassza ki a **Download updates to the Administration Server repository** feladatot.

Megnyílik a feladatok tulajdonságai ablak.

A *Download updates to the Administration Server repository* feladatot automatikusan létrehozza a Kaspersky Security Center Web Console Kezdeti beállító varázslója, a feladatnak pedig csak egy példánya lehet.

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

4. Az **Other settings** részben kattintson a **Configure** lehetőségre.

5. A **Folder for storing updates** mezőben adja meg az FTP vagy HTTP kiszolgáló, a hálózati vagy helyi mappa címét, ahova a Kaspersky Security Center lemásolja a Kaspersky frissítéskiszolgálóitól kapott frissítési csomagot.

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://dn1-01.geo.kaspersky.com/` vagy `93.191.13.103`.

FTP-kiszolgáló esetén megadhatja a hitelesítési beállításokat a webcímben a következő formátumban:
`ftp://<felhasználó_neve>:<jelszó>@<csomópont>:<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\AVP11\Update distribution\`.

6. Mentse el a módosításokat.

A Kaspersky Endpoint Security frissítésének konfigurálásához a megadott kiszolgáló tárhelyből:

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

Megnyílik a feladatok listája.

2. Kattintson a **Update** feladatra a Kaspersky Endpoint Security-nél.

Megnyílik a feladatok tulajdonságai ablak.

A *Update* feladatot a Kaspersky Security Center Kezdeti beállító varázslója hozza létre automatikusan. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows webes bővítményt, miközben futtatja a Varázslót.

3. Válassza az **Application settings** → **Local mode** lehetőséget.

4. A frissítési források listájában kattintson a **Add** gombra.

5. A **Source** mezőben adja meg az FTP vagy HTTP kiszolgáló, a hálózati vagy helyi mappa címét, ahol a Kaspersky Security Center lemásolja a Kaspersky kiszolgálótól kapott frissítési csomagot.

A frissítésforrás címének meg kell egyeznie az **Folder for storing updates** mezőben megadott címmel, mikor konfigurálja a kiszolgáló tárhely frissítéseinek letöltését (lásd a fenti utasítást).

6. A **Status** részben válassza az **Enabled** lehetőséget.

7. Kattintson az **OK** gombra.

8. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

9. Mentse el a módosításokat.

Ha egy frissítést nem lehet végrehajtani az első frissítésforrásról a Kaspersky Endpoint Security automatikusan átvált a következő forrásra.

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 frissítéskiszolgálótól, majd a kapott frissítési csomagot egy megosztott mappába másolja. A szervezet helyi hálózatán lévő egyéb számítógépek fogadhatnak frissítési csomagot ebből a megosztott mappából.

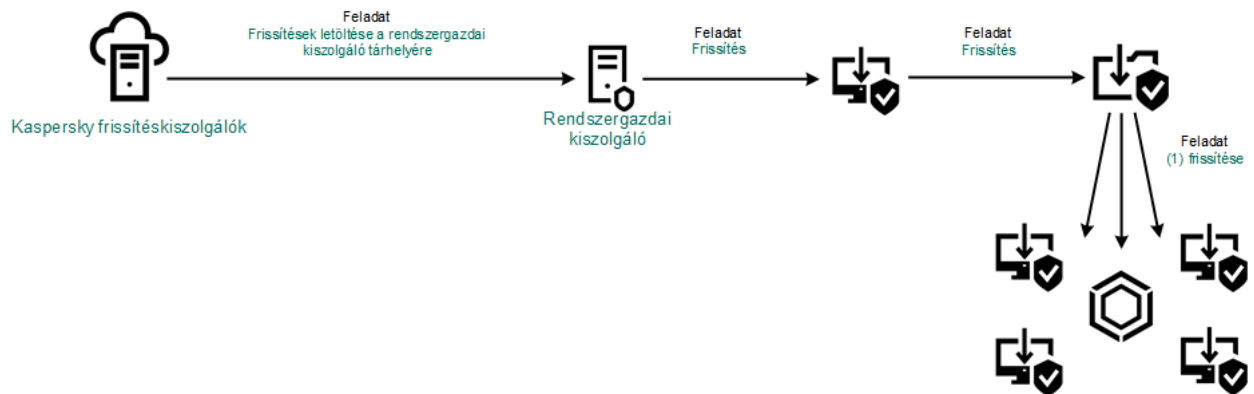
A megosztott mappák adatbázis és alkalmazásmodul-frissítéseinek konfigurálása két lépésből áll:

1. [Adatbázisok és alkalmazásmodul-frissítések konfigurálása a kiszolgáló tárhelyéből.](#)

2. A frissítési csomagok másolásának engedélyezése a vállalati helyi hálózat egyik számítógépén lévő megosztott mappába (lásd az alábbi utasításokat).

3. Az adatbázisok és alkalmazásmodulok frissítéseinek konfigurálása a megadott megosztott mappából a vállalat helyi hálózatának fennmaradó számítógépeire (lásd a lenti utasításokat).

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.



Megosztott mappából való frissítés

A frissítési csomag megosztott mappába történő másolásának engedélyezése:

1. A Web Console fő ablakában válassza ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a **Update** feladatra a Kaspersky Endpoint Security-nél.
Megnyílik a feladatok tulajdonságai ablak.
A *Update* feladatot a Kaspersky Security Center Kezdeti beállító varázslója hozza létre automatikusan. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows webes bővítményt, miközben futtatja a Varázslót.
3. Válassza az **Application settings** → **Local mode** lehetőséget.
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. Jelölje be a **Frissítések másolása mappába** jelölőnégyzetet.
6. Az **Elérési út** mezőben adja meg a megosztott mappa UNC-útvonalát (például \\Server\Share\Update distribution).
Ha a mező üres marad, a Kaspersky Endpoint Security a frissítési csomagot a C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\ mappába másolja.
7. Mentse el a módosításokat.

A *Frissítés* feladatot egy olyan számítógéphez kell hozzárendelni, ami a frissítések forrásaként működik.

Megosztott mappából való frissítések konfigurálásához:

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

b. A **Task type** legördülő listából válassza ki a **Update** lehetőséget.

c. A **Task name** mezőben adjon meg egy rövid leírást, például *Frissítés megosztott mappából*.

d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

A *Frissítés* 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. Menjen az **Alkalmazásbeállítások** részre.

8. Menjen a **Local mode** fülre.

9. A **Frissítésforrások** részen kattintson a **Hozzáadás** gombra.

10. A **Source** mezőbe írja be a megosztott mappa útvonalát.

A forráscímnek egyeznie kell azzal a címmel, amit korábban, az **Path** mezőben adott meg, amikor beállította a frissítési csomag másolását a megosztott mappába (lásd a *fenti utasításokat*).

11. Kattintson az **OK** gombra.

12. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.

13. Mentse el a módosításokat.

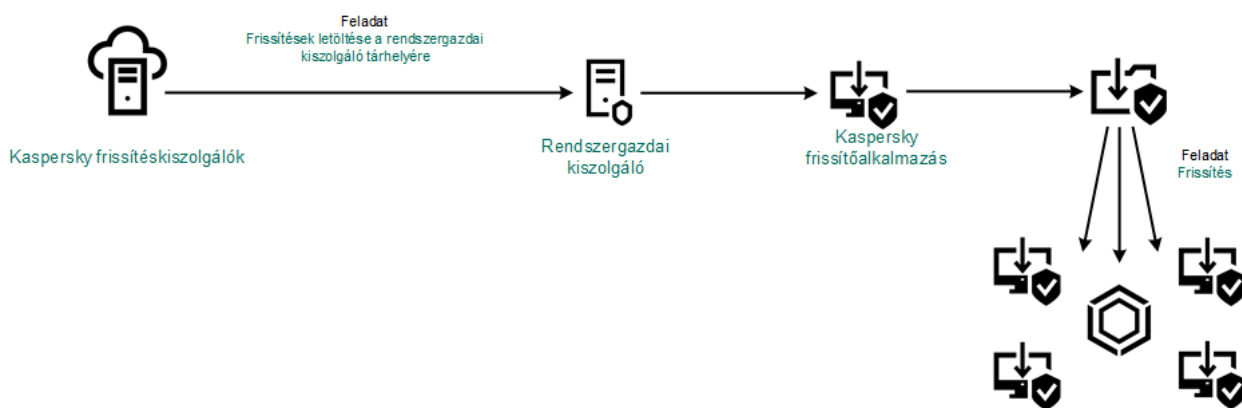
Frissítés a Kaspersky Update Utility használatával

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 frissítéskiszolgálótól, 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 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.
4. A megadott megosztott mappa adatbázisainak és alkalmazásmodul-frissítéseinek konfigurálása a helyi hálózat fennmaradó számítógépeire.

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.



Frissítés a Kaspersky Update Utility használatával

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](#).

Megosztott mappából való frissítések konfigurálásához:

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

Megnyílik a feladatok listája.

2. Kattintson a **Update** feladatra a Kaspersky Endpoint Security-nél.

Megnyílik a feladatok tulajdonságai ablak.

A *Update* feladatot a Kaspersky Security Center Kezdeti beállító varázslója hozza létre automatikusan. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows webes bővítményt, miközben futtatja a Varázslót.

3. Válassza az **Application settings** → **Local mode** lehetőséget.

4. A frissítési források listájában kattintson a **Add** gombra.
5. A **Forrás** mezőben adja meg a megosztott mappa UNC-útvonalát (például \\Server\Share\Update distribution).

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.
8. Mentse el a módosításokat.

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 tudnivalóért 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.

A mobil üzemmód frissítési beállításainak konfigurálásához:

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

Megnyílik a feladatok listája.

2. Kattintson a **Update** feladatra a Kaspersky Endpoint Security-nél.

Megnyílik a feladatok tulajdonságai ablak.

A *Update* feladatot a Kaspersky Security Center Kezdeti beállító varázslója hozza létre automatikusan. A *Update* feladat létrehozásához telepítse a Kaspersky Endpoint Security for Windows webes bővítményt, miközben futtatja a Varázslót.

Válassza az **Application settings** → **Mobile mode** lehetőséget.

3. A frissítések forrásainak beállítása. A frissítések forrásai lehetnek Kaspersky frissítéskiszolgálók, egyéb FTP és HTTP kiszolgálók, helyi mappák vagy hálózati mappák.

4. 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** elemre kattintva.


Frissítési feladat elindítása és leállítása az [egyszerűsített alkalmazásfelület](#) megjelenése közben:

1. Kattintson a jobb egérgombbal a tálcá 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. A Kaspersky Endpoint Security beállításáiban 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:


1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Ez megnyitja a feladatlistát; válassza ki a frissítési feladatot, majd kattintson rá .
3. Kattintson az **Adatbázis-frissítés futtatása mint** elemre.
4. Ez megnyit egy ablakot; ebben az ablakban válassza ki 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 **By schedule** 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:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Ez megnyitja a feladatlistát; válassza ki a frissítési feladatot, majd kattintson rá .
3. Kattintson az **Adatbázisok frissítési ütemezése** elemre.
4. A megnyitott 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.
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.

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.

Frissítésforrás hozzáadása:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Ez megnyitja a feladatlistát; válassza ki a frissítési feladatot, majd kattintson rá .
3. Kattintson a **Frissítésforrások kiválasztása** gombra.
4. A megnyitott ablakban kattintson a **Hozzáadás** 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://dn1-01.geo.kaspersky.com/` vagy `93.191.13.103`.
FTP-kiszolgáló esetén megadhatja a hitelesítési beállításokat a webcímben a következő formátumban:
`ftp://<felhasználó_neve>:<jelszó>@<csomópont>:<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\AVP11\Update distribution\`.

6. Kattintson a **Kiválasztás** gombra.
7. Adja meg a frissítési források prioritásait a **Up** és **Down** gombokkal.
8. Mentse el a módosításokat.


Megosztott mappából való frissítések beállítása

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 frissítéskiszolgálótól, majd a kapott frissítési csomagot egy megosztott mappába másolja. A szervezet helyi hálózatán lévő egyéb számítógépek fogadhatnak frissítési csomagot ebből a megosztott mappából.


A megosztott mappák adatbázis és alkalmazásmodul-frissítéseinek konfigurálása két lépésből áll:

1. A frissítési csomag másolásának engedélyezése a helyi hálózaton lévő egyik számítógép valamelyik megosztott mappájába.
2. A megadott megosztott mappa adatbázisainak és alkalmazásmodul-frissítéseinek konfigurálása a helyi hálózat fennmaradó számítógépeire.

A frissítési csomag megosztott mappába történő másolásának engedélyezése:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Ez megnyitja a feladatlistát; válassza ki a frissítési feladatot, majd kattintson rá .
3. A **Frissítések terjesztése** blokkban jelölje be a **Frissítések másolása mappába** jelölőnégyzetet.
4. Adja meg a megosztott mappa UNC-útvonalát (például, \\Server\Share\Update distribution).
5. Mentse el a módosításokat.




Megosztott mappából való frissítések konfigurálásához:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Ez megnyitja a feladatlistát; válassza ki a frissítési feladatot, majd kattintson rá .
3. Kattintson a **Frissítésforrások 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 a **Kiválasztás** 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 elérhetővé válik, az alkalmazás a Kaspersky Endpoint Security főablakában a következő értesítések egyikét jeleníti meg: fontos frissítés  vagy kritikus frissítés . 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 alkalmazás modulfrissítésének nyomon követésével és a frissítés Kaspersky Security Centerben való megerősítésével kapcsolatos részletekért lásd a [Kaspersky Security Center súgót](#) .

Az alkalmazásfrissítés telepítése után szükség lehet a számítógép újraindítására.

Az alkalmazásmodulok frissítéseinek beállítása:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Ez megnyitja a feladatlistát; válassza ki a frissítési feladatot, majd kattintson rá .

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 az **Configuring Internet access** szakaszt.
3. Jelölje be a **Use proxy server** jelölőnégyzetet.
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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Hálózati beállítások** elemhez.
5. A **Proxykiszolgáló beállításai** szakaszban válassza ki a **Proxykiszolgáló kihagyása helyi címek esetén** lehetőséget.

6. 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.
3. A **Proxykiszolgáló** blokkban kattintson a **Proxykiszolgáló beállításai** hivatkozásra.
4. A megnyitott ablakban a proxykiszolgáló címének meghatározása érdekében válassza ki az alábbi lehetőségek egyikét:
 - **Proxykiszolgáló beállításainak automatikus észlelése.**
Alapértelmezésben ez a lehetőség van kiválasztva. A Kaspersky Endpoint Security az operációs rendszer beállításában 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. Ha engedélyezni szeretné a hitelesítést a proxykiszolgálón, jelölje be a **Proxykiszolgáló-hitelesítés használata** jelölőnégyzetet, és adja meg a felhasználói fiók hitelesítő adatait.
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 funkció akkor hasznos például, ha az adatbázisok új verziója érvénytelen aláírást tartalmaz, ami miatt a Kaspersky Endpoint Security egy biztonságos alkalmazást blokkol.

A legutóbbi frissítés visszagörgetése:

1. Nyissa meg a fő alkalmazásablakban a **Frissítés** részt.
2. Az **Adatbázisok visszaállítása az előző verzióra** csempén kattintson a **Visszagörgetés** gombra.

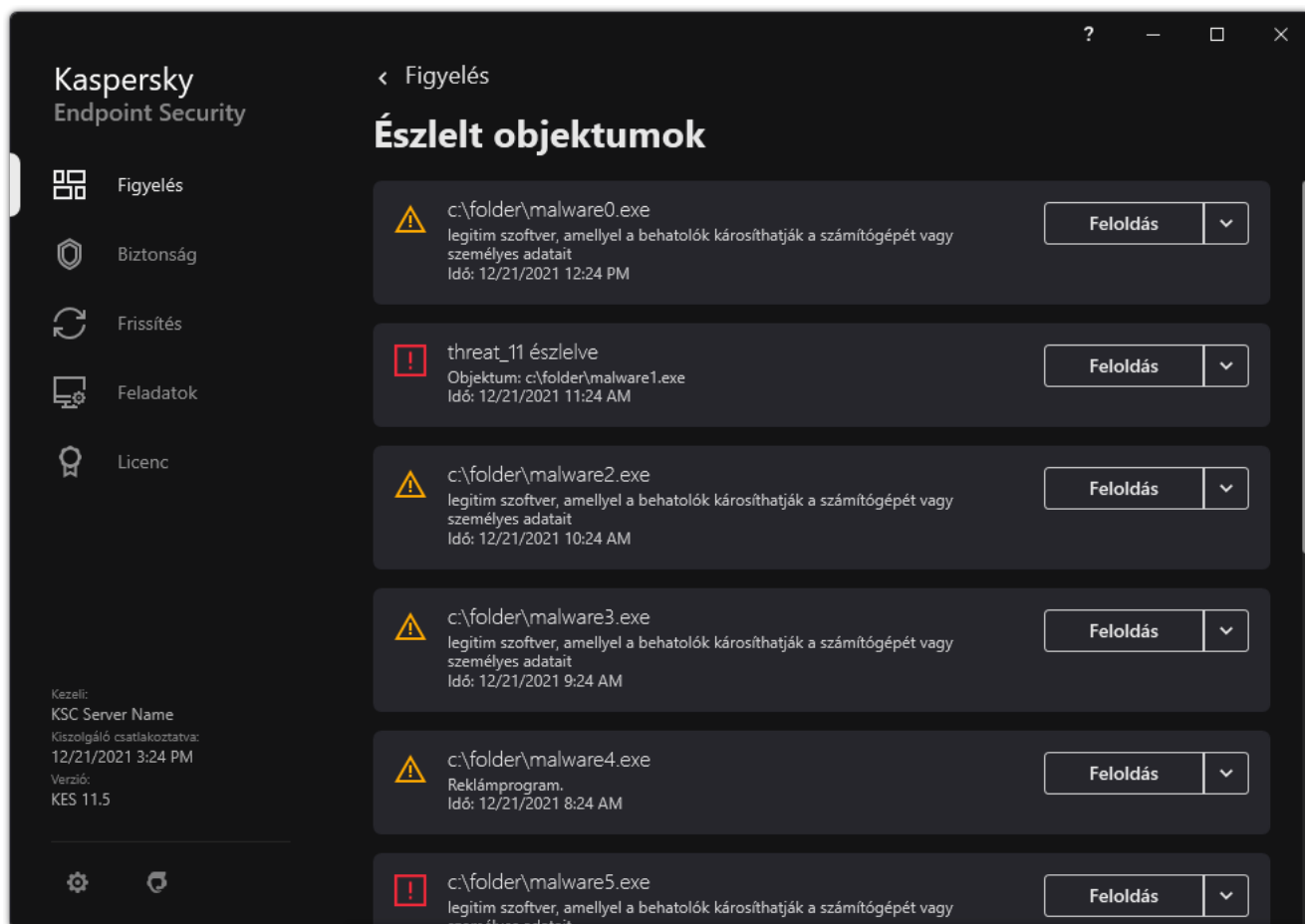
A Kaspersky Endpoint Security megkezdi az utolsó adatbázisfrissítés visszagörgetését. Az alkalmazás megjeleníti a visszagörgetés előrehaladását, a letöltött fájlok méretét és a frissítésforrást. A feladatot bármikor leállíthatja a **Frissítés leállítása** elemre kattintva.

Visszagörgetési 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 elindításához válasszon ki egy nem futó visszagörgetési feladatot.
 - A leállításához válasszon ki egy futó visszagörgetési feladatot.
 - A folytatásához vagy újraindításához válasszon ki egy szünetelő visszagörgetési feladatot.

Munkavégzés az aktív fenyegetésekkel

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 kezeléséhez a Kaspersky Endpoint Security a [Fejlett vírusmentesítő technológiát](#) használja. A Fejlett vírusmentesítés másként működik munkaállomásokon és kiszolgálókon. A fejlett vírusmentesítést a [Vírusvizsgálat feladat beállításában](#) és az [alkalmazásbeállításokban](#) konfigurálhatja.

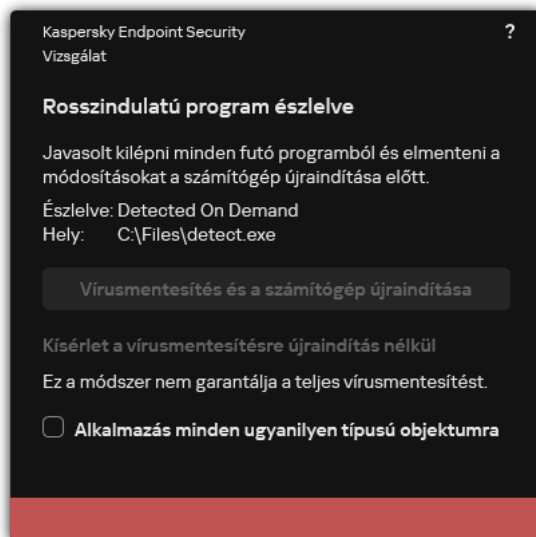


Az aktív fenyegetések listája

Aktív fenyegetések vírusmentesítése munkaállomásokon

Ha munkaállomásokon szeretne kezelni aktív fenyegetéseket, [engedélyezze a Fejlett vírusmentesítő technológiát](#) az alkalmazásbeállításokban. Ezután konfigurálja a felhasználói élményt a [Vírusvizsgálat](#) 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 *Vírusvizsgálat* 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 a felhasználó 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 *Vírusvizsgálat* feladat beállításában. Ezután el kell indítania a *Vírusvizsgálat* feladatot.

A Fejlett vírusmentesítő technológia be- és kikapcsolása

Ha a Kaspersky Endpoint Security nem tudja leállítani egy rosszindulatú program futtatását, használhatja a Fejlett vírusmentesítő technológiát. Alapértelmezés szerint a Fejlett vírusmentesítés ki van kapcsolva, mivel ez a technológia jelentős mértékű számítógép-erőforrást használ fel. Ezért csak akkor engedélyezheti a Fejlett vírusmentesítést, ha [aktív fenyegetéseket kezel](#).

A Fejlett vírusmentesítés másként működik munkaállomásokon és kiszolgálókon. A technológia kiszolgálókon történő használatához [engedélyeznie kell az azonnali fejlett vírusmentesítést](#) a *vírusvizsgálati* feladat tulajdonságaiban. Ez az előfeltétel nem szükséges a technológia munkaállomásokon történő használatához.


[A Fejlett vírusmentesítő technológia engedélyezése vagy letiltása az adminisztrációs konzolon \(MMC\) !\[\]\(73002692dd5e7a64e60946be3158e719_img.jpg\)](#)

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályablakban válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
6. Az **Operating mode** részen a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le a Fejlett vírusmentesítő technológiát.
7. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **General settings** → **Application settings** elemet.
5. Az **Operating mode** részen a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzettel engedélyezze vagy tiltsa le a Fejlett vírusmentesítő technológiát.
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.
3. A **Működési mód** részben 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 az aktív vírusmentesítés folyamatban van. A vírusmentesítés befejezésekor a számítógép újraindul.



Aktív fenyegetések feldolgozása

A fertőzött fájl *feldolgozott*nak 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 [Vírusvizsgálat](#) 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: *Kritikus* – .

[Fenyegetések feldolgozása a Felügyeleti konzolon](#)

1. A Felügyeleti konzolon nyissa meg az **Administration Server** → **Additional** → **Repositories** → **Active threats** lehetőséget.

Megnyílik az aktív fenyegetések listája.

2. Jelölje ki a feldolgozni kívánt objektumot.

3. Válassza ki, hogyan szeretné kezelni a fenyegetést:

- **Vírusmentesítés.** 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 törli a fájlokat.
- **Törlés.**

[Fenyegetések feldolgozása a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console főablakában 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:

- **Vírusmentesítés.** 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 törli a fájlokat.
- **Törlés.**

Fenyegetések feldolgozása az alkalmazás felületén

1. Az alkalmazás főablakának **Figyelés** részén kattintson **A védelem veszélyben van** csempre.

Megnyílik az aktív fenyegetések listája.

2. Jelölje ki a feldolgozni kívánt objektumot.

3. Válassza ki, hogyan szeretné kezelni a fenyegetést:

- **Feloldás.** 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 törli a fájlokat.
- **Hozzáadás a kizárásokhoz.** 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 Virus Encyclopedia weboldalát](#) .

Kaspersky
Endpoint Security

- Figyelés
- Biztonság
- Frissítés
- Feladatok
- Licenc

A biztonsága veszélyben van

→

- Biztonsági házirend által kezelt
- Vírusadatbázisok:
Verzió: 8/20/2021 2:16:08 PM

Jelentések

Biztonsági mentés

Fenyegetésész-
lelő
technológiák

Kaspersky Security Network
Olyan felhőalapú adatbázis, amely fájlok, webes erőforrások és szoftverek megbízhatóságáról tartalmaz információkat.

	<p>● Biztonságos objektumok a világban 4 672 183 300</p>
	<p>● Veszélyes objektumok a világban 1 644 992 581</p>
	<p>● Feldolgozás 2 287 436 398</p>

Kezeli:
KSC Server Name
Kiszolgáló csatlakoztatva:
8/20/2021 2:16 PM
Verzió:
KES 11.5

Alkalmazástevékeny-
ség-figyelő

Titkosítási figyelő

Hálózatfigyelő

Fő alkalmazásablak fenyegetés észlelésekor

Fájl védelem

A Fájl védelem összetevő lehetővé teszi a számítógép fájlrendszere fertőzéseinek megelőzését. Alapértelmezés szerint a „Fájl védelem” összetevő folyamatosan jelen van a számítógép memóriájában. Az összetevő vizsgálja a fájlokat a számítógép összes meghajtóján, valamint a csatlakoztatott meghajtókon. 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 megkísérel elérni egy olyan fájlt, amelynek tartalmát a OneDrive-felhő tárolja, 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 kézilleg is megadhatja a beállításokat. Ha módosítja a biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.

A Fájl védelem összetevő be- és kikapcsolása:

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 fájltypust 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. Az ajánlott biztonsági szint beállításainak értékeit az alábbi táblázat tartalmazza.

- **Alacsony.** E fájlbiztonsági szint beállításai biztosítják a maximális vizsgálati sebességet. A Fájl védelem összetevő a számítógép összes merevlemezen, 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 ablak felső részén található **Ajánlott biztonsági szint visszaállítása** gombra kattintva állíthatja vissza.

5. 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, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejléceket 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 alaposága, az operációs rendszer erőforrásainak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.
Csak az 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.
iSwift technológia	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.
iChecker technológia	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	Be	Megvizsgálja a Microsoft Office fájlokat (DOC, DOCX, XLS, PPT és egyéb Microsoft kiterjesztések). Az Office formátumú fájlok az OLE-


formátumú fájlok vizsgálata		objektumokat is magukban foglalják.
Vizsgálat módja	Intelligens mód	Ebben a módban a Fájlvédelem 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 közttes műveletek nem váltanak ki vizsgálatot.
Művelet fenyegetés észlelésekor	Vírusmentesítés; törlés, 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 törli a fájlokat.

A Fájlvédelem automatikus szüneteltetése

Beállíthatja, hogy a Fájlvédelem automatikusan szüneteltesse működését egy megadott időpontban, illetve adott alkalmazások kezelésekor.

A Fájlvédelem 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 Fájlvédelem összetevő beállításában, így az más alkalmazásokkal egy időben is futhat a számítógépen.


A Fájlvédelem automatikus szüneteltetésének beállítása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Fájlvédelem** opciót.
3. Kattintson a **Speciális beállítások** gombra.
4. A **Fájlvédelem szüneteltetése** blokkban kattintson a **Fájlvédelem szüneteltetése** hivatkozásra.
5. A megnyitott ablakban konfigurálja a beállításokat a Fájlvédelem szüneteltetéséhez:
 - a. Konfiguráljon ütemezést a Fájlvédelem automatikus szüneteltetéséhez.
 - b. Hozzon létre egy listát azokról az alkalmazásokról, amelyek működésének hatására a Fájlvédelem szünetelteti a tevékenységeit.
6. Mentse el a módosításokat.

A Fájlvédelem összetevő által fertőzött fájl észlelésekor elvégzett művelet módosítása

Alapértelmezett esetben a Fájlvédelem összetevő automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Fájlvédelem összetevő törli ezeket.


A Fájlvédelem 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** → **Fájlvédelem** 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 a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájl vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security törli a fájlokat.
 - **Vírusmentesítés; blokkolás, ha a vírusmentesítés nem sikerül.** Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájl vírusmentesíteni. Ha a vírusmentesítés nem lehetséges, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.
 - **Blokkolás.** Ennek a lehetőségnek a kiválasztása esetén a Fájlvédelem összetevő automatikusan blokkolja az összes észlelt fertőzött fájl, anélkül, hogy vírusmentesíteni próbálná őket.

Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájl, a Kaspersky Endpoint Security létrehozza a fájl egy biztonsági másolatát arra az esetre, ha [vissza kell állítani a fájl, vagy a jövőben az majd vírusmentesíthető lesz](#).

4. Mentse el a módosításokat.

A Fájlvédelem összetevő védelmi hatókörének kialakítása

A védelmi hatókör azon objektumok körére utal, amelyeket az összetevő vizsgál, ha engedélyezve van. A különböző összetevők védelmi hatókörének más-más tulajdonságai vannak. A vizsgálandó fájl helye és típusa a Fájlvédelem összetevő védelmi hatókörének tulajdonságai. Alapértelmezés szerint a Fájlvédelem összetevő csak a merevlemezekről, cserélhető meghajtókról és hálózati meghajtókról futtatott [potenciálisan megfertőzhető fájlokat](#)  vizsgálja.

A vizsgálandó fájl típusok 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 találhat. 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 fájl kiterjesztés alapján történő vizsgálatát választja, az alkalmazás kihagyja az ilyen fájl 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** gombra.
4. A **Fájl típusok** részben adja meg azokat a fájl típusokat, amelyeket a Fájl védelem összetevőnek meg kell vizsgálnia:
 - **Minden fájl.** Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájl megvizsgál (formátumtól és kiterjesztéstől függetlenül).
 - **Formátum alapján vizsgált fájlok.** Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security [csak a megfertőzhető fájlokat](#) vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejléceket a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájl kiterjesztésekkel rendelkező fájlokat is keres.
 - **Kiterjesztés alapján vizsgált fájlok.** Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security [csak a megfertőzhető fájlokat](#) vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.
5. Kattintson a **Védelem hatókörének szerkesztése** hivatkozásra.
6. A megnyílt 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 a **Add** gombra.

A mappafa nyílik meg.

- b. Válassza ki a védelem hatóköréhez hozzáadni kívánt objektumot.

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 erőforrásainak terhelése, valamint a vizsgálatához 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** gombra.
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** gombra.
4. A **Vizsgálati technológiák** blokkban jelölje be a jelölőnégyzeteket azon technológiák neve mellett, amelyeket a fájl védelemhez 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).
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** gombra.
4. A **Vizsgálatoptimalizáció** részben jelölje be a **Csak az új és módosult 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** gombra.
4. Adja meg az **Összetett fájlok vizsgálata** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, terjesztőcsomagok, illetve 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** gombra.
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.

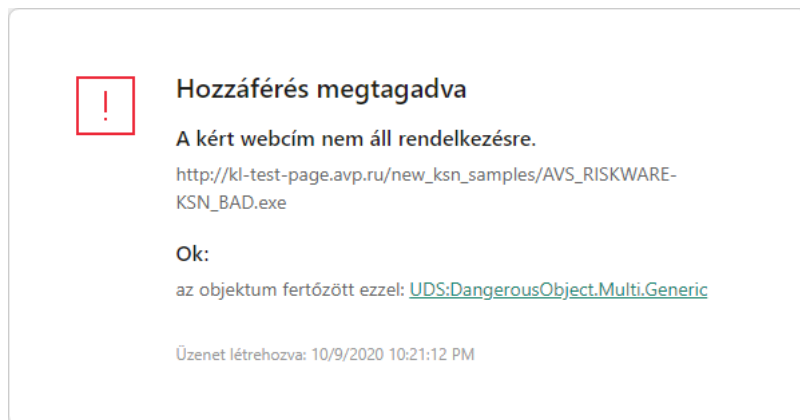
Web védelem

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. Ön [megadhat portokat, amelyeket a Kaspersky Endpoint Security megfigyel](#), vagy kiválaszthatja az összes portot.

A HTTPS forgalom megfigyeléséhez [engedélyeznie kell a titkosított kapcsolatok vizsgálatát](#).

Ha a felhasználó rosszindulatú vagy adathalász weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést és figyelmeztetést jelenít meg (lásd az alábbi ábrát).





A weboldal hozzáféréseinek megtagadásáról szóló üzenet

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 a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezeket az alkalmazásban mentett beállítás csoportokat *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 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 és FTP protokollon 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.** A Kaspersky Endpoint Security teljesítménye és a webes forgalom biztonsága közti optimális egyensúlyt nyújtó 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 közepes 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 ablak felső részén található **Ajánlott biztonsági szint visszaállítása** gombra kattintva állíthatja vissza.

5. 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 erőforrásainak terhelése, valamint a vizsgálatához szükséges idő közötti egyensúlyt.
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	Letöltés blokkolása	Ha ez a lehetőség be van jelölve, és a rendszer fertőzött objektumot észlel a webes adatforgalomban, a Web védelem blokkolja az objektumhoz

A webes forgalomban észlelt rosszindulatú objektumokon végrehajtandó művelet módosítása

Alapértelmezett esetben a Web védelem a fertőzött objektum webes forgalomban történő észlelésekor blokkolja az objektumhoz való hozzáférést, és értesítést jelenít meg a műveletről.

A webes forgalomban észlelt rosszindulatú objektumokon végrehajtandó művelet módosítása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** opciót.
3. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a webes forgalomban észlelt rosszindulatú objektumokon végez:
 - **Letöltés blokkolása.** 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.
 - **Értesítés.** 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.
4. Mentse el a módosításokat.

URL-címek vizsgálata adathalász és rosszindulatú webcímek adatbázisai ellen

A hivatkozások vizsgálata az adathalász webcímek listáján lehetővé teszi az *adathalász támadások* elkerülését. 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 ICQ-üzenetben 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.

Annak beállítása, hogy a Web védelem ellenőrizze a hivatkozásokat az adathalász és rosszindulatú webcímek adatbázisai alapján:

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** gombra.

4. Végezze el az alábbiakat:

- Ha azt szeretné, hogy a Web védelem a hivatkozásokat ellenőrizze a rosszindulatú webcímek adatbázisai alapján, akkor a **Vizsgálatmódok** részben jelölje be **A webcím ellenőrzése a rosszindulatú webcímek adatbázisában** jelölőnégyzetet. 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 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.

- 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.


A hivatkozásokat ellenőrizheti a [Kaspersky Security Network](#) megbízhatósági adatbázisai alapján is.

5. Mentse el a módosításokat.

Heurisztikus elemzés használata a Web védelem összetevő működése során

A védelem hatékonyságának fokozása érdekében használható a 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.

A heurisztikus elemzés beállítása:

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** gombra.
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 vizsgálatokor. Ezután állítsa be a csúszkával a heurisztikus elemzés szintjét: **Egyszerű vizsgálat**, **Közepes vizsgálat** vagy **Alapos vizsgálat**.
5. Az **Adathalászat elleni védelem** blokkban jelölje be a **Heurisztikus elemzés használata** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás heurisztikus elemzést használjon a weboldalak adathalászati hivatkozásokra való vizsgálatokor.


6. Mentse el a módosításokat.

Megbízható webcímek listájának létrehozása

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 megbízható webcímek listájának létrehozásához:

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** gombra.
4. Jelölje be a **Ne vizsgálja a megbízható URL-ekről érkező webes forgalmat** jelölőnégyzetet.
Ha a jelölőnégyzet 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.
6. Mentse el a módosításokat.

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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Web védelem** lehetőséget.
6. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
7. A megnyitott ablakban válassza ki a **Megbízható webcímek** lapot.
8. 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.
9. 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.
10. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Fenyegetések elleni alapvető védelem** → **Web védelem** szakaszt.
5. A kizárások listájának exportálása a **Megbízható webcímek** blokkban:
 - a. Jelölje ki az exportálni kívánt megbízható webcímeket.
 - 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.
6. A kizárások listájának importálása a **Megbízható webcímek** szakaszban:
 - 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.
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
- Microsoft Outlook Express
- Windows Mail

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 támogatja az Outlook 2010, 2013, 2016 és 2019 alkalmazásokkal történő műveleteket.


A „Levelezés védelem” összetevő nem vizsgálja az üzeneteket, ha a levelezési ügyfélprogram böngészőben van megnyitva.

Ha egy mellékletben rosszindulatú fájlt észlel, a Kaspersky Endpoint Security módosítja az üzenet tárgyát a következő módon: [Az üzenet figyelmet kíván a feldolgozás során] <üzenet tárgya> vagy [Üzenet fel lett dolgozva] <üzenet tárgya>.

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 a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezeket az alkalmazásban mentett beállítás csoportokat *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 Levelezés védelem összetevő be- és kikapcsolása:

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**. A Kaspersky Endpoint Security teljesítménye és az e-mail-biztonság közti optimális egyensúlyt nyújtó 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 ablak felső részén található **Ajánlott biztonsági szint visszaállítása** gombra kattintva állíthatja vissza.

5. Mentse el a módosításokat.

A Levelezés védelem Kaspersky szakértői által ajánlott beállításai (ajánlott biztonsági szint)


Paraméter	Érték	Leírás
Védelem hatóköre	Bejövő és kimenő üzenetek	<p>A <i>védelem hatóköre</i> magában foglalja azokat az objektumokat, amelyeket az összetevő a futtatáskor ellenőriz: bejövő és kimenő üzenetek vagy csak bejövő üzenetek.</p> <p>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.</p>
Microsoft Outlook-bővítmény csatlakoztatása	Be	<p>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.</p> <p>Ha az e-mailek vizsgálata a Microsoft Outlook bővítményével történik, akkor javasoljuk a Gyorsítótárazott Exchange-mód használatát. A gyorsítótáras Exchange móddal kapcsolatban további információ, valamint a használatára vonatkozó ajánlások a Microsoft Tudásbázisban található.</p>
Csatolt archívumok vizsgálata	Be	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb tömörített formátumok vizsgálata.
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.
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 megnyitáshoz 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 alaposságát, az operációs rendszer erőforrásainak terhelését, 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, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security törli a fertőzött objektumot. A Kaspersky Endpoint Security a végrehajtott művelettel kapcsolatosan információt fűz hozzá az üzenet tárgysorához: [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, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security törli a fertőzött objektumot. A Kaspersky Endpoint Security a végrehajtott művelettel kapcsolatosan információt fűz hozzá az üzenet tárgysorához: [Üzenet fel lett dolgozva] <üzenet tárgysora>.
 - **Vírusmentesítés; blokkolás, ha a vírusmentesítés nem sikerül.** Ha fertőzött objektumot észlel valamely bejövő üzenetben, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security figyelmeztetést fűz hozzá az üzenet tárgyához: [Az üzenet figyelmet kíván a feldolgozás során] <az üzenet tárgya>. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.
 - **Blokkolás.** Ha fertőzött objektumot észlel valamely bejövő üzenetben, a Kaspersky Endpoint Security figyelmeztetést fűz hozzá az üzenet tárgysorához: [Az üzenet figyelmet kíván a feldolgozás során] <üzenet tárgya>. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött


objektumot észlel valamely kimenő üzenetben, a Kaspersky Endpoint Security 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** gombra.
4. A **Vizsgálat 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 találhatóak, 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** gombra.
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.
 - **Csatolt archívumok vizsgálata.** ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb tömörített formátumok vizsgálata.

Ha a vizsgálat során a Kaspersky Endpoint Security egy archívum jelszavát észleli az üzenet szövegében, ezt a jelszót használja fel, hogy az archívumban rosszindulatú alkalmazásokat keressen. A jelszó nincs elmentve. Az archívum ki lesz csomagolva a vizsgálat előtt. 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.

- **Hagyja ki az archívumot, ha annak mérete több 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 erre az időtartamra.** 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 funkció nem érvényes a kimenő e-mailekre.

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** gombra.
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 fájl típusokkal 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.

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályablakban válassza az **Fenyegetések elleni alapvető védelem** → **Levelezés védelem** lehetőséget.
6. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
7. A megnyitott ablakban válassza ki a **Mellékletszűrő** fület.
8. A kiterjesztések listájának exportálása:
 - a. Jelölje ki az exportálni kívánt kiterjesztéseket. Több pont 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.
9. 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.
10. Mentse el a módosításokat.

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Fenyegetések elleni alapvető védelem** → **Levelezés védelem** szakaszt.
5. A kiterjesztések listájának exportálása a **Mellékletszűrő** blokkban:
 - a. Jelölje ki az exportálni kívánt kiterjesztéseket.
 - 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.
6. A kiterjesztések listájának importálása a **Mellékletszűrő** szakaszban:
 - 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.
7. 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). Ennek segítségével a Microsoft Office Outlookból megnyithatja a Levelezés védelem összetevő beállításait, és megadhatja, hogy keressen-e az e-mail üzenetekben vírusokat és más fenyegetéseket. Az Outlook Levelezés védelem kiterjesztése a POP3, SMTP, NNTP, IMAP és MAPI protokollok segítségével küldött és fogadott bejövő és kimenő üzeneteket képes vizsgálni. A Kaspersky Endpoint Security támogatja más e-mail ügyfélprogramok (köztük a Microsoft Outlook Express®, a Windows Mail és a Mozilla™ Thunderbird™) használatát is.


A Levelezés védelem bővítmény támogatja az Outlook 2010, 2013, 2016 és 2019 alkalmazásokkal történő műveleteket.

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.

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.

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](#)  található.

Az Outlook Levelezés védelem kiterjesztés üzem módjának beállítása a Kaspersky Security Center segítségével:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabályablakban válassza az **Fenyegetések elleni alapvető védelem** → **Levelezés védelem** lehetőséget.
6. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
7. A **Kapcsolat** részben kattintson a **Beállítások** gombra.
8. Az **E-mail védelem** ablakban:
 - 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.
9. Mentse el a módosításokat.


Hálózati védelem

A „Hálózati védelem” összetevő a hálózati támadásokra jellemző bejövő hálózati forgalmat vizsgálja. Ha a Kaspersky Endpoint Security hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában. A Kaspersky Endpoint Security adatbázisai 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 Hálózati védelem szükség esetén kikapcsolható.


A Hálózati védelem engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Hálózati védelem** opciót.
3. A **Hálózati védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ennek eredményeképpen, ha a Hálózati védelem engedélyezve van, a Kaspersky Endpoint Security vizsgálja a bejövő hálózati forgalmat a hálózati támadásokra jellemző tevékenységek után. Ha a Kaspersky Endpoint Security hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában.

Támadó számítógép blokkolása

Támadó számítógép blokkolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Hálózati védelem** opciót.
3. Jelölje be **A támadó számítógép hozzáadása a blokkolt számítógépek listájához N percig** jelölőnégyzetet.

Ha a jelölőnégyzet be van jelölve, 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 32 768 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.

1. Állítson be egy másik blokkolási időtartamot a támadó számítógép számára az **Adjon hozzá egy támadó számítógépet a blokkolt számítógépek listájához N percig** jelölőnégyzettől jobbra lévő mezőben.


2. 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 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.

A blokkolásból kizárt címek beállítása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Hálózati védelem** opciót.
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.
6. Mentse el a módosításokat.

Ennek eredményeképpen a Kaspersky Endpoint Security nem követi nyomon a kizárások listáján szereplő eszközök tevékenységét.

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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Hálózati védelem** lehetőséget.
6. A **Hálózati védelem beállításai** blokkban kattintson a **Kizárások** gombra.
7. A szabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt kizárásokat. Több pont kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.
 - b. Kattintson az **Exportálás** hivatkozásra.
 - 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.
8. A kizárások listájának importálása:
 - a. Kattintson az **Importálás** 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.
9. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Fenyegetések elleni alapvető védelem** → **Hálózati védelem** szakaszt.
5. A **Hálózati védelem beállításai** blokkban kattintson a **Kizárások** hivatkozásra.
Megnyílik a kizárások listája.
6. A szabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt kizárásokat.
 - b. Kattintson az **Export** gombra.
 - c. Erősítse meg, hogy csak a kijelölt kizárásokat, vagy a kizárások teljes listáját szeretné exportálni.
 - d. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.
 - e. Mentse a fájlt.
A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba.
7. A kizárások listájának importálása:
 - a. Kattintson az **Importálás** 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.
8. Mentse el a módosításokat.

Hálózati támadások elleni védelem beállítása 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.

A hálózati támadások elleni védelem konfigurálása típus szerint:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Hálózati védelem** opciót.
3. Használja **A portkeresés és hálózati elárasztás támadásként történő kezelése** kapcsolót az ilyen támadások észlelésének engedélyezéséhez vagy letiltásához.
4. Használja a **MAC-cím hamisítása elleni védelem** kapcsolót.
5. A **MAC-cím hamisításával történő támadás észlelésekor** blokkban válassza ki a következők egyikét:
 - **Csak értesítés.**
 - **Értesítés és blokkolás.**
6. Mentse el a módosításokat.

Firewall

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 [Behatólásmegelőző 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 Behatólásmegelőző rendszer összetevő számára helyezi megbízhatósági csoportba. Nem lehet módosítani a megbízhatósági csoportot kizárólag a Tűzfal vagy a Behatólásmegelőző rendszer esetében.

Ha nem vesz részt a KSN rendszerében vagy nincs hálózat, a Kaspersky Endpoint Security a [Behatólásmegelőző 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 végigvizsgálja, 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 a következő módon működnek: az alkalmazásokhoz tartozó hálózati szabály a hálózati állapot alapján foglalja magában a hozzáférési szabályokat: *nyilvános*, *helyi* vagy *megbízható*. 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 kapcsolatok állapota

A Tűzfal lehetővé teszi Önnek a hálózat tevékenység felügyeletét a hálózati kapcsolat állapotától függően. A Kaspersky Endpoint Security a számítógép operációs rendszerétől kapja meg a hálózati kapcsolat állapotát. Az operációs rendszerben a hálózati kapcsolat állapotát a felhasználó szabhatja meg a kapcsolat létrehozásakor. Lehetősége van [megváltoztatni a hálózati kapcsolat állapotát a Kaspersky Endpoint Security beállításai között](#). A Tűzfal a hálózati tevékenység nyomon követését a Kaspersky Endpoint Security beállításai alapján végzi, nem az operációs rendszer beállításai szerint.

A hálózati kapcsolat az alábbi állapottípusok egyikével rendelkezhet:

- **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* állapotot oszt ki. Az internet állapota 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 be- és kikapcsolása*:

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 a hálózati támadásokra jellemző bejövő hálózati forgalmat vizsgálja.

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 állapotának módosítása

A Tűzfal alapértelmezés szerint az internetnek *Nyilvános hálózat* állapotot oszt ki. Az internet állapota nem módosítható.

A hálózati kapcsolat státuszának módosítása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** opciót.
3. Kattintson a **Elérhető hálózatok** gombra.
4. Válassza ki azt a hálózati kapcsolatot, amelynek módosítani szeretné az állapotát.
5. A **Hálózat típusa** oszlopban válassza ki a hálózati kapcsolat állapotát:
 - **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

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 csomagszabályok létrehozásakor ne feledje, hogy azok az alkalmazások hálózati szabályai felett állnak.

1. Az alkalmazás főablakában a **Figyelés** részen kattintson a **Hálózatfigyelő** csempére.
2. Válassza ki a **Hálózati tevékenység** fület.
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. Kattintson a **Add** gombra.
Ezután megjelennek a hálózati szabály tulajdonságai.
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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** lehetőséget.
6. A **A Tűzfal beállításai** részen kattintson a **Beállítások** gombra.
Ez megnyitja a hálózati csomagszabályok és az alkalmazás hálózati szabályainak listáját.
7. Válassza ki a **Hálózati csomagszabályok** fület.
Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
8. Kattintson a **Add** gombra.
Ez megnyitja a csomagszabályok tulajdonságait.
9. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.
10. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).
Kiválaszthat egy előre meghatározott szabálysablonot a  gombra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.
A hálózati szabály összes beállítása automatikusan kitöltődik.
11. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a [jelentésben](#), jelölje be az **Események naplózása** jelölőnégyzetet.
12. Mentse az új hálózati szabályt.
13. Állítsa be a **Fel / Le** gombokkal a hálózati szabály prioritását.
14. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza a **Essential Threat Protection** → **Firewall** lehetőséget.
5. A **Firewall settings** részen kattintson a **Network packet rules** hivatkozásra.
Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
6. Kattintson a **Add** gombra.
Ez megnyitja a csomagszabályok tulajdonságait.
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 **Select 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 **Események naplózása** jelölőnégyzetet.
10. Mentse a hálózati szabályt.
Az új hálózati szabály felkerül a listára.
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. A **Státusz** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le a csomagszabályt.


Hálózati csomagszabály beállításai

Paraméter	Leírás
Művelet	<p>Engedélyezés.</p> <p>Blokkolás.</p> <p>Alkalmazásshabályok szerint. Ha ezt az opciót választja, a Tűzfal az alkalmazás hálózati szabályait alkalmazza a hálózati kapcsolatra.</p>
Protokoll	<p>Hálózati tevékenység felügyelete a kiválasztott protokollon: TCP, UDP, ICMP, ICMPv6, IGMP és GRE.</p> <p>Ha az ICMP vagy ICMPv6 protokollt választotta, meghatározhatja az ICMP csomag típusát és a kódját.</p> <p>Ha a TCP vagy UDP protokolltípust választotta, akkor megadhatja azon helyi és a távoli számítógépek portszámait vesszővel elválasztva, amelyek között a kapcsolatot figyeli a rendszer.</p>

<p>Irány</p>	<p>Bejövő (csomag). A Tűzfal az összes bejövő hálózati csomagra alkalmazza a hálózati szabályt.</p> <p>Bejövő. A Tűzfal a távoli számítógép által kezdeményezett kapcsolaton keresztül küldött összes hálózati csomagra alkalmazza a hálózati szabályt.</p> <p>Bejövő / kimenő. A Tűzfal a bejövő és kimenő hálózati csomagokra egyaránt alkalmazza a hálózati szabályt, függetlenül attól, hogy a hálózati kapcsolatot a felhasználó számítógépe vagy egy távoli számítógép kezdeményezte-e.</p> <p>Kimenő (csomag). A Tűzfal az összes kimenő hálózati csomagra alkalmazza a hálózati szabályt.</p> <p>Kimenő. A Tűzfal a felhasználó számítógépe által kezdeményezett kapcsolaton keresztül küldött összes hálózati csomagra alkalmazza a hálózati szabályt.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>A TCP protokoll hoz létre kapcsolatot. A TCP esetében használja a Bejövő, Kimenő és Bejövő / kimenő irányokat. Az összes többi protokoll nem hoz létre kapcsolatot, de küld csomagokat. Az összes többi protokoll esetében használja a Bejövő (csomag), Kimenő (csomag) és Bejövő/kimenő irányokat.</p> </div>
<p>Hálózati adapterek</p>	<p>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.</p>
<p>Élettartam (TTL)</p>	<p>Korlátozza a hálózati csomagok felügyeletét az élettartamuk (TTL) alapján.</p>
<p>Távoli cím</p>	<p>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-címelistát, 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.</p>
<p>Helyi cím</p>	<p>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-címelistát, vagy meghatározhat egy IP-címtartományt. 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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Néha a helyi címet alkalmazásoknál nem lehet beszerezni. Ebben az esetben ez a paraméter figyelmen kívül marad.</p> </div>

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 kézzel 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 beállításában 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** lehetőséget.
6. A **A Tűzfal beállításai** részen kattintson a **Beállítások** gombra.
Ez megnyitja a hálózati csomagszabályok és az alkalmazás hálózati szabályainak listáját.
7. Válassza ki a **Hálózati csomagszabályok** fület.
8. Hálózati csomagszabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt szabályokat. Több pont 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.
9. 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.
10. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza a **Essential Threat Protection** → **Firewall** lehetőséget.
5. Kattintson a **Network packet rules** hivatkozásra.
6. Hálózati csomagszabályok listájának 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. 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.

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. Válassza ki 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 **Alkalmazáshálózati 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 a **Add** 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 a **Szabályok az alkalmazásokhoz** 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 a **Add** 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 szabálysablon 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni alapvető védelem** → **Tűzfal** lehetőséget.
6. A **A Tűzfal beállításai** részen kattintson a **Beállítások** gombra.
Ez megnyitja a hálózati csomagszabályok és az alkalmazás hálózati szabályainak listáját.
7. Válassza ki az **Alkalmazás hálózati szabályai** lapot.
8. Kattintson a **Add** gombra.
9. A megnyílt 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.
10. Kattintson a **Frissítés** gombra.
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.
11. Válassza ki a szükséges alkalmazást.
12. 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.
13. Válassza ki a megfelelő alkalmazást, majd válassza az **Alkalmazásjogok** lehetőséget az alkalmazás helyi menüjében.
Az alkalmazásszabályok és tulajdonságok ablak nyílik meg.
14. Válassza ki a **Hálózati szabályok** lapot.
Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
15. Kattintson a **Add** gombra.
Ezután megjelennek a hálózati szabály tulajdonságai.
16. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.
17. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).
Kiválaszthat egy előre meghatározott szabálysablonot a  gombra kattintva. A szabálysablonok a leggyakrabban használt hálózati kapcsolatokat írják le.
A hálózati szabály összes beállítása automatikusan kitöltődik.

18. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a [jelentésben](#), jelölje be az **Események naplózása** jelölőnégyzetet.
19. Mentse az új hálózati szabályt.
20. Állítsa be a **Fel / Le** gombokkal a hálózati szabály prioritását.
21. Mentse el a módosításokat.

[Alkalmazás hálózati szabályának létrehozása a Web Console-ban és a Cloud Console-ban](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza a **Essential Threat Protection** → **Firewall** lehetőséget.
5. A **A Tűzfal beállításai** részen kattintson az **Alkalmazás hálózati szabályai** hivatkozásra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
6. Válassza ki az **Application rights** fület.
Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.
7. 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. Nyomja meg a **Next** gombot.
Ha több alkalmazáshoz szeretne létrehozni hálózati szabályt, válassza ki a **Csoport** 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. Az **OK** gombra kattintva zárhatja be a varázslót.
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 **Hálózati szabályok** elemet a legördülő listából.
Ez megnyitja a Tűzfal által beállított alapértelmezett hálózati szabályok listáját.
14. Kattintson a **Add** gombra.
Ez megnyitja az alkalmazásszabályok tulajdonságait.
15. Adja meg manuálisan a hálózati szolgáltatás nevét a **Név** mezőben.
16. Konfigurálja a hálózati szabály beállításait (lásd az alábbi táblát).
Kiválaszthat egy előre meghatározott szabálysablont a **Select 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 **Események naplózása** jelölőnégyzetet.
18. Mentse a hálózati szabályt.

Az új hálózati szabály felkerül a listára.

19. Állítsa be a **Fel / Le** gombokkal 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 UDP protokolltípust választotta, akkor megadhatja azon helyi és a távoli számítógépek portszámait vesszővel elválasztva, amelyek között a kapcsolatot figyeli a rendszer.
Irány	Bejövő. Bejövő / kimenő. Kimenő.
Távoli cím	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.
Helyi cím	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. 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. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">Néha a helyi címet alkalmazásoknál nem lehet beszerezni. Ebben az esetben ez a paraméter figyelmen kívül marad.</div>

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 a **Szabályok az alkalmazásokhoz** 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 a **Szabályok az alkalmazásokhoz** 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 kézilleg 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 a **Szabályok az alkalmazásokhoz** 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 beállításaiiban jelzett címhez és porthoz.

A kézzel 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 a **Szabályok az alkalmazásokhoz** 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.

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.

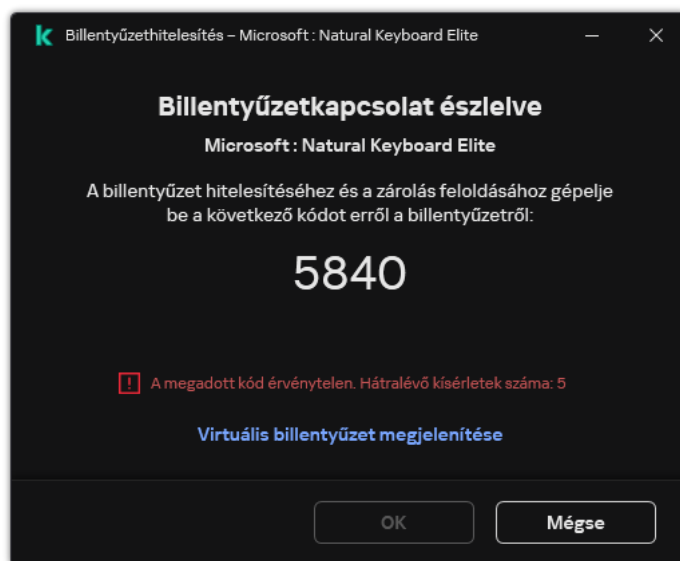
A kód megfelelő beírása esetén az alkalmazás menti az azonosító paramétereket – a billentyűzet VID/PID azonosítóját és a csatlakoztatás portszámát – a hitelesített billentyűzetek listájára. A billentyűzethitelesítést a billentyűzet ismételt csatlakoztatásakor és az operációs rendszer újraindításakor nem kell újra elvégezni.

Ha a hitelesített billentyűzetet a számítógép egy másik USB portjához csatlakoztatja, az alkalmazás ismét megjeleníti a billentyűzet 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 alkalmazás-összetevőket](#) 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 be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.


2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni alapvető védelem** → **BadUSB védelem** lehetőséget.
3. A **BadUSB védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Az **USB-billentyűzethitelesítés csatlakozáskor** részen módosítsa a biztonsági beállításokat hitelesítési kód megadása esetén:
 - **Az USB-készülék-hitelesítési 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. Például, ha 5 kísérletet engedélyez a hitelesítési kód megadására, az USB-eszköz blokkolva lesz az ötödik sikertelen kísérlet után. A Kaspersky Endpoint Security megjeleníti az USB-eszköz blokkolásának időtartamát. Ezen időtartam letelte után 5 alkalommal kísérrelheti meg beírni a hitelesítési kódot.
 - **Időkorlát a kísérletek maximális számának elérésekor.** Az USB-eszköz blokkolásának időtartama a hitelesítési kód megadott számú sikertelen kísérlet utáni beírásakor. 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 megtörténteig 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 (pl. a vonalkódolvasók). Ismeretlen USB eszközök hitelesítéséhez nem javasoljuk a képernyőn megjelenő billentyűzet használatát.

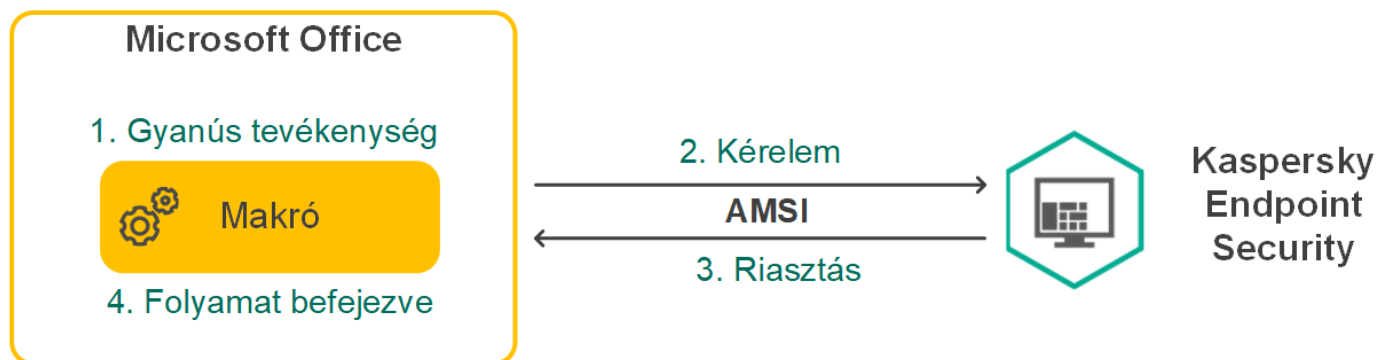
Képernyőn megjelenő billentyűzet hitelesítéshez történő használatának engedélyezése és tiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni alapvető védelem** → **BadUSB védelem** lehetőséget.
3. **Virtuális billentyűzet használatának tiltása az USB-eszközök hitelesítésére** jelölőnégyzettel engedélyezze vagy tiltsa le a képernyőn megjelenő billentyűzet engedélyezésre történő használatát.
4. Mentse el a módosításokat.

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 hajthat végre rosszindulatú tevékenységeket (például bezárásokat).



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;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Az AMSI védelem engedélyezése és letiltása

Alapértelmezésben az AMSI védelem engedélyezve van.


Az AMSI védelem engedélyezése vagy letiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **AMSI védelem** opciót.
3. Az **AMSI védelem** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Az AMSI védelem használata összetett fájlok vizsgálatához

A vírusok és egyéb rosszindulatú programok álcázásának gyakori módja az összetett fájlalba, 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 típusait, így felgyorsíthatja a vizsgálatot.

Az AMSI védelem összetett fájl vizsgálatának való használatának beállítása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Fenyegetések elleni alapvető védelem** → **AMSI védelem** opciót.
3. Adja meg az **Összetett fájl vizsgálat** részben a vizsgálni kívánt összetett fájl 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 a **Maximális fájl méret** mezőben. 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.

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 be- és kikapcsolása

A Biztonsági rések kihasználásának megelőzése alapértelmezés szerint be van kapcsolva, és a Kaspersky által javasolt módban működik. A Biztonsági rések kihasználásának megelőzése összetevőt szükség esetén kikapcsolhatja.

A Biztonsági rések kihasználásának megelőzése be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.


2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Biztonsági rések kihasználásának megelőzése** lehetőséget.
3. A **Biztonsági rések kihasználásának megelőzése** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ennek eredményeképpen, ha a Biztonsági-rések kihasználásának megelőzése engedélyezve van, a Kaspersky Endpoint Security figyelni fogja a sebezhető alkalmazások által futtatott futtatható fájlkat. Ha a Kaspersky Endpoint Security azt észleli, hogy egy sebezhető alkalmazáshoz tartozó futtatható fájl a felhasználótól eltérő entitás indított el, akkor a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet (például blokkolni fogja a műveletet).

Sebezhetőség kihasználásának észlelésekor végzendő művelet kiválasztása

Alapértelmezett esetben a Kaspersky Endpoint Security kihasználás észlelésekor blokkolja a kihasználás által megkísérelt műveleteket.


Sebezhetőség kihasználásának észlelésekor végzendő művelet kiválasztása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Biztonsági rések kihasználásának megelőzése** lehetőséget.
3. Válassza ki a vonatkozó műveletet a **Sebezhetőség kihasználásának észlelésekor** blokkban:
 - **Művelet blokkolása.** 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.
 - **Értesítés.** 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](#).
4. Mentse el a módosításokat.

Rendszerfolyamatok memóriavédelme

Alapértelmezés szerint a rendszerfolyamatok memóriavédelme be van kapcsolva.

A rendszerfolyamatok memóriavédelmének ki- és bekapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Biztonsági rések kihasználásának megelőzése** lehetőséget.
3. A **Rendszerfolyamatok memóriavédelmének engedélyezése** kapcsolóval engedélyezze vagy tiltsa le a funkciót.
4. Mentse el a módosításokat.

Ennek eredményeképpen a Kaspersky Endpoint Security blokkolni fogja azokat a külső folyamatokat, amelyek megpróbálnak hozzáférni a rendszerfolyamatokhoz.

Viselkedéselemzés


A Viselkedéselemzés összetevő a számítógépen futó alkalmazások műveleteiről fogad adatokat, és a teljesítmény növelése érdekében átadja ezeket az információkat a többi védelmem összetevőinek. A Viselkedéselemzés 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 viselkedésfolyam-aláíráson alapuló funkciói a számítógép számára proaktív védelmet nyújtanak.

A Viselkedéselemzés be- és kikapcsolása

A Viselkedéselemzés alapértelmezés szerint be van kapcsolva, és a Kaspersky által javasolt módban működik. A Viselkedéselemzést szükség esetén kikapcsolhatja.

Ha nem feltétlenül szükséges, nem javasolt kikapcsolni a Viselkedéselemzést, mivel kihat a védelmi összetevők eredményességére. A védelmi összetevők a Viselkedéselemzés által gyűjtött adatokat kikérhetik, hogy segítségükkel észleljék a fenyegetéseket.


A Viselkedéselemzés be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Viselkedéselemzés** lehetőséget.
3. A **Behavior analysis** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ennek eredményeképpen, ha a Viselkedéselemzés engedélyezve van, a Kaspersky Endpoint Security viselkedésfolyam-aláírásokat fog használni az alkalmazások operációs rendszerben végzett tevékenységének elemzéséhez.

A rosszindulatú tevékenység észlelése esetén végrehajtandó művelet kiválasztása

Annak kiválasztása érdekében, hogy mi a teendő, ha egy alkalmazás rosszindulatú tevékenységet folytat, végezze el az alábbi lépéseket:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Viselkedéselemzés** lehetőséget.
3. Válassza ki a vonatkozó műveletet a **Rosszindulatú program tevékenységének észlelése esetén** blokkban:

- **Fájl törlése.** 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.
- **Alkalmazás leállítása.** Ha ez az elem van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security az érintett alkalmazást bezárja.
- **Értesítés.** 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.

4. Mentse el a módosításokat.

A megosztott mappák védelme a külső titkosítás ellen

Az összetevő csak az NTFS fájlrendszerű tárolóeszközökön tárolt, EFS-titkosítással nem rendelkező fájlkon történő műveleteket figyeli.

A megosztott mappák külső titkosítás elleni védelme a megosztott mappákban lévő tevékenységet elemzi. Ha ez a tevékenység megegyezik a külső titkosításra jellemző viselkedésfolyamat-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet.


Alapértelmezett esetben a megosztott mappák külső titkosítás elleni védelme ki van kapcsolva.

A Kaspersky Endpoint Security telepítése után a megosztott mappák külső titkosítás elleni védelme korlátozva lesz a számítógép újraindításáig.

Megosztott mappák külső titkosítás elleni védelmének be- és kikapcsolása


A Kaspersky Endpoint Security telepítése után a megosztott mappák külső titkosítás elleni védelme korlátozva lesz a számítógép újraindításáig.

Megosztott mappák külső titkosítás elleni védelmének be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Viselkedéselemzés** lehetőséget.
3. **A megosztott mappák külső forrásból történő titkosítás elleni védelmének engedélyezése** kapcsolóval engedélyezze vagy tiltsa le a külső titkosításra jellemző tevékenység észlelését.
4. Mentse el a módosításokat.

Megosztott mappák külső titkosításának észlelése esetén végzendő művelet kiválasztása

Megosztott mappák külső titkosításának észlelése esetén végzendő művelet kiválasztása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Viselkedéselemzés** lehetőséget.
3. Válassza ki a vonatkozó műveletet **A megosztott mappák védelme a külső titkosítás ellen** blokkban:
 - **Kapcsolódás blokkolása N perc (1 és 43800 között)**. Ha a következő opció van kiválasztva, és a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észleli, a következőt teszi:
 - Blokkolja a fájlmodosítási hozzáférést a rosszindulatú tevékenységet kiváltó munkamenet számára (a fájl írásvédett lesz).
 - Másolatot hoz létre a fájlokról, amik módosítva vannak.
 - Hozzáad egy bejegyzést a [helyi alkalmazásfelület jelentéseihez](#).
 - Elküldi az észlelt rosszindulatú tevékenység információit a Kaspersky Security Center számára.Továbbá, ha a Kármentesítő motor összetevő be van kapcsolva, a módosított fájlok vissza lesznek állítva a biztonsági mentésből.
 - **Értesítés**. Ha a következő opció van kiválasztva, és a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észleli, a következőt teszi:
 - Hozzáad egy bejegyzést a [helyi alkalmazásfelület jelentéseihez](#).
 - Bejegyzést ad hozzá az aktív fenyegetések listájához.
 - Elküldi az észlelt rosszindulatú tevékenység információit a Kaspersky Security Center számára.
4. Mentse el a módosításokat.

Kizárás létrehozása a megosztott mappák külső titkosítás elleni védelmére

Egy mappa kizárása csökkentheti az álpozitív találatok számát, ha a cég adattitkosítást használ a megosztott mappák segítségével történő fájlcsere során. A Viselkedélemzés 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.

[Kizárás létrehozása a megosztott mappák védelmére az Adminisztrációs 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályok ablakában válassza az **General settings** → **Exclusions** lehetőséget.
6. A **Scan exclusions and trusted applications** részben kattintson a **Settings** gombra.
7. A megnyíló ablakban válassza ki a **Kizárások a vizsgálatból** lapot.
Ez megnyitja a kizárások listáját tartalmazó ablakot.
8. 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.
9. Jelölje be a **Allow use of local trusted applications** 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. Ha helyi listát hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt fájlokat a vizsgálatokból.
10. Kattintson **Hozzáadás** gombra.
11. A **Properties** részben jelölje be a **File or folder** jelölőnégyzetet.
12. Kattintson a **válasszon fájlt vagy mappát** hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben a **Fájl vagy mappa neve** ablak megnyitásához.
13. 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:\Mappa***.txt maszk a Mappa nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a Mappát. 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.

14. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.
15. Kattintson a **bármelyik** hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben a **válassza ki az összetevőket** hivatkozás aktiválásához.
16. A **válassza ki az összetevőket** hivatkozásra kattintva megnyílik a **Védelmi összetevők** ablak.
17. Jelölje be a **Viselkedéselemzés** összetevő melletti jelölőnégyzetet.
18. Mentse el a módosításokat.

[Kizárás létrehozása a megosztott mappák védelmére a Web Console és a Cloud Console használatával](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Exclusions** helyre.
5. A **Scan exclusions and trusted applications** részben kattintson a **Scan exclusions** hivatkozásra.
6. 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.
7. Jelölje be a **Allow use of local trusted applications** 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. Ha helyi listát hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt fájlokat a vizsgálatokból.
8. Kattintson a **Add** gombra.
9. Válassza ki, hogyan kívánja hozzáadni a kizárási fájlt vagy mappát.
10. 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 karakterhalmazzal helyettesíthet (az üres halmazzal is) a fájlban, beleértve a \ és / karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a C:\Mappa***.txt maszk a Mappa nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a Mappát. 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 útját, aminek TXT-kiterjesztése van és három karakterből áll.
11. A **Védelmi összetevők** részen válassza ki a **Viselkedéselemzés** összetevőt.
12. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

13. Válassza ki az **Aktív** állapotot a kizáráshoz.

Bármikor használhatja a kapcsolót [egy kizárás megszüntetéséhez](#).

14. Mentse el a módosításokat.

Kizárás létrehozása a megosztott mappák védelmére az alkalmazás felületén

1. Kattintson a fő alkalmazásablakban a  gombra.

2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Fenyegetések és kizárások** 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 karakterhalmazzal helyettesíthet (az üres halmazzal is) a fájlban, beleértve a \ és / karaktereket (ezek választják el a fájlok és mappák neveit az elérési útvonalban). Például a C:\Mappa***.txt maszk a Mappa nevű mappában és az azon belüli mappákban található TXT kiterjesztésű fájlok összes elérési útját tartalmazza, kivéve magát a Mappát. 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 útját, aminek TXT-kiterjesztése van és három karakterből áll.

6. A **Védelmi összetevők** részen válassza ki a **Viselkedéselemzés** 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.

Megosztott mappák külső titkosítás elleni védelméből való kizárások címeinek beállítása

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 megosztott mappák külső titkosítását végző távoli számítógépek kizárása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Viselkedéselemzés** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Kizárások címének konfigurálása** hivatkozásra.
4. Ha hozzá akar adni egy IP-címet vagy számítógépet a kizárások listájához, kattintson a **Hozzáadás** gombra.
5. Adja meg az IP-címet vagy a számítógépet, melynek külső titkosítási kísérleteit nem szabad kezelni.
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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behavior analysis** lehetőséget.
6. A **Hálózati védelem beállításai** blokkban kattintson a **Kizárások** gombra.
7. A szabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt kizárásokat. Több pont kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.
 - b. Kattintson az **Exportálás** hivatkozásra.
 - 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.
8. A kizárások listájának importálása:
 - a. Kattintson az **Importálás** 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.
9. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Fenyegetések elleni fejlett védelem** → **Viselkedéselemzés** szakaszt.
5. A kizárások listájának exportálása a **Kizárások** blokkban:
 - a. Jelölje ki az exportálni kívánt kizárásokat.
 - b. Kattintson az **Export** gombra.
 - c. Erősítse meg, hogy csak a kijelölt kizárásokat, vagy a kizárások teljes listáját szeretné exportálni.
 - d. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.
 - e. Mentse a fájlt.
A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba.
6. A kizárások listájának importálása a **Kizárások** blokkban:
 - a. Kattintson az **Importálás** 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.

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](#) összetevő 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 meglévő 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. A **Behatolásmegelőző rendszer** jelölőnégyzet használatával engedélyezze vagy tiltsa le az összetevőt.
7. Mentse el 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. A **Behatolásmegelőző rendszer** 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.

Kiválaszthatja azt a megbízhatósági csoportot, amelybe a Kaspersky Endpoint Security [minden ismeretlen alkalmazást automatikusan besorol](#). A Kaspersky Endpoint Security előtt elindított alkalmazások automatikusan a [Behatolásmegelőző rendszer összetevő beállításai](#) ablakban meghatározott megbízhatósági csoportba lesznek áthelyezve.

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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
7. Válassza ki az **Application rights** fület.
8. Kattintson a **Add** gombra.
9. A megnyílt 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.
10. Kattintson a **Frissítés** gombra.
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.
11. Válassza ki a szükséges alkalmazást.
12. A **Kijelölt alkalmazás hozzáadása a megbízhatósági csoporthoz** legördülő listában válassza ki az alkalmazáshoz szükséges megbízhatósági csoportot.
13. Mentse el a módosításokat.

[Egy alkalmazás megbízhatósági csoportjának módosítása a Web Console-ban, illetve a Cloud Console-ban](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. Az **Application rights and protected resources** részen kattintson az **Application rights and protected resources** hivatkozásra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
6. Válassza ki az **Application rights** fület.
Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.
7. 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. Nyomja meg a **Next** gombot.
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. Az **OK** gombra kattintva zárhatja be a varázslót.
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 **Manage applications** gombra.
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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
7. Válassza ki az **Application rights** fület.
8. Válassza ki a szükséges megbízhatósági csoportot.
9. A megbízhatósági csoport helyi menüjéből válassza ki a **Csoportjogok** lehetőséget.
Ez megnyitja a megbízhatósági csoport tulajdonságait.
10. 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** lapot.
 - 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](#) összetevő felügyeli *hálózati szabályok* alkalmazásával.

11. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában, és válassza ki a szükséges lehetőséget: **Öröklés**, **Engedélyezés** (✓) vagy **Blokkolás** (⊘).
12. 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.
13. Mentse el a módosításokat.


[Megbízhatósági csoport jogainak módosítása a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. Az **Application rights and protected resources** részen kattintson az **Application rights and protected resources** hivatkozásra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
6. Válassza ki az **Application rights** fület.
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 **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](#) összetevő felügyeli *hálózati szabályok* alkalmazásával.

9. A megfelelő erőforrás és a megfelelő művelet oszlopában válassza ki a szükséges opciót: **Öröklés**, **Engedélyezés** (✓) vagy **Tiltás** (✗).
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. 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 **Manage applications** gombra.
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** lapot.
 - 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](#) összetevő 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 (*Felhasználói 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazásjogok és védett erőforrások** részen kattintson a **Szerkesztés** gombra.
7. A **Kaspersky Endpoint Security for Windows működésének megkezdése előtt elindított alkalmazások megbízhatósági csoportja** beállításánál válassza ki a megfelelő megbízhatósági csoport.
8. Mentse el 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. A **Kaspersky Endpoint Security for Windows működésének megkezdése előtt elindított alkalmazások megbízhatósági csoportja** beállításánál válassza ki a megfelelő megbízhatósági csoport.
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 **Kaspersky Endpoint Security for Windows működésének megkezdése előtt elindított alkalmazások megbízhatósági csoportja** részen válassza ki a megfelelő [megbízhatósági csoport](#).
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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem → Behatolásmegelőző rendszer** lehetőséget.
6. Az **Application processing rules** részen használja az **Trust group for applications that could not be added to existing groups** legördülő listát a szükséges megbízhatósági csoport kiválasztásához.
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 beállításaiiban megadottól eltérő megbízhatósági csoportba kerülhet.
7. Használja az **Update rights for previously unknown applications from KSN database** jelölőnégyzetet az ismeretlen alkalmazások jogainak automatikus frissítéséhez.
8. Mentse el a módosításokat.

[Megbízhatósági csoport kiválasztása ismeretlen alkalmazásokhoz a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. Az **Application processing rules** részen használja az **Trust group for applications that could not be added to existing groups** legördülő listát a szükséges megbízhatósági csoport kiválasztásához.
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 beállításaiiban megadottól eltérő megbízhatósági csoportba kerülhet.
6. Használja az **Update rights for previously unknown applications from KSN database** jelölőnégyzetet az ismeretlen alkalmazások jogainak automatikus frissítéséhez.
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 **Application processing rules** részen 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 beállításaiiban 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazás-feldolgozási szabályok** részen használja **Megbízik a digitálisan aláírt alkalmazásokban** jelölőnégyzetet a megbízható gyártók digitális aláírásait tartalmazó alkalmazások 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](#).
7. Mentse el a módosításokat.

[Megbízhatósági csoport kiválasztása digitálisan aláírt alkalmazásokhoz a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. Az **Alkalmazás-feldolgozási szabályok** részen használja **Megbízik a digitálisan aláírt alkalmazásokban** jelölőnégyzetet a megbízható gyártók digitális aláírásait tartalmazó alkalmazások 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. Az **Alkalmazás-feldolgozási szabályok** részen használja **Megbízik a digitálisan aláírt alkalmazásokban** jelölőnégyzetet a megbízható gyártók digitális aláírásait tartalmazó alkalmazások 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 alkalmazásokként, 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 alkalmazást indirekt módon indít egy másik alkalmazás, de az nem az azt futtató alkalmazás gyermeke, a szabályok nem öröklődnek.

[Alkalmazásjogok módosítása 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
7. Válassza ki az **Application rights** fület.
8. Kattintson a **Add** gombra.
9. A megnyílt ablakban írja be annak az alkalmazásnak a keresési feltételeit, amelyek 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.
10. Kattintson a **Frissítés** gombra.
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.
11. Válassza ki a szükséges alkalmazást.
12. 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.
13. Válassza ki a megfelelő alkalmazást, majd válassza az **Alkalmazásjogok** lehetőséget az alkalmazás helyi menüjében.
Ez megnyitja az alkalmazás tulajdonságait.
14. 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** lapot.
 - 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](#) összetevő felügyeli *hálózati szabályok* alkalmazásával.

15. A helyi menü megnyitására kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában, és válassza ki a szükséges lehetőséget: **Öröklés**, **Engedélyezés** (✓) vagy **Blokkolás** (⊘).

16. 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.

17. Mentse el a módosításokat.





[Alkalmazásjogok módosítása a Web Console-ban és a Cloud Console-ban](#) ?

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
 2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
 3. Válassza ki az **Application settings** fület.
 4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
 5. Az **Application rights and protected resources** részen kattintson az **Application rights and protected resources** hivatkozásra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
 6. Válassza ki az **Application rights** fület.
Az ablak bal oldalán megjelenik a megbízhatósági csoportok listája, a jobb oldalon pedig azok tulajdonságai.
 7. 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. Nyomja meg a **Next** gombot.
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. Az **OK** gombra kattintva zárhatja be a varázslót.
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 **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](#) összetevő felügyeli *hálózati szabályok* alkalmazásával.
14. A megfelelő erőforrás és a megfelelő művelet oszlopában válassza ki a szükséges opciót: **Öröklés**, **Engedélyezés** (✓) vagy **Tiltás** (✗).
 15. 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.

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 **Manage applications** gombra.
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** lapot.
 - 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 vizsgáljon 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. Az alkalmazástevékenységet a következő összetevők figyelik: Behavior analysis , Biztonsági rések kihasználásának megelőzése , Behatolásmegelőző rendszer , Kármentesítő motor és Tűzfal .
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	A Kaspersky Endpoint Security nem figyeli az ezen alkalmazás által

alkalmazás tevékenységét	elindított alkalmazások fájl- vagy hálózati tevékenységét.
Az alkalmazásfelülettel való interakció engedélyezése	A Kaspersky Endpoint Security Önvédelem blokkolja az alkalmazásslolgáltatások 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.

Operációsrendszer-erőforrások és személyes adatok védelme

A Behatolásmegelőző rendszer összetevő kezeli az alkalmazások jogosultságát az operációs rendszer különböző kategóriákba sorolt erőforrásaiban 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazásjogok és védett erőforrások** részben kattintson a **Beállítások** gombra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
7. Válassza ki 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.
8. Jelölje ki a védett erőforrások azon kategóriáját, amelyhez új védett erőforrást szeretne hozzáadni.
Ha alkategóriát szeretne hozzáadni, kattintson a **Add** → **Category** elemre.
9. Kattintson a **Add** gombra. A legördülő listában válassza ki a hozzáadni kívánt erőforrás típusát: **Fájl vagy mappa** vagy **Beállításkulcs**.
10. A megnyitott 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.
11. Mentse el a módosításokat.

[Védett erőforrás hozzáadásának menete a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. Az **Application rights and protected resources** részen kattintson az **Application rights and protected resources** hivatkozásra.
Ezután megnyílik az alkalmazásjogok konfigurációs ablaka és a védett erőforrások listája.
6. Válassza ki 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 a **Add** gombra.
Elindul az Új erőforrás varázsló.
8. Kattintson a **Group name** hivatkozásra a védett erőforrások azon kategóriájának kiválasztásához, amelyhez szeretné hozzáadni az új védett erőforrást.
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. Az **OK** gombra kattintva zárhatja be a varázslót.
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 **Manage resources** 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 **Add** gombra. A legördülő listában válassza ki a hozzáadni kívánt erőforrás típusát: **Fájl vagy mappa** vagy **Beállításkulcs**.
6. A megnyitott 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. Letilthatja az alkalmazástevékenység erőforrásokkal történő vezérlését is a  **Felügyelet letiltása** gombra kattintva az **Státusz** 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 hozzáférést. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A házirend ablakában válassza a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
6. Az **Alkalmazás-feldolgozási szabályok** részen végezze el az alábbiak egyikét:
 - Ha be szeretné állítani az automatikus törlést, jelölje be a **Delete rules for applications that have not been started for longer than N days** 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 a **Delete rules for applications that have not been started for longer than N days** jelölőnégyzet bejelölését.

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.
7. Mentse el 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza ki a **Fenyegetések elleni fejlett védelem** → **Behatolásmegelőző rendszer** lehetőséget.
5. Az **Alkalmazás-feldolgozási szabályok** részen végezze el az alábbiak egyikét:
 - Ha be szeretné állítani az automatikus törlést, jelölje be a **Delete rules for applications that have not been started for longer than N days** 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 a **Delete rules for applications that have not been started for longer than N days** jelölőnégyzet bejelölését.
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 **Alkalmazás-feldolgozási szabályok** részen végezze el az alábbiak egyikét:

- Ha be szeretné állítani az automatikus törlést, jelölje be a **Delete rules for applications that have not been started for longer than N days** 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 a **Delete rules for applications that have not been started for longer than N days** jelölőnégyzet bejelölését.

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 beállításában](#).

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 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 az alábbiak szerint szabályozza az alkalmazások hozzáférését az audio- és videofolyamhoz:

- A megbízható és az alacsony korlátozású alkalmazások alapértelmezés szerint megkapják a hang- és video-adatfolyamot az eszközökről.
- A magas korlátozású és a nem megbízható alkalmazásoknak alapértelmezés szerint nem engedélyezett a hang- és video-adatfolyam fogadása 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 a 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 eszközhez 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 hozzáféréseire 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.

Kármentesítő motor

A Kármentesítő motor révén a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben elvégzett 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:

- Megszünteti 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 tevékenység utáni visszagörgetés elindulhat a [Fájl védelem](#) vagy [Viselkedéselemzés](#) összetevővel, illetve a [vírusvizsgálat](#) 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A házirend ablakában válassza ki a **Fenyegetések elleni fejlett védelem** → **Kármentesítő motor** lehetőséget.
6. A **Kármentesítő motor** jelölőnégyzettel engedélyezze vagy tiltsa le az összetevőt.
7. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Fenyegetések elleni fejlett védelem** → **Kármentesítő motor** szakaszt.
5. A **Kármentesítő motor** 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 *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 részt vesz a Kaspersky Security Networkben, a KSN szolgáltatás megadja a Kaspersky Endpoint Security számára a vizsgált fájlok kategóriáját és hírnevét, valamint a vizsgált webcímek hírnevét.

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](#)  található. A Kaspersky Security Network nyilatkozatának szövegét tartalmazó ksn_<nyelv azonosítója>.txt fájl megtalálható az alkalmazás [terjesztőkészletében](#).

A KSN kiszolgálók terhelésének csökkentése érdekében előfordulhat, hogy a Kaspersky szakértők az alkalmazás olyan frissítéseit adja ki, amelyek átmenetileg kikapcsolják vagy részlegesen korlátozzák a Kaspersky Security Network részére küldött kéréseket. Ebben az esetben a KSN-kapcsolat állapota az alkalmazás helyi felületén a következő: *Korlátozásokkal engedélyezve*.

KSN-infrastruktúra

A Kaspersky Endpoint Security a következő KSN-infrastrukturális megoldásokat támogatja:


- *Globális KSN*: a Kaspersky alkalmazások által használt leggyakoribb megoldás. A KSN-részvevők információkat kapnak a Kaspersky Security Networktól, és elküldik a Kaspersky számára a felhasználó számítógépén észlelt objektumokat, hogy a Kaspersky is elemezze azokat, és belevegye a Kaspersky Security Network hírnév- és statisztikai adatbázisába.
- *A Privát KSN* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky Security Network hírnévadatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a KSN-re a saját számítógépükről. A privát KSN 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.

Alapértelmezés szerint a Kaspersky Security Center a Globális KSN hálózatot használja. Lehetősége van konfigurálni a privát KSN használatát az adminisztrációs konzolon (MMC), a Kaspersky Security Center Web Console-ban és a [parancssorban](#). A privát KSN használatát nem lehet konfigurálni a Kaspersky Security Center Cloud Console-ban.

A Privát KSN-ről szóló további részletekért lásd a *Kaspersky Private Security Network dokumentációját*.

A Kaspersky Security Network használatának engedélyezése és letiltása

A Kaspersky Security Network használatának engedélyezése és letiltása:

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.
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.
4. Szükség esetén kapcsolja át a **Kiterjesztett KSN mód engedélyezése** kapcsolót.
5. Mentse el a módosításokat.

Ennek eredményeként, ha a KSN használata engedélyezett, a Kaspersky Endpoint Security a Kaspersky Security Networktól kapott információkat használja a fájlok, webes erőforrások és alkalmazások megbízhatóságával kapcsolatban.

A privát KSN korlátozásai

A privát KSN (a továbbiakban KPSN) 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. Képzelve 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 fájl „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 beállításai között 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](#).

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 Security Network 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.

Felhő mód be- és kikapcsolása a védelmi összetevőknél:

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 felügyeleti kiszolgáló által kezelt felhasználói számítógépek a KSN-nel a KSN Proxyszolgáltatáson keresztül léphetnek interakcióba.

A KSN Proxyszolgáltatás 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 Network-höz 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 konfigurálás részleteiért lásd a Kaspersky Security Center Sűgót. Engedélyezheti vagy letilthatja a KSN Proxyt az egyes számítógépeken a Kaspersky Endpoint Security házirendben.

[A KSN Proxy engedélyezése vagy letiltása a Felügyeleti konzolon \(MMC\)](#) 

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Fenyegetések elleni fejlett védelem → Kaspersky Security Network** lehetőséget.
3. A **KSN proxy beállítások** blokkban használja a **KSN Proxy használata** jelölőnégyzetet KSN Proxy engedélyezéséhez vagy letiltásához.
4. Szükség esetén válassza ki a **KSN kiszolgálók használata, amennyiben a KSN Proxy 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 (Globális KSN használata esetén) és harmadik felek oldalán (Privát KSN használata esetén).
5. Mentse el a módosításokat.

[Az KSN Proxy engedélyezése vagy letiltása a webkonzolban](#)

1. A Web Console fő ablakában válassza ki a **Devices → Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Advanced Threat Protection → Kaspersky Security Network** szakaszt.
5. Használja a **Use KSN Proxy** jelölőnégyzetet KSN Proxy engedélyezéséhez vagy letiltásához.
6. Szükség esetén válassza ki a **Use KSN servers when KSN Proxy is not available** 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 (Globális KSN használata esetén) és harmadik felek oldalán (Privát KSN használata esetén).
7. Mentse el a módosításokat.

A KSN proxy címe megegyezik a felügyeleti kiszolgáló címével. Amikor a Felügyeleti kiszolgáló tartománynevét megváltoztatja, manuálisan kell frissítenie a KSN Proxy címét.

A KSN Proxy címének beállítása:

1. Az Adminisztrációs Konzolon nyissa meg az **Administration Server → Additional → Remote installation → Installation packages** mappát.
2. Az **Installation packages** mappa helyi menüjében válassza ki a **Properties** elemet.
3. A megnyitott ablak **General** lapon adja meg a KSN proxykiszolgáló új nevét.
4. Mentse el a módosításokat.

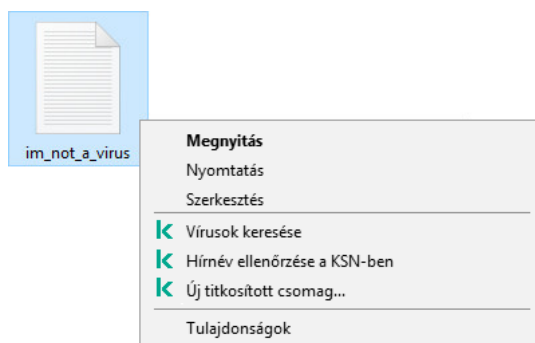
Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével

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). A Kaspersky Security Network legtöbb felhasználója megbízhatónak ítélte a fájlt.

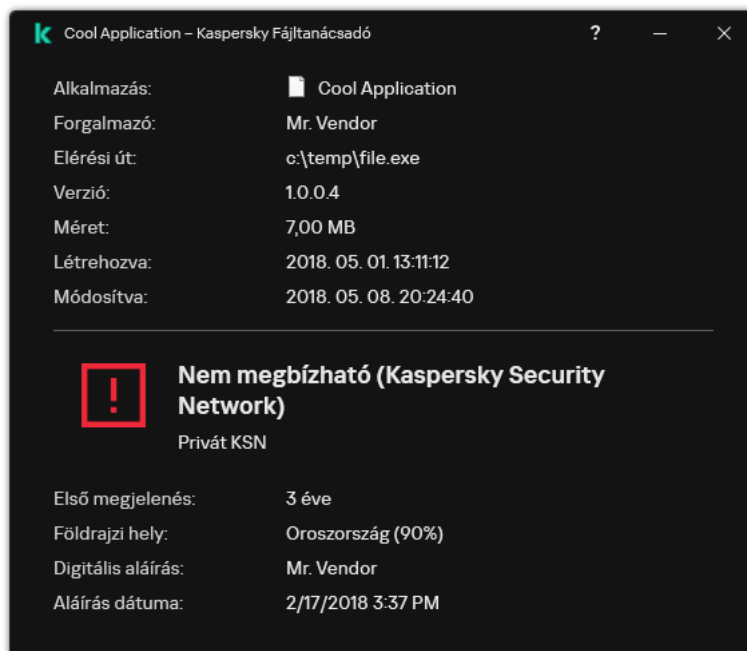
⚠ Legitim szoftver, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait. Miközben ezeknek az alkalmazásoknak nincs rosszindulatú funkciója, a behatolók felhasználhatják őket rosszindulatú eljárásaik során. A jogszerű szoftverek részleteiért, amelyekkel a bűnözők károsíthatják a számítógépet 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: *Globális KSN* vagy *Privát KSN*.

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 emellett használja a Firefox és a Thunderbird megbízható tanúsítványainak rendszertárolóját is ezen alkalmazások adatforgalmának vizsgálatához.

A [Webfelügyelő](#), a [Levelezés védelem](#) és a [Web védelem](#) 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.

A titkosított kapcsolatok vizsgálata beállításainak konfigurálása

A titkosított kapcsolatok vizsgálata beállításainak konfigurálása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Titkosított kapcsolat vizsgálata** részben 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 Fájl védelem, a Levelezés védelem vagy a Webfelügyelő

összetevő ezt kéri.

- **Mindig vizsgálja a titkosított kapcsolatokat.** A Kaspersky Endpoint Security akkor is vizsgálja 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 kapcsolat vizsgálatának beállításait (lásd az alábbi táblázatban).
6. Mentse el a módosításokat.

Titkosított kapcsolatok vizsgálatának beállításai

Paraméter	Leírás
Nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása esetén	<ul style="list-style-type: none">• Engedélyezés. Ha ez az opció van kijelölve, akkor 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. 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.• Kapcsolat blokkolása. Ha ez az opció van kijelölve, akkor 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.
Ha a titkosított kapcsolat vizsgálatakor hiba lép fel	<ul style="list-style-type: none">• Kapcsolat blokkolása. Ha ez az elem van kijelölve, és egy titkosított kapcsolat vizsgálata közben hiba történik, akkor a Kaspersky Endpoint Security blokkolja a hálózati kapcsolatot.• Tartomány hozzáadása a kizárásokhoz Ha ez az elem van kijelölve, és egy titkosított kapcsolat vizsgálata közben hiba történik, akkor a Kaspersky Endpoint Security hozzáadja a hibát okozó tartományt a tartományok vizsgálati hibákkal listájához, és nem figyel a titkosított hálózati forgalmat ennek a tartománynak a felkeresésekor. Azoknak a tartományoknak a listáját, amelyeknél a titkosított kapcsolatok vizsgálata során hiba jelentkezett, csak az alkalmazás helyi felületén lehet megtekinteni. A lista törléséhez ki kell választania a Kapcsolat blokkolása lehetőséget.

SSL 2.0 kapcsolatok blokkolása (ajánlott)	<p>Ha a jelölőnégyzet be van jelölve, akkor a Kaspersky Endpoint Security blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat.</p> <p>Ha a jelölőnégyzet nincs bejelölve, akkor a Kaspersky Endpoint Security nem blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat, és nem figyel kapcsolatokon keresztül küldött hálózati forgalmat.</p>
Titkosított kapcsolat visszafejtése EV- tanúsítványt használó webhelyeken	<p>Az EV-tanúsítványok (Extended Validation Certificates) 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.</p> <p>Ha van jelölés ebben a jelölőnégyzetben, a Kaspersky Endpoint Security visszafejti és figyel az EV-tanúsítványt használó rendelkező webhelyeket.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem fér hozzá a HTTPS-forgalom tartalmához. Ezen okokból az alkalmazás csak a webcím alapján figyel meg a HTTPS-forgalmat, például: <code>https://google.com</code>.</p> <p>Ha először nyit meg egy EV-tanúsítvánnyal rendelkező weboldalt, a titkosított kapcsolat attól függetlenül vissza lesz fejtve, hogy Ön kijelölte-e a jelölőnégyzetet.</p>

Titkosított kapcsolatok vizsgálata a Firefoxban és a Thunderbirdben


A telepítést követően a Kaspersky Endpoint Security hozzáadja a Kaspersky tanúsítványt a rendszer által tárolt megbízható tanúsítványok közé (Windows tanúsítványtároló). Alapértelmezés szerint a Firefox és a Thunderbird a saját tulajdonú Mozilla tanúsítványtárolót használja a Windows tanúsítványtároló helyett. Ha a Kaspersky Security Center telepítve van a szervezetben és házirend van alkalmazva a számítógépre, a Kaspersky Endpoint Security a Firefox és a Thunderbird alkalmazásokban automatikusan engedélyezi a Windows tanúsítványtárolójának használatát az alkalmazások forgalmának vizsgálatára. Ha nincs házirend alkalmazva a számítógépen, kiválaszthatja a Mozilla alkalmazások által használt tanúsítványtárolót. Ha a Mozilla tanúsítványtárolót választotta, adja hozzá manuálisan a Kaspersky tanúsítványt. 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, a Kaspersky Endpoint Security nem vizsgálja a Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmát.

Mielőtt tanúsítványt adna a Mozilla tárolójához, exportálja a Kaspersky tanúsítványt a Windows Vezérlőpulttól (böngésző tulajdonságai). A Kaspersky-tanúsítvány exportálásával kapcsolatos részleteket a [Terméktámogatási tudásbázis](#) webhelyen találja. A tanúsítvány tárolóhoz való hozzáadásával kapcsolatos részletekért keresse fel a [Mozilla terméktámogatás webhelyét](#).

A tanúsítványtárolót csak az alkalmazás helyi felületén választhatja ki.

Tanúsítványtároló kiválasztása a titkosított kapcsolatok vizsgálatához a Firefoxban és a Thunderbirdben:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Mozilla Firefox és Thunderbird** szakaszban jelölje be **A kiválasztott tanúsítványtár használata titkosított kapcsolatok vizsgálatához a Mozilla-alkalmazásokban jelölőnégyzetet**.

4. Válasszon egy tanúsítványtárolót:


- **Windows tanúsítványtároló használata (ajánlott).** A Kaspersky főtanúsítvány bekerül ebbe a tárolóba a Kaspersky Endpoint Security telepítése során.
- **A Mozilla tanúsítványtárolójának használata.** 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 beállításáiban.

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 címek*hez. 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.

Webcím kizárása a titkosított kapcsolatok vizsgálatából:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Titkosított kapcsolat vizsgálata** részen kattintson a **Megbízható címek** gombra.
4. Kattintson a **Add** 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 IP-címmaszkokat. Az alkalmazás helyi felületén megadhat egy IP-címtartományt (például 198.51.100.0/24). A Kaspersky Security Center konzolban nem adhat meg IP-címtartományt.


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 kapcsolat vizsgálata** részen 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 paramétereit 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 kapcsolat vizsgálata** részen 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 törődnek.
- 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 ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a **Add** gombra.
Elindul a Feladatvarázsló.
3. Adja meg a feladatok beállításait:
 - a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.
 - b. A **Task type** legördülő listából válassza ki az **Wipe data** lehetőséget.
 - c. A **Task name** mezőben adjon meg egy rövid leírást, például olyat, hogy *Wipe data (Anti-Theft)*.
 - d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.
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 percen belül teljesül.

5. Lépjen ki a varázslóból.

Egy új feladat jelenik meg a feladatok listájában.

6. Válassza ki a Kaspersky Endpoint Security **Adatok törlése** feladatát.

Megnyílik a feladatok tulajdonságai ablak.

7. Válassza ki az **Application settings** fület.

8. Válassza ki az adattörlés módszerét:

- **Törlés az operációs rendszer eszközeivel.** A Kaspersky Endpoint Security az operációs rendszer erőforrásait használja arra, hogy törölje a fájlokat anélkül, hogy a lomtárba küldené azokat.
- **Végleges törlés, visszaállítás nem lehetséges.** A Kaspersky Endpoint Security véletlenszerű adatokkal felülírja a fájlokat. A törlés után gyakorlatilag lehetetlen visszaállítani az adatokat.

9. Ha el akarja halasztani az adattörlést, válassza az **Adatok automatikus törlése, ha több mint N napja nincs kapcsolat a Kaspersky Security Centerrel** 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.

Ha az eltolt adattörlést állítja be, akkor tartsa észben, hogy az alkalmazottak kikapcsolhatták a számítógépüket, mielőtt vakációra mentek volna. Ebben az esetben a kapcsolathány ideje növekszik, az adatok pedig törlődve lesznek. Vegye figyelembe az offline felhasználók munkarendjét is. Az offline számítógépekkel és az irodán kívüli felhasználókkal való együttműködéssel kapcsolatos további tudnivalóért lásd a [Kaspersky Security Center súgót](#).

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:
 - **Dokumentumok.** Az operációs rendszer szokványos *Dokumentumok* mappájában, valamint az azon belüli almappákban található fájlok.
 - **Sütik.** Fájlok, amelyekben a böngésző elmenti a felhasználó által meglátogatott weboldalak adatait (például a hitelesítő adatokat).

- **Asztal.** Az operációs rendszer szokványos *Asztal*/mappájában, valamint az azon belüli almappákban található fájlok.
- **Ideiglenes Internet Explorer fájlok.** Az Internet Explorer működéséhez kapcsolódó ideiglenes fájlok, például a weboldalak, képek és médiafájlok másolata.
- **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).
- **Felhasználóprofil.** 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 a **Futtatás** gombra.

Ennek eredményeképpen a felhasználók számítógépein lévő adatok a kiválasztott módnak megfelelően törölődnek: 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.

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 Kaspersky Endpoint Security csak a HTTP és a HTTPS forgalmat figyeli meg.

A HTTPS forgalom megfigyeléséhez [engedélyeznie kell a titkosított kapcsolatok vizsgálatát](#).

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 weboldal adataihoz, elrejthet grafikus 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 „Archívum” adattípusként azonosítja azokat, nem pedig „Grafikus fájlokként”.

- **Egyedi címek.** Megadhat webcímet vagy [használhat maszkokat](#).

Egyszerre több módszert is használhat a weboldalak elérésének szabályozására. Például, ha korlátozhatja az „Office fájlok” adattípus elérést a „Webalapú e-mail” weboldalkategória 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.



A kért weboldal nem jeleníthető meg.

Cím: <http://kaspersky.ru/>.

A weboldalt a(z) test_block szabály blokkolta.

Ok: a webes erőforrás a(z) Nem megadott tartalomkategóriá(k)ba és a(z) Nem megadott adattípus kategóriá(k)ba tartozik.

Ez a webes erőforrás tiltva van a vállalatnál. Ha Ön szerint a blokkolás téves vagy mindenképp hozzá kell férnie ehhez a webes erőforráshoz, lépjen kapcsolatba a vállalati helyi hálózat rendszergazdjával ([Hozzáférés kérése](#)).

Üzenet létrehozva: 10/29/2020 4:58:30 AM



Elképzelhető, hogy a kért weboldal nem biztonságos, vagy tiltja a vállalat szabályzata.

Cím: <http://kaspersky.com/>.

A weboldalt a(z) test_warning szabály blokkolta.

Ok: a webes erőforrás a(z) Nem megadott tartalomkategóriá(k)ba és a(z) Nem megadott adattípus kategóriá(k)ba tartozik.

Kattintson a(z) <http://kaspersky.com/> hivatkozásra a kért weboldal megnyitásához.

Ha azon teljes webhely tartalmához szeretne hozzáférni, amelyen a kért weboldal található, kattintson a(z) http://kaspersky.com/* hivatkozásra.

Ha a "*" szimbólummal megjelölt tartománynévnél alacsonyabb vagy azzal azonos minden létező tartományhoz szeretne hozzáférni, kattintson a(z) */*.kaspersky.com/* hivatkozásra.

A hozzáférés a fenti webes erőforrásokhoz az alkalmazás jelenlegi munkamenetének idejére érvényes.

Ha a figyelmeztetés téves, lépjen kapcsolatba a vállalati helyi hálózat rendszergazdjával ([Hozzáférés kérése](#)).


Üzenet létrehozva: 10/29/2020 5:00:10 AM

Webfelügyelő üzenet

A Webfelügyelő be- és kikapcsolása

Alapértelmezés szerint a Webfelügyelő engedélyezve van.

A Webfelügyelő be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
3. A **Webfelügyelő** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

A webes erőforrások hozzáférési szabályainak műveletei

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 felhasználócsoporthoz 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. Két szabály előre be van állítva:

- **Parancsfájlok és stíluslapok szabály,** amely mindig, minden felhasználónak engedélyezi a hozzáférést az olyan webes erőforrásokhoz, amelyek címei CSS, JS vagy VBS kiterjesztésű fájlneveket tartalmaznak. Például: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.

- Alapértelmezett szabály. Ez a szabály minden olyan webes erőforrásra alkalmazva lesz, amiket nem fed más szabály, és engedélyezi vagy letiltja ezeket az erőforrásokat a felhasználók számára.

Webes erőforrás hozzáférési szabályainak megadása

Webes erőforrások hozzáférési szabályainak megadása és szerkesztése:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
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.** Ha az érték ki van választva, a Kaspersky Endpoint Security engedélyezi a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
 - **Blokkolás.** Ha az érték ki van választva, a Kaspersky Endpoint Security blokkolja a szabály paramétereinek megfelelő webes erőforrásokhoz való hozzáférést.
 - **Figyelmeztetés.** Ha az érték ki van választva, a Kaspersky Endpoint Security megjelenít egy figyelmeztetést arról, hogy egy webes erőforrás nem kívánatos, amikor a felhasználó megpróbál egy olyan webes erőforráshoz hozzáférni, amely megfelel a szabálynak. 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 hozzáféréseit a webes erőforrásokhoz.
 - **Adattípus alapján.** A webes erőforrásokhoz való felhasználói hozzáférést a közzétett adatok meghatározott adattípusa (például *Grafikus képek*) 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 **Címek** blokkban válassza ki a releváns webes erőforrások címszűrőt:

- **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. A webes erőforrások címei listájának létrehozásához:

a. Kattintson a **Cím hozzáadása** vagy a **Címcsoport hozzáadása** gombra.

b. A megnyitott ablakban hozza létre a webes erőforrás címeinek listáját. Megadhat webcímet vagy [használhat maszkokat](#). [A webes erőforrás címek listáját TXT fájlból is exportálhatja](#).

c. Térjen vissza az ablakhoz a webes erőforrás hozzáférési szabályának konfigurálásához.

Ha a [Titkosított kapcsolatok vizsgálata](#) ki van kapcsolva, a HTTPS protokollnál csak kiszolgálónév szerint szűrhet.

10. A **Felhasználók** blokkban válassza ki a felhasználókra releváns szűrőt:

- **Minden felhasználónak.** A Webfelügyelet nem fogja szűrni a webes erőforrásokat az adott felhasználóhoz.
- **Egyéni felhasználóknak és/vagy csoportoknak.** A Webfelügyelet csak az adott felhasználóknak fogja szűrni a webes erőforrásokat. Lista létrehozása azokról a felhasználókról, akikre alkalmazni szeretné a szabályt:

a. Kattintson a **Add** gombra.

b. A megnyitott ablakban jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, akikre alkalmazni szeretné a webes erőforrás hozzáférési szabályt.

c. Térjen vissza az ablakhoz a webes erőforrás hozzáférési szabályának konfigurálásához.

11. Válassza ki a **Szabályütemezés** legördülő listán a szükséges ütemezés nevét, illetve állítson elő új ütemezést a kiválasztott szabályütemezés alapján. Ehhez:

a. Kattintson a **Szerkesztés vagy új hozzáadása** gombra.

b. Az ablakban kattintson a **Hozzáadás** gombra.

c. A megnyílt 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.

12. Mentse el a módosításokat.

Prioritás hozzárendelése webes erőforrások hozzáférési szabályaihoz


Az egyes szabályokhoz a szabályok listáján rendelhet hozzá prioritást úgy, hogy a szabályokat a kívánt sorrendben rendezi.

Prioritás hozzárendelése webes erőforrások hozzáférési szabályához:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
3. A **Beállítások** részen kattintson a **Szabályok a webes erőforrásokhoz való hozzáférésre** gombra.
4. A megnyitott ablakban válassza ki azt a szabályt, amelynek módosítani szeretné a prioritását.
5. A szabályt a webes erőforrások hozzáférési szabályai listán a **Fel** és **Le** gombokkal helyezheti a kívánt helyre.
6. Mentse el a módosításokat.

A webes erőforrások hozzáférési szabályainak engedélyezése és letiltása

A webes erőforrások hozzáférési szabályainak engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
3. A **Beállítások** részen kattintson a **Szabályok a webes erőforrásokhoz való hozzáférésre** gombra.
4. A megnyitott ablakban válassza ki azt a szabályt, amelyet be, illetve ki szeretne kapcsolni.
5. Az **Állapot** oszlopban végezze el az alábbiakat:
 - Ha a szabály használatát be szeretné kapcsolni, válassza ki a **Be** értéket.
 - Ha a szabály használatát ki szeretné kapcsolni, válassza ki a **Ki** értéket.
6. Mentse el a módosításokat.

Megbízható webcímek listájának exportálása és importálása

A Webfelügyelő-szabályok listáját exportálhatja egy XML-fájlba. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
6. A Webfelügyelő-szabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt szabályokat. Több pont 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. 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.
8. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen a **Security controls** → **Webfelügyelő** lehetőségre.
5. A szabályok listájának exportálása a **Rule list** blokkban:
 - 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.
6. A szabályok listájának importálása a **Rule list** blokkban:
 - 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.
7. Mentse el a módosításokat.

A webes erőforrások hozzáférési szabályainak tesztelése

A Webfelügyelő szabályainak konzisztenciaellenőrzése érdekében tesztelheti a szabályokat. E célból a Webfelügyelő összetevő Szabálydiagnosztika funkciót tartalmaz.

A webes erőforrások hozzáférési szabályainak tesztelése:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
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, és 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 erőforrások címlistájának exportálása és importálása

Ha webes erőforrások hozzáférési szabályában elkészítette a webes erőforrások címeinek listáját, a listát exportálhatja .txt fájlba. Ezután ebből a fájlból importálhatja a listát, hogy ne kelljen kézzel 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.

Webes erőforrások címlistájának importálása vagy exportálása fájlba:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.
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 megnyitott 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 **Címek** blokkban:

a. Kattintson az **Importálás** 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 felhasználó internetes tevékenységének megfigyelése

A Kaspersky Endpoint Security segítségével naplózhatja a weboldalak látogatását, köztük az engedélyezett weboldalakat 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 számítógépen, a képernyőn lévő értesítések megjelenítését is.


A Kaspersky Endpoint Security a következő internetes felhasználói tevékenységeket hozza létre:

- Weboldal blokkolása (*Kritikus események* állapot .
- Látogasson meg egy nem javasolt weboldalt (*Figyelmeztetések* állapot .
- Engedélyezett weboldal meglátogatása (*Információs üzenetek* 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 injektálása a webes forgalomba:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
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 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 **Értesítési beállítások** 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>, és <http://www.example.com/gallery> nemkívánatos weboldalt, a Kaspersky Endpoint Security csak egy eseményt küld, a <http://www.example.com> objektummal.

Az engedélyezett weboldalak látogatásainak naplózása:

1. Kattintson a fő alkalmazásablakban a  gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Webfelügyelő** lehetőséget.

3. A **További** szakaszban kattintson a **Speciális beállítások** gombra.

4. A megnyíló ablakban válassza **Az engedélyezett oldalak megnyitásának naplózása** jelölőnégyzetet.

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 választ):

- 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 beállításában.


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, ha a **Blokkolás** lehetőség van kiválasztva a webes erőforrást leíró szabály beállításában.

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.

Külön sablonok állnak rendelkezésre a figyelmeztető üzenethez, a webes erőforrás blokkolásáról tájékoztató üzenethez, illetve ahhoz, amelyet a rendszergazda kap. Tartalmukat módosítani lehet.

A Webfelügyelő üzenetsablonjainak módosítása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Security controls** → **Webfelügyelő** lehetőséget.
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 hozzáféréseinek 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.
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 `*.pelda.com` maszk a következő címeket jelöli:

- `http://kepek.pelda.com`. A `*` tartománymaszk `képeket` jelöl.
- `http://felhasznalo.kepek.pelda.com`. A `*` tartománymaszk `képeket` és `felhasználót` jelöl.
- `http://pelda.com`. A `*` tartománymaszk üres sorként értelmezendő.

3. A címmaszk elején álló `www.` karaktorsorozatot a rendszer `*` sorozatként értelmezi.

Példa: a `www.pelda.com` címmaszkot a rendszer `*.pelda.com` címmaszkként kezeli. Ez a maszk a `www2.pelda.com` és a `www.kepek.pelda.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.pelda.com` címmaszk lefedi az olyan címeket, mint a `http://www.pelda.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 `/*` karaktorsorozatot 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: a `example.com` címmaszk a `http://example.com` és a `https://example.com` címeket is magában foglalja.

- Ha a címmaszkban szerepel a hálózati protokoll, akkor csak az ilyen hálózati protokollt tartalmazó címeket fedi le.

Példa: a `http://*.pelda.com` címmaszk magában foglalja a `http://www.pelda.com` címet, de a `https://www.pelda.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	<code>*.pelda.com</code>	<code>http://www.123example.com</code>	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.

A webes erőforrások hozzáférési szabályainak áttelepítése az alkalmazás korábbi verzióiból

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows terméknek vagy az alkalmazás korábbi verziójának Kaspersky Endpoint Security for Windows 11.8.0 verzióra történő frissítéskor a webes erőforrások tartalomkategóriáin alapuló webes erőforrások hozzáférési szabályainak áttelepítése az alábbiak szerint történik:

- A „Csevegőszobák és fórumok”, a „Webalapú e-mail” és a „Közösségi hálózatok” tartalomkategóriái közül egyen vagy többön alapuló hozzáférési szabályok az „Hálózati kommunikáció” webes erőforrás tartalomkategóriába kerülnek.
- Az „Elektronikus áruházak” és a „Fizetési rendszerek” tartalmi kategóriái közül egyen vagy többön alapuló hozzáférési szabályok az „Online üzletek, bankok, fizetési rendszerek” webes erőforrás tartalmi kategóriába kerülnek.
- A „Szerencsejáték” tartalmi kategórián alapuló hozzáférési szabályok a „Szerencsejáték, lottó, sorsolás” webes erőforrás tartalmi kategóriába kerülnek.
- A „Böngészőben futó játékok” tartalmi kategórián alapuló hozzáférési szabályok a „Számítógépes játékok” webes erőforrás tartalmi kategóriába kerülnek.

- A fenti listán fel nem sorolt tartalmi kategóriákon alapuló hozzáférési szabályok változás nélkül kerülnek áttelepítésre.

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 védje számítógépét a fertőzésektől, ha ilyen eszközök vannak csatlakoztatva, valamint megelőzi az adatvesztés- vagy szivárgást.

Eszközhozzáférési szintek

Az Eszközfelügyelő a következő szinteken felügyeli a hozzáférést:

- **Eszköztípus.** Például nyomtatók, cserélhető meghajtók és CD/DVD meghajtók.

Az eszköz hozzáféréseinek beállításait az alábbiak szerint lehet megadni:

- Engedélyezés – ✓.
- Blokkolás – ⓧ.
- A csatlakozóbusztól függ (kivéve a Wi-Fi-hez) – 🌈.
- Blokkolás kivételekkel (csak Wi-Fi) – 📄.
- **Csatlakozási busz.** A *csatlakozási busz* egy felület, amivel csatlakoztatni lehet eszközöket a számítógéphez (például USB vagy FireWire). Ennek megfelelően például USB-n keresztül is korlátozhatja az eszközök kapcsolatát.

Az eszköz hozzáféréseinek 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 beállításában 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. Eszközazonosító példája:
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 azonosítómászk alapján.** Ha több eszközt használ, amelyek azonosítója megegyezik, akkor maszkok segítségével veheti fel azokat a megbízható listára. A * karakter akármilyen karakterláncot

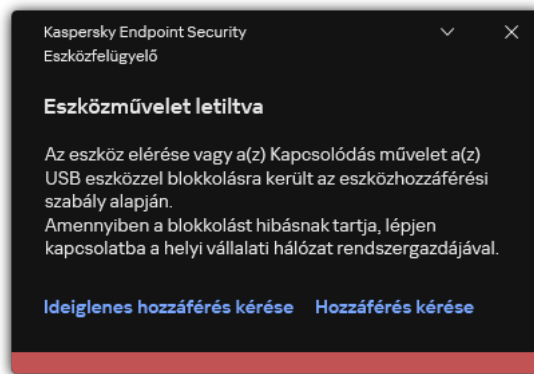
helyettesíthet. A Kaspersky Endpoint Security nem támogatja a `?` karaktert az eszköz maszkjának megadásakor. Például: `WDC_C*`.

- **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.

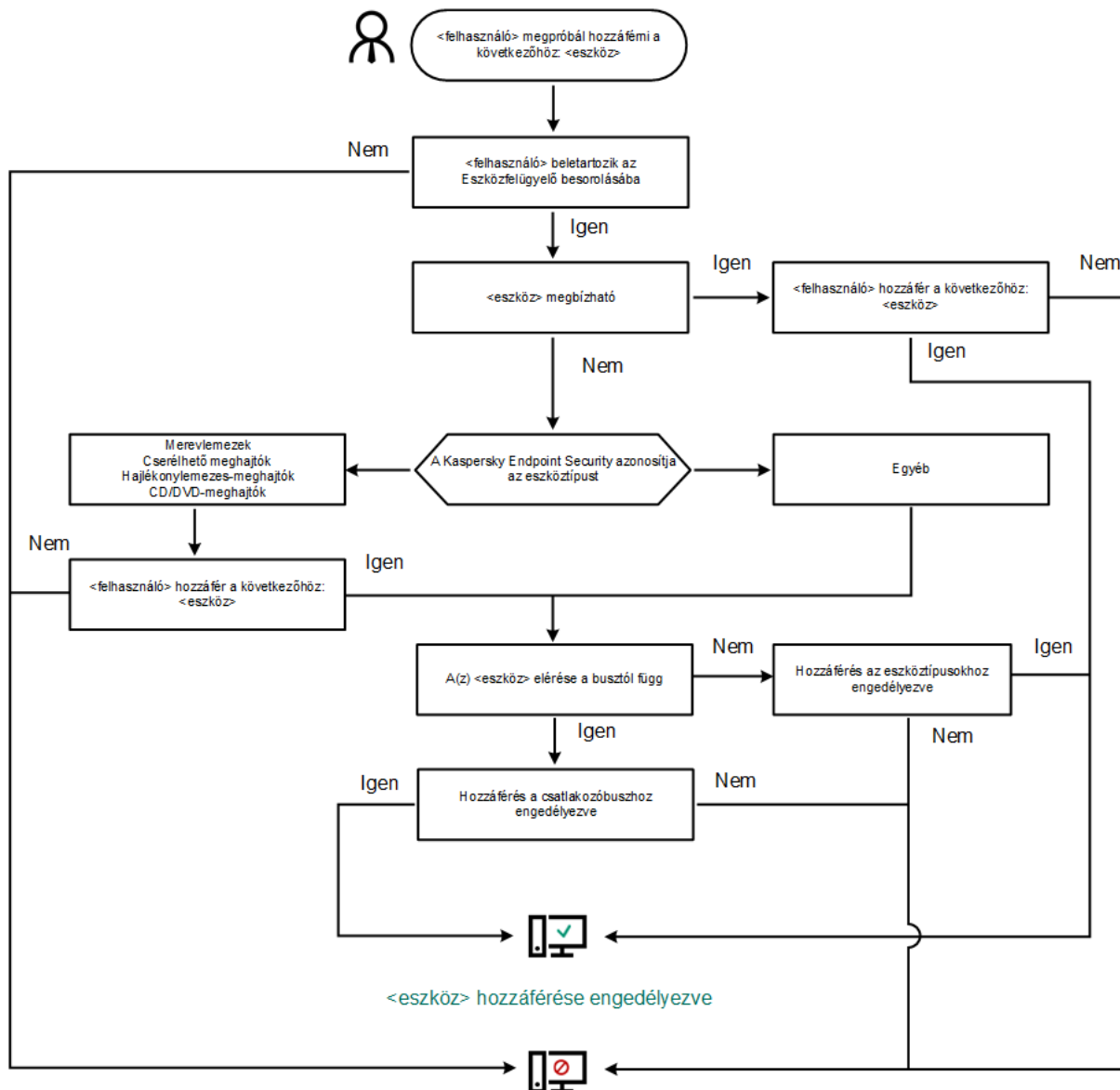
Ha egy olyan eszköz csatlakozik a számítógéphez, ami blokkolva van az Eszközfelügyelő által, akkor a Kaspersky Endpoint Security blokkolja az elérést, és megjelenít egy értesítést (lásd az alábbi ábrát).



Eszközfelügyelő értesítés

Eszközfigyelő műveleti algoritmus

A Kaspersky Endpoint Security döntést hoz az eszközök hozzáféréseinek engedélyezéséről, miután a felhasználó a számítógéphez csatlakoztatja őket (lásd az alábbi ábrát).



<eszköz> hozzáférése blokkolva

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](#).

Az Eszközfelügyelő be- és kikapcsolása

Alapértelmezés szerint az Eszközfelügyelő engedélyezve van.

Az Eszközfelügyelő be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.

2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.

3. Az **Eszközfelügyelő** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.

4. Mentse el a módosításokat.

Ennek eredményeképpen, ha az Eszkőfelügyelő engedélyezve van, az alkalmazás továbbítja a csatlakoztatott eszközökre vonatkozó információkat a Kaspersky Security Centernek. A csatlakoztatott eszközök listáját a Kaspersky Security Center **Speciális** → **Tárhely** → **Hardver** mappájában tekintheti meg.

A hozzáférési szabályokról

A *Hozzáférési szabályok* olyan csoportbeállításokat takarnak, amelyek meghatározzák, hogy milyen felhasználók érhetnek el olyan eszközöket, amik telepítve vannak vagy csatlakoztatva vannak a számítógéphez. Nem adhat hozzá olyan eszközt, ami kívül esik az Eszkőfelügyelő 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	✓	✓	✓	✓	✓
Nyomtatók	✓	–	–	–	–
Hajlékonylemezek	✓	✓	✓	✓	✓
CD/DVD meghajtók	✓	✓	✓	✓	✓
Modemek	✓	–	–	–	–
Szalagos eszközök	✓	–	–	–	–
Többfunkciós eszközök	✓	–	–	–	–
Intelligens kártyaolvasók	✓	–	–	–	–
Windows CE USB ActiveSync eszközök	✓	–	–	–	–
Külső hálózati csatlók	✓	–	–	–	–


Hordozható eszközök (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	–	–	–	–
Kamerák és szkennerek	✓	–	–	–	–

Mobileszköz hozzáférési szabályai




Az Android vagy iOS rendszert futtató mobileszközök hordozható eszköznek (MTP) minősülnek. 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. A készülék típusa a mobilkészülék modelljétől függ.

Kérjük, legyen tekintettel a következő különleges szempontokra ADB- vagy iTunes-eszközök esetén:



- Nem ütemezheti az eszköz hozzáférését. Ha az eszközhöz való hozzáférést szabályok korlátozzák (a státuszuk ) , akkor az ADB- és iTunes-eszközök folyamatosan hozzáférhetők.
- Az eszköz elérését nem konfigurálhatja az egyes felhasználók számára és nem konfigurálhatja a hozzáférési jogokat (írás/olvasás) sem. Ha az eszközhöz való hozzáférést szabályok korlátozzák (a státuszuk  status), akkor az ADB- és iTunes-eszközök hozzáférhetők minden jogosultsággal rendelkező felhasználó számára.
- A megbízható ADB- vagy iTunes-eszközök elérését nem konfigurálhatja az egyes felhasználók számára. Ha az eszköz megbízható, akkor az ADB- és iTunes-eszközök minden felhasználó számára hozzáférhetők.
- 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.

Alapértelmezetten a hozzáférési szabályok minden felhasználó részére mindig teljes hozzáférést biztosítanak az eszközökhöz, ha az adott eszköztípusok csatlakozóbuszaihoz való hozzáférés engedélyezve van. (a  állapot).

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.

A csatlakozási busz hozzáférési szabály dönti el, hogy a csatlakoztatott eszközök engedélyezett-e (a  állapot) vagy tiltottak-e (a  állapot). Az Eszközfelügyelő összetevő osztályozásában jelen lévő összes csatlakozási buszhoz alapértelmezés szerint a hozzájuk való hozzáférést engedélyező szabályok jönnek létre.

Az eszközhozzáférési szabályok szerkesztése

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.

Eszköz hozzáférési szabályának 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 **Készülékek és Wi-Fi hálózatok** gombra.

A megnyitott ablak az Eszközfelügyelő összetevő-besorolásban szereplő összes eszköz hozzáférési szabályait megjeleníti.

4. A **Hozzáférés tárolóeszközökhöz** részen válassza ki a szerkeszteni kívánt hozzáférési szabályt. A szakasz fájlrendszerrel rendelkező eszközöket tartalmaz, amelyekhez további hozzáférési beállításokat konfigurálhat. Alapértelmezés szerint az eszközök hozzáférési szabályai minden felhasználó részére mindig teljes hozzáférést adnak az adott eszköztípushoz.

a. A **Hozzáférés** oszlopban válassza a megfelelő eszközhozzáférési opciót:

- **Engedélyezés.**

- **Blokkolás.**

- **A csatlakozási busztól függ.**

Az eszökhöz való hozzáférés blokkolásához vagy engedélyezéséhez [konfigurálja a csatlakozási buszhoz való hozzáférést](#).

- **Korlátozás szabályokkal.**

Ez a beállítás lehetővé teszi a felhasználói jogok, engedélyek és ütemezés konfigurálását az eszközhozzáféréshez.

b. A **Felhasználói jogok** részen kattintson a **Hozzáadás** gombra.

Ekkor megnyitja az új eszközhozzáférési szabály hozzáadására szolgáló ablakot.

c. Rendeljen prioritást a *szabályhoz*. 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.

- d. Állítsa be az eszközhozzáférési szabály **Engedélyezve** állapotát.
 - e. Konfigurálja a felhasználók eszközhozzáférési jogosultságait: olvasás és/vagy írás.
 - f. Jelölje ki azokat a felhasználókat vagy felhasználói csoportokat, akikre alkalmazni szeretné az eszközhozzáférési szabályt.
 - g. Eszközhozzáférési ütemezés konfigurálása a felhasználók számára.
 - h. Kattintson a **Add** gombra.
5. A **Hozzáférés külső eszközökhöz** részen válassza ki a szabályt, és konfigurálja a hozzáférést: **Engedélyezés, Blokkolás** vagy **A csatlakozási busztól függ**. Ha szükséges, [konfigurálja a hozzáférést a csatlakozási buszhoz](#).
 6. A **Hozzáférés Wi-Fi-hálózatokhoz** részen kattintson a **Wi-Fi** hivatkozásra, és konfigurálja a hozzáférést: **Engedélyezés, Blokkolás** vagy **Blokkolás kivételekkel**. Ha szükséges, [vegyen fel Wi-Fi-hálózatokat a megbízható elemek listájára](#).
 7. Mentse el a módosításokat.

A csatlakozóbuszok hozzáférési szabályainak szerkesztése


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**.
6. Mentse el a módosításokat.

Wi-Fi-hálózat felvétele a megbízható listára

Engedélyezheti, hogy a felhasználók biztonságosnak tekintett Wi-Fi-hálózatokhoz – például vállalati Wi-Fi-hálózatokhoz – kapcsolódjanak. Ehhez az adott hálózatot fel kell venni megbízható Wi-Fi hálózatok listájára. Az Eszközfelügyelő a megbízható listán megadottak kivételével az összes Wi-Fi-hálózatokhoz való hozzáférést blokkolja.

Wi-Fi-hálózat felvétele a megbízható listára:

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.

5. A **Hozzáférés** részen válassza a **Blokkolás kivételekkel** lehetőséget.

6. A **Megbízható Wi-Fi-hálózatok** részen kattintson a **Hozzáadás** gombra.

7. A megnyitott ablakban végezze el az alábbiak egyikét:

a. Adja meg a **Hálózat neve** mezőben a megbízható listára felvenni kívánt Wi-Fi-hálózat nevét.

b. Válassza ki a **Hitelesítés típusa** legördülő listán a megbízható Wi-Fi hálózathoz kapcsolódáskor használt hitelesítés típusát.

c. Válassza ki a **Titkosítás típusa** legördülő listán a megbízható Wi-Fi hálózat forgalmát biztonságossá tevő titkosítás típusát.

d. A **Megjegyzés** mezőben a felvett Wi-Fi-hálózatra vonatkozóan bármilyen információt megadhat.

A Wi-Fi-hálózatok akkor minősülnek megbízhatónak, ha beállításai a szabályban megadott összes szabállyal egyeznek.

8. Mentse el a módosításokat.

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 *Tájékoztató 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.

4. A **Hozzáférés tárolóeszközökhöz** részen válassza a **Cserélhető meghajtók** lehetőséget.

5. A megnyitott ablakban válassza ki a **Naplózás** lapot.

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 naplózni 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 fájlalba 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 **Események** 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 beállításai](#)ban.

A gyorsítótárzás időtartamának módosítása

Az Eszközfelügyelő összetevő regisztrálja a felügyelt eszközökkel kapcsolatos eseményeket, például egy eszköz csatlakoztatását és leválasztását, fájlolvasást eszközzől, 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 *gyorsítótárzás időtartamáig*, információkat tárol az eseményekről. Ha az eseményre vonatkozó információk gyorsítótárzva 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;
- alkalmazásengedély-ítélet ehhez a művelethez: engedélyezett vagy elutasított;
- a művelethez használt folyamat elérési útja;
- az elérni kívánt fájl.

A gyorsítótárzási időtartam megváltoztatása előtt [tiltsa le a Kaspersky Endpoint Security Önvédelmet](#). A gyorsítótárzási időtartam megváltoztatása után engedélyezze az Önvédelmet.

A gyorsítótárázási 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 percre 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 beállításában 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 ilyen 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 1000-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 *Tájékoztató* súlyossági szinttel rendelkeznek.

A Kaspersky Endpoint Security a következő korlátozásokkal rendelkezik a megbízható eszközökkel való munka során:

- A Kaspersky Endpoint Security adminisztrációs bővítmény 11.0.0–11.2.0 verziói nem tudnak együttműködni a megbízható eszközöknek a Kaspersky Endpoint Security 11.3.0 és 11.4.0 verzióiban létrehozott listájával. A


megbízható eszközök ezen verziókból származó listájának kezeléséhez az adminisztrációs bővítményt 11.3.0, illetve 11.4.0 verzióra kell frissíteni.

- A Kaspersky Endpoint Security adminisztrációs bővítmény 11.3.0–11.4.0 verziói nem tudnak együttműködni a megbízható eszközöknek a Kaspersky Endpoint Security 11.2.0 és korábbi verzióiban létrehozott listájával. Ahhoz, hogy ezek a verziók együttműködjenek a megbízható eszközök listájával, az alkalmazást a 11.3.0, illetve a 11.4.0 verzióra kell frissíteni. A helyzet leírását tartalmazó kérelmet a [Kaspersky CompanyAccount](#) oldalon keresztül is elküldheti a Terméktámogatásnak.
- A megbízható eszközök listájának a Kaspersky Endpoint Security 11.2.0 verziójából a 11.3.0 verzióba való áttelepítéséhez küldjön egy a helyzet leírását tartalmazó kérést a Terméktámogatásnak a [Kaspersky CompanyAccount](#) oldalon keresztül.

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 a **Kiválasztás** 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 megbízható listájához.
6. A **Megjegyzés** mezőben a megbízható eszközre vonatkozó minden lényeges információt megadhat.
7. Válassza ki azokat a felhasználókat vagy felhasználói csoportokat, akiknek engedélyezni szeretné a hozzáférést a megbízható eszközökhöz.
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 [aktíválva 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.
Eszközazonosító példája: 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 azonosítomaszk 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_ *.

Eszköz hozzáadása a megbízható eszközök listájához:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
6. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.
7. Válassza az **Értékek egyesítése örökléskor** 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 örökléskor az értékek egyesítése örökléskor 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.
8. Kattintson a **Hozzáadás** gombra, és válasszon módszert az eszköz megbízható listára történő felvételéhez.
9. Az eszközök szűréséhez válasszon egy eszköztípust az **Eszköztípus** legördülő listában (például: **Cserélhető meghajtók**).
10. A **Név/modell** mezőben adja meg az eszközazonosítót, a modellt (VID és a PID-azonosító) vagy a maszkot a választott hozzáadási módszernek 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 **Frissítés** gombra kattint. Ahhoz, hogy helyesen jelenítse meg az eszközök listáját, hozzáadhat eszközöket azonosítómaszk alapján.

11. Az eszközök szűréséhez a **Számítógépnév** 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.

12. Kattintson a **Frissítés** gombra.

A táblázatban szerepel a megadott szűrési feltételeknek megfelelő eszközök listája.

13. A nevük melletti jelölőnégyzettel válassza ki a megbízható eszközök listájára felvenni kívánt eszközöket.

14. A **Megjegyzés** mezőben írja le, hogy mi indokolja az eszközök felvételét a megbízható eszközök listájára.

15. Kattintson a **Kiválasztás** gombra, amely az **Engedélyezve a következő felhasználók és/vagy csoportok számára** mezőtől jobbra található.

16. Válasszon ki egy felhasználót vagy csoportot az Active Directory helyről, és erősítse meg a választását.

Alapértelmezés szerint a megbízható eszközök a „Mindenki” csoport számára érhetőek el.

17. 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 zárt 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 beállításában 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.
Ha a számítógépen már létezik egy lista a megbízható eszközökről, a Kaspersky Endpoint Security rákérdez, hogy törölje-e a meglévő listát, vagy új bejegyzéseket vegyen fel abba az XML-fájlból.
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 beállításában. 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.

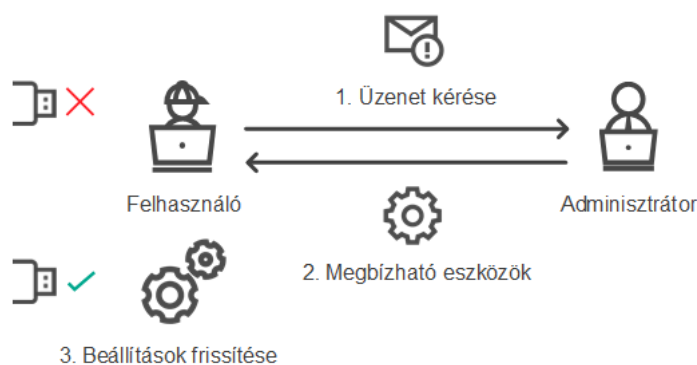
Ha online módban ad hozzáférést, az a következő lépésekből áll:

1. A felhasználó üzenetet küld a rendszergazdának, ami egy hozzáférési kérelmet tartalmaz.

2. A rendszergazda hozzáadja az eszközt a megbízható listához.

Hozzáadhat egy megbízható eszközt egy egyéni számítógépnek az adminisztrációs csoport rendszabályában vagy a helyi alkalmazásbeállításokban.

3. A rendszergazda frissíti a Kaspersky Endpoint Security beállításait a felhasználói számítógépen.



Vázlat az eszközök hozzáféréseinek 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 **Eszközfelügyelő** részben az **Ideiglenes hozzáférési kérelem engedélyezése** jelölőnégyzetet be kell jelölni.

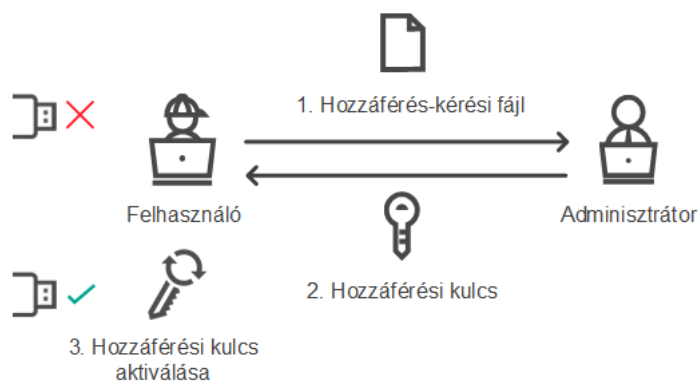
Ha átmeneti hozzáférést akar adni egy blokkolt eszköznek, de nem tudja [hozzáadni az eszközt a megbízható listához](#), akkor offline módban is hozzáférést adhat az eszközhez. Így még akkor is hozzáférést adhat egy blokkolt eszközhez, ha a számítógépen nincs hálózati hozzáférés, vagy akkor, ha a számítógép 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 hozzáféréseinek 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 következők:

1. Csatlakoztassa az eszközt a számítógéphez.

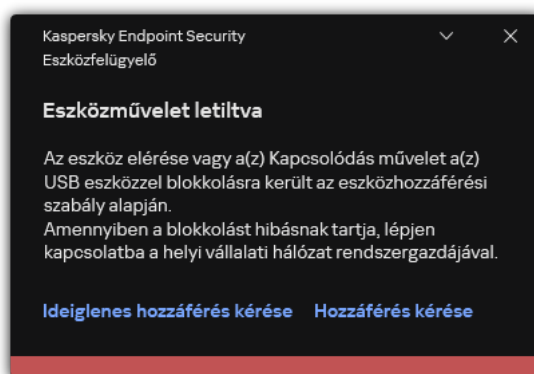
A Kaspersky Endpoint Security megjelenít egy értesítést, miszerint az eszköz elérést blokkolva van (lásd az alábbi ábrát).

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.

A rendszergazda üzenetet kap (amely egy elérési kérelem), például e-mailben. A felhasználói kérelmek feldolgozásáról szóló további információért lásd: [Kaspersky Security Center Súgó](#). Miután [hozzáadta az eszközt a megbízható listához](#) és frissítette a Kaspersky Endpoint Security beállításait a számítógépen, a felhasználó hozzáférést fog kapni az eszközhez.



Eszközfelügyelő értesítés

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 **Allow request for temporary access** jelölőnégyzetet be kell jelölni.

A blokkolt eszközök elérésére irányuló felhasználói kérelmek a következők:

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.

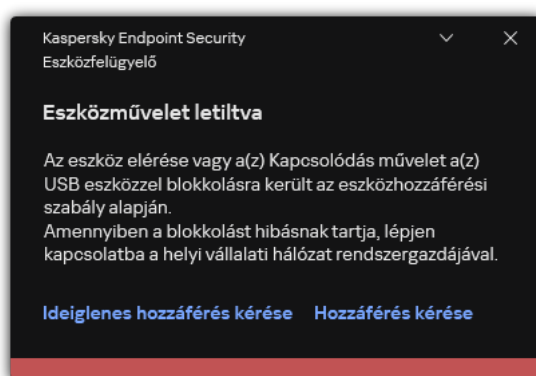
3. Válassza ki a csatlakoztatott eszközök listáján azt az eszközt, amelyhez hozzáférést szeretne kapni.

4. Kattintson a **Hozzáférés-kérési fájl előállítás** elemre.

5. Adja meg a **Hozzáférés időtartama** mezőben azt az időszakot, ameddig hozzáférést szeretne az eszközhez.

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 eszközhez 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. A megnyíló ablakban válassza az **Eszközfelügyelő** lapot.
7. Kattintson a **Tallózás** gombra, és töltsse 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 **Devices** → **Managed 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 az **Device Control** szakaszt.
5. Kattintson a **Browse** gombra, és töltsse 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 [adj a 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. 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.

Sablonok állnak rendelkezésre az eszközökhöz való hozzáférés blokkolásáról és az eszközök tartalmán végzett műveletek tiltásáról szóló üzenetekhez és a rendszergazda részére elküldött üzenethez. Az üzenetsablonokat módosítani lehet.

Az Eszközfelügyelő üzenetsablonjainak szerkesztése:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakban válassza a **Biztonsági felügyelet** → **Eszközfelügyelő** lehetőséget.
3. Az **Üzenetsablonok** részen konfigurálja a sablonokat az Eszközfelügyelő 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. 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.
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 kapcsolaton;

- 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 Anomáliafigyelő

Ez az összetevő csak a Kaspersky Endpoint Security for Business Advanced és a Kaspersky Total Security for Business termékben érhető el. A Kaspersky Endpoint Security for Business további részleteiért látogasson el a [Kaspersky webhelyére](#).

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 Anomáliafigyelő összetevő megfigyeli és letiltja azokat a tevékenységeket, amelyek nem megszokottak a cég hálózatán található számítógépeken. Az Adaptív Anomáliafigyelő egy szabálycsoport alapján követi nyomon a nem megszokott viselkedést (például a *Microsoft PowerShell indítása egy Office-alkalmazásból* szabályt). A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján. Konfigurálhatja, hogy az Adaptív Anomáliafigyelő 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 Anomáliafigyelő beállításai

Az Adaptív Anomáliafigyelő beállításai a következő lépésekből állnak:

1. Az Adaptív Anomáliafigyelő betanítása.

Miután engedélyezte az Adaptív Anomáliafigyelőt, a szabályok *tanuló módban* vannak. A tanulás során az Adaptív Anomáliafigyelő 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 Anomáliafigyelő 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 **Triggering of rules in Smart Training state** gyűjteményben.

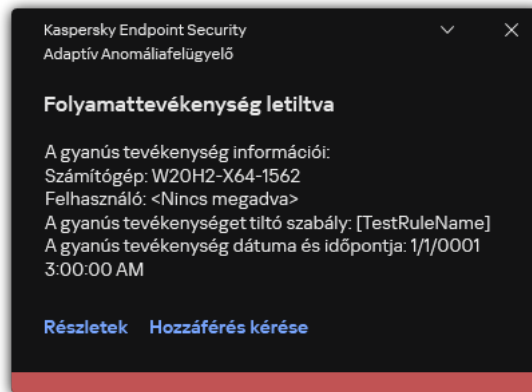
2. A szabálykiváltó jelentés értelmezése.

A [szabálykiváltó jelentést](#) vagy a **Triggering of rules in Smart Training state** gyűjteményt a rendszergazdának kell értelmezni. A rendszergazda ezt követően kiválaszthatja az Adaptív Anomáiafelügyelő 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 Anomáiafelügyelő konfigurálása valós időben történik. Az Adaptív Anomáiafelügyelő konfigurálása a következő csatornákon történik:

- Az Adaptív Anomáiafelügyelő 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 Anomáiafelügyelő működését, hogy áttekintette a szabálykiváltó jelentést és a **Triggering of rules in Smart Training state** gyűjtemény tartalmát. Javasoljuk, hogy ellenőrizze a szabálykiváltó jelentést és a **Triggering of rules in Smart Training state** gyűjtemény tartalmát.

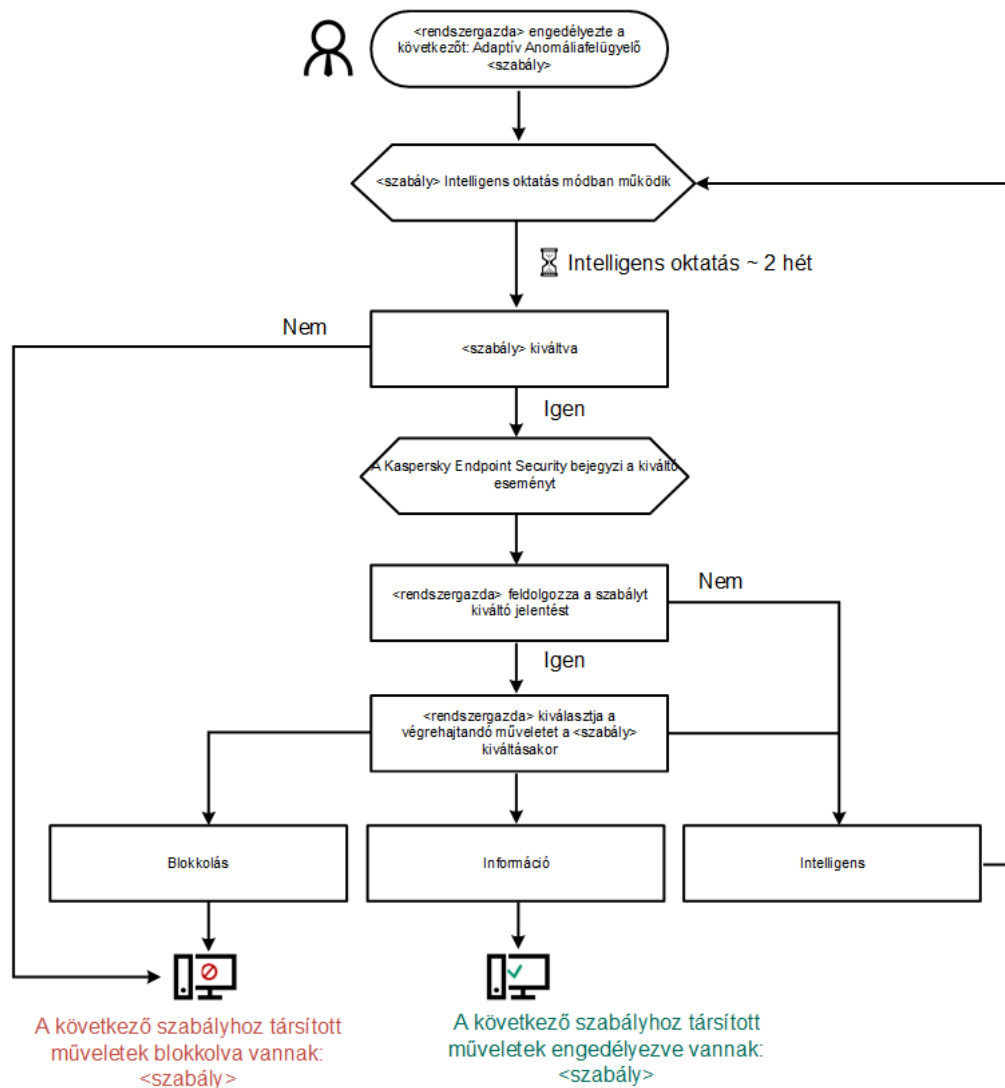
Amikor egy rosszindulatú alkalmazás megpróbál műveletet végrehajtani, a Kaspersky Endpoint Security letiltja a műveletet és értesítést jelenít meg (lásd az alábbi ábrát).



Adaptív Anomáiafelügyeleti értesítés

Adaptive Anomaly Control operating algorithm

A Kaspersky Endpoint Security a következő algoritmus alapján dönti el, hogy engedélyezze vagy letiltja az adott szabályhoz társított műveletet (lásd az alábbi ábrán).




Adaptive Anomaly Control operating algorithm

Az Adaptív Anomáiafelügyelő engedélyezése és letiltása

Az Adaptív Anomáiafelügyelő engedélyezve van alapértelmezésben.

Az *Adaptív Anomáiafelügyelő* be- és kikapcsolása:


1. Kattintson a [fő alkalmazásablakban](#) a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáiafelügyelő** lehetőséget.
3. Az **Adaptív Anomáiafelügyelő** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ennek eredményeképpen az Adaptív Anomáiafelügyelő betanítási üzemmódba lép. A betanítás során az Adaptív Anomáiafelügyelő figyeli a szabályok indítását. A betanítás befejeztével az Adaptív Anomáiafelügyelő blokkolni kezdi azokat a műveleteket, amelyek nem jellemzőek a vállalat hálózatában lévő számítógépekre.

Ha a vállalat új eszközöket kezdett el használni, és az Adaptív Anomáiafelügyelő blokkolja ezen eszközök műveleteit, akkor visszaállíthatja a betanítási mód eredményeit, és megismételheti a betanítást. Ehhez [meg kell változtatnia a szabály indításakor végrehajtandó műveletet](#) (például beállítás **Értesítés** műveletre). Ezután újra engedélyeznie kell a betanítási módot (állítsa be az **Intelligens** értéket).


Adaptív Anomáiafelügyeleti szabály engedélyezése és letiltása

Egy Adaptív Anomáiafelügyeleti szabály engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáiafelügyelő** lehetőséget.
3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.
Az Adaptív Anomáiafelügyeleti szabálylista nyílik meg.
4. A táblázatban válassza ki a szabálykészletet (például *Az Office-alkalmazások tevékenysége*), és bontsa ki a készletet.
5. Jelöljön ki egy szabályt (például a *Windows PowerShell elindítása az irodai alkalmazásokból*).
6. Az **Állapot** oszlopban lévő kapcsolóval engedélyezze vagy tiltsa le az Adaptív Anomáiafelügyelő szabályát.
7. Mentse el a módosításokat.

Az Adaptív Anomáiafelügyeleti szabály kiváltásakor végrehajtott művelet módosítása

Az Adaptív Anomáiafelügyeleti szabály kiváltásakor végrehajtott művelet szerkesztése:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáiafelügyelő** lehetőséget.
3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.
Az Adaptív Anomáiafelügyeleti szabálylista nyílik meg.
4. Jelöljön ki egy szabályt a táblázatban.
5. Nyomja meg a **Szerkesztés** gombot.
Az Adaptív Anomáiafelügyeleti 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 Anomáiafelügyeleti szabály Intelligens tanulás állapotban működik a Kaspersky szakemberei által megadott ideig. Ebben a módban egy Adaptív

Anomáiafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security engedélyezi a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a Kaspersky Security Center felügyeleti kiszolgáló **Intelligens tanulás állapotban kiváltott szabályok** tárolójában. Ha véget ér az Intelligens tanulás állapothoz beállított időtartam, a Kaspersky Endpoint Security blokkolja az Adaptív Anomáiafelügyeleti szabályok tevékenységeit, és naplóz egy bejegyzést a tevékenységről.

- **Blokkolás.** Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáiafelügyeleti szabály kiváltásakor a Kaspersky Endpoint Security blokkolja a szabály alá tartozó tevékenységet, és bejegyezi a naplóba a tevékenységre vonatkozó információkat.
- **Értesítés.** Ha ez a művelet van kiválasztva, akkor egy Adaptív Anomáiafelügyeleti 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 Anomáiafelügyeleti szabályhoz

1000 kizárásnál többet nem hozhat létre az Adaptív Anomáiafelügyeleti szabályokból. Nem javasolt 200 kizárásnál többet létrehozni. A használt kizárások számának csökkentéséhez javasolt maszkokat használni a kizárások beállításában.

Az Adaptív Anomáiafelügyeleti 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 cél fájl, a Böngésző pedig a célobjektum.

Kizárás létrehozása Adaptív Anomáiafelügyeleti szabályhoz:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáiafelügyelő** lehetőséget.
3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.
Az Adaptív Anomáiafelügyeleti szabálylista nyílik meg.
4. Jelöljön ki egy szabályt a táblázatban.
5. Nyomja meg a **Szerkesztés** gombot.
Az Adaptív Anomáiafelügyeleti 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.

Az Adaptív Anomáiafelügyelő 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.** Fájl hash-kód.
- **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` fájllelési útvonal, amely parancsfájl vagy makró használatával indítja el a célfolyamatokat.

Megadhat egyéb objektumokat a kizáráshoz, például webcímekeket, 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.** Fájl hash-kód.

Az Adaptív Anomáiafelügyeleti 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.** Fájl hash-kód.
- **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.** Fájl hash-kód.

Az Adaptív Anomáiafelügyeleti 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 Anomáiafelügyeleti 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 Anomáiafelügyelő** lehetőséget.
3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.
Az Adaptív Anomáiafelügyeleti 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 szabályok listájának importálása:
 - a. Kattintson az **Importálás** 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 Anomáiafelügyeleti szabályok frissítéseinek alkalmazása

Új Adaptív Anomáiafelügyeleti szabályok adhatók hozzá a szabályok táblázatához, és a meglévő Adaptív Anomáiafelügyeleti szabályok törölhetők a szabályok táblázatából a víruskereső-adatbázisok frissítésekor. A Kaspersky Endpoint Security megkülönbözteti a táblázatból törölni, vagy ahhoz hozzáadni kívánt Adaptív Anomáiafelügyeleti 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 törölendő Adaptív Anomáiafelügyeleti szabályokat, és a *Letiltott* állapotot rendeli hozzájuk. E szabályok beállításainak módosítása nem lehetséges.

Az Adaptív Anomáiafelügyeleti szabályok frissítéseinek alkalmazása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáiafelügyelő** lehetőséget.
3. A **Szabályok** blokkban kattintson a **Szabályok szerkesztése** gombra.
Az Adaptív Anomáiafelügyeleti szabálylista nyílik meg.

4. Az ablakban kattintson a **Frissítések jóváhagyása** gombra.

A **Frissítések elfogadása** gomb elérhető, ha van elérhető frissítés az Adaptív Anomáiafelügyeleti szabályokhoz.

5. Mentse el a módosításokat.

Adaptív Anomáiafelügyelő üzenetsablonok szerkesztése

Ha egy felhasználó megpróbál végrehajtani egy tevékenységet, amit blokkolnak az Adaptív Anomáiafelügyeleti 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 érhetők el a potenciálisan rosszindulatú tevékenységek blokkolásáról szóló üzenetekhez és a rendszergazdának küldött üzenetekhez. Az üzenetsablonokat módosítani lehet.

Üzenetsablonok szerkesztése:

1. Kattintson a fő alkalmazásablakban a  gombra.

2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáiafelügyelő** lehetőséget.

3. A **Sablonok** blokkban konfigurálja a sablonokat az Adaptív Anomáiafelügyelő üzeneteihez:

- **Üzenet a blokkolásról.** Üzenetsablon, ami akkor jelenik meg a felhasználónak, amikor aktiválódik az Adaptív Anomáiafelügyelő 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.

4. Mentse el a módosításokat.

Az Adaptív Anomáiafelügyelő jelentéseinek megtekintése

Az Adaptív Anomáiafelügyelő jelentéseinek megtekintéséhez:

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. A munkaterületen válassza ki a **Policies** lapot.

4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.

5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Adaptív Anomáliafelügyelő** lehetőséget.

Az ablak jobb oldali részén megjelennek a Adaptív Anomáliafelügyelő összetevő beállításai.

6. Végezze el az alábbiak egyikét:

- Ha meg akar tekinteni egy jelentést az Adaptív Anomáliafelügyeleti szabályok beállításairól, kattintson az **Adaptív Anomáliafelügyelői szabályok állapotáról szóló jelentés** elemre.
- Ha meg akar tekinteni egy jelentést az Adaptív Anomáliafelügyeleti szabályok kiváltásáról, kattintson a **Jelentés az Adaptív Anomáliafelügyelő aktívan alkalmazott szabályairól** elemre.

7. Megkezdődik a jelentés előállítási folyamata.

A jelentés egy új ablakban jelenik meg.

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 létrehozása érdekében a következő feltételeket használhatja: KL kategória (például *Böngészők*), fájlkivonat, alkalmazásforgalmazó 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”.

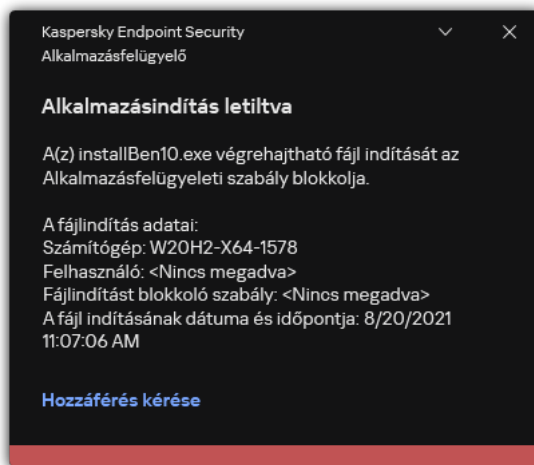
3. [Az Alkalmazásfelügyelő módjának kiválasztása.](#)

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.
- **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.

E olvashatja 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.

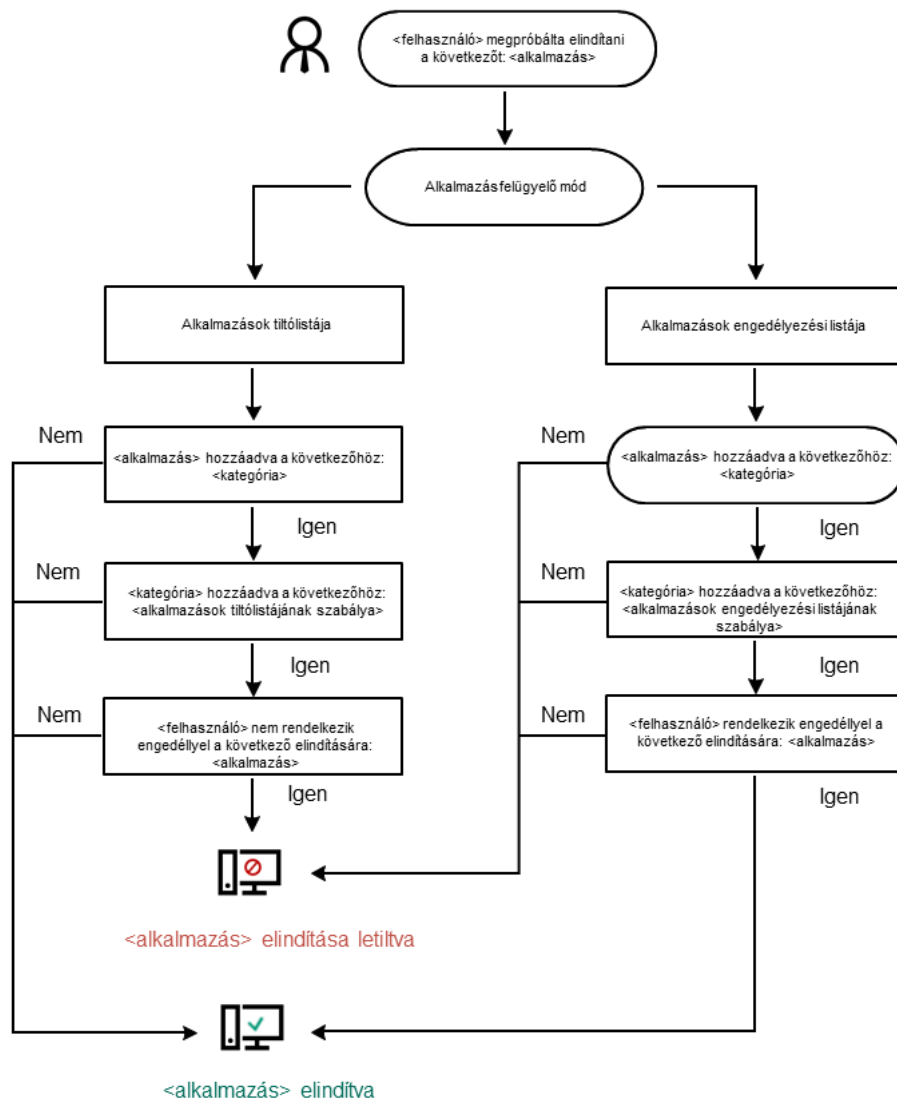
A Kaspersky Security Center azonban olyan eszközöket is kínál, amelyek a Kaspersky Endpoint Security helyi felületén nem találhatóak meg, köztük az alábbi feladatokhoz szükséges eszközöket:

- [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 algoritmus

A Kaspersky Endpoint Security algoritmust használva hoz döntést egy adott alkalmazás elindításáról (részletek a lentebbi ábrán).



Alkalmazásfelügyelő műveleti algoritmus

Az Alkalmazásfelügyelő funkciók korlátozásai

Az Alkalmazásfelügyelő összetevő működése az alábbi esetekben korlátozott:

- Az alkalmazás verziófrissítésekor az Alkalmazásfelügyelő összetevő beállításainak importálása nem támogatott.
- Az alkalmazás verziójának frissítésekor az Alkalmazásfelügyelő összetevő beállításainak importálása csak akkor támogatott, ha a Kaspersky Endpoint Security 10 Service Pack 2 for Windows vagy egy újabb verzió frissítése történik a Kaspersky Endpoint Security 11.8.0 for Windows verzióra.

Ha a Kaspersky Endpoint Security 10 Service Pack 2 for Windows-tól eltérő alkalmazásverzió lett frissítve, az összetevő működési állapotának helyreállítása érdekében új Alkalmazásfelügyelő beállításokat kell konfigurálni.

- 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 applications \ Alkalmazások, a KSN-ben nyilvántartott hírnév alapján megbízhatóak** eltérhet attól függően, hogy van-e kapcsolat a KSN kiszolgálóival.

- A Kaspersky Security Center adatbázisában 150 000 feldolgozott fájlra vonatkozó adat tárolható. E bejegyzésszám elérével 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.

Az Alkalmazásfelügyelő engedélyezése és letiltása

Alapértelmezés szerint az Alkalmazásfelügyelő le van tiltva.


Az Alkalmazásfelügyelő engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
3. Az **Alkalmazásfelügyelő** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
4. Mentse el a módosításokat.

Ennek eredményeképpen, ha az Alkalmazásfelügyelő engedélyezve van, az alkalmazás továbbítja a futó futtatható fájlokra vonatkozó információkat a Kaspersky Security Centernek. A futó futtatható fájlok listáját a Kaspersky Security Center **Executable files** mappájában tekintheti meg. Ha az összes futtatható fájlról szeretne információt kapni, és nem csak futtatni a futtatható fájlokat, futtassa a [Leltár feladatot](#).

Az Alkalmazásfelügyelő módjának kiválasztása

Az Alkalmazásfelügyelő módjának kiválasztása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
3. Válassza ki a következő lehetőségek egyikét az **Alkalmazásindítás vezérlésének módja** részben:
 - **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.

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.

A kiválasztott módban létrehozott összes szabály a módváltást követően mentésre kerül, így ismét felhasználható. Az ezen szabályok használatához való visszatéréshez csak annyit kell tennie, hogy kiválasztja a szükséges módot.

4. A **Művelet blokkolt alkalmazások indításakor** részben válassza ki azt a műveletet, amelyet az összetevő akkor végez el, ha egy felhasználó megpróbál egy, az Alkalmazásfelügyeleti szabályok által blokkolt alkalmazást elindítani.
5. Jelölje be a **DLL-modulok betöltésének vezérlése** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security a DLL-modulok betöltését is figyelje, amikor a felhasználók alkalmazásokat indítanak el.

A modullal és az azt betöltő alkalmazással kapcsolatos információk bekerülnek egy jelentésbe.

A Kaspersky Endpoint Security kizárólag a jelölőnégyzet bejelölését követően betöltött DLL modulokat és illesztőprogramokat figyel. Ha azt szeretné, hogy a Kaspersky Endpoint Security az összes DLL-modult és illesztőprogramot – így a Kaspersky Endpoint Security indítása előtt betöltötteket is – figyelje, akkor indítsa újra a számítógépet a jelölőnégyzet bejelölését követően.

Amikor engedélyezi a DLL-modulok és illesztőprogramok betöltésének vezérlését, győződjön meg arról, hogy az Alkalmazásfelügyelő beállításában engedélyezve van a következő szabályok egyike: **Golden Image** szabály, illetve egy másik szabály, amely tartalmazza a Megbízható tanúsítványok 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.

Javasolt bekapcsolni a [jelszóvédelem](#) lehetőséget az alkalmazásbeállítások megadásához, így ki lehet kapcsolni a szabályokat blokkoló kritikus DLL modulokat és illesztőprogramokat anélkül, hogy módosítaná a Kaspersky Security Center rendszabály beállításait.

6. Mentse el a módosításokat.

Munka az Alkalmazásfelügyeleti szabályokkal az alkalmazás felületén

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 összetevő 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.
- **Tesztelés.** 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 szabály hozzáadása

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 a **Add** 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. Állítsa össze vagy szerkessze azon felhasználók és / vagy felhasználói csoportok listáját, akik számára engedélyezett vagy nem engedélyezett a szabály kiváltó feltételeinek megfelelő alkalmazások elindítása. Ehhez kattintson az **Alanyok és jogaik** táblázatban a **Hozzáadás** gombra.

Alapértelmezés szerint a felhasználók listájára a **Mindenki** érték kerül. A szabály minden felhasználóra vonatkozik.

Ha a táblázatban nincs megadva felhasználó, a szabályt nem lehet menteni.

- d. Az **Alanyok 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 programok futtatását az olyan felhasználóknál, akik nem szerepelnek az **Alanyok és jogaik** táblázatban, és nem tagjai az **Alanyok 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 **Alanyok és jogaik** táblázatban, és nem is tartoznak az **Alanyok és jogaik** táblázatban megadott felhasználói csoportok valamelyikébe.

f. Ha azt szeretné, hogy a Kaspersky Endpoint Security a szabályt kiváltó feltételeknek megfelelő alkalmazásokat olyan megbízható frissítőknek tekintse, melyek más utólag futtatható fájlokat hoznak létre, jelölje be a **Megbízható frissítéstelepítők** jelölőnégyzetet.

6. A **Feltételek** lapon [hozza létre](#) vagy módosítsa a befogadási feltételeket a szabály kioldásához.


7. A **Kizárások** 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.

Alkalmazásfelügyeleti szabályt kiváltó feltétel hozzáadása

Alkalmazásfelügyeleti szabályt kiváltó új feltétel hozzáadása:

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** 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 közősek 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 Alkalmazásfelügyeleti szabály cserélhető meghajtón futó fájlokra vonatkozik.

- **Feltételek a megadott mappában található fájlok tulajdonságai alapján.** Az Alkalmazásfelügyeleti 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 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 **Tárgy** kritériumokat alkalmazni. 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 feloldása** gombra.

Alkalmazásfelügyeleti szabály állapotának módosítása

Alkalmazásfelügyeleti szabály állapotának módosítása:

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.
 - **Tesztelés.** 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.

Az Alkalmazásfelügyeleti szabályok kezelése a Kaspersky Security Centerben

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 összetevő 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.
- **Tesztelés.** 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.

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.

A vállalati hálózatokon lévő számítógépek által használt alkalmazásokra vonatkozó információk az **Applications registry** mappában és a **Végrehajtható fájlok** mappában található. Az **Alkalmazások jegyzéke** mappa és a **Végrehajtható fájlok** mappa a Kaspersky Security Center Adminisztrációs Konzol fájának **Alkalmazáskezelés** mappájában található.

Az **Alkalmazások jegyzéke** mappa tartalmazza a számítógépen telepített [Hálózati ügynök](#) által észlelt alkalmazások listáját.

A **Végrehajtható fájlok** mappa az ügyfélszámítógépeken valaha elindított, illetve a Kaspersky Endpoint Security leltározási feladata során észlelt összes végrehajtható fájl listáját tartalmazza.

Az alkalmazással és végrehajtható fájljaival kapcsolatos általános információk és számítógépek listájának megtekintéséhez, amelyeken az alkalmazás telepítve van, nyissa meg az **Applications registry** mappában vagy a **Végrehajtható fájlok** mappában kiválasztott alkalmazás tulajdonságainak ablakát.

Az alkalmazástulajdonságok ablak megnyitásához az Applications registry mappában:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Az Adminisztrációs Konzol fájában válassza a **További** → **Application management** → **Applications registry** elemet.
3. Válasszon ki egy alkalmazást.
4. Az alkalmazás helyi menüjében válassza ki a **Tulajdonságok** elemet.

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 a **További** → **Application management** → **Végrehajtható fájlok** mappát.
3. Válasszon ki egy végrehajtható fájlt.
4. A végrehajtható fájl helyi menüjében válassza ki a **Tulajdonságok** elemet.

Alkalmazáskategóriák létrehozása

A nagyobb kényelem érdekében az Alkalmazásfelügyeleti szabályok létrehozása során létrehozhat alkalmazáskategóriákat.

Javasoljuk, hogy hozzon létre egy „Munkaal alkalmazások” 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:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában a **További** → **Alkalmazáskezelés** → **Alkalmazáskategóriák** mappát.
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.** Ha ezt a kategóriatípust választotta, az „Alkalmazások kategóriához való hozzáadásának feltételeinek beállítása” és az „Alkalmazások kategóriából való kizárásának feltételeinek beállítása” lépésben meghatározhatja a kritériumokat, melyek végrehajtható fájljait tartalmazni fogja a kategória.
- **Category that includes executable files from selected devices.** Ha ezt a kategóriatípust választotta, a „Beállítások” lépésnél megadhat egy számítógépet, melynek végrehajtható fájljait a rendszer automatikusan beleveszi a kategóriába.

- **Kategória a megadott mappák végrehajtható fájljaival.** Ha ezt a kategóriatípust választotta, a „Tárolómappa” 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

Ez a lépés akkor elérhető, 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 thumbprint** 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 „Irodai alkalmazások” néven ismert KL kategória például a Microsoft Office csomag alkalmazásait, az Adobe Acrobat alkalmazást és másokat tartalmaz.

Kiválaszthatja az összes KL kategóriát, hogy létrehozzanak egy kiterjesztett listát a megbízható alkalmazásokról.

- **Specify path to application.** 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 thumbprint** paraméter.

- **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 elérhető, 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 a „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 közősek a témaattribútumai. 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.

Kiválaszthatja az összes KL kategóriát, hogy létrehozzanak egy kiterjesztett listát a megbízható alkalmazásokról.

- **Specify path to application.** 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 elérhető, ha kiválasztotta a **Category that includes executable files from selected devices** kategóriatípust.

Ennél a lépésnél kattintson a **Hozzáadás** 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:

- A Kaspersky Security Center hash függvény kiszámításának algoritmus. Az algoritmus kiválasztásához be kell jelölnie legalább az egyik jelölőnégyzetet:
 - **Calculate SHA-256 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).**
- **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.

- **Scan period (h)** mező. Ebben a mezőben megadhatja az időtartamot (órában), melynek lejártá után a Kaspersky Security Center törli az alkalmazáskategóriát, majd hozzáadja az adott számítógépek végrehajtható fájljait, melyek a **Executable files** mappában találhatóan.

A mező akkor használható, ha az **Synchronize data with Administration Server repository** jelölőnégyzet ki van jelölve.

Step 6. Tárhely mappa

Ez a lépés akkor elérhető, ha kiválasztotta a **Category that includes executable files from a specific folder** kategóriatípust.

Ennél a lépésnél kattintson a **Tallózás** gombra, majd adja meg a mappát, melyben a Kaspersky Security Center végrehajtható fájlokat fog keresni, hogy automatikusan hozzáadjon alkalmazásokat az alkalmazáskategóriához.

Ennél a lépésnél beállíthatja a következő beállításokat is:

- **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.

- **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.

- A Kaspersky Security Center hash függvény kiszámításának algoritmus. Az algoritmus kiválasztásához be kell jelölnie legalább az egyik jelölőnégyzetet:

- **Calculate SHA-256 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).**

- **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.

- **Scan period (h)** 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.

Ez a mező akkor elérhető, ha a **Force folder scan for changes** jelölőnégyzet be van jelölve.

7. lépés Egyéni kategória létrehozása

Lépjen ki a varázslóból.

Futtatható fájlok hozzáadása a Futtatható fájlok mappából az alkalmazáskategóriákba

A **Végrehajtható fájlok** 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 végrehajtható fájlok a Végrehajtható fájlok mappából az alkalmazáskategóriákba történő hozzáadásához:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában a **További** → **Application management** → **Végrehajtható fájlok** mappát.
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 megnyitott ablakban végezze el az alábbiak egyikét:
 - 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** részben válasszon egyet a következő lehetőségek közül:
 - **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).**
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 **Események** lapot.
3. Válassza ki az Alkalmazásfelügyelő összetevő működéséhez köthető eseményeket ([Viewing events resulting from operation of the Application Control component](#), [Viewing events resulting from test operation of the Application Control component](#)) az **Event selections** legördülő listából.

4. Kattintson a **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** részben válasszon egyet a következő lehetőségek közül:
 - **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 vagy módosítása a Kaspersky Security Center használatával

Alkalmazásfelügyeleti szabály hozzáadása vagy módosítása a Kaspersky Security Center segítségével:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.

6. Végezze el az alábbiak egyikét:

- Szabályt az **Add** gombra kattintva adhat meg.
- Ha meglévő szabályt szeretne szerkeszteni, válassza ki a listáról, és kattintson a **Szerkesztés** gombra.

Megnyílik az **Alkalmazásfelügyeleti szabály** ablak.

7. Végezze el az alábbiak egyikét:

- Ha létre akar hozni egy új kategóriát:
 - a. Kattintson az **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.

8. Kattintson az **Alanyok és jogaik** táblázatban a **Hozzáadás** gombra.

9. A megnyitott ablakban adja meg azon felhasználók és/vagy felhasználói csoportok listáját, akiknél be szeretné állítani a kiválasztott kategóriába tartozó alkalmazások indítási jogosultságát.

10. Az **Alanyok és a 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 **Tiltás** jelölőnégyzetet.

11. 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 **Tárgy** oszlopban, és nem is tartozik a **Tárgy** oszlopban megadott felhasználói csoportok valamelyikébe.

12. 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.

13. Mentse el a módosításokat.

Az Alkalmazásfelügyeleti szabályok állapotának módosítása a Kaspersky Security Center segítségével

Alkalmazásfelügyeleti szabály állapotának módosítása:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.
6. 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 szabályt az Alkalmazásfelügyelő bekapcsolt állapotában felhasználja.
 - **Ki.** Ez az állapot azt jelenti, hogy a szabályt az Alkalmazásfelügyelő bekapcsolt állapotában mellőzi.
 - **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.
7. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
6. Az Alkalmazásfelügyeleti szabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt szabályokat. Több pont 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. 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.
8. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** szakaszt.
5. Kattintson a **Rules Lists Settings** hivatkozásra.
6. Válassza ki a szabályok listáját: alkalmazás tiltólista vagy engedélyezési lista.
7. Az Alkalmazásfelügyeleti szabályok listájának 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.
8. 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.
9. Mentse el a módosításokat.

Az Alkalmazásfelügyeleti szabályok tesztelése a Kaspersky Security Center segítségével

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-szabályok tesztelésének be- és kikapcsolása a Kaspersky Security Centerben:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.
6. 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.
7. Végezze el az alábbiak egyikét:
 - Ha szeretné engedélyezni az Alkalmazásfelügyeleti szabályainak tesztelését, válassza a **Teszt szabályok** 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.
8. Mentse el a módosításokat.

Az Alkalmazásfelügyelő összetevő testtműködéséből 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 **Események** lapot.
3. Kattintson a **Create a selection** gombra.
4. A megnyíló ablakban válassza az **Events** szakaszt.
5. Kattintson a **Clear all** gombra.
6. Jelölje be az **Events** táblázatban az **Alkalmazásindítás letiltva teszt üzemmódban** és **Alkalmazásindítás engedélyezve teszt üzemmódban** jelölőnégyzeteket.

7. Mentse el a módosításokat.
8. Az **Event selections** legördülő listán válassza ki a létrehozott választást.
9. Kattintson a **Run selection** gombra.

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 a **Reports** lapot.
3. Kattintson a **New report template** gombra.
Ekkor elindul az új Jelentéssablon varázsló.
4. Kövesse a Jelentéssablon-varázsló utasításait. Válassza ki a **Selecting the report template type** lépésben az **Other** → **Report on prohibited applications in test mode** lehetőséget.
Miatán 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 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 **Események** lapot.
3. Kattintson a **Create a selection** gombra.
4. A megnyíló ablakban válassza az **Events** szakaszt.
5. Kattintson a **Clear all** gombra.
6. Jelölje be az **Events** táblázatban az **Alkalmazásindítás letiltva** jelölőnégyzetet.
7. Mentse el a módosításokat.
8. Az **Event selections** legördülő listán válassza ki a létrehozott választást.
9. Kattintson a **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 a **Reports** lapot.
3. Kattintson a **New report template** gombra.
Ekkor elindul az új Jelentéssablon varázsló.
4. Kövesse a Jelentéssablon-varázsló utasításait. Válassza ki a **Selecting the report template type** lépésben 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.

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.

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 **Tesztelés** 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.

Alkalmazástevékenység-figyelő

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 Behatólásmegelőző 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.

Megnyílik az **Alkalmazások tevékenysége** ablak. 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 rejtetni 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályok ablakában válassza az **Általános beállítások** → **Felület** lehetőséget.
6. Használja **Hide Application Activity Monitor section** jelölőnégyzetet az eszközhöz való hozzáférés engedélyezéséhez vagy visszavonásához.
7. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Felület** helyre.
5. Használja **Hide Application Activity Monitor section** jelölőnégyzetet az eszközhöz való hozzáférés engedélyezéséhez vagy visszavonásához.
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 `Fo1der` 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. 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.

Külön sablonok állnak rendelkezésre az olyan üzenethez, amely az alkalmazás indításának blokkolásakor jelenik meg, illetve amelyet a rendszergazda kap. Az üzenetsablonokat módosítani lehet.

Üzenetsablonok szerkesztése:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Biztonsági felügyelet** → **Alkalmazásfelügyelő** lehetőséget.
3. A **Sablonok** blokkban konfigurálja a sablonokat az Alkalmazásfelügyelő üzeneteihez:

- **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 hozzáféréseinek 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.

4. Mentse el a módosításokat.

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 Alkalmazásmappa feltételnek a használata kockázatos lehet, mivel a megadott mappában lévő összes alkalmazás elindítható lesz. Ajánlott alkalmazni a szabályokat – amik az Alkalmazás mappa 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 [Végrehajtható fájlok](#) 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 **Tárgy** 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 kategóriasabályokban 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 „Alkalmazásmappa” feltétellel, és adja meg az adott mappa elérési útját. Ezután hozzon létre egy engedélyezőszabályt, és válassza ki ezt a kategóriát.

Ennek az Alkalmazásmappa feltételnek a használata kockázatos lehet, mivel a megadott mappában lévő összes alkalmazás elindítható lesz. Ajánlott alkalmazni a szabályokat – amik az Alkalmazás mappa 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 teszteléséből 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 kéréseit 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](#) és a [Web védelem](#) összetevők figyelik 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.


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.
3. A **Figyelt portok** részben válassza ki a **Csak a kijelölt hálózati portok figyelése** elemet.
4. Mentse el a módosításokat.

A figyeltek hálózati portok listájának létrehozása

A figyeltek hálózati portok listájának létrehozása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
3. A **Figyeltek portok** részben válassza ki a **Csak a kijelölt hálózati portok figyelése** elemet.
4. Kattintson a **Kiválasztás** 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 a **Add** 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 figyel.

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 **Figyeltek portok** részben válassza ki a **Csak a kijelölt hálózati portok figyelése** 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 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 a **Kiválasztás** gombra.

Ez megnyitja az alkalmazások listáját, amelyekenél 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 a **Add** 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A házirend ablakban válassza az **Általános beállítások** → **Hálózati beállítások** lehetőséget.
6. A **Figyelt portok** részben válassza ki a **Csak a kijelölt hálózati portok figyelése** elemet.
7. Kattintson a **Beállítások** gombra.

Megnyílik a **Hálózati portok** ablak. A **Hálózati portok** ablakban megjelenik az e-mailekhez és a hálózati forgalomhoz általában használt hálózati portok listája. A hálózati portok listája megtalálható a Kaspersky Endpoint Security csomagjában.
8. 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 megnyitott 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.
9. 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.
10. 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.

11. Azon alkalmazások listájának importálása, amelyek portjait a Kaspersky Endpoint Security figyeli:

a. Az alkalmazások listájában kattintson az **Importálás** gombra.

A megnyitott 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.

12. Mentse el a módosításokat.

[A figyelt portok listáinak exportálása/importálása a Web Console-ban és a Cloud Console-ban](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Hálózati beállítások** elemhez.
5. Hálózati portok listájának exportálása:
 - a. A **Figyelt portok** részben válassza ki a **Csak a kijelölt hálózati portok figyelése** elemet.
 - b. Kattintson a **kiválasztott N port** hivatkozására.
Megnyílik a **Hálózati portok** ablak. A **Hálózati portok** 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 megnyitott 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 **Figyelt portok** szakaszban jelölje be a **A megadott alkalmazások figyelése minden porton** jelölőnégyzetet.
 - b. Kattintson a **kiválasztott N alkalmazás** hivatkozására.
 - 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 **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.

8. Azon alkalmazások listájának importálása, amelyek portjait a Kaspersky Endpoint Security figyeli:

a. Az alkalmazások listájában kattintson az **Importálás** gombra.

A megnyitott 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.

Jelszóvédelem

Egy-egy számítógépet több, a számítógéphez különböző méretékben 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.

- 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 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

Biztosan módosítja a beállításokat?

Felhasználónév:

A felhasználónév alapértelmezett értéke: KLAdmin.

Jelszó megadása:

Ne kérjen megerősítést a következő során:

Nincs kijelölve

A beviteli nyelvek közötti váltáshoz használja az ALT+SHIFT bil **ENU**

Megerősítés Mégse

Kaspersky Endpoint Security elérési jelszó kérése

Felhasználónév és jelszó

A Kaspersky Endpoint Security eléréséhez meg kell adnia a tartományfiók bejelentkezési adatait. A jelszóvédelem a következő fiókokat támogatja:

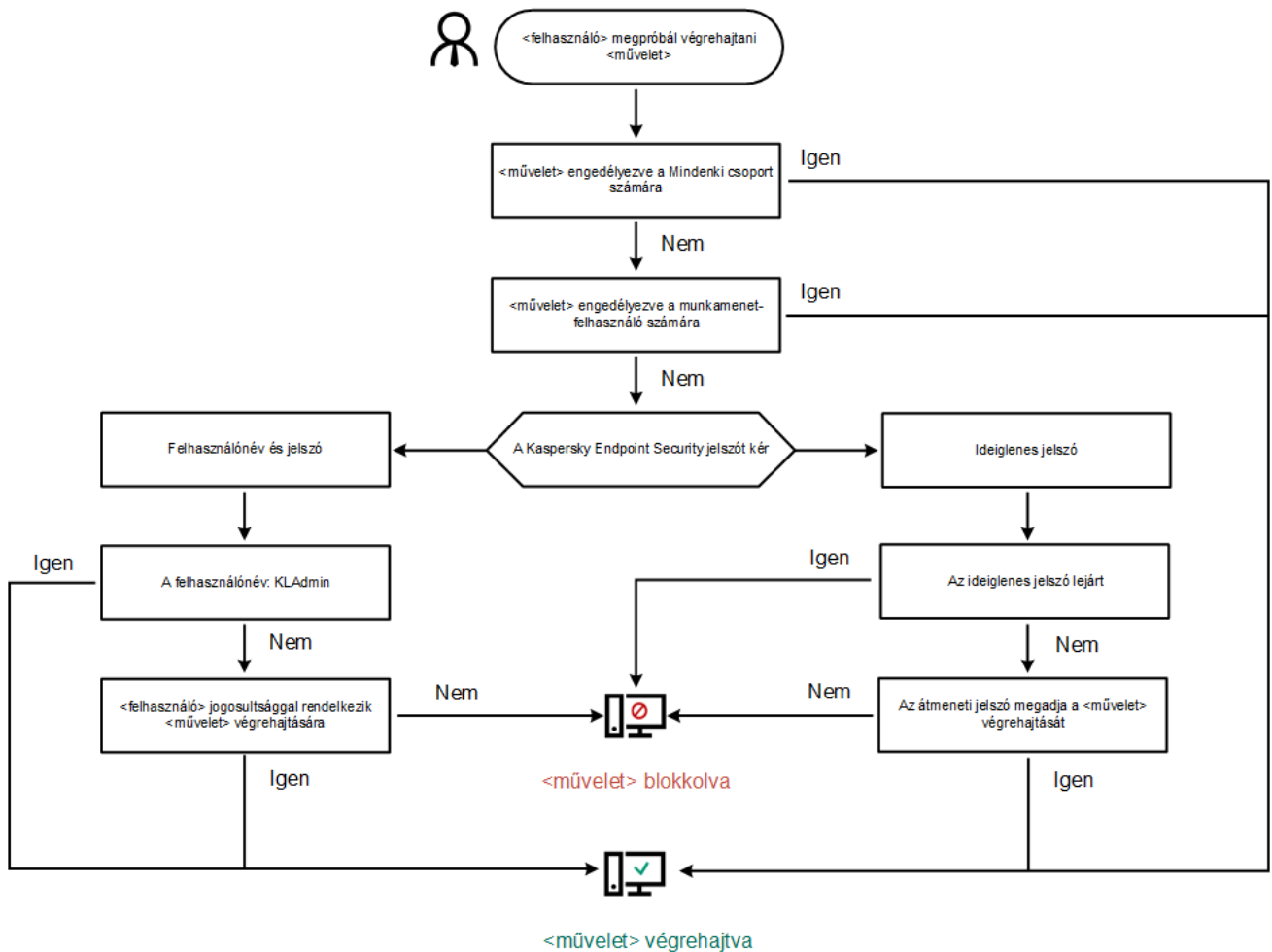
- **KLAdmin.** Egy Rendszergazda fiók, ami korlátozott hozzáféréssel rendelkezik a Kaspersky Endpoint Security-ben. A KLAdmin felhasználói fióknak joga van végrehajtani bármilyen olyan tevékenységet, ami jelszóvédelem. A KLAdmin fiók jogosultságait nem lehet megvonni. Ha engedélyezi a jelszóvédelmet, a Kaspersky Endpoint Security kérni fogja, hogy állítson be egy új jelszót a KLAdmin fiókhoz.
- **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:

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 KAdmin-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 KAdmin fiókot vagy egy jogosultságokkal rendelkező, másik fiókot használ, vagy akkor, ha megad egy átmeneti jelszót.

A jelszóvédelmet csak akkor kapcsolhatja ki, ha KAdminként 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

Megadhatja a Kaspersky Endpoint Security-hez történő hozzáférést egyéni 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 KAdmin 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 KAdmin fiókot vagy egy ideiglenes jelszót.

Jogosultságok megadásához egyéni felhasználóknak vagy csoportoknak:

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. A megnyíló ablakban kattintson a **Felhasználó vagy csoport kijelölése** gombra.

Megnyílik a Felhasználók vagy csoportok kiválasztása párbeszédpanel.

5. Válasszon ki egy felhasználót vagy csoportot az Active Directory helyről, és erősítse meg a választását.
6. 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.

7. 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

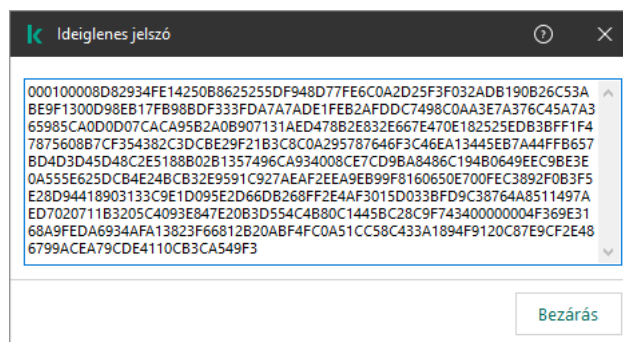
Az ideiglenes jelszó használható arra, hogy átmeneti elérést adjon a Kaspersky Endpoint Security-hez egy olyan egyéni számítógépnek, ami a vállalati hálózaton kívül található. Szükséges engedélyezni a felhasználónak, hogy tiltott tevékenységeket végezhesen el a KLAdmin fiók bejelentkezési adatai nélkül. 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 az **Applications** részt.
6. A számítógépre telepített Kaspersky alkalmazások listájából válassza ki a **Kaspersky Endpoint Security for Windows** elemet, majd kattintson duplán az alkalmazás tulajdonságainak megnyitásához.
Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
7. A **Jelszóvédelem** részen kattintson a **Beállítások** gombra.
8. A **Temporary password** részben kattintson a **Settings** gombra.
9. Megnyílik a **Create temporary password** ablak.
10. A **Expiration date** mezőben adja meg a dátumot, amikor az ideiglenes jelszó le fog járni.
11. Jelölje be az **Temporary password scope** táblázatban a jelölőnégyzeteket azon műveletek mellett, amelyeknek a felhasználó rendelkezésére kell állniuk, miután megadja az ideiglenes jelszót.
12. Kattintson a **Létrehozás** gombra.
Megnyílik az ideiglenes jelszót tartalmazó ablak (lásd az alábbi ábrát).
13. 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 ki a **Devices** → **Managed devices** lehetőséget.
2. Kattintson annak a számítógépnek a nevére, amelyen a felhasználónak engedélyezni kívánja a tiltott művelet végrehajtását.
3. Válassza ki a **Applications** lapot.
4. Kattintson a **Kaspersky Endpoint Security for Windows** lehetőségre.
Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** fület.
6. Az alkalmazásbeállítások ablakában válassza ki az **General settings** → **Interface** elemet.
7. A **Jelszóvédelem** részen kattintson az **Ideiglenes jelszó** 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

A Jelszóvédelem jogosultságok speciális szempontjai

A Jelszóvédelem jogosultságnak vannak bizonyos fontos szempontjai és korlátozásai, amiket figyelembe kell venni.


Alkalmazásbeállítások

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 beállításában.
- 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 beállításában.
- 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 beállításában.

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 meghajtókon 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.

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.

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 jogszerű szoftverek részleteiért, amelyekkel a bűnözők károsíthatják a számítógépet vagy a személyes adatokat, keresse fel a [Kaspersky IT Encyclopedia webhelyet](#).

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:

- [Viselkedéselemzés.](#)
- [Biztonsági rések kihasználásának megelőzése.](#)
- [Behatolásmeelőző rendszer.](#)
- [Fájl védelem.](#)
- [Web védelem.](#)
- [Levelezés védelem.](#)
- [Vizsgálati feladatok.](#)

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.

[Vizsgálatból való kizárások létrehozásának 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályok ablakában válassza az **General settings** → **Exclusions** lehetőséget.
6. A **Scan exclusions and trusted applications** részben kattintson a **Settings** gombra.
7. A megnyitott ablakban válassza ki a **Kizárás a vizsgálatból** lapot.
Ez megnyitja a kizárások listáját tartalmazó ablakot.
8. 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.
9. Jelölje be a **Helyi megbízható alkalmazások használatának engedélyezése** 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. Ha helyi listát hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt fájlokat a vizsgálatokból.
10. Kattintson a **Add** gombra.
11. Fájl vagy mappa vizsgálatból való kizárása:
 - a. A **Properties** részben jelölje be a **File or folder** jelölőnégyzetet.
 - b. Kattintson a **válasszon fájlt vagy mappát** hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben a **Fájl vagy mappa neve** ablak megnyitásához.
 - c. 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a **Mappa** nevű mappában és az almappáiban található. 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.

d. Mentse el a módosításokat.

12. Adott nevű objektumok kizárása a vizsgálatból:

a. A **Tulajdonságok** részben jelölje be az **Objektum neve** jelölőnégyzetet.

b. Kattintson az **adja meg az objektum nevét** hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben az **Objektum neve** ablak megnyitásához.

c. Adja meg az objektumtípus nevét a [Kaspersky Encyclopedia](#) osztályozási rendszerének megfelelően (például e-mail-féreg, 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.

d. Mentse el a módosításokat.

13. Ha ki szeretne zárni egy fájlt a vizsgálatokból:

a. A **Tulajdonságok** részben jelölje be az **Objektum ellenőrzőösszege** jelölőnégyzetet.

b. Kattintson az objektum ellenőrzőösszeg bevitele hivatkozásra az **Objektum ellenőrzőösszege** ablak megnyitásához.

c. 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.

d. Mentse el a módosításokat.

14. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

15. Adja meg, mely Kaspersky Endpoint Security összetevők használják a vizsgálatból való kizárást:

a. Kattintson a **bármelyik** hivatkozásra a **Vizsgálati kizárás leírása (szerkesztéshez kattintson az aláhúzott elemekre)** részben a **válassza ki az összetevőket** hivatkozás aktiválásához.

b. A **válassza ki az összetevőket** hivatkozásra kattintva megnyílik a **Védelmi összetevők** ablak.

c. Jelölje be a jelölőnégyzeteket azokkal az összetevőkkel szemben, amelyekben alkalmazni szeretné a vizsgálatból való kizárást.

d. Mentse el a módosításokat.

Ha a vizsgálatból való kizárás beállításában 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 beállításában nincsenek megadva összetevők, akkor a kizárás a Kaspersky Endpoint Security összes összetevője által végzett vizsgálat során érvényre jut.

16. Bármikor használhatja a jelölőnégyzetet [egy kizárás megszüntetéséhez](#).

17. Mentse el a módosításokat.

[Vizsgálatból kizárás létrehozásának menete a Web Console-ban és a Cloud Console-ban](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Kizárások** helyre.
5. A **Scan exclusions and trusted applications** részben kattintson a **Scan exclusions** hivatkozásra.
6. 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.
7. Jelölje be a **Helyi megbízható alkalmazások használatának engedélyezése** 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. Ha helyi listát hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt fájlokat a vizsgálatokból.
8. Kattintson a **Add** gombra.
9. Válassza ki, hogyan szeretné hozzáadni a kizárást: **Fájl vagy mappa**, **Objektum neve** vagy **Objektum ellenőrzőösszege**.
10. 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 * 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a Mappa nevű mappában és az almappáiban található. 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.
11. Ha egy adott típusú objektumot szeretne kizárni a vizsgálatokból, az **Objektum** mezőben adja meg az objektumtípus nevét a [Kaspersky Encyclopedia](#) osztályozási rendszerének megfelelően (például: e-

mail-féreg, 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 **Fájlkivonat** mezőben.
Ha a fájl megváltozik, a fájl ellenőrzőösszege is megváltozik. Ebben az esetben a módosított fájl nem lesz hozzáadva a kizárásokhoz.
13. A **Védelmi összetevők** blokkban válassza ki az összetevőket, amelyekre alkalmazni szeretné a kizárást a vizsgálatból.
14. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.
15. 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 a **Speciális beállítások** → **Fenyegetések és kizárások** lehetőséget.

3. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

4. Kattintson a **Add** gombra.

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 * 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a Mappa nevű mappában és az almappáiban található. 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.

6. Ha egy adott típusú objektumot szeretne kizárni a vizsgálatokból, az **Objektum** mezőben adja meg az objektumtípus nevét a [Kaspersky Encyclopedia](#) osztályozási rendszerének megfelelően (például: e-mail-féreg, 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 a **Fájlkivonat** 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.

Bármikor használhatja a kapcsolót [egy kizárás megszüntetéséhez](#).

11. Mentse el a módosításokat.

Elérési utak a mappákban található fájlokhoz:

- A `*.exe` maszk tartalmazza az exe kiterjesztésű fájlok elérési útvonalait.
- A `példa*` maszk tartalmazza a PÉLDA 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 tartalmazza a C:\dir\ mappában található fájlok elérési útvonalát, azonban a C:\dir\ almappa fájljaiét nem.
- A `C:\dir\` maszk tartalmazza a C:\dir\ mappában található fájlok elérési útvonalát, azonban a C:\dir\ almappa fájljaiét nem.
- 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 tartalmazza a C:\dir\ mappában található, „test” nevű fájlok elérési útvonalát, valamint a C:\dir\ almappa fájljaiét.

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.

A vizsgálatból való kizárás be- és kikapcsolása



A vizsgálatból való kizárás be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Speciális beállítások** → **Fenyegetések és kizárások** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Kizárások kezelése** hivatkozásra.

4. Válassza ki a vizsgálatból való kizárások listáján a kívánt kizárást.
5. Az objektum melletti kapcsolóval helyezze az objektumot a vizsgálat hatókörébe vagy zárja ki abból.
6. Mentse el a módosításokat.

Az észlelhető objektumok típusának kiválasztása

Az észlelhető objektumok típusának kiválasztása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Speciális beállítások** → **Fenyegetések és kizárások** lehetőséget.
3. Az **Észlelt objektumok típusai** részben jelölje be a jelölőnégyzeteket azokkal az objektumtípusokkal szemben, amelyeket észlelni szeretne a Kaspersky Endpoint Security alkalmazással:
 - [Vírusok és férgek](#) 

Alkategória: vírusok és férgek (Viruses_and_Worms)

Fenyegetési szint: 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 továbbítja 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 *felülíró* vírusok saját kódjukkal felülírják a fertőzött fájlt, így törölve annak tartalmát. A fertőzött fájl működése leáll, így nem lehet helyreállítani. A *parazita* vírusok csak módosítják a fájlokat, azokat teljesen vagy részlegesen működésképes állapotban hagyva. A *társító* vírusok nem módosítják a fájlokat, csak másolatot készítenek róluk. Egy fertőzött fájl megnyitva annak másolata (azaz tulajdonképpen a vírus) indul el. Az alábbi vírusok szintén megtalálhatók: *hivatkozásvírusok*, *OBJ-vírusok*, *LIB-vírusok*, *forráskódú* vírusok és számos egyéb.

Féreg

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 féreget 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 megkezd a rosszindulatú műveleteket. Ezután megkezd lemásolni saját magát, újabb e-mail címek keresésébe kezd, és terjeszteni kezdi a fertőzött üzeneteket.
IM-féreg	IM kliens féreg	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-	Internetes	Ezek olyan internetes csevegő szolgáltatásokon keresztül terjednek,

féreg	csevegési féreg	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.
Hálózati féreg	Hálózati féreg	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-féreg	Fájlcsere hálózati féreg	Fájlcsere (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.
Féreg	Egyéb típusú férgek	Az egyéb típusú férgek a következők lehetnek: <ul style="list-style-type: none"> • 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 megkísérik azok lemez meghajtói 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

Fenyegetési szint: 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, weboldalnak 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
Trójai 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.
Hátsó kapu	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.
Trójai	Trójai programok	Ez a kategória az alábbi rosszindulatú alkalmazásokat tartalmazza: <ul style="list-style-type: none">• 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.
Váltásdíj-trójai	Váltásdíj trójai	Ezek a felhasználó adatait „túszul ejtik”, módosítva vagy blokkolva azt, esetleg meggátolják a számítógép működését, hogy a felhasználó számára elveszzenek az adatok. A betolakodó váltásdíjat követel a felhasználótól, azt ígérve, hogy küld egy alkalmazást,

		amellyel visszaállítható a számítógép normál állapota az elveszett adatokkal együtt.
Trójai-kattintó	Trójai kattintók	<p>Ezek a felhasználó számítógépéről weboldalakat látogatnak meg, saját maguk utasítva a webböngészőt, vagy módosítva az operációs rendszer fájljaiban megadott webcímet.</p> <p>Az ilyen programokkal a betolakodó hálózati támadást indíthat, valamint webhelyek látogatottságát növelheti, hogy a reklámcsíkhirdetések megjelenítésének a száma növekedjen.</p>
Trójai-letöltő	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 weboldaltól is.
Trójaitelepítő	Trójaitelepítők	<p>Más trójai programokat tartalmaznak, melyeket a számítógép merevlemezére mentenek, majd telepítenek.</p> <p>A betolakodók a telepítő típusú trójai programokat az alábbi célokból használhatják:</p> <ul style="list-style-type: none"> • 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.
Trójai-értesítő	Trójai-értesítők	<p>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.</p> <p>Ezek a programok gyakran több trójai programból álló programcsomag részét képezik. Ezek értesítik a betolakodót a többi trójai program sikeres telepítéséről.</p>
Trójai-proxy	Trójai-proxyk	Segítségükkel a betolakodó névtelenül érhet el weboldalakat a felhasználó számítógépéről; gyakran alkalmazzák őket levélszemét küldésére.
Trójai-PSW	Jelszólopó programok	<p>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.</p> <p>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).</p>

Trójai-kém	Trójai-kémek	Ezek kémkednek a felhasználó után, információkat gyűjtenek az általa a számítógépen végzett műveletekről. Eltéríthetik a felhasználó által a billentyűzeten begépelte 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.
Trójai-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 hackerok 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.
Trójai-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.
Trójai-SMS	SMS-üzenetek formájában megjelenő trójai programok	Ezek mobiltelefonokat fertőznek meg, SMS-üzeneteket küldve fizetős telefonszámokra.
Trójai 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.
Trójai bankár	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.
Trójai 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. Így 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
Konstruktor	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).
Biztonsági rés	Biztonsági rések	<p>Az exploit olyan adatsomag 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” weboldalnak.</p> <p>A különböző exploitok különböző alkalmazások vagy hálózati szolgáltatások sebezhetőségét használják ki. Az exploit hálózati csomagok 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.</p> <p>A hálózati férgek a hálózaton exploitok segítségével terjednek. A <i>Nuker</i> exploitok számítógépeket leállító hálózati csomagok.</p>
Fájltitkosító	Titkosítók	Ezek más rosszindulatú alkalmazásokat titkosítanak, hogy elrejtse azokat a víruskereső alkalmazások elől.
Elárasztó	Hálózatokat „szennyező” programok	<p>Ezek nagy mennyiségű üzenetet küldenek hálózati csatornákon. Az ilyen eszközök között található az internetes csevegéseket szennyező programok is.</p> <p>Az elárasztó eszközök nem tartalmazzák 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.</p>
HackTool	Hackelő	Az ilyenek teszik lehetővé azon számítógép feletti uralom

	eszközök	átvételét, amelyre feltelepültek, vagy más számítógépek megtámadását (például új rendszerfiók felvételét a felhasználó engedélye nélkül, a rendszernapló törlését, hogy elrejtethő legyen a jelenlétük az operációs rendszerben). Ebbe a típusba tartoznak némely szimatoló programok, amelyek jelszavakat térítnek 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.
Hamisító	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 elrejtsek azokat víruskereső alkalmazások elől.
E-mail-elárasztó	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-elárasztó	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-elárasztó	A forgalmat SMS üzenetekkel „szennyező” programok	Ezek nagy mennyiségű SMS-üzenetet küldenek a mobiltelefonra.

- [Reklámprogram](#) 

Alkategória: hirdetési szoftver (reklámprogram);

Fenyegetési szint: 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: jogszerű szoftverek, amelyekkel a bűnözők károsíthatják a számítógépét vagy személyes adatait

Veszély szintje: közepes

A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetnek 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
Kliens 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.
Tárcsázó	Autotárcsázók	Ezek modemén keresztül rejtve hoznak létre kapcsolatot.
Letöltő	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.
Kiszolgáló FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Kiszolgáló proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Kiszolgáló	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók

Telnet		ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Kiszolgáló Web	Web kiszolgálók	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 számítógépen 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.
Kliens P2P	P2P-hálózati kliensek	Segítségükkel a felhasználó fájlcsere (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.
Kliens 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	Pszedoprogramok	Ezek más programoknak adják ki magukat. Lehetnek például pszeudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.

- [Egyéb olyan szoftverek észlelése, amelyekkel a behatolók károsíthatják a számítógépét vagy személyes adatait](#) 

Alkategória: jogszerű szoftverek, amelyekkel a bűnözők károsíthatják a számítógépét vagy személyes adatait

Veszély szintje: közepes

A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetnek 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
Kliens 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.
Tárcsázó	Autotárcsázók	Ezek modemem keresztül rejtve hoznak létre kapcsolatot.
Letöltő	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.
Kiszolgáló FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Kiszolgáló proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Kiszolgáló	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók

Telnet		ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Kiszolgáló Web	Web kiszolgálók	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.
Kliens P2P	P2P-hálózati kliensek	Segítségükkel a felhasználó fájlcsere (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.
Kliens 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	Pseudoprogramok	Ezek más programoknak adják ki magukat. Lehetnek például pseudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.

• [Csomagolt objektumok, melyek tömörítése felhasználható károkozásra képes kód védelmére](#) 

A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található csomagolt objektumokat és az önkicsomagoló modult is ellenőrzi.

A veszélyes programoknak a víruskereső alkalmazások elől való elrejtéséhez a betolakodók különleges csomagolók segítségével tömörítik azokat, vagy többszörösen tömörített fájlokat hoznak létre.

A Kaspersky víruslemez azonosították a hackerek által leggyakrabban alkalmazott tömörítőprogramokat.

Ha a Kaspersky Endpoint Security egy fájlban ilyen tömörítőt talál, az nagy valószínűséggel rosszindulatú alkalmazást vagy olyan alkalmazást tartalmaz, amelyet a betolakodó a számítógép vagy az adatok ellen felhasználhat.

A Kaspersky Endpoint Security az alábbi programokat választja ki:

- *Esetleg kárt okozó csomagolt fájlok* – rosszindulatú programok, például vírusok, férgek és trójaiak becsomagolására kerülnek használatra.
- *Többszörösen csomagolt fájlok* (közepes fenyegetettségi szint) – a fájl háromszorosan be van csomagolva egy vagy több tömörített fájlba.

• [Többszörösen csomagolt objektumok](#) 

A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található csomagolt objektumokat és az önkicsomagoló modult is ellenőrzi.

A veszélyes programoknak a víruskereső alkalmazások elől való elrejtéséhez a betolakodók különleges csomagolók segítségével tömörítik azokat, vagy többszörösen tömörített fájlokat hoznak létre.

A Kaspersky víruselemzői azonosították a hackerek által leggyakrabban alkalmazott tömörítőprogramokat.

Ha a Kaspersky Endpoint Security egy fájlban ilyen tömörítőt talál, az nagy valószínűséggel rosszindulatú alkalmazást vagy olyan alkalmazást tartalmaz, amelyet a betolakodó a számítógép vagy az adatok ellen felhasználhat.

A Kaspersky Endpoint Security az alábbi programokat választja ki:

- *Esetleg kárt okozó csomagolt fájlok* – rosszindulatú programok, például vírusok, férgek és trójaiak becsomagolására kerülnek használatra.
- *Többszörösen csomagolt fájlok* (közepes fenyegetettségi szint) – a fájl háromszorosan be van csomagolva egy vagy több tömörített fájlba.

4. Mentse el a módosításokat.

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 megvizsgálja a megnyitott, végrehajtott vagy bármilyen alkalmazásfolyamat által mentett objektumokat, és felügyeli az összes alkalmazás tevékenységét és az általuk generált hálózati forgalmat. A megbízható alkalmazások listájához hozzáadott alkalmazást azonban a Kaspersky Endpoint Security kizárja a vizsgálatokból.

Ha például úgy véli, hogy a szokásos Microsoft Windows Jegyzettömb alkalmazás vizsgálat nélkül is biztonságos, azaz megbízik ebben az alkalmazásban, akkor a Microsoft Windows Jegyzettömböt felveheti a megbízható alkalmazások listájára. Ekkor a vizsgálat kihagyja azokat az objektumokat, amelyeket ez az alkalmazás használ.

Ezenkívül bizonyos, a Kaspersky Endpoint Security által gyanúsként osztályozott műveletek számos alkalmazás funkcióinak kontextusában biztonságos lehet. A billentyűzetten begépelte 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 vizsgálatokból való kizárásával elkerülhetők a kompatibilitási ütközések a Kaspersky Endpoint Security és más programok között (pl. a hálózati forgalom kettős vizsgálata harmadik fél számítógépén a Kaspersky Endpoint Security alkalmazással és más víruskereső alkalmazással is), ezenkívül növeli a számítógép teljesítményét, ami kiszolgálók alkalmazásai esetén kritikus fontosságú lehet.

A megbízható alkalmazás végrehajtható fájljában és folyamatában ugyanakkor továbbra is sor kerül a vírusok és egyéb rosszindulatú programok jelenlétének vizsgálatára. Az alkalmazásokat a Kaspersky Endpoint Security vizsgálataiból teljes körűen vizsgálatból való kizárásokkal lehet kizárni.

[Alkalmazás megbízható listához 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabályok ablakában válassza az **General settings** → **Exclusions** lehetőséget.
6. A **Scan exclusions and trusted applications** részben kattintson a **Settings** gombra.
7. A megnyitott ablakban válassza ki a **Megbízható alkalmazások** lapot.
Ez megnyitja a megbízható alkalmazások listáját tartalmazó ablakot.
8. 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 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.
9. 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. Ha helyi listát hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt megbízható alkalmazásokat a vizsgálatokból.
10. Kattintson a **Add** gombra.
11. A megnyitott ablakban adja meg a megbízható alkalmazás futtatható fájljának elérési útját.
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.

12. Konfigurálja a megbízható alkalmazás speciális beállításait (lásd az alábbi táblázatot).
13. A jelölőnégyzet segítségével bármikor [kizárhat egy alkalmazást a megbízható zónából](#).
14. Mentse el a módosításokat.




1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Általános beállítások** → **Kizárások** helyre.
5. A **Scan exclusions and trusted applications** blokkban kattintson a **Trusted applications** hivatkozásra.
Ez megnyitja a megbízható alkalmazások listáját tartalmazó ablakot.
6. 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 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 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. Ha helyi listát hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt megbízható alkalmazásokat a vizsgálatokból.
8. Kattintson a **Add** gombra.
9. A megnyitott ablakban adja meg a megbízható alkalmazás futtatható fájljának elérési útját.
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.

10. Konfigurálja a megbízható alkalmazás speciális beállításait (lásd az alábbi táblázatot).
11. A jelölőnégyzet segítségével bármikor [kizárhat egy alkalmazást a megbízható zónából](#).
12. Mentse el a módosításokat.

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Speciális beállítások** → **Fenyegetések és kizárások** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.
4. Az ablakban kattintson a **Hozzáadás** gombra.
5. Válassza ki a megbízható alkalmazás futtatható fájlját.

Manuálisan is megadhatja az elérési utat. A Kaspersky Endpoint Security támogatja a környezeti változókat, és a  és  karaktereket egy maszk megadásakor.

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 (lásd az alábbi táblázatot).
7. A kapcsoló segítségével bármikor [kizárhat egy alkalmazást a megbízható zónából](#).
8. Mentse el a módosításokat.


Megbízható alkalmazás beállításai

Paraméter	Leírás
Ne vizsgálja a fájlokat megnyitás előtt	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. Az alkalmazástevékenységet a következő összetevők figyelik: Behavior analysis , Biztonsági rések kihasználásának megelőzése , Behatolásmegelőző rendszer , Kármentesítő motor és Tűzfal .
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	A Kaspersky Endpoint Security nem figyeli az ezen alkalmazás által elindított alkalmazások fájl- vagy hálózati tevékenységét.

tevékenységét	
Az alkalmazásfelülettel való interakció engedélyezése	A Kaspersky Endpoint Security Önvédelem blokkolja az alkalmazásslolgáltatások 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.
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.
Megjegyzés	Ha szükséges, rövid megjegyzést adhat a megbízható alkalmazáshoz. A megjegyzések megkönnyítik a megbízható alkalmazások keresését és rendezését.
Státusz	A megbízható alkalmazás állapota: <ul style="list-style-type: none"> • 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.

Megbízható zónaszabályok engedélyezése és letiltása a megbízható alkalmazások listáján szereplő alkalmazásnál


Megbízható zónaszabályok műveletének engedélyezése és letiltása a megbízható alkalmazások listáján szereplő alkalmazásnál:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Speciális beállítások** → **Fenyegetések és kizárások** lehetőséget.
3. A **Kizárások** blokkban kattintson a **Megbízható alkalmazások megadása** hivatkozásra.
4. Válassza ki a megbízható alkalmazások listáján a szükséges megbízható alkalmazást.
5. A **Státusz** oszlopban lévő kapcsolóval vegyen be egy megbízható alkalmazást a vizsgálat hatókörébe vagy zárja ki abból.
6. Mentse el a módosításokat.

Megbízható rendszertanúsítványok tárolójának használata

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.

Megbízható rendszertanúsítvány tárhelye használatának megkezdése:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza a **Speciális beállítások** → **Fenyegetések és kizárások** lehetőséget.
3. Válassza ki a **Megbízható rendszertanúsítvány tárhelye** legördülő listán, hogy a Kaspersky Endpoint Security melyik rendszertárhelye tekintendő megbízhatónak.
4. Mentse el a módosításokat.

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\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 lejáratát 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 válassza ki az **Általános beállítások** → **Jelentések és tároló** részt.
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 válassza ki az **Általános beállítások** → **Jelentések és tároló** részt.
3. Ha korlátozni szeretné a biztonsági mentés méretét, jelölje be **A biztonsági mentés méretének korlátozása N MB-ra** jelölőnégyzetet a **Biztonsági mentés** részen. Adja meg a Biztonsági mentés maximális méretét.
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 *Fertőzött* állapotot, majd elhelyezi másolatát a Biztonsági mentésbe, és megkísérli a vírusmentesítést. Ha a fájl vírusmentesítése sikerül, akkor biztonsági másolatának állapota *Vírusmentesített* értékre 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 vírusmentesítve lesznek* állapottal rendelkező fájlok nem állíthatók 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 a Microsoft Windows 8 operációs rendszer megfelelő eszközeivel állítható vissza (a Windows Store alkalmazások visszaállításával kapcsolatos részleteket lásd a *Microsoft Windows 8 súgófájjaiban*).

A fájlok biztonsági másolatait 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.

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 kézzel 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 törendő fájlokat, majd kattintson a **Törlés** gombra.

A Kaspersky Endpoint Security a kiválasztott fájlok biztonsági másolatait törli a Biztonsági mentésből.

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 alkalmazásmódulok 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 **Értesítési beállítások** 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 Alkalmazás 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 **Értesítési beállítások** 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 értesítési beállítások** 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 Anomáiafelügyelő](#) 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 Eszkőfelügyelő 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 **Események** 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\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 érhetőek 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 találhatóak. 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 Internet 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 jelentésszlopok 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 törölhető](#) 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.
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 alsó részén megjelenik egy rész, melyben az esemény összegzése látható.

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 válassza ki az **Általános beállítások** → **Jelentések és tároló** részt.
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 válassza ki az **Általános beállítások** → **Jelentések és tároló** részt.
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.
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 válassza ki az **Általános beállítások** → **Jelentések és tároló** részt.
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).


A Kaspersky Endpoint Security önvédelmi technológiái

Technológia	Leírás	x86 rendszerű számítógép	x64 rendszerű számítógép
Önvédelmi mechanizmus	A technológia blokkolja a hozzáférést a következő alkalmazásösszetevőkhöz: <ul style="list-style-type: none">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 ² . <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Az AM-PPL technológia a Windows 10 1703-as (RS2) vagy újabb verziói, valamint a Windows Server 2019 operációs rendszerek számára érhető el.</div>	✓	✓
Külső kezelés elleni védelmi mechanizmus	Ez a technológia megakadályozza, hogy a távadminisztrációs 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 önvédelmi mechanizmusa alapértelmezés szerint be van kapcsolva.

Az önvédelem be- és kikapcsolása:

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

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.

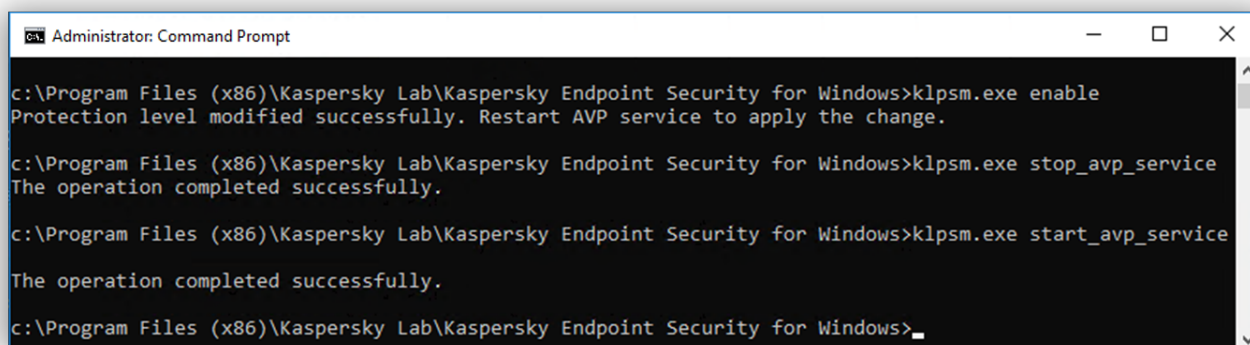
3. Lépjen abba a mappába, ahol a Kaspersky Endpoint Security végrehajtható fájl telepítve van.

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.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Az AM-PPL technológia támogatásának engedélyezése

A külső kezelésvédelem be- és kikapcsolása

A külső felügyeleti védelem megakadályozza, hogy a távadminisztrációs alkalmazások (például a TeamViewer vagy a RemotelyAnywhere) hozzáférjenek a Kaspersky Endpoint Security szolgáltatáshoz. Ez a technológia a következő külső felügyeleti védelmi funkciókat tartalmazza:

- Védelem a Kaspersky Endpoint Security beállításainak módosítása ellen.
- A Kaspersky Endpoint Security szolgáltatásainak (például az avp szolgáltatás) védelme.
- Az alkalmazás folyamatainak védelme.

A külső felügyelet elleni védelem csak 32 bites operációs rendszert futtató számítógépeken érhető el, kivéve a Windows 7 esetében. A Windows 7 esetében a technológia 32 bites és 64 bites operációs rendszerekhez is elérhető.

Külső felügyelettel szembeni védelem engedélyezése vagy letiltása:

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

3. **A Kaspersky Endpoint Security beállításainak távoli vezérlőalkalmazásokból való kezelésének engedélyezése** jelölőnégyzetben engedélyezheti vagy letilthatja a külső felügyelettel szembeni védelmet.

Ha a jelölőnégyzet be van jelölve, akkor távfelügyeleti alkalmazások segítségével konfigurálhatja a Kaspersky Endpoint Security szolgáltatást, és kezelheti annak szolgáltatásait és folyamatait.

Ha a jelölőnégyzet nincs bejelölve, a külső felügyelettel szembeni védelem megakadályozza, hogy a távadminisztrációs alkalmazások hozzáférjenek a Kaspersky Endpoint Security szolgáltatáshoz. Engedélyezheti a Kaspersky Endpoint Security konfigurálását egyes távfelügyeleti alkalmazások használatával. Ehhez [fel kell vennie a távfelügyeleti alkalmazást a megbízható alkalmazások listájába](#). Ebben az esetben a távfelügyelettel szembeni védelem továbbra is megakadályozza, hogy távadminisztrációs alkalmazások hozzáférjenek a Kaspersky Endpoint Security szolgáltatásaihoz és folyamataihoz.

4. **A Külső szolgáltatásvezérlés engedélyezése** jelölőnégyzettel engedélyezheti vagy letilthatja a Kaspersky Endpoint Security szolgáltatásainak külső felügyelettel szembeni védelmét.

Ha az alkalmazást kis szeretné léptetni a parancssorból, tiltsa le a Kaspersky Endpoint Security szolgáltatásainak külső felügyelettel szembeni védelmét.


5. Mentse el a módosításokat.

Ennek eredményeképpen, ha a külső felügyelettel szembeni védelem engedélyezve van, a Kaspersky Endpoint Security megakadályozza, hogy az egérmutató az alkalmazás ablakába kerüljön. Amikor egy távoli felhasználó megpróbálja leállítani az alkalmazásszolgáltatást, egy hibaüzenetet tartalmazó rendszerablak jelenik meg.

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 a **Speciális beállítások** → **Fenyegetések és kizárások** 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 a **Ne figyelje az alkalmazástevékenységet** jelölőnégyzetet.
7. Mentse el a módosításokat.

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:

- Frissítési feladat;
- 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 Kaspersky Endpoint Security általi használata hatással lehet más alkalmazások teljesítményére is. A CPU és a merevlemez alrendszerek több alkalmazás egyidejű működése által okozott fokozott terhelése problémájának megoldása érdekében a Kaspersky Endpoint Security képes szüneteltetni az ütemezett vizsgálatokat, és erőforrásokat átengedni a többi alkalmazásnak.

Számos alkalmazás azonban azonnal elindul, amint a CPU erőforrásai rendelkezésre állnak, és a háttérben fut. Annak megelőzése érdekében, hogy a vizsgálat a többi alkalmazás teljesítményétől függjön, célszerűbb, ha az operációs rendszer erőforrásait nem engedi át részükre.

Szükség esetén kézzel indíthatja el a feladatokat.

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 felhasználotól 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 Aktív vírusmentesítés szükséges. Kiszolgáló aktív fertőzésének megszüntetéséhez engedélyezze a kiszolgálóknak szánt Aktív vírusmentesítés technológiát, és indítson *Vírusvizsgálat* csoportos feladatot a fájlkiszolgáló felhasználóinak megfelelő időpontban.

Az energiatakarékos mód be- és kikapcsolása

Az energiatakarékos mód be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
3. A **Teljesítmény** részben használja az **Ütemezett feladatok elhalasztása, amíg a számítógép akkumulátorról üzemel** jelölőnégyzetet az energiatakarékos mód engedélyezéséhez vagy letiltásához.


Ha az energiatakarékos mód be van kapcsolva, a számítógép pedig akkumulátorról működik, az alábbi feladatok akkor sem futnak, ha be vannak ütemezve:

- Frissítési feladat;
- Teljes vizsgálat feladat;
- Kritikus területek vizsgálata feladat;
- Egyéni vizsgálat feladat;
- Integritás-ellenőrzés feladat.

4. Mentse el a módosításokat.

Erőforrások más alkalmazásoknak történő átadásának engedélyezése és letiltása

Erőforrások más alkalmazásoknak történő átadásának engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a  gombra.
2. Az alkalmazásbeállítások ablakában válassza az **Általános beállítások** → **Alkalmazásbeállítások** lehetőséget.
3. A **Teljesítmény** részben jelölje be az **Erőforrások adása más alkalmazásoknak** jelölőnégyzetet az erőforrások más alkalmazásoknak való átadása engedélyezéséhez vagy letiltásához.

Ha a Kaspersky Endpoint Security úgy van beállítva, hogy az erőforrásokat átadja más alkalmazásoknak, akkor a többi alkalmazást lelassító ütemezett vizsgálatokat elhalasztja:

- Frissítési feladat;
- Teljes vizsgálat feladat;
- Kritikus területek vizsgálata feladat;
- Egyéni vizsgálat feladat;
- Integritás-ellenőrzés feladat.

Az alkalmazás alapértelmezés szerint úgy van beállítva, hogy az erőforrásokat átadja más alkalmazásoknak.

4. Mentse el a módosításokat.

Ajánlott eljárások a Kaspersky Endpoint Security teljesítményének optimalizálásához

A Kaspersky Endpoint Security for Windows telepítéskor a következő javaslatok segítségével konfigurálhatja a számítógép védelmét és optimalizálhatja a teljesítményt.

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.

Vírusvizsgálat munkaállomásokon

Ajánlott a [háttérbeli vizsgálat](#) engedélyezése a munkaállomások vírusvizsgálatához. A *Vizsgálat a háttérben* a Kaspersky Endpoint Security egy olyan vizsgálati módja, ami nem jeleníti meg az értesítéseket a felhasználónak. A háttérvizsgálat 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 számítógép vírusvizsgálatához csak a háttérbeli vizsgálat módot használhatja egyéb vizsgálati feladatok nélkül.

Ha a háttérbeli vizsgálat nem felel meg az Ön igényeinek, konfigurálja a *Vírusvizsgálat* feladatot az alábbi ajánlásoknak megfelelően:

1. [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 a nap végén kikapcsolják számítógépüket, a következőképpen konfigurálhatja a vizsgálati feladatot:

- Hálózati ébresztés engedélyezése. A Hálózati ébresztés funkció lehetővé teszi a számítógép távoli bekapcsolását speciális jelet küldve annak a helyi hálózaton keresztül. A funkció használatához engedélyeznie kell a Hálózati ébresztés funkciót a BIOS beállításaiiban. Azt is beállíthatja, hogy a számítógép automatikusan kikapcsoljon a vizsgálat befejezése után.
- Tiltsa le az „Elmulasztott feladatok futtatása” funkciót. A Kaspersky Endpoint Security kihagyja az elmulasztott feladatokat, amikor a felhasználó bekapcsolja a számítógépet. A számítógép bekapcsolása után a feladatok futtatása kényelmetlenséget okozhat a felhasználónak, mivel a vizsgálat nagy mennyiségű erőforrást igényel.

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.

2. [Határozzon meg egy vizsgálati hatókört.](#)

Válassza ki a következő objektumokat a vizsgálatához:

- Kernelmemória;
- A futó folyamatok és indítási objektumok;
- Rendszerindító szektorok;
- Rendszermeghajtó (%systemdrive%).

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 a Felügyeleti 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.

Vírusvizsgálat kiszolgálókon

Konfigurálja a *Vírusvizsgálat* feladatot az alábbi ajánlásoknak megfelelően:

1. [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.

2. [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 a Felügyeleti konzolon (MMC) és a Kaspersky Endpoint Security felületén kapcsolhatja be. Ezek a technológiák nem kapcsolhatók be a Kaspersky Security Center Web Console-ban.

3. 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.

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 részt vesz a Kaspersky Security Networkben, a KSN szolgáltatás megadja a Kaspersky Endpoint Security számára a vizsgált fájlok kategóriáját és hírnevét, valamint a vizsgált webcímek hírnevét.

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 KSN-t.

A *Privát KSN* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky Security Network hírnévadatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a KSN-re 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 Security Network letölti az antivírus adatbázisok teljes verzióját a Kaspersky szerverekről.

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 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 fejt 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 készítetté.

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 egyszerű bejelentkezés \(SSO\) 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 merevlemezekben 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 adatokéről 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 kezel, 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.

A Kaspersky lemeztitkosítási technológiával történő teljes lemeztitkosítás a hardver- és szoftverkövetelményeknek meg nem felelő merevlemezeken nem használható.

A Kaspersky Endpoint Security és a Kaspersky Anti-Virus for UEFI a teljes lemezes titkosítási funkciói közötti 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 fájl szintű 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, IEEE1394, 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-közvetítői 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.
 - Tíznel 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 bájtól 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 Express Cache 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 Think Center 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 100
- MSI 760GM-E51 (alapláp)

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 számítógépen telepített alkalmazás verziójával. Ilyenkor először el kell távolítani az alkalmazást.

Kaspersky lemeztitkosítás

A Kaspersky Lemeztitkosítás csak olyan számítógépeken érhető el, melyek a munkáállomásokhoz 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 merevlemezre 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 felhasználónevet 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 beállításában, 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 felhasználovének 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

Teljes lemeztitkosítás a Kaspersky lemeztitkosítás technológiával

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.

Teljes lemeztitkosítás végzése a Kaspersky lemeztitkosítás technológiával:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
6. A **Titkosítási technológia** legördülő listán válassza a **Kaspersky lemeztitkosítás** lehetőséget.

A Kaspersky lemeztitkosítási technológia nem használható, ha a számítógépen BitLocker segítségével titkosított merevlemezek találhatók.

7. 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 merevlemezokről](#).

8. Konfigurálja a Hitelesítési ügynöki fiókok hozzáadásának szabályait a lemeztitkosítás során. Az Ügynök lehetővé teszi a felhasználónak a titkosított meghajtókhoz való hozzáféréshez és az operációsrendszer-betöltéshez szükséges hitelesítés végrehajtását. A Hitelesítési ügynöki fiókok automatikus hozzáadásához konfigurálja a következő beállításokat:

- **Hitelesítési ügynöki fiókok automatikus létrehozása a felhasználóknak 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 automatikus 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 ügynöki fiókok kezelése* feladattal.

Ha letiltotta a Hitelesítési ügynöki fiókok automatikus létrehozását, [manuálisan hozzáadhatja a Hitelesítési ügynöki fiókokat](#) a *Fiókok kezelése* feladattal. Ezzel a feladattal módosíthatja az automatikusan létrehozott Hitelesítési ügynöki fiókok beállításait is.

9. A kényelmes használat céljából elmentheti a felhasználónevet a Hitelesítési ügynök memóriájába, így a felhasználónak csak a rendszerbe történő következő bejelentkezéskor kell megadnia egy jelszót. Ehhez jelölje be a **Hitelesítési ügynökben megadott felhasználónév mentése** jelölőnégyzetet.

10. Válasszon ki egyet a következő titkosítási módok közül:

- Ha azt szeretné, hogy a Kaspersky Endpoint Security csak a fájlok által elfoglalt lemezszektorokat titkosítsa, jelölje be a **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** jelölőnégyzetet.
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 információkat hordozó adatokról is. A **Csak a használt lemezterület titkosítása** funkció új, korábban nem használt meghajtók esetén javasolt.
- Ha a teljes merevlemez titkosítani szeretné, törölje a **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** jelölőnégyzet jelölését.

Ha egy eszköz titkosítására korábban már sor került a **Csak a felhasznált lemezterület titkosítása (csökkenti a titkosítás idejét)** opcióval, akkor az **Összes merevlemez titkosítása** módú rendszabály alkalmazását követően a fájlok által el nem foglalt szektorok továbbra sem lesznek titkosítva.

11. Ha hardveres inkompatibilitási probléma jelentkezik a számítógépen végzett titkosítás közben, bejelölheti az **Örökölt USB-támogatás használata (nem ajánlott)** jelölőnégyzetet.

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 *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, amelyek fennáll a probléma.

12. 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.

Titkosított rendszermerevlemezek esetén a Hitelesítési ügynök az operációs rendszer elindulása előtt betöltődik. A Hitelesítési ügynök segítségével hitelesítést végezhet, így hozzáférést szerezhethet a titkosított rendszermerevlemezhez, 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 titkosításból kizárt merevlemezek listájának létrehozása

Titkosítási kizárások listáját kizárólag Kaspersky lemeztitkosítási technológia esetén lehet létrehozni.

A titkosításból kizárt merevlemezek listájának létrehozása:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
6. A **Titkosítási technológia** legördülő listán válassza a **Kaspersky lemeztitkosítás** lehetőséget.
A titkosításból kizárt merevlemeznek megfelelő bejegyzések megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban. Ez a táblázat üres, ha korábban nem készített listát a titkosításból kizárt merevlemezekről.
7. Merevlemez felvétele a titkosításból kizárt merevlemez listájára:
 - a. Kattintson a **Add** gombra.
 - b. Ekkor megnyílik egy ablak, amelyben szerkesztenie kell az **Eszköz neve**, **Számítógépnév**, **Lemeztípus**, **Kaspersky lemeztitkosítás** beállítást.
 - c. Kattintson a **Frissítés** gombra.
 - d. Jelölje be a **Név** oszlopban azon merevlemeznek megfelelő táblázatsorokban a jelölőnégyzeteket, amelyeket fel szeretne venni a titkosításból kizárt merevlemez listájára.
 - e. Kattintson az **OK** gombra.

A kiválasztott merevlemez megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban.

8. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
6. A **Titkosítási technológia** legördülő listán válassza a **Kaspersky lemeztitkosítás** lehetőséget.
A titkosításból kizárt merevlemezeknek megfelelő bejegyzések megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban.
7. A kizárások listájának exportálása:
 - a. Jelölje ki az exportálni kívánt kizárásokat. Több pont kiválasztásához használja a **CTRL** vagy **SHIFT** billentyűket.
Ha nem jelölt ki kizárást, a Kaspersky Endpoint Security az összes kizárást exportálja.
 - b. Kattintson az **Exportálás** hivatkozásra.
 - 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.
8. A szabályok listájának importálása:
 - a. Kattintson az **Importálás** 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.
9. Mentse el a módosításokat.

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
5. Válassza a **Kaspersky Lemeztitkosítás** technológiát, és kövesse a hivatkozást a beállítások konfigurálásához.
Megnyílik a titkosítási beállítások oldala.
6. Kattintson a **Kizárások** hivatkozásra.
7. A szabályok listájának exportálása:
 - a. Jelölje ki az exportálni kívánt kizárásokat.
 - b. Kattintson az **Export** gombra.
 - c. Erősítse meg, hogy csak a kijelölt kizárásokat, vagy a kizárások teljes listáját szeretné exportálni.
 - d. A megnyíló ablakban adja meg az XML-fájl nevét, amelybe exportálni szeretné a kizárások listáját, és válassza a fájl mentésére kiszemelt mappát.
 - e. Mentse a fájlt.
A Kaspersky Endpoint Security a kizárások teljes listáját exportálja az XML-fájlba.
8. A szabályok listájának importálása:
 - a. Kattintson az **Importálás** 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.
9. 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.

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 nem kompatibilis a fiókok bejelentkezési adatait szolgáltató harmadik felekkel.

[A Single Sign-On technológia használatának engedélyezése 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Általános titkosítási beállítások** lehetőséget.
6. A **Jelszóbeállítások** területen kattintson a **Beállítások** gombra.
7. A megnyíló ablak **Hitelesítési ügynök** lapján tegyen jelölést az **Egyszeri bejelentkezés (SSO) technológia használata** jelölőnégyzetbe.
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 engedélyezésének menete a Web Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
5. Válassza a **Kaspersky Lemeztitkosítás** technológiát, és kövesse a hivatkozást a beállítások konfigurálásához.
Megnyílik a titkosítási beállítások oldala.
6. A **Jelszóbeállítások** szakaszban jelölje be az **Egyszeri bejelentkezés (SSO) technológia használata** jelölőnégyzetet.
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 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. Ezt követően a Kaspersky Endpoint Security lecseréli a Windows-fiók jelszavát a Hitelesítési ügynök fiókjának jelszavára.

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. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 (11.8.0)** → **Hitelesítési ügynök fiókok kezelése** lehetőséget.

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 kézzel, 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 **Feladat futtatása, ha a varázsló végzett** 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.

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

2. A **Task type** legördülő listában válassza ki a **Manage Authentication Agent accounts** lehetőséget.

3. A **Task name** mezőben adjon meg egy rövid leírást, például: *Administrator accounts*.

4. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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 **Indítás** 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 létrehozjon Hitelesítési ügynök-fiókokat a meghajtó titkosítása előtt. A Hitelesítési ügynök-fiókok automatikus létrehozását a [teljes lemeztitkosítás rendszabályának beállításai](#)ban 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 ügynöki 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 token vagy okoskártyát. Válasszon tanúsítványfajlt 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** alatt konfigurálja a parancsban megadott felhasználó a hitelesítéshez való hozzáférést a Hitelesítési ügynökben.
12. Mentse el a módosításokat.

[Hitelesítési ügynök hozzáadásának menete a Web Console-on keresztül](#) 

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

Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security alkalmazás **Hitelesítési ügynök fiókok kezelése** feladatára.

Megnyílik a feladatok tulajdonságai ablak.

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

4. A Hitelesítési ügynök-fiókok listájában kattintson a **Hozzáadás** gombra.

Ezzel elindítja a Hitelesítési ügynök-fiókok kezelésének varázslóját.

5. Válassza a **Hozzáadás** 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.
- **Felhasználónév** A Hitelesítési ügynök-fiók alapértelmezett felhasználóneve megegyezik a felhasználó tartománynevével.
- **Jelszóalapú hitelesítés engedélyezése.** 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.
- **Tanúsítványalapú hitelesítés engedélyezése.** 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.
- **Megjegyzés.** Ha szükséges, adjon meg fiókleírást.

8. Mentse el a módosításokat.

9. Tegyen jelölést a feladat melletti jelölőnégyzetbe, majd kattintson az **Indítás** 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 begépelte 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 ki a **Devices** → **Tasks** lehetőséget.

Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security alkalmazás **Hitelesítési ügynök fiókok kezelése** feladatára.

Megnyílik a feladatok tulajdonságai ablak.

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

4. A Hitelesítési ügynök-fiókok listájában kattintson a **Hozzáadás** gombra.

Ezzel elindítja a Hitelesítési ügynök-fiókok kezelésének varázslóját.

5. Válassza a **Módosítás** 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.
- **Felhasználónév** A Hitelesítési ügynök-fiók alapértelmezett felhasználóneve megegyezik a felhasználó tartománynevével.
- **Jelszóalapú hitelesítés engedélyezése.** 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.
- **Tanúsítványalapú hitelesítés engedélyezése.** Válasszon tanúsítványfajlt 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.
- **Megjegyzés.** Ha szükséges, adjon meg fiókleírást.

9. Mentse el a módosításokat.

10. Tegyen jelölést a feladat melletti jelölőnégyzetbe, majd kattintson az **Indítás** 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 ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a Kaspersky Endpoint Security alkalmazás **Hitelesítési ügynök fiókok kezelése** feladatára.
Megnyílik a feladatok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. A Hitelesítési ügynök-fiókok listájában kattintson a **Hozzáadás** gombra.
Ezzel elindítja a Hitelesítési ügynök-fiókok kezelésének varázslóját.
5. Válassza a **Törlés** 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 **Indítás** 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. 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 **Feladatok** részt.
Megnyílik a helyi feladatok listája.
6. Válassza ki a **Hitelesítési ügynök fiókok kezelése** feladatot.
7. 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 ki a **Devices** → **Managed devices** lehetőséget.
2. Kattintson annak a számítógépnek a nevére, amelyen szeretné megtekinteni a Hitelesítési ügynök-fiókok listáját.
Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki a számítógép tulajdonságainak ablakában a **Feladatok** részt.
Megnyílik a helyi feladatok listája.
4. Válassza ki a **Hitelesítési ügynök fiókok kezelése** feladatot.
5. A feladat tulajdonságai között válassza az **Application settings** lapfület.

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 token 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 fejtetni, ha nincs adattitkosítást lehetővé tevő aktív licenc.

A merevlemezek visszafejtése:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
6. Válassza ki a **Titkosítási technológia** legördülő listán a merevlemezek titkosításához használt technológiát.
7. Végezze el az alábbiak egyikét:
 - Válassza ki a **Titkosítási mód** legördülő listán az **Összes merevlemez visszafejtése** lehetőséget, ha az összes titkosított merevlemez vissza szeretné fejtetni.
 - Adja hozzá a visszafejtetni kívánt titkosított merevlemezeket **Ne titkosítsa a következő merevlemezeket** táblázathoz.

Ez a lehetőség csak a Kaspersky lemeztitkosítási technológia esetén használható.

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.

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 merevlemez 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.

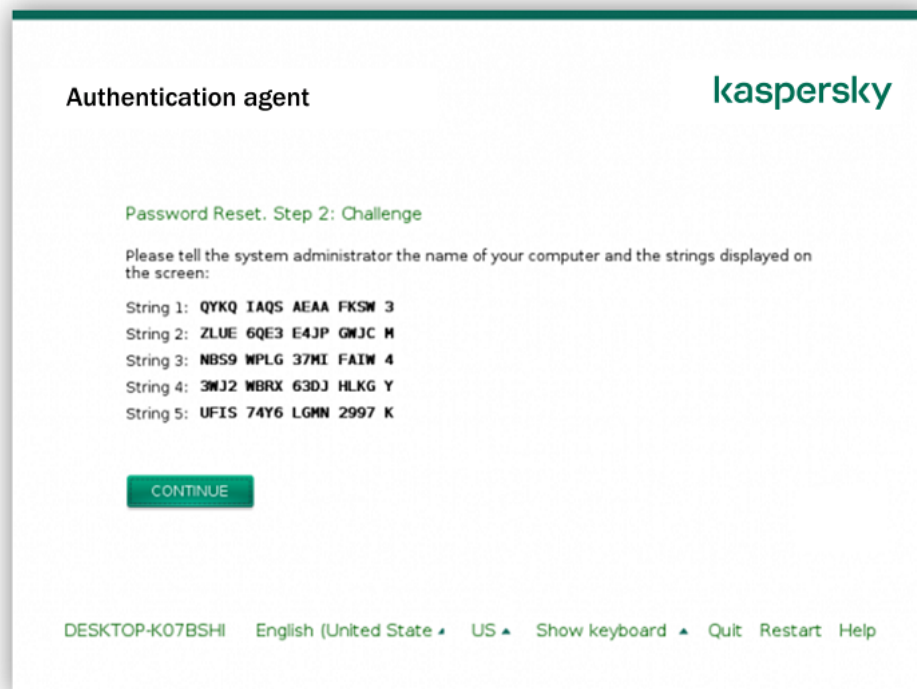
A hozzáférés visszaállítása Kaspersky lemeztitkosítási technológiával védett meghajtóhoz

Ha egy felhasználó elfelejtette a hozzáférési jelszót egy Kaspersky lemeztitkosítási technológiával védett merevlemezhez, el kell indítania a visszaállítási eljárást (kérés–válasz).

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. 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. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
5. A helyi menüben válassza ki a **Grant access in offline mode** lehetőséget.
6. A megnyíló ablakban válassza ki a **Hitelesítési ügynök** lapfület.
7. A **Használatban lévő titkosító algoritmus** területen válasszon titkosítási algoritmust: **AES56** vagy **AES256**.
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.
8. A **Fiók** legördülő listán válassza ki annak a Hitelesítési ügynök-fióknak a nevét, amely a meghajtóhoz való hozzáférése visszaállítását kérő felhasználóhoz tartozik.
9. Válassza ki a **Merevlemez** legördülő listán azt a titkosított merevlemez, amelyhez vissza szeretné állítani a hozzáférést.
10. 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.

[Válaszblokkok beszerzése Kaspersky lemeztitkosítási technológiával védett rendszermerevlemezhez a Web Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.
2. Jelölje be annak a számítógépnek a neve melletti jelölőnégyzetet, amely számítógépben az ismét elérni kívánt meghajtó található.
3. Kattintson a **Grant access to the device in offline mode** gombra.
4. A megnyíló ablakban válassza ki a **Hitelesítési ügynök** részt.
5. Válassza ki a **Felhasználói fiók** 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 hozzáféréseinek 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 beszerzése titkosított, rendszert nem futtató merevlemezhez 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. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
5. A helyi menüben válassza ki a **Grant access in offline mode** lehetőséget.
6. A megnyíló ablakban válassza az **Adattitkosítás** lapfület.
7. Az **Adattitkosítás** lapon kattintson a **Tallózás** gombra.
8. 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.

[Titkosított, rendszert nem futtató merevlemez hozzáférési kulcsfájljának beszerzése a Web Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.
 2. Tegyen jelölést annak a számítógépnek a neve mellé, amelynek adataihoz szeretné visszaállítani a hozzáférést.
 3. Kattintson a **Grant access to the device in offline mode** gombra.
 4. Válassza az **Data encryption** részt.
 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.

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 megkezdji 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 betöltő nem tudja elérni a titkosított meghajtót.

Az operációs rendszer biztonságos frissítéséhez lásd: [Terméktámogatási tudásbázis](#).

Az operációs rendszer automatikus frissítése a következő feltételek esetén lehetséges:

1. Az operációs rendszer a WSUS-on (Windows Server Update Services) keresztül frissül.
2. A Windows 10 1607-es (RS1) vagy újabb verziója van telepítve a számítógépen.
3. A Kaspersky Endpoint Security 11.2.0 vagy újabb verziója van telepítve a számítógépen.

Ha az összes feltétel teljesül, akkor az operációs rendszer a szokásos módon frissíthető.

Ha a Kaspersky lemeztitkosítás (FDE) technológiát használja és a Kaspersky Endpoint Security for Windows 11.1.0 vagy 11.1.1 verzió van telepítve a számítógépen, akkor nem kell visszafejteni a merevlemezeket a Windows 10 frissítéséhez.

Az operációs rendszer frissítéséhez a következőket kell tennie:

1. A rendszer frissítése előtt másolja a cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf és klfdefsf.sys nevű illesztőprogramokat egy helyi mappába. Például, C:\fde_drivers.
2. Futtassa a rendszerfrissítés telepítését a /ReflectDrivers kapcsolóval, és határozza meg a mentett illesztőprogramokat tartalmazó mappát:
`setup.exe /ReflectDrivers C:\fde_drivers`

Ha BitLocker meghajtótitkosítás technológiát használ, akkor a Windows 10 frissítéséhez nem kell visszafejtenie a merevlemezeket. A BitLocker működésének részleteiért lásd a [Microsoft weboldalt](#).

A titkosítás funkció hibáinak elhárításával kapcsolatos frissítés

A Teljes lemeztitkosítás funkció frissítésére az alkalmazásnak a Kaspersky Endpoint Security for Windows 11.8.0 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 nyomkövetési szintjének kiválasztása

Az alkalmazás a nyomkövetési fájlban naplózza a Hitelesítési ügynök működéséről szóló szolgáltatásadatokat, valamint a felhasználó Hitelesítési ügynökkel végzett műveleteiről szóló információkat.

A Hitelesítési ügynök nyomkövetési szintjének kiválasztása:

1. Amint elindul a titkosított merevlemezeket tartalmazó számítógép, nyomja meg az **F3** billentyűt a Hitelesítési ügynök beállításainak megadására szolgáló ablak előhívásához.
2. Válassza ki a nyomkövetési szintet a Hitelesítési ügynök beállításainak ablakában:
 - **Hibakeresési naplózás kikapcsolása (alapértelmezett).** Ha ezt a lehetőséget választja, az alkalmazás nem naplózza a nyomkövetési fájlban a Hitelesítési ügynökre vonatkozó információkat.

- **Hibakeresési naplózás bekapcsolása.** 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.
- **Részletes naplózás bekapcsolása.** 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 **Hibakeresési naplózás bekapcsolása** lehetőségnél. A magas részletességi szint lelassíthatja a Hitelesítési ügynök és az operációs rendszer indítását.

- **Hibakeresési naplózás bekapcsolása és soros port kiválasztása.** 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.

- **Részletes hibakeresési naplózás bekapcsolása és soros port kiválasztása.** 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 **Hibakeresési naplózás bekapcsolása és soros port kiválasztása** lehetőségnél. A magas részletességi szint lelassíthatja a Hitelesítési ügynök és az operációs rendszer indítását.

Adatok akkor kerülnek rögzítésre a Hitelesítési ügynök nyomkövetési fájljába, ha a számítógépen vannak titkosított merevlemezek, illetve a teljes lemeztitkosítás folyamatban van.

Az alkalmazás nyomkövetési fájljaival ellentétben a Hitelesítési ügynök nyomkövetési fájlját nem kapja meg a Kaspersky. Szükség esetén elemzés céljából kézzel 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

5. A rendszabály ablakában válassza az **Adattitkosítás** → **Általános titkosítási beállítások** lehetőséget.

6. A megnyíló **Sablonok** részen kattintson a **Súgó** gombra.

7. A megnyitott ablakban végezze el az alábbiak egyikét:

- 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.

8. 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.

9. 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 sűgőüzeneteiben 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.

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 Security Centeren keresztül 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](#) ².

A BitLocker egy Trusted Platform Module segítségével a hozzáférési kulcsok biztonságos tárolását biztosítja. A *Trusted Platform Module (TPM)* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplaján 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.

A meghajtó titkosítása után a BitLocker főkulcsot hoz létre. A Kaspersky Endpoint Security elküldi a főkulcsot a Kaspersky Security Center számára, hogy Ön [vissza tudja állítani a lemez hozzáférést](#), például akkor, ha a felhasználó elfelejtette a jelszót.

Ha a felhasználó BitLocker használatával titkosítja a lemezt, a Kaspersky Endpoint Security elküldi a [lemeztitkosítás információit a Kaspersky Security Center számára](#). A Kaspersky Endpoint Security azonban nem küldi el a főkulcsot a Kaspersky Security Center számára, szóval a Kaspersky Security Center használatával nem lehet visszaállítani a lemezhez való hozzáférést. Ahhoz, hogy a BitLocker megfelelően működjön a Kaspersky Security Center alkalmazással, [fejtse vissza a meghajtót](#), majd [titkosítsa újra](#) rendszabállyal. Meghajtót helyileg, illetve házirenddel is titkosíthat.

Miután titkosítja a rendszer merevlemezét, a felhasználónak végig kell mennie a BitLocker hitelesítések, hogy elindítsa az operációs rendszert. A BitLocker a hitelesítést követően lehetővé teszi a felhasználó bejelentkezését. A BitLocker nem támogatja az egyszeri bejelentkezési technológiát (SSO).

Ha Windows csoportrendszabályokat használ, kapcsolja ki a BitLocker kezelést a rendszabály-beállításokban. A Windows rendszabály-beállítások összeférhetetlenek lehetnek a Kaspersky Endpoint Security rendszabály-beállításával. 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 működéséptelenné 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](#) ² talál.

[A BitLocker meghajtótitkosítás futtatásának menete az Adminisztrációs Konzolban \(MMC\)](#) ²

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
6. A **Titkosítási technológia** legördülő listán válassza ki az **BitLocker meghajtótitkosítás** lehetőséget.
7. A **Titkosítási mód** legördülő listában 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.

8. Konfigurálja a fejlett BitLocker meghajtótitkosítás opciókat (lásd az alábbi táblázatot).
9. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza az **Data Encryption** → **Full Disk Encryption** lehetőséget.
5. A **Manage encryption** részen válassza ki a **BitLocker meghajtótitkosítás** lehetőséget.
6. Kattintson a **BitLocker meghajtótitkosítás** hivatkozásra.
Ez megnyitja a Bitlocker meghajtótitkosítás beállítási ablakát.
7. 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.

8. Konfigurálja a fejlett BitLocker meghajtótitkosítás opciókat (lásd az alábbi táblázatot).
9. 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.

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 tárolóeszköze, vagy elvesztette).

A BitLocker meghajtótitkosítás összetevő beállításai

Paraméter	Leírás
Rendszerindítás előtt, billentyűzetten keresztül történő BitLocker hitelesítés bekapcsolása táblagépeken	<p>Ez a jelölőnégyzet engedélyezi/letiltja az adatbevitt igénylő hitelesítést rendszerindítás előtti környezetben, még akkor is, ha a platformon nem lehetséges a bevitel rendszerindítás előtt (például táblagépek érintőképernyős billentyűzetei esetén).</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"><p>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.</p></div> <p>Ha a jelölőnégyzet be van jelölve, a rendszerindítás előtti bevitt 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.</p> <p>Ha a jelölőnégyzet üres, a BitLocker meghajtótitkosítás nem érhető el táblagépeken.</p>
Hardveres titkosítás használata (Windows 8 és újabb verziók)	<p>Ha a jelölőnégyzet be van jelölve, az alkalmazás hardveres titkosítást használ. Ennek köszönhetően felgyorsul a titkosítás, és kevesebb számítógépes erőforrást vesz igénybe.</p>
Csak a felhasznált lemezterület titkosítása (Windows 8 és újabb verziók)	<p>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.</p>

A Csak a felhasznált lemezterület titkosítása (Windows 8 és újabb verziók)
funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemez 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 merevlemezeken alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről – azokról is, amelyeket már letörölt, de még visszakereshető információkat tartalmaznak.

Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.

Hitelesítési beállítások

Jelszó használata (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) használata

Ha ez a lehetőség van kiválasztva, a BitLocker Trusted Platform Module-t (TPM) használ.

A *Trusted Platform Module (TPM)* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapiján 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:

- **Use PIN for TPM.** Ezzel a jelölőnégyzettel 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.

Engedélyezheti a felhasználónak a bővített PIN-kód használatát. A *bővített PIN-kód* lehetővé teszi a számokon kívül más karakterek használatát is: latin nagy- és kisbetűket, speciális karaktereket és szóközöket.

- **A Trusted Platform Module (TPM) használata; ha nem érhető el - használja a jelszót.** Ha a jelölőnégyzet be van jelölve, 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.

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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
6. A **Titkosítási technológia** legördülő listán válassza ki az **BitLocker meghajtótitkosítás** lehetőséget.
7. A **Titkosítási mód** legördülő listában válassza ki az **Összes merevlemez titkosítása** elemet.
8. 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza az **Adattitkosítás** → **Teljes lemeztitkosítás** lehetőséget.
5. Válassza a **BitLocker meghajtótitkosítás** technológiát, és kövesse a hivatkozást a beállítások konfigurálásához.
Megnyílik a titkosítási beállítások oldala.
6. A **Titkosítási mód** legördülő listán válassza ki az **Összes merevlemez visszafejtése** elemet.
7. Kattintson az **OK** gombra.

A Titkosítási figyelő eszközzel vezérelheti a lemez titkosítási vagy visszafejtési folyamatát a felhasználó számítógépén. A Titkosítási figyelő eszközt a [fő alkalmazásablakból](#) futtathatja.

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 visszaállítási kulcs–azonosítók megegyeznek, a rendszergazda elküldi a felhasználónak a visszaállítási kulcsot vagy a visszaállítási kulcs-fájlt.

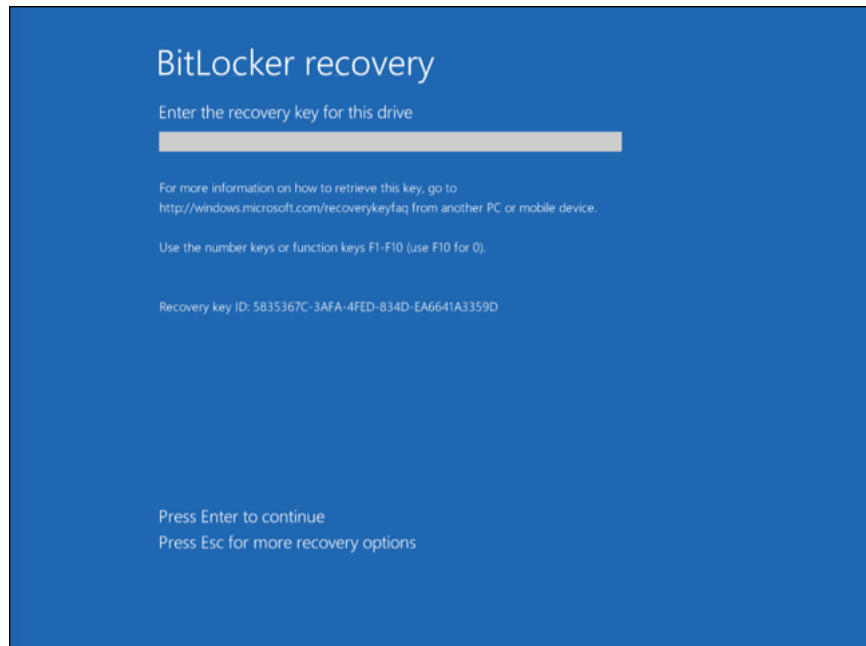
Visszaállítási kulcs-fájl használata a következő operációs rendszert futtató számítógépek esetében indokolt:

- Windows 7;
- Windows 8;
- Windows Server 2008;
- Windows Server 2011;

- Windows Server 2012.

Minden egyéb operációs rendszer esetén visszaállítási kulcs használatos.

4. A felhasználó megadja a visszaállítási kulcsot, és hozzáférést kap a merevlemezhez.



A hozzáférés visszaállítása BitLockerrel titkosított merevlemezhez

Rendszermeghajtó hozzáféréseinek 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. 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. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
5. A helyi menüben válassza ki a **Grant access in offline mode** lehetőséget.
6. A megnyíló ablakban válassza a **Hozzáférés BitLocker-védelemmel rendelkező rendszer meghajtóhoz** lapfület.
7. 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 rendszer meghajtóhoz 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 továbbítani kell a felhasználónak.

[BitLockerrel titkosított rendszer meghajtó visszaállítási kulcsának megtekintése a Web Console-ban és a Cloud Console-ban](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.
2. Jelölje be annak a számítógépnek a neve melletti jelölőnégyzetet, amely számítógépben az ismét elérni kívánt meghajtó található.
3. Kattintson a **Grant access to the device in offline mode** gombra.
4. A megnyíló ablakban válassza a **BitLocker** részt.
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 rendszer meghajtóhoz való hozzáférés visszaállítására. Győződjön meg arról, hogy a kiválasztott számítógép neve egyezik a felhasználó számítógépének nevével.

6. Kattintson a **Receive key** gombra.

Ekkor hozzáférést kap a visszaállítási kulcshoz vagy a visszaállítási kulcs fájljához, amelyet továbbítani 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 főkulcsot, és elküldi a kulcsot 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 titkosítani a merevlemezt.

Hozzáférés visszaállítása rendszert nem futtató meghajtóhoz

A helyreállítási eljárás elindításához a felhasználónak rá kell kattintania a **Forgot your password** hivatkozásra a meghajtó elérését kínáló ablakban. Miután megkapta a hozzáférést a titkosított meghajtóhoz, a felhasználó a BitLocker beállításaiiban 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 a Felügyeleti konzol fájában a **További** → **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 for Windows 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.

[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 a **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 a **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 a **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. Az Adminisztrációs Konzolon nyissa meg az **Administration Server** → **Tasks** mappát.

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 (11.8.0)** → **BitLocker-védelem felügyelete** lehetőséget.

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 lejáratási 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 kézzel, 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 **Feladat futtatása, ha a varázsló végzett** jelölőnégyzetbe. A feladat előrehaladását a feladat tulajdonságainál tudja nyomon követni.

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló. Kövesse a varázsló utasításait.

1. lépés. Általános feladatbeállítások megadása

Az általános feladatok beállításainak megadása:

1. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.
2. A **Task type** legördülő listából válassza ki a **BitLocker-védelem felügyelete** lehetőséget.
3. A **Task name** mezőben adjon meg egy rövid leírást, például *Updating to Windows 10*.
4. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

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 lejárat 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 **Indítás** 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 Kaspersky Security Center konzolban megtudhatja a számítógép tulajdonságaiban lévő fennmaradó újraindítások számát is.

Amikor eléri a megadott számú újraindítást vagy a feladat lejárat 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

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 fájl titkosítás a következő speciális tulajdonságokkal rendelkezik:

- A Kaspersky Endpoint Security csak az operációs rendszer helyi felhasználói profiljai esetén titkosítja és fejt 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 fejt 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 fájl titkosítási 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 találhatóak, 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Fájl szintű titkosítás** lehetőséget.

6. A **Titkosítási mód** legördülő listában válassza ki **A szabályoknak megfelelően** elemet.

7. 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 profilk 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.
- **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 kézzel 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. Használhatja a \..\ karakterláncot (pl. C:\Users\..\UserFolder\). A \..\ karakterlánc a szülőkönyvtárra való áttérést jelöli.
- 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.

8. 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 visszafejteni 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 visszafejteni 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

A titkosított fájlok hozzáférési szabályainak kialakítása az alkalmazások számára:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Fájl szintű titkosítás** lehetőséget.
6. 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.

7. Az ablak jobb oldalán válassza ki a **Szabályok az alkalmazásokhoz** lapot.
8. 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** gombra.

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 **Szabályok az alkalmazásokhoz** legördülő listán azt a szabályt, amely az alkalmazások titkosított fájlokhoz való hozzáférését megszünteti.

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 a **Szabályok az alkalmazásokhoz** lapon lévő táblázatban jelennek meg.

9. Ha kézilleg 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 **Szabályok az alkalmazásokhoz** legördülő listán azt a szabályt, amely az alkalmazások titkosított fájlokhoz való hozzáférését megszünteti.

Az alkalmazások titkosított fájlokhoz való hozzáférési szabályainak adatai a **Szabályok az alkalmazásokhoz** lapon lévő táblázatban jelennek meg.

10. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Fájl szintű titkosítás** lehetőséget.
6. 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.

7. Az ablak jobb oldalán válassza ki a **Szabályok az alkalmazásokhoz** lapot.
8. 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** gombra.

A táblázatban megjelennek alkalmazott szűrőknek megfelelő alkalmazások.
 - c. Az **Alkalmazás** oszlopban tegyen jelölést azon alkalmazások jelölőnégyzetébe, amelyek létrehozott fájljait titkosítani szeretné.
 - d. A **Szabályok 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 a **Szabályok az alkalmazásokhoz** lapon lévő táblázatban láthatók.

9. Ha kézíleg 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 **Szabályok az alkalmazásokhoz** legördülő listán válassza ki az **Összes létrehozott fájl titkosítása** elemet.

A kiválasztott alkalmazások által létrehozott és módosított fájlok titkosítási szabályára vonatkozó információk a **Szabályok az alkalmazásokhoz** lapon lévő táblázatban láthatók.

10. Mentse el a módosításokat.

Visszafejtési szabály előállítása

Visszafejtési szabály előállítása:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Fájl szintű titkosítás** lehetőséget.
6. A **Titkosítási mód** legördülő listában válassza ki **A szabályoknak megfelelően** elemet.
7. 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 proflok mappáiban lévő fájlok visszafejtési szabályhoz való hozzáadásához.
 - b. Válassza ki az **Egyéni mappa** elemet kézzel 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.
8. 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. 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. A munkaterületen válassza ki a **Policies** lapot.

4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Fájl szintű titkosítás** lehetőséget.
6. Az ablak bal oldalán válassza ki a **Titkosítás** fület.
7. 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 az **Eltávolítás** gomb helyi menüjében.
A titkosítási listáról eltávolított fájlok és mappák automatikusan a visszafejtési listára kerülnek.
8. [Fájlvisszafejtési lista kialakítása.](#)
9. 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 fejt 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 felhasználtól. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Általános titkosítási beállítások** lehetőséget.
6. A **Jelszóbeállítások** területen kattintson a **Beállítások** gombra.
7. A megnyíló ablakban válassza a **Titkosított csomagok** lapfület.
8. Adja meg a jelszóösszetettségi 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Válassza az **Adattitkosítás** → **Fájl szintű titkosítás** lehetőséget.
5. A **Titkosított csomag jelszóbeállításai** 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.

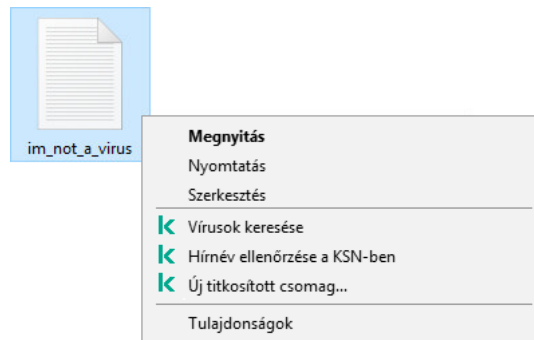
Egy fájl olyan titkosított csomaghoz történő hozzáadásánál, ami tartalma a OneDrive felhőtárhelyen van, a Kaspersky Endpoint Security letölti a fájl tartalmát, majd végrehajtja a titkosítást.

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).
3. A megnyíló ablakban válassza ki egy helyet a cserélhető meghajtón, hogy elmentse a titkosított csomagot → adja meg a csomag nevét majd kattintson a **Mentés** gombra.
4. A megnyíló ablakban adja meg a jelszót, majd erősítse meg azt.
A jelszónak meg kell felelnie a rendszabályban meghatározott összetettségi kritériumoknak.

5. Kattintson a **Létrehozás** gombra.

Elindul a titkosított csomag létrehozásának folyamata. A Kaspersky Endpoint Security nem végez fájlömörítést 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.



Titkosított csomag létrehozása

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 hozzáféréseinek 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 fiókban 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 lemezekben lévő titkosított fájlokat megnyithatja, de tartalmuk titkosítottan jelenik meg.

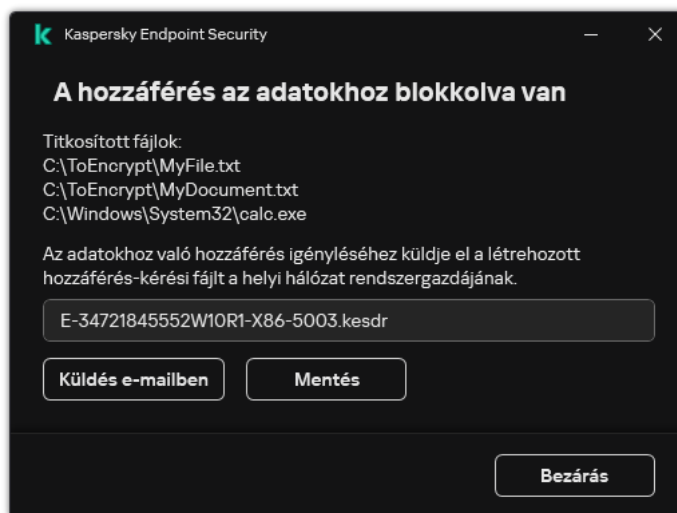
A felhasználó az alábbi körülmények esetén dolgozhat titkosított fájlokkal:

- 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 (kérelemválasz).

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 hozzáféréseinek 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. 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. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
5. A helyi menüben válassza ki a **Grant access in offline mode** lehetőséget.
6. A megnyíló ablakban válassza az **Adattitkosítás** lapfület.
7. Az **Adattitkosítás** lapon kattintson a **Tallózás** gombra.
8. 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.

Titkosítottadat-hozzáférési kulcsfájl beszerezésének menete a Web Console-ban

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.
2. Tegyen jelölést annak a számítógépnek a neve mellé, amelynek adataihoz szeretné visszaállítani a hozzáférést.
3. Kattintson a **Grant access to the device in offline mode** gombra.
4. Válassza az **Data encryption** részt.
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 meghajtóként külön hozzáférési kulcsfájlt kell beszerezni.

Titkosított adatokhoz való hozzáférés visszaállítása az operációs rendszer hibáját követően

Operációs rendszerhiba után csak fájl szintű 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Általános titkosítási beállítások** lehetőséget.
6. A megnyíló **Sablonok** részen kattintson a **Sablonok** gombra.
7. A megnyitott ablakban végezze el az alábbiak egyikét:
 - Ha a felhasználói üzenetsablont szeretné szerkeszteni, válassza ki a **Felhasználó üzenete** lapot. Az **A hozzáférés az adatokhoz blokkolva van** 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. Ha a **Küldés e-mailben** gombra kattint **A hozzáférés az adatokhoz blokkolva van** ablakban, automatikusan létrejön a felhasználói üzenet. Ezt az üzenetet a vállalati helyi hálózati rendszergazda kapja meg a titkosított fájlokhoz való hozzáférést kérő fájljal együtt.
 - Ha a rendszergazdai üzenetsablont szeretné szerkeszteni, válassza ki a **Rendszergazda üzenete** lapot. Ez az üzenet automatikusan létrejön, amikor a **Küldés e-mailben** gombra kattint a **Hozzáférés kérése a titkosított fájlokhoz** ablakban, és elküldésre kerül a felhasználó részére, miután a felhasználó hozzáférést kapott a titkosított fájlokhoz.
8. Szerkessze az üzenetsablonokat.
9. Mentse el a módosításokat.

Cserélhető meghajtók titkosítása

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:

- Teljes lemeztitkosítás (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 vállalati hálózaton belül sem lehetséges, ha a számítógép nincs csatlakoztatva a Kaspersky Security Centerhez (pl „vendég” számítógépen).

- Fájl szintű titkosítás (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. Visszafejt 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 fejt 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 és az NTFS fájlrendszerek titkosítását támogatja. Ha egy nem támogatott fájlrendszerű cserélhető meghajtó van csatlakoztatva a számítógéphez, a cserélhető meghajtó titkosítása hibás lesz, a Kaspersky Endpoint Security pedig csak olvasható állapotot rendel a cserélhető meghajtóhoz.

Cserélhető meghajtók titkosítása:

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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.

5. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.

6. 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.

7. 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.

8. 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.

9. Ha konfigurálni szeretné az egyéni cserélhető meghajtót titkosítását, akkor adjon meg [titkosítási szabályokat](#).

10. 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.

11. Mentse el a módosításokat.

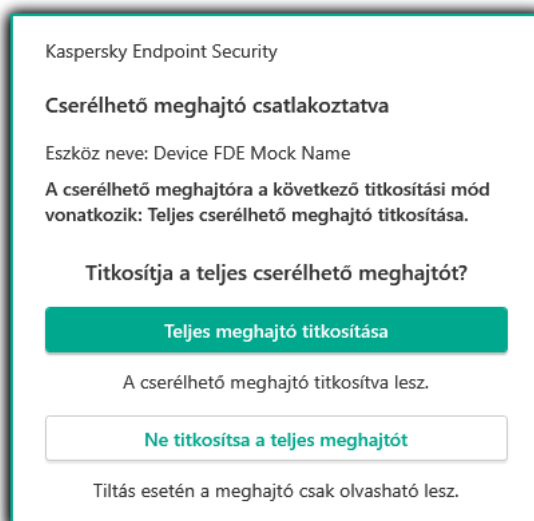
A rendszabály alkalmazása után, ha a felhasználó csatlakozik egy cserélhető meghajtóhoz, vagy egy cserélhető meghajtó már csatlakoztatva van, a Kaspersky Endpoint Security a felhasználó megerősítését kéri, hogy titkosítási műveletet végezzen el (lásd az alábbi ábrát).

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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.
6. 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 eszközlístájából** lehetőséget.

7. Válassza ki a **Titkosítási mód a kiválasztott eszközökhöz** legördülő listán azt a műveletet, amelyet a Kaspersky Endpoint Security a kiválasztott cserélhető meghajtókon tárolt fájlokra végez.

8. 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.

9. 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 – azokról is, amelyeket már letörölt, de még visszakereshető információkat tartalmaznak. 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 nem foglalt szektorok továbbra sem lesznek titkosítva.

10. 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.

11. 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.
6. Cserélhető meghajtók titkosítási szabályait tartalmazó lista exportálása:
 - a. Jelölje ki az exportálni kívánt szabályokat. Több pont 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. 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.
8. Mentse el a módosításokat.

[A cserélhető meghajtó titkosítási szabályait tartalmazó lista exportálása és importálása a Web Console-ban](#) 

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** elemre.
5. A **Titkosítási szabályok a kiválasztott eszközökhöz** blokkban kattintson a **Titkosítási szabályok** 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 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.

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:

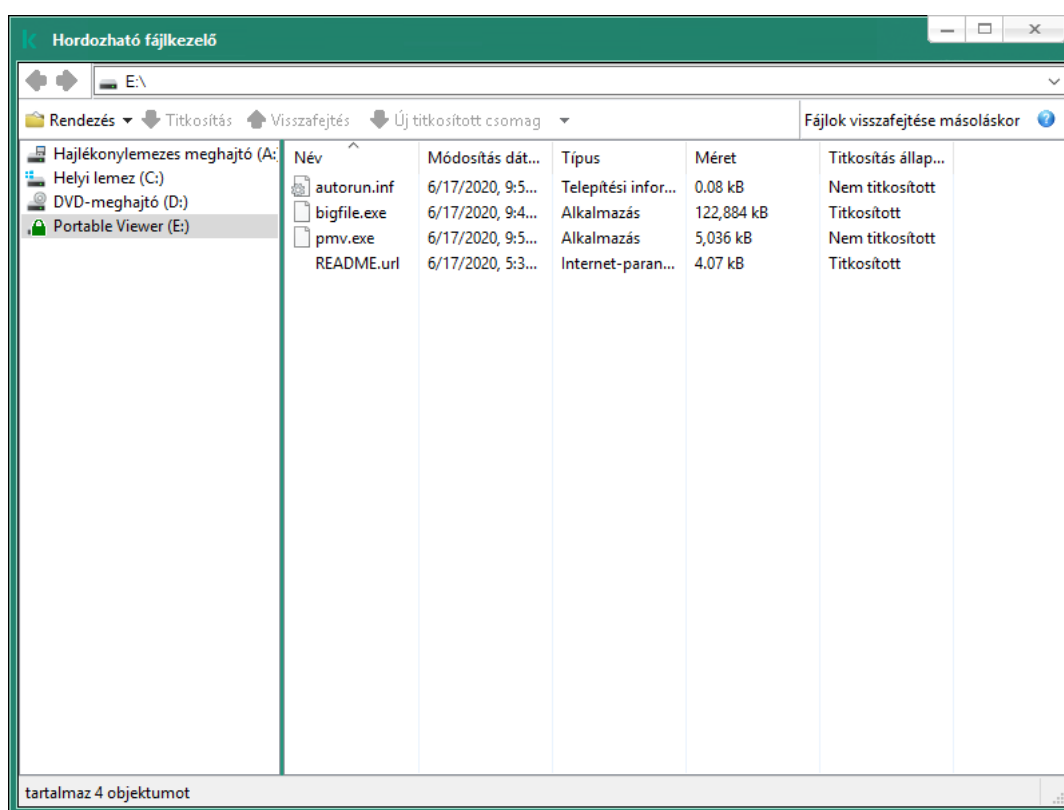
- ha nincs kapcsolat a számítógép és a Kaspersky Security Center felügyeleti kiszolgáló között;
- ha megváltozott az infrastruktúra a Kaspersky Security Center felügyeleti kiszolgáló módosításakor;
- ha a Kaspersky Endpoint Security nincs telepítve a számítógépre.

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 fájl titkosításához. A kulcs titkosítása a felhasználó jelszavával történik. A felhasználó beállít egy jelszót a cserélhető meghajtón tárolt fájl 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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitására.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.
6. 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 fájl szintű titkosítás (FLE) esetében érhető el. Nincs mód a hordozható mód támogatására aktiválására FDE (Full Disk Encryption – Teljes lemeztitkosítás) esetén.

7. Jelölje be a **Hordozható mód** jelölőnégyzetet.
8. Ha szükséges, [adjon hozzá titkosítási szabályokat az egyes cserélhető meghajtókhoz](#).
9. Mentse el a módosításokat.
10. A rendszabály alkalmazását követően csatlakoztassa a cserélhető meghajtót a számítógéphez.
11. Erősítse meg a cserélhető meghajtó titkosítási műveletét.
Ekkor megnyílik egy ablak, amelyben jelszót hozhat létre a Hordozható fájlkezelő számára.
12. Adjon meg a jelszóerősségi követelményeknek megfelelő jelszót, és erősítse meg.
13. 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.

[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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Lépjen az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** elemre.
5. A **Titkosítás kezelése** részen válassza az **Összes fájl titkosítása** vagy a **Csak az új fájlok titkosítása** lehetőséget.

A hordozható mód kizárólag a fájl szintű titkosítás (FLE) esetében érhető el. Nincs mód a hordozható mód támogatására aktiválására FDE (Full Disk Encryption – Teljes lemeztitkosítás) esetén.

6. Jelölje be a **Hordozható mód** jelölőnégyzetet.
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.
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.

- 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.

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. 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. A **Devices** lapon válassza ki a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
5. A helyi menüben válassza ki a **Grant access in offline mode** lehetőséget.
6. A megnyíló ablakban válassza az **Adattitkosítás** lapfület.
7. Az **Adattitkosítás** lapon kattintson a **Tallózás** gombra.
8. 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.

Titkosítottadat-hozzáférési fájl beszerezésének menete a Web Console-ban

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.
2. Tegyen jelölést annak a számítógépnek a neve mellé, amelynek adataihoz szeretné visszaállítani a hozzáférést.
3. Kattintson a **Grant access to the device in offline mode** gombra.
4. Válassza az **Data encryption** részt.
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. 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A rendszabály ablakában válassza az **Adattitkosítás** → **Cserélhető meghajtók titkosítása** lehetőséget.
6. Ha a cserélhető meghajtókon lévő összes titkosított fájlt vissza szeretné fejtetni, válassza a **Titkosítási mód** legördülő listán a **Teljes cserélhető meghajtó visszafejtése** lehetőséget.
7. Ha egyes cserélhető meghajtókon lévő adatokat szeretne visszafejtetni, szerkessze azon cserélhető meghajtók titkosítási szabályait, amelyek az adatait vissza szeretné fejtetni. 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 kattintson a **Teljes cserélhető meghajtó visszafejtése** elemre.
8. 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 következő titkosítási állapotértékek lehetségesek:

- *Nincs definiált titkosítási házirend.* A számítógépen nincs Kaspersky Security Center titkosítási házirend definiálva.
- *Alkalmazandó rendszabály.* A számítógépen adattitkosítás és / vagy -visszafejtés zajlik.

- *Hiba.* A számítógépen adattitkosítás és / vagy -visszafejtés közben hiba történt.
- *Újraindítás szükséges.* A számítógépen az adattitkosítás és / vagy -visszafejtés elkezdéséhez vagy befejezéséhez újra kell indítani az operációs rendszert.
- *Rendszabálynak megfelel.* A számítógépen az adattitkosítás a Kaspersky Security Center számítógépre alkalmazott rendszabályában megadott titkosítási beállításoknak megfelelően elkészült.
- *Felhasználó által megszakítva.* A felhasználó nem erősítette meg a fájlitkosítási műveletet a cserélhető meghajtón.

A titkosítási állapot megtekintése

A számítógép adatai titkosítási állapotának megtekintése:

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. A munkaterület **Devices** lapján csúsztassa a görgetősávot a jobb szélső állásba.
5. Ha az **Encryption status** oszlop nem jelenik meg:
 - a. Kattintson a jobb egérgombbal a táblázat fejléc helyi menüjének megnyitására.
 - b. A helyi menüben, a **Megtekintés** legördülő listán válassza ki az **Add/Remove columns** lehetőséget.
 - c. A megnyíló ablakban jelölje be a **Titkosítás állapota** jelölőnégyzetet.
 - d. Kattintson az **OK** gombra.

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.

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. A megnyitott ablakban kattintson a **Hozzáadás** gombra.
- c. Ekkor megnyílik egy ablak, amelyben a **General** részbe írja be az oldal nevét.
- d. Az **Information panels** részen kattintson az **Add** gombra.
- e. A megnyitott 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 **Cserélhető meghajtók titkosítása** 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 a **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. 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. Válassza ki a számítógép nevét a listán, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.
5. A számítógép helyi menüjében válassza ki a **Properties** elemet. A megnyíló ablakban válassza a **Protection** szakaszt.
6. Kattintson a **View data encryption errors** hivatkozásra a **Data encryption errors** ablak megnyitásához.

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

Az adattitkosítási jelentés megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol **Administration Server** csomópontján válassza ki a **Reports** lapot.
3. Kattintson a **New report template** gombra.
Ekkor elindul az új Jelentéssablon varázsló.
4. Kövesse a Jelentéssablon-varázsló utasításait. Válassza ki a **Selecting the report template type** ablak **Other** részében az alábbi elemek közül valamelyiket:
 - **Report on encryption status of managed devices.**
 - **Report on encryption status of mass storage devices.**
 - **Report on file encryption errors.**
 - **Report on blockage of access to encrypted files.**

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 előállítás 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 eszközökhöz 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 található. 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 rendszermeleveleken 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.

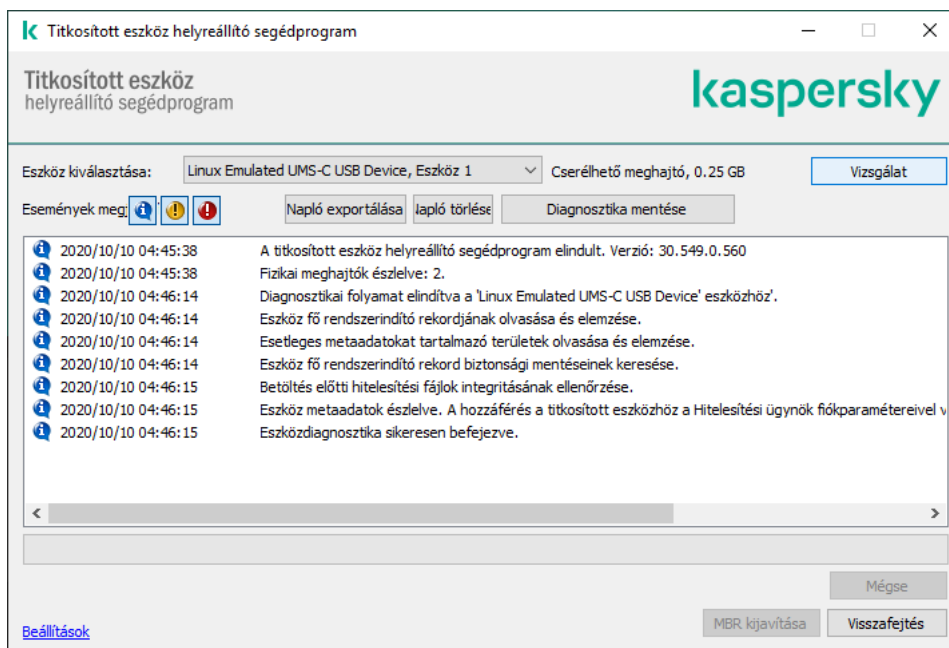
Javasoljuk, hogy a titkosított eszközökön lévő adatok visszaállítása előtt szakítsa meg azon a számítógépen a Kaspersky Security Center titkosítási rendszabályát, illetve tiltsa le a titkosítást a Kaspersky Security Center rendszabály-beállításában, amelyen a műveletet elvégzi. Ez megakadályozza az eszköz 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 található. Az ilyen adatok illetéktelen elérésének kockázata csökkentése érdekében javasoljuk, hogy a titkosított eszközökhöz való hozzáférést megbízható számítógépeken állítsa vissza.

Adatok visszaállítása merevlemezen

Titkosított eszközökhöz 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 a Felügyeleti konzol fájlában a **További** → **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 for Windows alkalmazásban** lehetőségre.

Ha nem biztos abban, hogy a hozzáférés-kérési fájl melyik számítógéphez készült, válassza ki a Felügyeleti konzol fájlában a **További** → **Adattitkosítás- és védelem** mappát, és a munkaterületen kattintson az **Eszköztitkosítási kulcs beszerzése a Kaspersky Endpoint Security for Windows 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: *Erős titkosítás (AES256)* vagy *Könnyű titkosítás (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 **Open** 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 a **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 a **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: *Erős titkosítás (AES256)* vagy *Könnyű titkosítás (AES56)*. Az AES-titkosítási könyvtár az alkalmazással együtt van telepítve.

- c. Kattintson a **Fájl kijelölése** gombra, és jelölje ki a felhasználótól kapott hozzáférés-kérési (FDERTC kiterjesztésű) fájlt.

- d. Kattintson a **Save key** gombra, és válasszon egy mappát a titkosított adatok eléréséhez használandó (FDERTR kiterjesztésű) kulcsfájl mentéséhez.

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 találhatóak (például a [Microsoft TechNet erőforrásban](#)).

Detection and Response-megoldások

A Kaspersky Endpoint Security beépített ügynök használatával támogatja a Detection and Response-megoldásokat. A Detection and Response használatához az alkalmazás telepítésekor engedélyeznie kell a megoldások integrálását. 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 Sandbox 2.0.

A Kaspersky Endpoint Security a Kaspersky Endpoint Agent terjesztőkészletet is tartalmazza. A Kaspersky Endpoint Agent támogatja a Kaspersky Anti Targeted Attack Platform (Endpoint Detection and Response Expert (KATA EDR) összetevőt). A Kaspersky Endpoint Security telepítéséhez az alkalmazás telepítésekor ki kell választania az Endpoint Agent összetevőt.

Nem lehet a beépített ügynököt és a Kaspersky Endpoint Agentet is kiválasztani a telepítéskor. Ha a beépített ügynök és a Kaspersky Endpoint Agent telepítése is szükséges, a Kaspersky Endpoint Agentet külön kell telepítenie.

A Kaspersky Endpoint Security a Detection and Response megoldással együtt különböző konfigurációkban használható, amilyen például az [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

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 for Windows és az önálló megoldással kapcsolatos részletes információkért olvassa el a megfelelő termék súgóját:

- *A Kaspersky Célzott Támadások Elleni Platform súgója*
- *A Kaspersky Sandbox súgója*
- *A Kaspersky Endpoint Detection and Response Optimum súgója*
- *A Kaspersky Managed Detection and Response súgója*

A Kaspersky Endpoint Agent beletartozik a [Kaspersky Endpoint Security terjesztőkészletbe](#). A Kaspersky Endpoint Agent alkalmazást a Kaspersky Endpoint Security telepítése során telepítheti. Ehhez válassza az Endpoint Agent összetevőt az alkalmazás telepítése során (például a [telepítőcsomagban](#)). Miután az Endpoint Agent segítségével telepíti az alkalmazást, a Kaspersky Endpoint Security és a Kaspersky Endpoint Agent hozzá lesz adva a telepített alkalmazások listájához. Miután törli a Kaspersky Endpoint Security alkalmazást, a Kaspersky Endpoint Agent is automatikusan törölve lesz.

A Kaspersky Endpoint Agent-terjesztőkészlet a Kaspersky Endpoint Security for Windows-terjesztőkészlet része.

A KES- és KEA-verziók megfeleltetése

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

Szabályzatok és feladatok áttelepítése a Kaspersky Endpoint Agent számára

A Kaspersky Endpoint Security 11.7.0 most már rendelkezik egy olyan varázslóval, amellyel elvégezhető a Kaspersky Endpoint Agent szolgáltatásról a Kaspersky Endpoint Security szolgáltatásra való áttérés. A szabályzat- és feladatbeállításokat a következő megoldások esetén telepítheti át:

- Kaspersky Sandbox;
- Kaspersky Endpoint Detection and Response (EDR);
- Kaspersky Managed Detection and Response (MDR).

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 főablakában válassza ki 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 listában 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:

- 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 szabályzat *inaktív* állapotú. A folytatáshoz módosítsa a Kaspersky Endpoint Agent és a Kaspersky Endpoint Security szabályzatok állapotát *Inaktív* 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 feladatok másolatai a Kaspersky Endpoint Detection and Response és a Kaspersky Sandbox számára. Emellett a varázsló változatlanul hagyja a Kaspersky Endpoint Agent feladatait.

A [KES+KEA] konfiguráció migrálása a [KES+beépített ügynök] konfigurációra

A Kaspersky Endpoint Security 11.7.0 mostantól beépített ügynökökkel rendelkezik a Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) és a Kaspersky Sandbox 2.0 megoldásokhoz. Az ezekkel a megoldásokkal való együttműködéshez már nincs szükség külön Kaspersky Endpoint Agent alkalmazásra. A Kaspersky Endpoint Security 11.7.0 verzióra történő frissítésekor az EDR Optimum és a Kaspersky Sandbox megoldások továbbra is együttműködnek a Kaspersky Endpoint Security-vel. Emellett a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről.

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 verzióra, beleértve a felhasználói számítógépeken lévő Felügyeleti 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 verzióra. Az EDR Optimum és a Kaspersky Sandbox összetevők kezeléséhez a Web Console-t kell használnia.

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 szabályzat *inaktív* állapotú. A házirend alkalmazásához nyissa meg a házirend tulajdonságait, fogadja el a Kaspersky Security Network nyilatkozatot, és állítsa az állapotot *Aktív* értékre.

4 Licenelési 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 más 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 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 [Kulcs hozzáadása](#) 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.

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 az Endpoint Detection and Response Optimum vagy a Kaspersky Sandbox összetevőket a telepítőcsomag beállításában.
- Hagyja ki a Kaspersky Endpoint Agent összetevőt a telepítőcsomag beállításában.

Az alkalmazást a következő módszerekkel is frissítheti:

- A Kaspersky frissítési szolgáltatás használatával (zökkenőmentes frissítés – SMU).
- Helyben, a Telepítővarázsló segítségével.

Ebben az esetben ellenőrizze a számítógépre telepített Kaspersky Endpoint Agent konfigurációját. Ha a telepített Kaspersky Endpoint Agent tartalmazza a KATA EDR (Endpoint Detection and Response Expert) összetevőt, az alkalmazás frissítése előtt távolítsa el ezt az összetevőt. Ha nem tudja eltávolítani az Endpoint Detection and Response Expert (KATA EDR) összetevőt, a Kaspersky Endpoint Security az alkalmazás frissítésekor kihagyja az EDR Optimum és a Kaspersky Sandbox összetevőket. Az összetevők telepítését az alkalmazás frissítése után az [Alkalmazásösszetevők módosítása](#) feladattal végezheti el.

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 aktív 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 aktív licenceihez. Ilyenkor a Kaspersky Endpoint Security automatikusan a következőképpen választja ki az összetevőket a Kaspersky Endpoint Agent konfigurációja alapján:

- Ha az Endpoint Detection and Response Expert (KATA EDR) összetevő telepítve van, a Kaspersky Endpoint Security kiválasztja az Endpoint Agent összetevőt. A Kaspersky Endpoint Security csak az Endpoint Agent összetevőt választja ki, akkor is, ha a Kaspersky Endpoint Agent rendelkezik egyéb telepített összetevőkkel is, amilyen például a [KATA EDR+KSB] konfiguráció.
- Ha a Kaspersky Sandbox összetevő, az EDR Optimum vagy a [Kaspersky Sandbox+EDR Optimum] konfiguráció telepítve van, a Kaspersky Endpoint Security kiválasztja a megfelelő összetevőket. Ezáltal 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 *Kritikus*:

- Győződjön meg arról, hogy a számítógépen telepítve van a 13.2 verziójú Felügyeleti ügynök.
- Ellenőrizheti az EDR Optimum és a Kaspersky Sandbox összetevők működési állapotát az *alkalmazás-összetevői állapotjelentés* megtekintésével. Ha egy összetevő állapota *Nincs telepítve*, telepítse az összetevőt az [Alkalmazásösszetevők módosítása](#) 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 *Alkalmazásösszetevők állapotjelentés* 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](#).

Az alkalmazás frissítése a KATA EDR részeként

Ha a Kaspersky Endpoint Agent telepítve van a Kaspersky Anti Targeted Attack Platformmal (Endpoint Detection and Response Expert [KATA EDR] összetevő) való integrációhoz, akkor a Kaspersky Endpoint Security for Windows megoldást a következő módokon frissítheti:

- Távoli telepítés feladat használata.

Ehhez az alábbi beállításokat kell módosítania:

- Hagyja ki az Endpoint Detection and Response Optimum vagy a Kaspersky Sandbox összetevőket a telepítőcsomag beállításaiban.
- Válassza ki a Kaspersky Endpoint Agent összetevőt a telepítőcsomag beállításaiban. Ha a számítógépen már telepítve van a Kaspersky Endpoint Agent, az alkalmazás a 3.11-es verzióra frissül.

- A Kaspersky frissítési szolgáltatás használatával (SMU).

Ehhez meg kell erősítenie az alkalmazás frissítését. A Kaspersky Endpoint Security kizárja a telepítésből az Endpoint Detection and Response Optimum és a Kaspersky Sandbox szolgáltatást. A Kaspersky Endpoint Agent frissítése nem támogatott. A Kaspersky Endpoint Agent manuálisan is frissíthető.

- Helyben, a Telepítővarázsló segítségével.

A Kaspersky Endpoint Security kizárja a telepítésből az Endpoint Detection and Response Optimum és a Kaspersky Sandbox szolgáltatást. Ha a számítógépen már telepítve van a Kaspersky Endpoint Agent, az alkalmazás a 3.11-es verzióra frissül.

Managed Detection and Response



A Kaspersky Endpoint Security 11.6.0 bevezeti a Managed Detection and Response megoldáshoz készült beépített ügynököt. 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](#).

Integráció az MDR-rel

A Kaspersky Managed Detection and Response integrációjának beállításához engedélyeznie kell a Managed Detection and Response összetevőt, és konfigurálnia kell a Kaspersky Endpoint Security alkalmazást.

A Managed Detection and Response összetevő nem kompatibilis az Endpoint Detection and Response Expert összetevővel.

Engedélyeznie kell a következő összetevőket a Managed Detection and Response használatához:

- [Kaspersky Security Network \(kiterjesztett mód\)](#).
- [Viselkedéselemzés](#).

Ezen összetevők engedélyezése nem opcionális. Ellenkező esetben a Kaspersky Managed Detection and Response nem tud működni, mert nem kapja meg a szükséges telemetriai adatokat.

Ezenkívül a Kaspersky Managed Detection and Response a más alkalmazásösszetevőktől kapott adatokat használja. Ezen összetevők engedélyezése opcionális. A további adatokat szolgáltató összetevők a következők:

- [Web védelem](#).
- [Levelezés védelem](#).
- [Tűzfal](#).

Ahhoz, hogy a Kaspersky Managed Detection and Response működni tudjon a Felügyeleti kiszolgálóval a Kaspersky Security Center Web Console-on keresztül, létre kell hoznia egy új, biztonságos kapcsolatot, egy *háttérkapcsolatot*. A Kaspersky Managed Detection and Response a megoldás telepítésekor rákérdez a háttérkapcsolat létrehozására. Győződjön meg arról, hogy létrejött a háttérkapcsolat. A Kaspersky Security Center és más Kaspersky-megoldások integrálásával kapcsolatos részletekért tekintse meg a [Kaspersky Security Center](#) [☞] [súgóját](#).

A Kaspersky Managed Detection and Response integrálása a következő lépéseket foglalja magában:

1 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 helyi Kaspersky Security Network szolgáltatást az MDR bővítmény telepítésekor.

A Privát KSN támogatja a számítógépek és a Kaspersky Security Network dedikált kiszolgálói közötti adatcserét, de a globális KSN nem.

Töltse fel a Kaspersky Security Network konfigurációs fájlt 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 fájlt 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 KSN 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 Private KSN-t használja a fájlok, az alkalmazások és a webhelyek megbízhatóságának meghatározására. A **Kaspersky Security Network** részen a szabályzat beállításai a következő működési állapotot mutatják: *KSN hálózat: Privát KSN*.

[Engedélyeznie kell a kiterjesztett KSN módot](#) a Managed Detection and Response használatához.

2 Aktiválja a Managed Detection and Response szolgáltatást

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](#) [?] talál.

[A Managed Detection and Response aktiválásának 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. A munkaterületen válassza ki a **Policies** lapot.
4. Válassza ki a szükséges rendszabályt, és kattintson duplán a házirend tulajdonságainak megnyitásához.
5. A házirend ablakban válassza ki a **Detection and Response** → **Managed Detection and Response** lehetőséget.
6. Jelölje be a **Managed Detection and Response** jelölőnégyzetet.
7. A **Beállítások** területen kattintson az **Importálás** elemre, és válassza ki a Kaspersky Managed Detection and Response konzoljában kapott BLOB fájlt. A fájl P7 kiterjesztéssel rendelkezik.
8. Mentse el a módosításokat.

[A Managed Detection and Response aktiválásának menete a Web Console-ban és a Cloud Console-ban](#) [?]

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Managed Detection and Response** elemet.
5. Kapcsolja be a **Managed Detection and Response** kapcsolót.
6. Kattintson az **Import** elemre, és válassza ki a Kaspersky Managed Detection and Response konzoljában kapott BLOB fájlt. A fájl P7 kiterjesztéssel rendelkezik.
7. Mentse el a módosításokat.

[A Managed Detection and Response aktiválásának 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 feltölti a fájlt, és elküldi azt a számítógépre a Kaspersky Security Centerrel való következő szinkronizálás során. Ellenőrizheti az összetevő működési állapotát az *alkalmazás-összetevői állapotjelentés* 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.

Áttelepítés a Kaspersky Endpoint Agentből

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 megoldással való használathoz az alkalmazás telepítésekor ki kell választania a Managed Detection and Response összetevőt. Ebben az esetben nem kell telepítenie a Kaspersky Endpoint Agent szolgáltatást.

Áttérés a Kaspersky Endpoint Agentről a Kaspersky Endpoint Security for Windows termékre:

1. A Kaspersky Managed Detection and Response szolgáltatással való integrációt a Kaspersky Endpoint Security házirendjében konfigurálhatja.
2. A Managed Detection and Response összetevőt a Kaspersky Endpoint Agent házirendjében tilthatja le.

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.

Endpoint Detection and Response



A Kaspersky Endpoint Security 11.7.0 beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Optimum megoldáshoz (a továbbiakban: „EDR Optimum”). A Kaspersky Endpoint Security 11.8.0 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](#)² és a [Kaspersky Endpoint Detection and Response Expert súgóban](#)² 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. 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](#)² és a [Kaspersky Endpoint Detection and Response Expert súgóban](#)² találja.

A Kaspersky Endpoint Detection and Response a következő fenyegetéselemző eszközöket használja:

- 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 Kaspersky Endpoint Detection and Response a Kaspersky Private Security Network (KPSN) megoldást használja, amely anélkül küldi az adatokat a regionális kiszolgálónak, hogy az eszközökről adatokat küldene a KSN-be.
- Integráció a [Kaspersky Threat Intelligence portállal](#)², amely információkat tartalmaz és jelenít meg fájl és webcímek megbízhatóságáról.
- [Kaspersky Threats](#)² adatbázis.

Integráció a Kaspersky Endpoint Detection and Response szolgáltatással

A Kaspersky Endpoint Detection and Response integrálásához hozzá kell adnia az Endpoint Detection and Response Optimum (EDR Optimum) vagy az Endpoint Detection and Response Expert (EDR Expert) összetevőt, és konfigurálnia kell a Kaspersky Endpoint Security-t.

Az EDR Optimum és az EDR Expert összetevők nem kompatibilisek. Ezenkívül az EDR Expert összetevő nem kompatibilis a Managed Detection and Response összetevővel.

A következő feltételeknek kell teljesülniük ahhoz, hogy az Endpoint Detection and Response működjön:

- Kaspersky Security Center 13.2. A Kaspersky Security Center korábbi verzióiban nem lehetett aktiválni az Endpoint Detection and Response szolgáltatást.
- 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 működőképeseek. Az Endpoint Detection and Response a következő összetevőktől függ:
 - [Fájl védelem](#).
 - [Web védelem](#).
 - [Levelezés védelem](#).
 - [Biztonsági rések kihasználásának megelőzése](#).
 - [Viselkedéselemzés](#).
 - [Behatolásmegelőző rendszer](#).
 - [Kármentesítő motor](#).
 - [Adaptív Anomálifelügyelő](#).

A Kaspersky Endpoint Detection and Response integrálása a következő lépéseket foglalja magában:

1 Az Endpoint Detection and Response összetevők telepítése

Kiválaszthatja az EDR Optimum vagy EDR Expert összetevőt [telepítés](#) vagy [frissítés](#) közben, valamint a [Change application components](#) feladat használatával. Újra kell indítania a számítógépét az alkalmazás új elemekkel történő frissítésének befejezéséhez.

A *Change application components* feladat végrehajtása után a feladat állapota hibásan jelenik meg. A feladat *Sikeresen befejezve* helyett *Ütemezett* állapottal rendelkezik. Azonban a feladat így is sikeresen elvégezhető. Győződjön meg arról, hogy az új összetevő telepítve van a Kaspersky Security Center konzol számítógép-tulajdonságaiban (**Alkalmazások** → **Kaspersky Endpoint Security for Windows** → **Összetevők**) vagy az alkalmazás helyi felületén.

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 szolgáltatás a [Kaspersky Endpoint Security for Windows aktiválása](#) után azonnal elérhetővé válik.

- Licencbővítés az EDR Optimum vagy EDR Expert (Kaspersky Endpoint Detection and Response bővítmény) használatához.

A szolgáltatás a Kaspersky Endpoint Detection and Response külön kulcsának hozzáadását követően lesz elérhető. Ennek eredményeképpen két kulcs kerül telepítésre a számítógépre: 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.

3 Az Endpoint Detection and Response összetevők engedélyezése

Engedélyezheti vagy letilthatja az összetevőt a Kaspersky Endpoint Security for Windows házirend-beállításában.

[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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
5. Kapcsolja be az **Endpoint Detection and Response** kapcsolót.
6. Mentse el a módosításokat.

A Kaspersky Endpoint Detection and Response összetevő engedélyezve van. Ellenőrizheti az összetevő működési állapotát az *alkalmazás-összetevői állapotjelentés* 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** 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:

- o 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.

- o 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **General Settings** → **Reports and Storage** elemet.
5. Jelölje be a következő jelölőnégyzeteket az **Adatátvitel az adminisztrációs kiszolgálóra** részen:
 - **A karanténba helyezett fájlokról.**
 - **About a threat development chain.**
6. Mentse el a módosításokat.

Áttelepítés a Kaspersky Endpoint Agentből

Ha a Kaspersky Endpoint Security 11.7.0-s vagy újabb verzióját használja, és telepítve van az EDR Optimum összetevő (beépített ügynök), akkor a Kaspersky Endpoint Detection and Response Optimum megoldással való integráció támogatása a telepítés után azonnal elérhető. Az EDR Optimum összetevő nem kompatibilis a Kaspersky Endpoint Agent szolgáltatással. Ha a Kaspersky Endpoint Agent telepítve van a számítógépre, a Kaspersky Endpoint Security 11.7.0-s verzióra történő frissítések a Kaspersky Endpoint Detection and Response Optimum továbbra is együttműködik a Kaspersky Endpoint Security szolgáltatással ([a \[KES+KEA\] konfiguráció áttelepítése a \[KES+beépített ügynök\] termékbe](#)). Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről. A Kaspersky Endpoint Agentről a Kaspersky Endpoint Security for Windows-ra történő áttérés befejezéséhez a házirend- és feladatbeállításokat az [áttelepítési varázslóval](#) kell áthelyeznie.

Ha a Kaspersky Endpoint Security 11.4.0–11.6.0 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 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 Securityt használja (11.8.0 vagy újabb verzió).

Az EDR Optimum összetevő a Kaspersky Endpoint Security részeként támogatja a Kaspersky Endpoint Detection and Response Optimum 2.0 megoldással való kommunikációt. A Kaspersky Endpoint Detection and Response Optimum 1.0 verzióval való kommunikáció nem támogatott.

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 vizsgálat* feladatok lehetővé teszik a biztonsági sérülési indikátorok (IOC) megtalálását a számítógépen, valamint biztosítják 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 vizsgálat feladat futtatási módja

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](#)

IOC vizsgálati feladat létrehozása

Az *IOC vizsgálat* feladatokat manuálisan hozhatja létre:

- A riasztás részleteiben.

Az *Észlelés részletei* egy eszköz az észlelt fenyegetéssel kapcsolatos összesített információk megtekintésére és a válaszintézkedések kezelésére. 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 vizsgálati feladatok létrehozása:

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

- a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** 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 **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.
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. 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** fület.
9. Menjen az **IOC scan settings** részre.
10. Töltse be az IOC-fájlokat biztonsági sérülésre utaló indikátorok kereséséhez.
Az IOC-fájlok betöltése után megtekintheti a IOC-fájlok indikátorainak listáját.

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. Az IOC-észlelésre vonatkozó műveletek konfigurálása:
 - **Isolate computer 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 beállításában](#).
 - **Másolat áthelyezése a karanténba, objektum törlése.** 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.
 - **Kritikus területek vizsgálatának futtatása.** Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a [Kritikus területek vizsgálata](#) feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a

rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.

12. Nyissa meg a **Speciális** szakaszt.

13. Válassza ki az adattípusokat (IOC-dokumentumok), amelyeket a feladat részeként elemezni kell.

A Kaspersky Endpoint Security automatikusan kiválasztja az adattípusokat (IOC-dokumentumokat) az *IOC vizsgálat* 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 logs - EventLogItem.** Adja meg azt az időszakot, amikor az események naplózva lettek. Azt is kiválaszthatja, hogy mely Windows eseménynaplókat kell használni az IOC vizsgálatához. Alapértelmezés szerint a következő eseménynaplók vannak kiválasztva: alkalmazási eseménynapló, rendszer-eseménynapló és biztonsági eseménynapló.

A **Windows registry - RegistryItem** adattípus esetén a Kaspersky Endpoint Security átvizsgálja a [beállításkulcsok készletét](#).

14. Mentse el a módosításokat.

15. Válassza ki a feladat melletti jelölőnégyzetet.

16. Kattintson a **Futtatás** gombra.

Ennek eredményeként a Kaspersky Endpoint Security futtatja a biztonsági sérülési indikátorok keresését a számítógépen. A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Eredmények** szakaszban. Az észlelt biztonsági sérülési indikátorokra vonatkozó információkat a feladat tulajdonságaiban tekintheti meg: **Alkalmazásbeállítások** → **IOC vizsgálat eredményei**.

Az IOC vizsgálat eredményeinek megőrzése 30 napig történik. Ezt követően a Kaspersky Endpoint Security automatikusan törli a legrégebbi bejegyzéseket.

Fájl áthelyezése a Karanténba

A fenyegetésekre reagálva a Kaspersky Endpoint Detection and Response Optimum létrehozhat *Fájl karanténba helyezése* feladatokat. A *Karantén* egy speciális helyi tároló a számítógépen, ahová a vírusokkal vagy nem fertőtleníthető fájlokkal fertőzött fájlokat helyezi át az alkalmazás. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha a Kaspersky Sandbox és a Kaspersky Endpoint Detection and Response megoldásokkal dolgozik együtt. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a [Biztonsági mentésbe](#) helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért lásd a [Kaspersky Sandbox súgót](#), a [Kaspersky Endpoint Detection and Response Optimum súgót](#) és a [Kaspersky Endpoint Detection and Response Expert súgót](#).

Fájl karanténba helyezése 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.

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 karanténba helyezése feladat létrehozása:

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

- a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.

- b. A **Task type** legördülő listából válassza ki a **Move file to Quarantine** lehetőséget.

- c. A **Task name** mezőben adjon meg egy rövid leírást.

- d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Nyomja meg a **Next** gombot.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Nyomja meg a **Next** gombot.

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** fület.

9. A fájlok listájában kattintson a **Hozzáadás** 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. Kattintson a **Mentés** gombra.

12. Válassza ki a feladat melletti jelölőnégyzetet.

13. Kattintson a **Futtatás** gombra.

Ennek eredményeként a Kaspersky Endpoint Security karanténba helyezi a fájlt. Ha a fájlt egy másik folyamat zárolja, a feladat *Befejezve* 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 *Fájl karanténba helyezése* feladat *Hozzáférés megtagadva* hibaüzenettel is végződhet, ha a feladat egy éppen futó végrehajtható fájlt próbál karanténba helyezni. [Hozzon létre egy folyamatmegszakítási feladatot](#) a fájlhoz, és próbálkozzon újra.

A *Fájl áthelyezése a Karanténba* feladat meghiúsulhat 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 fájl lekéréséhez létre kell hoznia egy dedikált feladatot. A feladat végrehajtásának eredményeként a fájl karanténba kerül. Letöltheti ezt a fájlt a karanténból a számítógépére a Web Console segítségével. 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 ki a **Devices** → **Tasks** lehetőséget.

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

- a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.
- b. A **Feladat típusa** legördülő listából válassza ki a **Fájl lekérése** lehetőséget.
- c. A **Task name** mezőben adjon meg egy rövid leírást.
- d. A **Select devices to which the task will be assigned** részről válassza ki a feladat hatókörét.

4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Nyomja meg a **Next** gombot.

5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Nyomja meg a **Next** gombot.

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** fület.

9. A fájlok listájában kattintson a **Hozzáadás** 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. Kattintson a **Mentés** gombra.

12. Válassza ki a feladat melletti jelölőnégyzetet.

13. Kattintson a **Futtatás** 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

Távolról is törölhet fájlokat a *Fájl törlése* feladattal. Például távolról törölhet egy fájlt fenyegetésre történő reagálás során.

Az EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetőek el.

Fájl törlése feladat létrehozása:

1. A Web Console fő ablakában válassza ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a **Add** gombra.
Elindul a Feladatvarázsló.
3. Adja meg a feladatok beállításait:
 - a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.
 - b. A **Task type** legördülő listából válassza ki a **Delete file** lehetőséget.
 - c. A **Task name** mezőben adjon meg egy rövid leírást.
 - d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.
4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Nyomja meg a **Next** gombot.
5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Nyomja meg a **Next** gombot.

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** fület.
9. A fájlok listájában kattintson a **Hozzáadás** 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. Kattintson a **Mentés** gombra.
12. Válassza ki a feladat melletti jelölőnégyzetet.

13. Kattintson a **Futtatás** gombra.

Ennek eredményeként a Kaspersky Endpoint Security törli a fájlt a számítógépről. Ha a fájlt egy másik folyamat zárolja, a feladat *Befejezve* állapotúként jelenik meg, de maga a fájl csak a számítógép újraindítása után fog törölődni. A számítógép újraindítása után győződjön meg arról, hogy a fájl törölődött.

A *Fájl törlése* feladat *Hozzáférés megtagadva* hibaüzenettel is végződhet, ha a feladat egy éppen futó végrehajtható fájlt próbál törölni. [Hozzon létre egy folyamatmegszakítási feladatot](#) a fájlhoz, és próbálkozzon újra.

Folyamat indítása

A távolról futtathat fájlokat a *Folyamat indítása* feladattal. Például távolról futtathat egy segédprogramot, amely létrehozza a számítógép konfigurációs fájlját. Ezután használhatja a [Fájl lekérése 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.

Folyamatindítási feladat létrehozása:

1. A Web Console fő ablakában válassza ki a **Devices** → **Tasks** lehetőséget.
Megnyílik a feladatok listája.
2. Kattintson a **Add** gombra.
Elindul a Feladatvarázsló.
3. Adja meg a feladatok beállításait:
 - a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.
 - b. A **Task type** legördülő listából válassza ki a **Process start** lehetőséget.
 - c. A **Task name** mezőben adjon meg egy rövid leírást.
 - d. A **Select devices to which the task will be assigned** részből válassza ki a feladat hatókörét.
4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Nyomja meg a **Next** gombot.
5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Nyomja meg a **Next** gombot.

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** fület.

10. Írja be a folyamatindítási parancsot.

Ha például egy segédprogramot szeretne futtatni (`utility.exe`), amely menti a számítógép konfigurációjával kapcsolatos információkat egy `conf.txt` nevű fájlba, akkor a következő értékeket kell megadnia:

- **Executable command** – `utility.exe`
- **Command-line arguments** – `/R conf.txt`
- **Path to the working folder** – `C:\Users\admin\Diagnostic\`

Alternatív megoldásként a **Executable command** mezőbe beírhatja a `C:\Users\admin\Diagnostic\utility.exe /R conf.txt` parancsot is. Ebben az esetben nem kell megadnia a többi beállítást.

11. Kattintson a **Mentés** gombra.

12. Válassza ki a feladat melletti jelölőnégyzetet.

13. Kattintson a **Futtatás** 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 **Eredmények** szakaszban.

Folyamat megszakítása

Távrolól is leállíthat folyamatokat a *Folyamat megszakítása* feladattal. Például távrolól leállíthat egy internetes sebességtesztelő segédprogramot, amelyet a [Folyamat indítása feladattal](#) indítottak el.

Ha meg szeretné tiltani egy fájl futtatását, konfigurálhatja a [végrehajtásmegelőzési összetevőt](#). Letilthatja futtatható fájlok, szkriptek, Office formátumú fájlok végrehajtását is.

A *Folyamat megszakítása* 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 for Windows 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.

Folyamat megszakítása feladat létrehozása:

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

Megnyílik a feladatok listája.

2. Kattintson a **Add** gombra.

Elindul a Feladatvarázsló.

3. Adja meg a feladatok beállításait:

- a. Az **Application** legördülő listában válassza a **Kaspersky Endpoint Security for Windows (11.8.0)** lehetőséget.
 - b. A **Task type** legördülő listából válassza ki a **Process termination** lehetőséget.
 - c. A **Task name** mezőben adjon meg egy rövid leírást.
 - d. A **Select devices to which the task will be assigned** részről válassza ki a feladat hatókörét.
4. Válassza ki az eszközöket a kiválasztott feladat hatókör lehetőséghez. Nyomja meg a **Next** gombot.
 5. Adja meg azon felhasználó fiókjának hitelesítő adatait, akinek jogait használni kívánja a feladat futtatásához. Nyomja meg a **Next** gombot.

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** fület.
9. A folyamat befejezéséhez ki kell választania a leállítani kívánt fájlt. Egy fájl 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 **Ütemezés** részt.
11. Állítsa be a feladat ütemezését.

A hálózati ébresztés nem érhető el ennél a feladatnál. Győződjön meg arról, hogy a számítógép be van kapcsolva a feladat futtatásához.

12. Kattintson a **Mentés** gombra.
13. Válassza ki a feladat melletti jelölőnégyzetet.
14. Kattintson a **Futtatás** gombra.

Ennek eredményeként a Kaspersky Endpoint Security megszakítja a folyamatot a számítógépen. Például, ha egy „JÁTÉK” alkalmazás fut, és leállítja a jatek.exe folyamatot, az alkalmazás adatmentés nélkül bezárul. A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Eredmények** 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. 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-megakadályozási szabály* olyan feltételkészletnek minősül, amelyet figyelembe kell venni a blokkolásakor. 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](#) ² és a [Kaspersky Endpoint Detection and Response Expert súgóban](#) ² 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.

Nem ajánlott 5000-nél több futtatás-megakadályozási szabályt létrehozni, mivel ez a rendszer instabilitását okozhatja.

A megelőzési szabályok nem terjednek ki CD-n vagy ISO-lemezeképen található fájlokra. Az alkalmazás nem blokkolja ezen fájlok végrehajtását vagy megnyitását.

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 EDR Optimum feladatát a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert feladatbeállításai csak a Cloud Console-ban érhetők el.

A végrehajtás megakadályozása:

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
5. A **Végrehajtás megakadályozása** kapcsolóval engedélyezze vagy tiltsa le az összetevőt.
6. Az **Action on execution or opening of forbidden object** részen válassza ki az összetevő működési módját:
 - **Block and write to report.** 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.
 - **Log events only.** 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.
7. Végrehajtásmegelőzési szabályok listájának létrehozása:
 - a. Kattintson a **Add** gombra.
 - b. Ezzel megnyit egy ablakot; ebben az ablakba írja be a végrehajtásmegelőzési szabály nevét (például *A alkalmazás*).
 - c. A **Type** legördülő listában válassza ki a blokkolni kívánt objektumot: **Executable file, Script, Microsoft Office dokumentum**.
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.

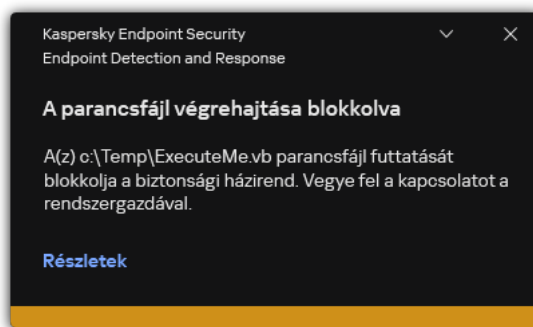
Ha a fájl hálózati meghajtón található, adja meg a fájl elérési útját, amely a meghajtó betűjele helyett `\\` értékkel kezdődjön. Például `\\server\shared_folder\file.exe`. Ha a fájl elérési útja hálózati meghajtó betűjelét tartalmazza, a Kaspersky Endpoint Security nem blokkolja a fájlt vagy a szkriptet.

A végrehajtás megakadályozása támogatja az [Office-fájlkiterjesztések](#) és a [szkriptértelmezők](#) készletét.

e. Kattintson az **OK** gombra.

8. 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 hálózatkülönítése

A számítógép hálózatkülönítése lehetővé teszi a számítógép automatikus leválasztását a hálózatról, válaszul a biztonsági sérülési indikátorok (IOC) észlelésére.

Amikor a Hálózatkülönítés be van kapcsolva, az alkalmazás leválaszt minden aktív kapcsolatot, és blokkol minden új TCP/IP-hálózati kapcsolatot a számítógépen az alábbi kapcsolatok kivételével:

- A Hálózatkülönítés kizárásaiban felsorolt kapcsolatok.
- A Kaspersky Endpoint Security szolgáltatásai által kezdeményezett kapcsolatok.
- A Kaspersky Security Center Felügyeleti ügynök által kezdeményezett kapcsolatok.

A hálózatkülönítés kezelése

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.

Beállíthatja, hogy a Hálózatkülönítés automatikusan bekapcsoljon az IOC észlelésre adott válaszként. A Hálózatkülönítést manuálisan is be- és kikapcsolhatja.

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](#) ² és a [Kaspersky Endpoint Detection and Response Expert súgóban](#) ² találja.

- Helyi alkalmazásbeállítások használata.

[A Hálózatelkülönítés beállítása, hogy automatikusan bekapcsoljon az IOC észlelésre adott válaszként](#) ²

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

Megnyílik a feladatok listája.

2. Kattintson a Kaspersky Endpoint Security **IOC scan** feladatára.

Megnyílik a feladatok tulajdonságai ablak.

Ha szükséges, hozza létre az [IOC scan](#) feladatot.

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

4. Az **Action on IOC detection** részen válassza a **Take response actions after an IOC is found** lehetőséget, és jelölje be az **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.

[A számítógép hálózatelkülönítésének manuális bekapcsolása](#) ²

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.

2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.

Ez megnyitja a számítógép tulajdonságait.

3. Válassza ki a **Applications** lapot.

4. Kattintson a **Kaspersky Endpoint Security for Windows** lehetőségre.

Ez megnyitja a helyi alkalmazásbeállításokat.

5. Válassza ki az **Application settings** fület.

6. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.

7. A **Hálózatelkülönítés** területen kattintson az **Isolate computer from the network** lehetőségre.

Beállíthatja, hogy a Hálózatkülönítés automatikusan kikapcsoljon egy meghatározott idő elteltével. Alapértelmezés szerint az alkalmazás kikapcsolja a Hálózatkülönítést a bekapcsolástól számított 8 óra elteltével. A Hálózatkülönítést manuálisan is kikapcsolhatja. A Hálózatkülönítés kikapcsolása után a számítógép korlátozások nélkül használhatja a hálózatot.

[A számítógépes hálózatkülönítés automatikus kikapcsolásának késleltetési beállítása](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
5. A **Network isolation** területen kattintson a **Configure computer unlock settings** elemre.
6. Ezzel megnyit egy ablakot; ebben az ablakban jelölje be az **Automatically unlock isolated computer in N hours** jelölőnégyzetet, és adja meg a Hálózatkülönítés automatikus kikapcsolásának késleltetését.
7. Mentse el a módosításokat.

[A számítógép hálózatkülönítésének manuális kikapcsolása](#)

1. A Web Console fő ablakában válassza ki a **Devices** → **Managed devices** lehetőséget.
2. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás helyi beállításait.
Ez megnyitja a számítógép tulajdonságait.
3. Válassza ki a **Applications** lapot.
4. Kattintson a **Kaspersky Endpoint Security for Windows** lehetőségre.
Ez megnyitja a helyi alkalmazásbeállításokat.
5. Válassza ki az **Application settings** fület.
6. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
7. A **Network isolation** területen kattintson a **Unblock computer isolated from the network** lehetőségre.

Helyileg is letilthatja a Hálózatkülönítést a [command line](#) használatával.

Network isolation exclusions

Beállíthatja a Hálózatkülönítés kizárásait. Az e szabályoknak megfelelő hálózati kapcsolatok nincsenek blokkolva a számítógépen, ha a Hálózatkülönítés be van kapcsolva.

A Hálózatkülönítés 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 hálózatkülönítés automatikusan bekapcsol az észlelt fenyegetés hatására. A számítógép tulajdonságaiban megadott kizárások csak akkor érvényesek, ha a hálózatkülönítést a Kaspersky Security Center konzoljának számítógép-tulajdonságaiban vagy a riasztási részletekben manuálisan kapcsolják be.

Egy aktív szabályzat nem akadályozza meg a számítógéptulajdonságokban konfigurált Hálózatkülönítésből történő kizárások alkalmazását, mivel ezek a paraméterek eltérő használati forgatókönyvekkel rendelkeznek.

Hálózatkülönítési kizárás hozzáadása

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Endpoint Detection and Response** elemet.
5. A **Hálózatkülönítési kizárások** részen kattintson a **Kizárások** gombra.
6. Ezzel megnyit egy ablakot; ebben az ablakban kattintson a **Add from profile** elemre, és válassza ki a szabványos hálózati profilokat a kizárások konfigurálásához.
A profilból származó hálózatkülönítési kizárások hozzáadódnak a Hálózatkülönítés kizárásainak listájához. Megtekintheti a hálózati kapcsolatok tulajdonságait. Ha szükséges, módosíthatja a hálózati kapcsolatok beállításait.
7. Ha szükséges, adjon hozzá manuálisan egy hálózatkülönítési kizárást. Ehhez a kizárások listáját tartalmazó ablakban kattintson a **Hozzáadás** gombra, és manuálisan szerkessze a hálózati kapcsolat beállításait.
8. Mentse el a módosításokat.

A Hálózatkülönítés kizárásainak listáját helyben is megtekintheti a [parancssor](#) használatával. Ebben az esetben a számítógépet el kell különíteni.

1. 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 xltn xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

2. melléklet Támogatott szkriptértelmezők

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
- msixexec.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).

3. melléklet IOC vizsgálat hatóköre a rendszerleíró adatbázisban (RegistryItem)

Amikor hozzáadja a RegistryItem adattípust az IOC vizsgálat hatóköréhez, a Kaspersky Endpoint Security a következő beállításkulcsokat vizsgálja:

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

4. melléklet IOC-fájl követelményei

Az IOC vizsgálati feladatok létrehozásakor vegye figyelembe az [IOC-fájlról](#) 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.
- Ha az IOC vizsgálat 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 vizsgálat 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 fájl használata az IOC vizsgálati feladatok hibával történő leállítását okozza. Ennek ellenére az IOC-gyűjteményhez hozzáadott összes fájl teljes mérete meghaladhatja a 2 MB-ot.
- Fenyegetésenként egy IOC-fájlt ajánlott létrehozni. Ez megkönnyíti az IOC vizsgálat 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.

Támogatott feltételek	<p>OpenIOC 1.0:</p> <p>is isnot (kivétel a halmazból) contains containsnot (kivétel a halmazból)</p> <p>OpenIOC 1.1:</p> <p>is contains starts-with ends-with matches greater-than less-than</p>
Támogatott feltételattribútumok	<p>OpenIOC 1.1:</p> <p>preserve-case negate</p>
Támogatott operátorok	<p>AND OR</p>
Támogatott adattípusok	<p>„date”: dátum (alkalmazható feltételek: is, greater-than, less-than)</p> <p>„int”: egész szám (alkalmazható feltételek: is, greater-than, less-than)</p> <p>„string”: karakterlánc (alkalmazható feltételek: is, contains, matches, starts-with, ends-with)</p> <p>„duration”: időtartam másodpercben (alkalmazható feltételek: is, greater-than, less-than)</p>
Az adattípusok értelmezésének jellemzői	<p>A „boolean string”, a „restricted string”, az „md5”, az „IP”, az „sha256” és a „base64Binary” adattípusok értelmezése karakterláncként történik.</p> <p>Az alkalmazás támogatja az int és a date adattípusokhoz tartozó Content beállítás értelmezését, ha az intervallum formájában van megadva:</p> <p>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></p> <p>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 adattípusok értelmezését, ha az indikátorok ISO 8601, Zulu Time Zone, UTC formátumban vannak megadva.</p>



A Kaspersky Endpoint Security 11.7.0 mostantól beépített ügynököt tartalmaz a Kaspersky Sandbox megoldással való integrációhoz. A *Kaspersky Sandbox megoldás* észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Kaspersky Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Kaspersky Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (Kaspersky Sandbox-kiszolgálók). A megoldás részleteit a [Kaspersky Sandbox súgóban](#) találja.

A Kaspersky Sandbox-megoldás alábbi konfigurációi lehetségesek:

Kaspersky Sandbox 2.0

A Kaspersky Sandbox 2.0 a [KES+beépített ügynök] konfigurációt támogatja.

Minimális követelmények:

- Kaspersky Endpoint Security 11.7.0 for Windows vagy újabb.
- A Kaspersky Endpoint Agent nem szükséges.
- Kaspersky Security Center 13.2.

Kaspersky Sandbox 1.0

A Kaspersky Sandbox 1.0 a [KES+KEA] konfigurációt támogatja.

Minimális követelmények:

- Kaspersky Endpoint Security 11.2.0 – 11.6.0 for Windows.
- Kaspersky Endpoint Agent 3.8.
A Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows-terjesztőkészletből telepíthető.
- Kaspersky Security Center 11.

Integráció a Kaspersky Sandbox szolgáltatással

A Kaspersky Sandbox összetevővel való integrációhoz a Kaspersky Sandbox összetevő hozzáadása szükséges. Kiválaszthatja a Kaspersky Sandbox összetevőt [telepítés](#) vagy [frissítés](#) közben, valamint az [Change application components](#) feladat használatával.

A *Change application components* feladat végrehajtása után a feladat állapota hibásan jelenik meg. A feladat *Completed successfully* helyett *Scheduled* állapottal rendelkezik. Azonban a feladat így is sikeresen elvégezhető. Győződjön meg arról, hogy az új összetevő telepítve van a Kaspersky Security Center konzol számítógép-tulajdonságaiban (**Alkalmazások** → **Kaspersky Endpoint Security for Windows** → **Összetevők**) vagy az alkalmazás helyi felületén.

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 adatátvitelre 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 ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **General Settings** → **Reports and Storage** elemet.
5. Az **Adatátvitel az adminisztrációs kiszolgálóra** szakaszban jelölje be **A karanténba helyezett fájlokról** 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 főablakában válassza ki a **Console settings** → **Integration** lehetőséget.
2. Nyissa meg a **Cross-service integration** szakaszt.
3. Kapcsolja be a **Establish a background connection for cross-service integration** 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.

- A Kaspersky Sandbox összetevő engedélyezve van.
A Kaspersky Sandbox integrációt engedélyezheti vagy letilthatja a Web Console-ban vagy helyileg a [parancssorból](#).

A Kaspersky Sandbox-szal való integráció engedélyezése vagy letiltása:

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Kaspersky Sandbox** részt.
5. Használja az **Integration with Kaspersky Sandbox** kapcsolót az összetevő engedélyezéséhez vagy letiltásához.
6. Mentse el a módosításokat.

Ennek eredményeként a Kaspersky Sandbox összetevő engedélyezve van. Ellenőrizheti az összetevő működési állapotát az *alkalmazás-összetevői állapotjelentés* megtekintésével. Az összetevők működési állapotát a Kaspersky Endpoint Security helyi felületén található [jelentésekben](#) is megtekintheti. A **Kaspersky Sandbox** összetevő hozzá lesz adva a Kaspersky Endpoint Security összetevők listájához.

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: Hibakód: XXX (például 0xa67b01f4).

Áttelepítés a Kaspersky Endpoint Agentből

Ha a Kaspersky Endpoint Security 11.7.0-s vagy újabb verzióját használja, és telepítve van a Kaspersky Sandbox összetevő (beépített ügynök), a Kaspersky Sandbox megoldással való együttműködés azonnal elérhető a telepítés után. A Kaspersky Sandbox összetevő nem kompatibilis a Kaspersky Endpoint Agent szolgáltatással. Ha a Kaspersky Endpoint Agent telepítve van a számítógépre, a Kaspersky Endpoint Security 11.7.0-s verzióra történő frissítésekor a Kaspersky Sandbox továbbra is együttműködik a Kaspersky Endpoint Security szolgáltatással ([a \[KES+KEA\] konfiguráció áttelepítése a \[KES+beépített ügynök\] termékbe](#)). Ezen túlmenően a Kaspersky Endpoint Agent is eltávolításra kerül a számítógépről. A Kaspersky Endpoint Agentről a Kaspersky Endpoint Security for Windows-ra történő áttérés befejezéséhez a házirend- és feladatbeállításokat az [áttelepítési varázslóval](#) kell áthelyeznie.

Ha a Kaspersky Endpoint Security 11.4.0–11.6.0 verzióját használja a Kaspersky Sandbox összetevővel 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 részeként a Kaspersky Sandbox összetevő támogatja a Kaspersky Sandbox 2.0 megoldással való együttműködést. A Kaspersky Sandbox 1.0 megoldás nem támogatott.

TLS-tanúsítvány hozzáadása

Ha megbízható kapcsolatot szeretne konfigurálni a Kaspersky Sandbox kiszolgálóival, elő kell készítenie egy TLS-tanúsítványt. Ezután hozzá kell adnia a tanúsítványt a Kaspersky Sandbox-kiszolgálókhoz és a Kaspersky Endpoint Security házirendjéhez. A tanúsítvány előkészítéséről és a tanúsítványnak a kiszolgálókhoz való hozzáadásáról részletesen lásd a [Kaspersky Sandbox súgót](#).

TLS-tanúsítványt helyileg is hozzáadhat a Web Console-ban vagy helyileg a [parancssor](#) segítségével.

TLS-tanúsítvány hozzáadása a Web Console-ban:

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.

2. Kattintson a Kaspersky Endpoint Security házirend nevére.

Megnyílik a rendszabályok tulajdonságai ablak.

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

4. Nyissa meg a **Detection and Response** → **Kaspersky Sandbox** részt.

5. Kattintson a **Kiszolgáló kapcsolódási beállításai** hivatkozásra.

Ekkor megnyílik a Kaspersky Sandbox-kiszolgáló kapcsolódási beállításai ablak.

6. A **Kiszolgálói TLS-tanúsítvány** részen kattintson a **Hozzáadás** elemre, és válassza ki a TLS-tanúsítványfájlt.

A Kaspersky Endpoint Security csak egy TLS-tanúsítvánnyal rendelkezhet egy Kaspersky Sandbox-kiszolgáló esetében. Ha korábban már felvett egy TLS-tanúsítványt, akkor azt az alkalmazás visszavonja. Csak az utoljára felvett tanúsítvány lesz felhasználva.

7. Speciális kapcsolódási beállítások konfigurálása a Kaspersky Sandbox-kiszolgálókhoz:

- **Időtűllépés.** A Kaspersky Sandbox-kiszolgáló kapcsolódási időtűllépése. A beállított időtűllépés letelte után a Kaspersky Endpoint Security kérést küld a következő kiszolgálónak. Növelheti a Kaspersky Sandbox kapcsolódási időtűllépését, ha a kapcsolat sebessége alacsony, vagy ha a kapcsolat instabil. A kérések ajánlott időtűllépése 0,5 másodperc vagy kevesebb.
- **Kaspersky Sandbox request queue.** A kérési várólista mappájának mérete. Amikor a számítógépen hozzáfér egy objektumhoz (futtatható fájl indítása vagy egy dokumentum – például DOCX vagy PDF formátumú fájl – megnyitása), a Kaspersky Endpoint Security képes elküldeni az objektumot vizsgálatra a Kaspersky Sandbox számára. Több kérés esetén a Kaspersky Endpoint Security létrehoz egy kérési várólistát. Alapértelmezés szerint a kérési várólista mappamérete 100 MB-ra van korlátozva. A maximális méret elérése után a Kaspersky 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.

8. 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.

Kaspersky Sandbox-kiszolgálók hozzáadása

Ha számítógépeket szeretne csatlakoztatni a Kaspersky Sandbox operációs rendszerek virtuális képeivel rendelkező kiszolgálóihoz, meg kell adnia a kiszolgálói címet és egy portot. A virtuális képek telepítésével és a Kaspersky Sandbox-kiszolgálók konfigurálásával kapcsolatos részletekért lásd a [Kaspersky Sandbox](#) súgót.

A Kaspersky Sandbox-kiszolgálók hozzáadása a Web Console-hoz:

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissa meg a **Detection and Response** → **Kaspersky Sandbox** részt.
5. A **Kaspersky Sandbox-kiszolgálók** részen kattintson a **Hozzáadás** elemre.
6. Ezzel megnyílik egy ablak; itt adja meg a Kaspersky Sandbox-kiszolgáló címét (IPv4, IPv6, DNS) és portját.
7. Mentse el a módosításokat.

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 vizsgálat* feladatok lehetővé teszik a biztonsági sérülési indikátorok (IOC) megtalálását a számítógépen, valamint biztosítják 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 vizsgálat feladat futtatási módja

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 törölődnek. Az önálló IOC vizsgálati feladatokkal kapcsolatos további részletekért lásd a [Kaspersky Sandbox súgót](#).

Az IOC vizsgálati feladat beállításai

A Kaspersky Sandbox automatikusan létrehozhat és futtathat *IOC vizsgálat* 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 vizsgálati feladat beállításainak módosítása:

1. A Web Console fő ablakában válassza ki a **Devices** → **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** fület.

4. Menjen az **IOC scan settings** részre.

5. Az IOC-észlelésre vonatkozó műveletek konfigurálása:

- **Másolat áthelyezése a karanténba, objektum törlése.** 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.
- **Kritikus területek vizsgálatának futtatása.** Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a [Kritikus területek vizsgálata](#) feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.

6. Konfigurálja az IOC vizsgálati feladat futtatási módját a **Csak akkor fusson, ha a számítógép üresjáratban van** jelölőnégyzettel. Ez a jelölőnégyzet ki- és bekapcsolja az *IOC vizsgálat* feladatot felfüggesztő funkciót, ha a számítógép erőforrásai korlátozottak. A Kaspersky Endpoint Security a képernyőkímélő kikapcsolásakor és a számítógép feloldásakor szünetelteti az *IOC vizsgálat* feladatot.

Ez az ütemezési beállítás lehetővé teszi a számítógép erőforrásainak energiatakarékos használatát működés közben.

7. Mentse el a módosításokat.

A feladat eredményeit a feladat tulajdonságaiban tekintheti meg az **Eredmények** szakaszban. Az észlelt biztonsági sérülési indikátorokra vonatkozó információkat a feladat tulajdonságaiban tekintheti meg: **Alkalmazásbeállítások** → **IOC vizsgálat eredményei**.

Az IOC vizsgálat eredményeinek megőrzése 30 napig történik. Ezt követően a Kaspersky Endpoint Security automatikusan törli a legrégebbi bejegyzéseket.

Karantén kezelése

A *Karantén* egy speciális helyi tároló a számítógépen, ahová a vírusokkal vagy nem fertőtleníthető fájlokkal fertőzött fájlokat helyezi át az alkalmazás. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha a Kaspersky Sandbox és a Kaspersky Endpoint Detection and Response megoldásokkal dolgozik együtt. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a [Biztonsági mentésbe](#) helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért lásd a [Kaspersky Sandbox súgót](#), a [Kaspersky Endpoint Detection and Response Optimum súgót](#) és a [Kaspersky Endpoint Detection and Response Expert súgót](#).

A Kaspersky Endpoint Security a rendszerfiókot (SYSTEM) használja a fájlok karanténba helyezéséhez.

A karantén csak a Web Console segítségével konfigurálható. A Web Console 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 200 MB-ra van korlátozva. A Kaspersky Endpoint Security automatikusan törli a legrégebbi fájlokat a karanténból, ha a tároló eléri a maximális méretét.

A karantén maximális méretének megadása:

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.
3. Válassza ki az **Application settings** fület.
4. Nyissas meg a **General Settings** → **Reports and Storage** elemet.
5. A **Karantén** részen adhatja meg a karantén méretét:
 - **A karantén méretének korlátozása: N MB.** Maximális karanténméret MB-ban. Például beállíthatja a maximális karanténméretet 200 MB-ra. Amikor a karantén eléri a maximális méretet, a Kaspersky Endpoint Security elküldi a megfelelő 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.
 - **Értesítés, ha a karanténtár mérete N százalékhoz ér.** 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 fájlok adatainak küldése a Kaspersky Security Centerbe:

1. A Web Console fő ablakában válassza ki a **Devices** → **Policies & Profiles** lehetőséget.
2. Kattintson a Kaspersky Endpoint Security házirend nevére.
Megnyílik a rendszabályok tulajdonságai ablak.

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

4. Nyissa meg a **General Settings** → **Reports and Storage** elemet.

5. Az **Adatátvitel az adminisztrációs kiszolgálóra** szakaszban jelölje be **A karanténba helyezett fájlokról** jelölőnégyzetet.

6. Mentse el a módosításokat.

Ennek eredményeként a Web Console-ban megtekintheti a karanténba helyezett fájlok listáját a számítógépen (**Műveletek** → **Tárolók** → **Karantén**). A Web Console segítségével karanténba helyezett objektumokat kezelhet (visszaállítás, törlés, hozzáadás stb.).

Kaspersky Security for Windows Server



A Kaspersky Endpoint Security 11.8.0 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 működésével kapcsolatos részletes információért tekintse meg a [Kaspersky Security for Windows Server súgót](#) . A Kaspersky Endpoint Security 11.8.0-tól kezdve áttérhet a KSWs-ről a Kaspersky Endpoint Security for Windows termékre, és ugyanazt a megoldást használhatja a munkahelyi állomások és a kiszolgálók védelmére.

A KES telepítése a KSWs-re

A Kaspersky Endpoint Security (KES) támogatja a Kaspersky Security for Windows Server (KSWs) alkalmazás alapvető funkcióit. A Kaspersky Endpoint Security 11.8.0 verziójától kezdve a KSWs helyett a KES-t használhatja.

A KES telepítése előtt el kell távolítani a KSWs-t. Az alkalmazás eltávolítása történhet távolról az [Alkalmazás eltávolítása távolról](#) feladat segítségével vagy [helyileg a kiszolgálón](#) . A KSWs eltávolítása után szükség lehet a kiszolgáló újraindítására. Ha a Kaspersky Endpoint Security-t a számítógép újraindítása nélkül szeretné telepíteni, akkor javasoljuk, hogy győződjön meg arról, hogy a Kaspersky Security for Windows Server teljesen eltávolításra került. Az ellenőrizendő fájlok és szolgáltatások listáját az alábbiakban találja. Ha az alkalmazás nincs teljesen eltávolítva, a Kaspersky Endpoint Security telepítése után kiszolgálói hibák léphetnek fel. Akkor is ajánlott meggyőződni arról, hogy az alkalmazás teljesen eltávolításra került, ha a [Kavremover segédprogram](#) nem támogatja a KSWs-t.

A KSWs eltávolítása után telepítse a [Kaspersky Endpoint Security for Windows](#) terméket bármely rendelkezésre álló módszerrel.

A Kaspersky Security for Windows Server eltávolításának ellenőrzése

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 nem futnak:
 - Kaspersky Security Service (KAVFS)
 - Kaspersky Security Management Service (KAVFSGT)
 - Kaspersky Security Exploit Prevention Service (KAVFSSLP)
 - Kaspersky Security Script Checker Service (KAVFSSCS)

A futó szolgáltatásokat a Feladatkezelőben vagy az `sc query` parancs használatával ellenőrizheti (lásd az alábbi ábrát).

- A következő illesztőprogramok nincsenek telepítve:
 - klam.sys

- kflt.sys
- klramdisk.sys
- klelaml.sys
- kfltdev.sys
- klips.sys
- klids.sys
- klwtpee

A telepített illesztőprogramokat a C:\Windows\System32\drivers mappában vagy az `sc query` parancs használatával ellenőrizheti. Ha a szolgáltatás vagy az illesztőprogram hiányzik, a következő választ kapja:

```

Командная строка
Microsoft Windows [Version 10.0.17134.1304]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\testadmin>sc query kavfs
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>sc query klam
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>

```

A Kaspersky Security for Windows Server termékhez tartozó szolgáltatások és illesztőprogramok eltávolításának ellenőrzése

Ha az alkalmazásfájlok vagy illesztőprogramok továbbra is a kiszolgálón vannak, törölje őket manuálisan. Ha a Kaspersky Security for Windows Server egyes szolgáltatásai még futnak, állítsa le (`sc stop`) és törölje (`sc delete`) őket 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 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.

<p>A KSWs kulcs helyileg hozzáadásra kerül az alkalmazás felületén.</p>	<p>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.</p>
<p>A KSWs kulcs hozzáadásra került a telepítőcsomaghoz.</p>	<p>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.</p>

Az alkalmazás kezelése a parancssorból

Kezelheti a Kaspersky Endpoint Security alkalmazást a parancssorból. Megtekintheti az alkalmazáskezeléshez tartozó parancsok listáját, ha végrehajtja a `HELP` parancsot. A megadott parancs szintaxisának elolvasásához adja meg a `HELP <parancs>` 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: `%%`.

Az alkalmazás telepítése

A Kaspersky Endpoint Security telepíthető a parancssorból, a következő módon egyikében:

- Interaktív módban az Alkalmazástelepítő varázslóval.
- Csendes módban. A telepítés csendes módban való elindítását követően a felhasználónak nem szükséges beavatkoznia a telepítési folyamatba. 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.

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] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<felhasználónév>
/pKLPASSWD=<jelszó> /pKLPASSWDAREA=<jelszó hatóköre>] [/pENABLETRACES=1|0]
/pTRACESLEVEL=<nyomkövetési szint>] [/s]
```

vagy

```
msiexec /i <forgalmazási készlet neve> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1|0] [SKIPPRODUCTCHECK=1] [KLLOGIN=<felhasználónév> KLPASSWD=<jelszó>
KLPASSWDAREA=<jelszó hatóköre>] [ENABLETRACES=1|0 TRACESLEVEL=<nyomkövetési szint>]
/qn
```

Ennek eredményeként az alkalmazás telepítve lesz a számítógépre. A `status` paranccsal ellenőrizheti az alkalmazásbeállításokat, illetve hogy az alkalmazás telepítve van-e.

EULA=1	<p>A Végfelhasználói licencszerződés feltételeinek elfogadása. A Licencszerződés szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>A Végfelhasználói licencszerződés feltételeit az alkalmazás telepítéséhez, illetve verziójának frissítéséhez kötelező elfogadni.</p> </div>
PRIVACYPOLICY=1	<p>Az Adatvédelmi szabályzat elfogadása. Az Adatvédelmi szabályzat szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Az alkalmazás telepítéséhez, vagy a verziója frissítéséhez el kell fogadnia az Adatvédelmi szabályzatot.</p> </div>
KSN	<p>A Kaspersky Security Network való részvétel elfogadása vagy elutasítása. Ha nincs megadott érték a paraméterhez, a Kaspersky Endpoint Security kéri fogja, hogy erősítse meg a KSN-ben való részvételének hozzájárulását vagy elutasítását, amikor a Kaspersky Endpoint Security először elindul. Választható értékek:</p> <ul style="list-style-type: none"> • 1 – a KSN-ben való részvétel elfogadása. • 0 – a KSN-ben való részvétel elutasítása (alapértelmezett érték). <p>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.</p>
ALLOWREBOOT=1	<p>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.</p> <p>Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítani a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.</p>
SKIPPRODUCTCHECK=1	<p>Inkompatibilis szoftver keresésének letiltása. Azon inkompatibilis szoftverek listája, amik elérhetőek a terjesztőkészletben lévő incompatible.txt fájlban. Ha nincs megadva érték a paraméterhez, és inkompatibilis szoftver észlelhető, a Kaspersky Endpoint Security telepítése leáll.</p>
SKIPPRODUCTUNINSTALL=1	<p>Az észlelt, inkompatibilis szoftver automatikus eltávolításának letiltása. Ha nincs megadva érték a paraméterhez, a Kaspersky Endpoint Security megpróbálja eltávolítani az inkompatibilis szoftvert.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>A Kaspersky Endpoint Security msiexec telepítőprogrammal történő telepítésekor nem engedélyezhető az inkompatibilis szoftverek automatikus eltávolítása. Használja a setup_kes.exe programot az inkompatibilis szoftverek automatikus eltávolításának engedélyezéséhez.</p> </div>

KLLOGIN	Állítsa be a felhasználónevet a Kaspersky Endpoint Security funkcióinak és beállításainak eléréséhez (a Jelszóvédelem összetevő). A felhasználónevet a KLPASSWD and KLPASSWDAREA beállításokkal 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: <ul style="list-style-type: none"> • 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.
ENABLETRACES	Az alkalmazások nyomkövetésének engedélyezése vagy kikapcsolása. Indulása után a Kaspersky Endpoint Security elmenti a nyomkövetési fájlokat a %ProgramData%\Kaspersky Lab\KES\Traces mappába. Választható értékek: <ul style="list-style-type: none"> • 1 – a nyomkövetés engedélyezve van. • 0 – a nyomkövetés ki van kapcsolva (alapértelmezett érték).
TRACESLEVEL	A nyomkövetések részleteinek szintje. Választható értékek: <ul style="list-style-type: none"> • 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).

	<ul style="list-style-type: none"> • 600 (alacsony). Minden üzenet.
AMPPL	<p>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.</p> <p>Az AM-PPL technológia a Windows 10 1703-as (RS2) vagy újabb verziói, valamint a Windows Server 2019 operációs rendszerek számára érhető el.</p> <p>Választható értékek:</p> <ul style="list-style-type: none"> • 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.
RESTAPI	<p>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).</p> <p>Választható értékek:</p> <ul style="list-style-type: none"> • 1 – a REST API felületen keresztül történő kezelés engedélyezve van. • 0 – a REST API felületen keresztül történő kezelés blokkolva van (alapértelmezett érték). <p>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.</p>
RESTAPI_User	<p>Az alkalmazás REST API felületen keresztül történő kezeléséhez használt Windows tartományfőik felhasználóneve. A REST API felületen keresztül történő alkalmazáskezelés csak ennek a felhasználónak lehetséges. Adja meg a felhasználónevet a következő formátumban: <DOMAIN>\<Felhasználónév> (például RESTAPI_User=COMPANY\Administrator). A REST API-val történő munkálatokhoz csak egy felhasználót választhat ki.</p> <p>Egy felhasználónév megadása szükséges ahhoz, hogy az alkalmazást a REST API felületen keresztül kezelhesse.</p>
RESTAPI_Port	<p>Az alkalmazás REST API felületen keresztül történő kezeléséhez használt port. A 6782 az alapértelmezett port.</p>
RESTAPI_Certificate	<p>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.</p>
ADMINKITCONNECTOR	<p>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.</p> <p>Választható értékek:</p> <ul style="list-style-type: none"> • 1 – az adminisztrációs rendszerekkel történő alkalmazáskezelés engedélyezve van (alapértelmezett érték).

- 0 – az alkalmazáskezelés csak a helyi felületen keresztül van engedélyezve.

Példa:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1  
KSN=1 KLLOGIN=Rendszergazda KLPASSWD=Jelszó  
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 lesz aktiválva, ha nem adott meg aktiváló kódot a [setup.ini file](#) helyen. A próbalicenc általában rövid ideig érvényes. A próbalicenc lejáratá után a Kaspersky Endpoint Security minden funkciója letiltásra kerül. Az alkalmazás használatának folytatásához egy kereskedelmi licenccel kell aktiválnia az alkalmazást, amit az [Alkalmazás aktiváló 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](#) – általános beállítások az alkalmazás telepítéséhez
- [install.cfg](#) – a Kaspersky Endpoint Security művelet beállításai
- 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 setup.reg fájlt Kaspersky szakemberei hozzák létre. Ennek a fájlnek a tartalmát nem javasolt módosítani.

Ahhoz, hogy alkalmazza a beállításokat a setup.ini, install.cfg és setup.reg fájlokból, helyezze ezeket a fájlokat 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=<a setup.reg fájl elérési útja>`.

Alkalmazás aktiválása

Az alkalmazás aktiválása a parancssorból:

gépelje be a következő karakterláncot a parancssorba:

```
avp.com license /add <aktiváló kód vagy kulcsfájl> [/login=<felhasználónév> /password=  
<jelszó>]
```

Meg kell adnia a fiók bejelentkezési adatait (`/login=<felhasználónév> /password=<jelszó>`), ha a [Jelszóvédelem engedélyezve van](#).

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. 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 azonosítóját a következő paranccsal érheti el:

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

- Ha az eltávolítási folyamat rendelkezik [jelszavas védelemmel](#):

```
setup_kes.exe /pKLLOGIN=<felhasználónév> /pKLPASSWD=<jelszó> /s /x
```

vagy

```
msiexec.exe /x <GUID> KLLOGIN=<felhasználónév> KLPASSWD=<jelszó> /qn
```

Példa:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

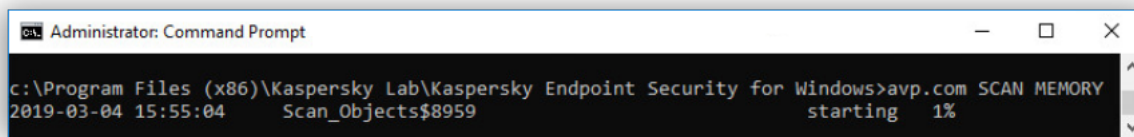
AVP parancsok

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.
3. A parancs végrehajtásához írja be:

```
avp.com <parancs> [options]
```


Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot (lásd az alábbi ábrát.)



Az alkalmazás kezelése a parancssorból

SCAN. Vírusvizsgálat

Futtassa a vírusvizsgálat feladatot.

A parancs szintaxisa

```
SCAN[<vizsgálat hatóköre>] [<művelet fenyegetés észlelések>] [<fájltípusok>]  
[<kizárás a vizsgálatból>] [/R[A]:<jelentésfájl>] [<vizsgálati technológiák>] [/C:  
<fájl vírusvizsgálati beállításokkal>]
```

Vizsgálat hatóköre	
<vizsgált fájlok>	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: <ul style="list-style-type: none">"C:\Program Files (x86)\Example Folder" – hosszú elérési útvonal.C:\PROGRA~2\EXAMPL~1 – rövid elérési útvonal.
/ALL	Futtassa a <i>Teljes vizsgálat</i> feladatot. A Kaspersky Endpoint Security az alábbi objektumokat vizsgálja: <ul style="list-style-type: none">Kernelmemória;Az operációs rendszer indulásakor betöltött objektumokRendszerindító szektorok;Az operációs rendszer biztonsági mentéseMinden merevlemez és cserélhető meghajtó
/MEMORY	A kernelmemória vizsgálata
/STARTUP	Az operációs rendszer indulásakor betöltött objektumok vizsgálata
/MAIL	Az Outlook postaláda 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 fájlnek új sorban kell lennie. A hosszú elérési útvonalakat idézőjelbe kell tenni. A rövid elérési útvonalakat (MS-DOS formátum) nem kell idézőjelbe tenni. Például: <ul style="list-style-type: none"> "C:\Program Files (x86)\Example Folder" – hosszú elérési útvonal. C:\PROGRA~2\EXAMPL~1 – rövid elérési útvonal.

Művelet fenyegetés észlelésekor	
/i0	Értesítés. 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; a vírusmentesítés sikertelensége esetén blokkolás. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájlt vírusmentesíteni. Ha a vírusmentesítés nem lehetséges, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.
/i2	Vírusmentesítés; a vírusmentesítés sikertelensége esetén törlés. 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 törli a fájlokat. Alapértelmezésben ez a művelet van kiválasztva.
/i3	Az észlelt, fertőzött fájlok vírusmentesítése. Ha a vírusmentesítés sikertelen, a fertőzött fájlok törlése. Az összetett fájlok törlése is (például archívumok), ha a fertőzött fájlt nem lehet vírusmentesíteni vagy törölni.
/i4	A fertőzött fájlok törlése. Az összetett fájlok törlése is (például archívumok), ha a fertőzött fájlt nem lehet törölni.
/i8	Fenyegetés észlelése esetén a felhasználó értesítése, hogy tegyen valamit.
/i9	A vizsgálat befejezése esetén a felhasználó értesítése.

Fájltípusok	
/fe	Kiterjesztés alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security 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, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejléceket 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, a Kaspersky Endpoint Security 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:b	A postaadatbázisok, a bejövő és kimenő e-mail-ek ki vannak zárva a vizsgálat hatóköréből.
-e: <fájlmazsk>	A fájlmaszkkal egyező fájlok ki vannak zárva a vizsgálat hatóköréből. Például: <ul style="list-style-type: none"> A *.exe maszk tartalmazza az exe kiterjesztésű fájlok elérési útvonalait. A példa* maszk tartalmazza a PÉLDA nevű fájlok elérési útvonalát.
-e: <másodperc>	A fájlok, amelyek vizsgálati ideje meghaladja a megadott időkorlátot (másodperc), ki vannak zárva a vizsgálat hatóköréből.
-es: <megabájt>	A fájlok, amelyek mérete meghaladja a megadott korlátot (megabájt), ki vannak zárva a vizsgálat hatóköréből.

Események mentése egy jelentésfájl módba	
/R:<jentésfájl>	Csak kritikus események mentése a jelentésfájlba.
/RA:<jentés>	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:<fájlok vírusvizsgálati beállításokkal>	Fájl vírusvizsgálati feladatbeállításokkal. A fájlt manuálisan kell létrehozni, és TXT formátumban kell elmenteni. A fájl a következő tartalmakkal rendelkezhet: [<vizsgálat hatóköre>] [<művelet fenyegetés észlelésekor>] [<fájltípusok>] [<kizárás a vizsgálatból>] [/R[A]:<jentésfájl>] [<vizsgálati technológiák>].

Példa:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Adatbázisok és alkalmazás-szoftvermodulok frissítése

A *Frissítés* feladat futtatása

A parancs szintaxisa

```
FRISSÍTÉS [local][ "<frissítésforrás>" ] [/R[A]:<jelentésfájl>] [/C:<fájl a frissítési beállításokkal>]
```

Frissítési feladat beállításai	
local	<p>Az alkalmazás telepítése után automatikusan létrehozott <i>Frissítés</i> feladat kezdete. A <i>Frissítés</i> feladat beállításait a helyi alkalmazásfelületen vagy a Kaspersky Security Center konzolján módosíthatja. Ha ez a beállítás nincs konfigurálva, a Kaspersky Endpoint Security elindítja a <i>Frissítés</i> feladatot az alapértelmezett beállításokkal vagy a parancsban megadott beállításokkal. A következőképpen konfigurálhatja a <i>Frissítés</i> feladat beállításait:</p> <ul style="list-style-type: none">• UPDATE – a <i>Frissítés</i> feladat alapértelmezett beállításokkal történő elindítása: a frissítésforrás a Kaspersky frissítési szerverei, a fiók a System, valamint más alapértelmezett beállítások is érvényesek.• UPDATE local – a <i>Frissítés</i> feladat indítása a telepítés után automatikusan létrehozott beállításaival (előre definiált feladat).• UPDATE <frissítési beállítások> – a <i>Frissítés</i> feladat indítása manuálisan konfigurált beállításokkal (lásd alább).

Frissítésforrás	
"<frissítésforrás>"	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 kiszolgálót – használja.

Események mentése egy jelentésfájl módba	
/R:<jelentésfájl>	Csak kritikus események mentése a jelentésfájlba.
/RA:<jelentés>	Minden esemény mentése a jelentésfájlba.

Speciális beállítások	
/C:<fájl frissítési beállításokkal>	Fájl a <i>Frissítés</i> feladatbeállításokkal. A fájlt manuálisan kell létrehozni, és TXT formátumban kell elmenteni. A fájl a következő tartalommal rendelkezhet: ["<frissítési forrás>"] [/R[A]:<jelentésfájl>].

Példa:

```
avp.com UPDATE local
```

ROLLBACK. Utolsó frissítés visszagörgetése

A legutóbbi víruskereső adatbázisfrissítés 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 szintaxisa

```
ROLLBACK [/R[A]:<jelentésfájl>]
```

Események mentése egy jelentésfájl módba	
/R:<jelentésfájl>	Csak kritikus események mentése a jelentésfájlba.
/RA:<jelentés>	Minden esemény mentése a jelentésfájlba.

Példa:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Nyomkövetés

Rendszernyomkövetés engedélyezése/kikapcsolása. A [nyomkövetési fájlok](#) a számítógépen vannak tárolva az alkalmazás használata során, az alkalmazás eltávolításakor pedig véglegesen törölődnek. A nyomkövetési fájlok, kivéve a Hitelesítési ügynökben lévő nyomkövetési fájlokat, a %ProgramData%\Kaspersky Lab\KES\Traces mappában vannak tárolva. A nyomkövetés alapértelmezetten ki van kapcsolva.

A parancs szintaxisa

```
TRACES on|off [<nyomkövetési szint>] [<speciális beállítások>]
```

Nyomkövetési szint	
<nyomkövetési szint>	<p>A nyomkövetések részleteinek szintje. Választható értékek:</p> <ul style="list-style-type: none"> 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 <code>dbg</code> , <code>file</code> and <code>mem</code> paraméterekkel.
dbg	A <code>OutputDebugString</code> funkció használata és a nyomkövetési fájl mentése. A <code>OutputDebugString</code> funkció egy karakterláncot küld az alkalmazás hibajavítója számára, amit megjelenít a képernyőn. A részletekért látogassa meg az MSDN weboldalt .
file	Egy nyomkövetési fájl mentése (nincs méretkorlát).
rot	Nyomkövetés mentése egy korlátozott méretű, megadott számú fájlba, és a régi fájlok felülírása, amikor elérte a maximális méretet.
mem	Nyomkövetés mentése memóriakiíratási fájllokba.

Példák:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Profil indítása

Profil indítása (például az adatbázisok frissítéséhez vagy a védelmi összetevő engedélyezéséhez).

A parancs szintaxisa

```
START <profil> [/R[A]:<jelentésfájl>]
```

Profil	
<profil>	Profilnév. A <i>Profil</i> egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. Megtekintheti az elérhető profilok listáját, ha végrehajtja a <code>HELP START</code> parancsot.

Események mentése egy jelentésfájl módba	
<code>/R:<jelentésfájl></code>	Csak kritikus események mentése a jelentésfájlba.
<code>/RA:<jelentés></code>	Minden esemény mentése a jelentésfájlba.

Példa:

```
avp.com START Scan_Objects
```

STOP. Profil leállítása

Futó profil leállítása (például vizsgálat leállítása, cserélhető meghajtók vizsgálatának leállítása vagy védelmi összetevő kikapcsolása).

A parancs végrehajtásához [engedélyezni kell a Jelszóvédelmet](#). A felhasználónak rendelkeznie kell a **Védelmi összetevők letiltása** és a **Felügyeleti összetevők letiltása** jogosultságokkal.

A parancs szintaxisa

```
STOP <profil> /login=<felhasználónév> /password=<jelszó>
```

Profil	
<profil>	Profilnév. A <i>Profil</i> egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. Megtekintheti az elérhető profilok listáját, ha végrehajtja a <code>HELP STOP</code> parancsot.

Hitelesítés	
/login=<felhasználónév> /password=<jelszó>	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

STATUS. Profilállapot

Állapotinformációkat jelenít meg az [alkalmazásprofilokhoz](#) (például `fut` vagy `kész`). Megtekintheti az elérhető profilok listáját, ha végrehajtja 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 szintaxisa

```
avp.com STATUS [<profil>]
```

Ha profil nélkül adja meg a parancsot, a Kaspersky Endpoint Security az összes profil állapotát megjeleníti az alkalmazásban.

STATISTICS. Profilműveleti statisztikák

Statisztikai adatok 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 szintaxisa

RESTORE. Fájlok visszaállítása a Biztonsági mentésből

A fájl a Biztonsági mentésből visszaállítható az eredeti mappába. Amennyiben már létezik egy ilyen nevű fájl a megadott útvonalon, akkor hozzá kell adni a „-copy” utótagot a fájl nevéhez. A visszaállított fájl úgy lesz másolva, hogy megtartsa 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\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 szintaxisa

```
RESTORE [/REPLACE] <fájlnév> /login=<felhasználónév> /password=<jelszó>
```

Speciális beállítások	
/REPLACE	Meglévő fájl felülírása.
<fájlnév>	A visszaállítani kívánt fájl neve.

Hitelesítés	
/login=<felhasználónév> /password=<jelszó>	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORTÁLÁS. Alkalmazásbeállítások exportálása

Kaspersky Endpoint Security beállítások exportálása egy fájlba. A fájl a C:\Windows\SysWOW64 mappában lesz megtalálható.

A parancs szintaxisa

```
EXPORT <profil> <fájlnév>
```

Profil	
<profil>	Profilnév. A <i>Profil</i> egy Kaspersky Endpoint Security összetevő, feladat vagy funkció. Megtekintheti az elérhető profilok listáját, ha végrehajtja a <code>HELP EXPORT</code> parancsot .

Fájl az exportáláshoz	
<fájlnév>	A fájl neve, ahová az alkalmazásbeállítások exportálva lesznek. A Kaspersky Endpoint Security beállításokat exportálhatja egy DAT vagy CFG konfigurációs fájlba, egy TXT szöveges fájlba vagy egy XML dokumentumba.

Példák:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Alkalmazásbeállítások importálása

Beállítások importálása a Kaspersky Endpoint Security számára egy fájlból, ami az `EXPORT` paranccsal lett létrehozva.

A parancs végrehajtásához [engedélyezni kell a Jelszóvédelmet](#). A felhasználónak rendelkeznie kell a **Alkalmazásbeállítások konfigurálása** jogosultsággal.

A parancs szintaxisa

```
IMPORT <fájlnév> /login=<felhasználónév> /password=<jelszó>
```

Importálni kívánt fájl	
<fájlnév>	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	
<code>/login=<felhasználónév></code> <code>/password=<jelszó></code>	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Kulcsfájl alkalmazása

Kulcsfájl megadása a Kaspersky Endpoint Security aktiválásához. Ha az alkalmazás már aktiválva van, a kulcs hozzáadása tartalék kulcsként történik.

A parancs szintaxisa

```
ADDKEY <fájlnev> /login=<felhasználónév> /password=<jelszó>
```

Kulcsfájl	
<fájlnev>	Kulcsfájl neve.

Hitelesítés	
/login= <felhasználónév> /password=<jelszó>	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

Műveletek végrehajtása Kaspersky Endpoint Security licenckulcsokkal.

A parancs végrehajtásához és a licenckulcs eltávolításához a [Jelszóvédelmet engedélyezni kell](#). A felhasználónak engedélyeznie kell a **Kulcs eltávolítása** jogosultságot.

A parancs szintaxisa

```
LICENSE <operation> [/login=<felhasználónév> /password=<jelszó>]
```

Művelet	
/ADD <fájlnev>	Kulcsfájl megadása a Kaspersky Endpoint Security aktiválásához. Ha az alkalmazás már aktiválva van, a kulcs hozzáadása tartalék kulcsként történik.
/ADD <aktiváló kód>	A Kaspersky Endpoint Security aktiválása az aktiváló kód segítségével. Ha az alkalmazás már aktiválva van, a kulcs hozzáadása tartalék kulcsként történik.
/REFRESH <fájlnev>	Licenc megújítása egy kulcsfájllal. Ekkor tartalék kulcs megadására kerül sor. A licenc lejártakor aktívvá válik. Nem lehetséges aktiváló kulcsot hozzáadni a parancs hozzáadásával.
/REFRESH <aktiváló kód>	Licenc megújítása aktiváló kóddal. Ekkor tartalék kulcs megadására kerül sor. A licenc lejártakor aktívvá válik. Nem lehetséges aktiváló kulcsot hozzáadni a parancs hozzáadásával.

```
/DEL /login=  
<felhasználónév>  
/password=<jelszó>
```

Licenckulcs eltávolítása A rendszer a tartalék kulcsot is eltávolítja.

Hitelesítés

```
/login=<felhasználónév>  
/password=<jelszó>
```

Felhasználói fiók bejelentkezési adatai a szükséges [Jelszóvédelem](#) jogosultságokkal.

Példa:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCC-DDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

RENEW. Licenc vásárlása

Nyissa meg a Kaspersky weboldalt, hogy licencet vásároljon, vagy megújítsa a licencét.

PBATESTRESET. Lemez ellenőrzési eredményeinek visszaállítása a lemez titkosítása előtt

Állítsa vissza a Teljes lemeztitkosítás (FDE) kompatibilitási ellenőrzésének eredményeit, a Kaspersky Lemeztitkosítás és a BitLocker Lemeztitkosítás 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.

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 szintaxisa

```
EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Szabályzat letiltása

Letiltja a Kaspersky Security Center szabályzatot 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 szintaxisa

```
EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Szabályzat engedélyezése

Engedélyezi a Kaspersky Security Center szabályzatot a számítógépen. Az alkalmazásbeállítások a szabályzat alapján lesznek konfigurálva.

DISABLE. Védelem kikapcsolása

Kikapcsolja a fájlvédelmet a számítógépen, amin le van járva a Kaspersky Endpoint Security licenc. Ezt a parancsot nem lehet olyan számítógépen futtatni, amelyen megtalálható az alkalmazás, ami nincs aktiválva, vagy amin érvényes a licenc.

SPYWARE. Spyware észlelés

Engedélyezi/kikapcsolja a spyware-észlelést. Alapértelmezés szerint a spyware-észlelés engedélyezve van.

A parancs szintaxisa

```
SPYWARE on|off
```

KSN. Globális/privát KSN átmenet

A Kaspersky Security Network megoldás kiválasztása a fájlok vagy webhelyek megbízhatóságának meghatározásához. A Kaspersky Endpoint Security a következő KSN-infrastrukturális megoldásokat támogatja:

- *Globális KSN*: a Kaspersky alkalmazások által használt leggyakoribb megoldás. A KSN-résztvevők információkat kapnak a Kaspersky Security Networktól, és elküldik a Kaspersky számára a felhasználó számítógépén észlelt objektumokat, hogy a Kaspersky is elemezze azokat, és belevegye a Kaspersky Security Network hírnév- és statisztikai adatbázisába.

- A *Privát KSN* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky Security Network hírnévadatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a KSN-re a saját számítógépükről. A privát KSN 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 szintaxisa

```
KSN /global | /private <file name>
```

A Privát KSN konfigurációs fájlja	
<fájlnev>	A KSN proxykiszolgálójának beállításait tartalmazó konfigurációs fájl neve. A fájl PKCS7 vagy PEM kiterjesztéssel rendelkezik.

Példa:

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

KESCLI parancsok

A KESCLI parancsokkal információt kaphat a számítógép védelmének állapotáról az OPSWAT összetevő használata esetén, valamint a parancsok lehetővé teszik a szokásos feladatok végrehajtását, például a vírusvizsgálatot és az adatbázis-frissítéseket.

A KESCLI parancsok listáját a `--help` parancssal vagy a rövidített `-h` parancssal 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.
3. A parancs végrehajtásához írja be:

```
kescli <parancs> [options]
```

Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot (lásd az alábbi ábrát.)

```

Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File"      1      3/16/2021 17:14:37      "https://secure.eicar.org/eicar.com.txt"      41      1
"EICAR-Test-File"      1      3/16/2021 17:14:38      "https://www.eicar.org/download/eicar.com"      41      1

```

Az alkalmazás kezelése a parancssorból

Scan. Vírusvizsgálat

Futtassa a vírusvizsgálat feladatot.

A parancs szintaxisa

```
kescli --opswat Scan "<vizsgálat hatóköre>" <művelet fenyegetés észlelésekor>
```

A [GetScanState](#) paranccsal ellenőrizheti a *Teljes vizsgálat* feladat befejezési állapotát, valamint a [GetLastScanTime](#) paranccsal megtekintheti a vizsgálat legutóbbi befejezésének dátumát és időpontját.

Vizsgálat hatóköre	
<vizsgált fájl>	; karakterrel elválasztott lista a fájlokról és mappákról. Például: "C:\Program Files (x86)\Example Folder".

Művelet fenyegetés észlelésekor	
0	Értesítés. 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; a vírusmentesítés sikertelensége esetén törlés. 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 törli a fájlokat. 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 lekérése a *Teljes vizsgálat* feladat befejezési állapotáról:

- 1 – a vizsgálat folyamatban van.
- 0 – a vizsgálat nem fut.

A parancs szintaxisa

```
--opswat GetScanState
```

Példa:

```
kescli --opswat GetScanState
```

GetLastScanTime. A vizsgálat befejezési időpontjának meghatározása

Információ lekérése az utolsó *Teljes vizsgálat* feladat befejezési dátumáról és időpontjáról.

A parancs szintaxisa

```
--opswat GetLastScanTime
```

Példa:

```
kescli --opswat GetLastScanTime
```

GetThreats. Az észlelt fenyegetésekre vonatkozó adatok beszerzése

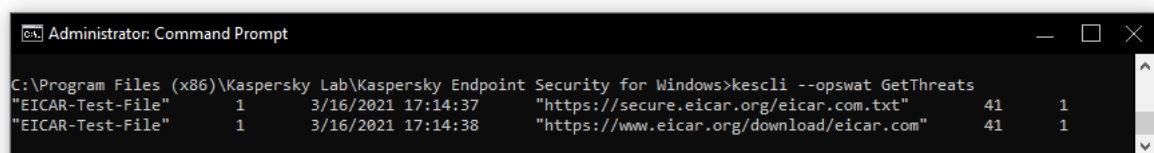
Az észlelt fenyegetések listájának lekérése (*Fenyegetések jelentés*). Ez a jelentés tartalmazza a jelentés elkészítését megelőző 30 nap során észlelt fenyegetések és vírusaktivitás információit.

A parancs szintaxisa

```
--opswat GetThreats
```

A parancs végrehajtásakor a Kaspersky Endpoint Security a következő formátumban küld választ:

```
<észlelt objektum neve> <objektumtípus> <észlelési dátum és idő> <fájl elérési útja>  
<művelet a fenyegetés észlelésekor> <fenyegetés veszélyszintje>
```



```
Administrator: Command Prompt  
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats  
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1  
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

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 módszere felhasználható károkozásra képes kód védelmére (Packed).
20	Ismeretlen objektumok (Xfiles).
21	Ismert alkalmazások (Software).
22	Rejtett fájlok (Hidden).
23	Figyelmet igénylő alkalmazás (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.
80	Nem kívánt e-mail-melléklet (Attachment).
90	Kaspersky Security Network által észlelt rosszindulatú program (Urgent).
100	Ismeretlen hivatkozás (Suspicious 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 (<code>added by user</code>).
30	Az objektum hozzá lett adva a kizárásokhoz (<code>added to exclude</code>).
31	Az objektum áthelyezve a biztonsági mentésbe a számítógép újraindításakor (<code>quarantine on reboot</code>).
36	Téves riasztás (<code>false alarm</code>).
38	A folyamat le lett állítva (<code>terminated</code>).
40	Az objektum nem lett észlelve (<code>not found</code>).
41	Nem lehet feloldani a fenyegetést (<code>untreatable</code>).
42	Az objektum vissza lett állítva (<code>rolled back</code>).
43	Az objektum fenyegetési tevékenység eredményeként jött létre (<code>produced by threat</code>).
44	Az objektum vissza lett állítva a számítógép újraindításakor (<code>roll back on reboot</code>).
0xffffffff	Az objektum nem lett feldolgozva (<code>discarded</code>).

Fenyegetés veszélyszintje	
0	Ismeretlen
1	Magas
2	Közepes vizsgálat
4	Alacsony
8	Információ (legfeljebb <i>Alacsony</i>)

UpdateDefinitions. Adatbázisok és alkalmazás-szoftvermodulok frissítése

A *Frissítés* feladat futtatása A Kaspersky Endpoint Security az alapértelmezett forrást használja: Kaspersky frissítési kiszolgálók.

A parancs szintaxisa

```
--opswat UpdateDefinitions
```

A [GetDefinitionsetState](#) paranccsal megtekintheti az utolsó befejezett *Frissítés* feladat dátumát és időpontját.

Példa:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. A frissítés befejezési időpontjának meghatározása

Információ lekérése az utolsó *Frissítés* feladat befejezési dátumáról és időpontjáról.

A parancs szintaxisa

```
--opswat GetDefinitionState
```

Példa:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Védelem engedélyezése

Engedélyezze a Kaspersky Endpoint Security védelmi összetevőket a számítógépen: Fájl védelem, Web védelem, Levelezés védelem, Hálózati védelem, Behatolásmegelőző rendszer.

A parancs szintaxisa

```
--opswat EnableRTP
```

A [GetRealTimeProtectionState](#) parancssal ellenőrizheti a Fájl védelem működési állapotát.

Példa:

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. Fájl védelem állapota

Információ lekérése a Fájl védelem összetevő működési állapotáról:

- 1 – az összetevő engedélyezve van.
- 0 – az összetevő le van tiltva.

A parancs szintaxisa

```
--opswat GetRealTimeProtectionState
```

Példa:

```
kescli --opswat GetRealTimeProtectionState
```

Version. Az alkalmazás verziójának azonosítása

A Kaspersky Endpoint Security for Windows verziójának azonosítása.

A parancs szintaxisa

```
--Version
```

Használhatja a rövidített `-v` parancsot is.

Példa:
`kescli -v`

Detection and Response felügyeleti parancsok

A parancssor segítségével kezelheti az Endpoint 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 végrehajtja a `HELP` parancsot. A megadott parancs szintaxisának elolvasásához adja meg a `HELP <parancs>` 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 írja be:

```
avp.com <parancs> [options]
```

Ennek eredményeképp a Kaspersky Endpoint Security végrehajtja a parancsot (lásd az alábbi ábrát.)

SANDBOX. A Kaspersky Sandbox felügyelete

A Kaspersky Sandbox összetevő felügyeletéhez tartozó parancsok:

- A Kaspersky Sandbox összetevő engedélyezése vagy letiltása.
A Kaspersky Sandbox összetevő lehetővé teszi a Kaspersky Sandbox megoldással való használatot.
- A Kaspersky Sandbox összetevő konfigurálása:
 - Csatlakoztassa a számítógépet a Kaspersky 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 képek telepítésével és a Kaspersky Sandbox-kiszolgálók konfigurálásával kapcsolatos részletekért lásd a [Kaspersky Sandbox súgót](#).
 - A Kaspersky Sandbox-kiszolgáló kapcsolódási időtúllépésének konfigurálása.
Időtúllépés a Kaspersky Sandbox-kiszolgálótól származó objektumvizsgálati kérésre adott válasz fogadásakor. Az időkorlát letelte után a Kaspersky Sandbox átirányítja a kérést a következő kiszolgálónak. Az időtúllépés értéke a kapcsolat sebességétől és stabilitásától függ. Az alapértelmezett érték 5 másodperc.
 - Konfigurálja a megbízható kapcsolatot a számítógép és a Kaspersky Sandbox-kiszolgáló között.

Ha megbízható kapcsolatot szeretne konfigurálni a Kaspersky Sandbox kiszolgálóival, elő kell készítenie egy TLS-tanúsítványt. Ezután hozzá kell adnia a tanúsítványt a Kaspersky Sandbox-kiszolgálókhoz és a Kaspersky Endpoint Security házirendjéhez. A tanúsítvány előkészítéséről és a tanúsítványnak a kiszolgálókhoz való hozzáadásáról részletesen lásd a [Kaspersky Sandbox súgót](#).

- Az összetevő aktuális beállításainak megjelenítése.

A parancs szintaxisa

```
stop sandbox [/login=<felhasználónév> /password=<jelszó>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<kiszolgáló címe>:<port>] [--timeout=
<Kaspersky Sandbox-kiszolgáló kapcsolódási időtúllépése (ms)>] [--pinned-certificate=
<TLS-tanúsítvány elérési útja>][/login=<felhasználónév> /password=<jelszó>]
sandbox /show
```

Művelet	
stop	A Kaspersky Sandbox összetevő letiltása.
start	A Kaspersky Sandbox összetevő engedélyezése.
set	A Kaspersky Sandbox összetevő konfigurálása. Az alábbi beállításokat módosíthatja: <ul style="list-style-type: none"> • Megbízható kapcsolat használata (--tls); • TLS-tanúsítvány hozzáadása (--pinned-certificate); • A Kaspersky Sandbox-kiszolgáló kapcsolódási időtúllépésének beállítása (--timeout); • Kaspersky Sandbox-kiszolgálók hozzáadása (--servers).
show	Az összetevő aktuális beállításainak megjelenítése. A következő választ kapja: <pre>sandbox.timeout=<Kaspersky Sandbox-kiszolgáló kapcsolódási időtúllépése (ms)> sandbox.tls=<megbízható kapcsolat állapota> sandbox.servers=<Kaspersky Sandbox-kiszolgálók listája></pre>

Hitelesítés	
/login=<felhasználónév> /password=<jelszó>	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa:

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

MEGELŐZÉS. A végrehajtás megakadályozásának kezelése

Letilthatja a végrehajtás megelőzését, vagy megjelenítheti az aktuális összetevői beállításokat, beleértve a végrehajtásmeelőzési szabályok listáját is.

A parancs szintaxisa

```
prevention disable  
prevention /show
```

A `prevention /show` parancs végrehajtása után a következő választ kapja:

```
prevention.enable=true|false
```

```
prevention.mode=audit|prevent
```

```
prevention.rules
```

```
id: <szabály azonosítója>
```

```
target: script|process|document
```

```
md5: <a fájl MD5 kivonata>
```

```
sha256: <a fájl SHA256 kivonata>
```

```
pattern: <objektum elérési útja>
```

```
case-sensitive: true|false
```

A parancs visszatérési értékei:

- A -1 azt jelenti, hogy a parancsot nem támogatja a Kaspersky Endpoint Security eszközre telepített 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).

ELKÜLÖNÍTÉS. A hálózatelkülönítés kezelése

Kikapcsolhatja a számítógép hálózatelkülönítését, vagy megjelenítheti az összetevő aktuális beállításait. Az összetevők beállításai tartalmazzák a kizárásokhoz hozzáadott hálózati kapcsolatok listáját is.

A parancs szintaxisa:

```
Isolation /OFF /login=<felhasználónév> /password=<jelszó>  
isolation /STAT
```

A `stat` parancs futtatásának eredményeként a következő választ kapja: `Network isolation on|off`.

RESTORE. Fájlok visszaállítása a Karanténból

A fájl a karanténból visszaállítható az eredeti mappába. Ha a célmappa törlésre került, az alkalmazás a fájlt a számítógép egy speciális mappájába helyezi. Ezután manuálisan át kell helyeznie a fájlt a célmappába. A *Karantén* egy speciális helyi tároló a számítógépen, ahová a vírusokkal vagy nem fertőtleníthető fájlokkal fertőzött fájlokat helyezi át az alkalmazás. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha a Kaspersky Sandbox és a Kaspersky Endpoint Detection and Response megoldásokkal dolgozik együtt. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a [Biztonsági mentésbe](#) helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért lásd a [Kaspersky Sandbox súgót](#), a [Kaspersky Endpoint Detection and Response Optimum súgót](#) és a [Kaspersky Endpoint Detection and Response Expert 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 parancs szintaxisa

```
RESTORE [/REPLACE] <fájlnév> /login=<felhasználónév> /password=<jelszó>
```

Speciális beállítások	
/REPLACE	Meglévő fájl felülírása.
<fájlnév>	A visszaállítani kívánt fájl neve.

Hitelesítés	
/login=<felhasználónév> /password=<jelszó>	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

A parancs visszatérési értékei:

- A -1 azt jelenti, hogy a parancsot nem támogatja a Kaspersky Endpoint Security eszközre telepített 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

Biztonsági sérülési indikátorok (IOC) vizsgálata feladat futtatása. 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 vizsgálat* feladatok lehetővé teszik a biztonsági sérülési indikátorok (IOC) megtalálását a számítógépen, valamint biztosítják a fenyegetésre reagáló intézkedések megtételét.

A parancs szintaxisa

```
IOCSAN <IOC-fájl teljes elérési útvonala>|/path=<IOC-fájlok mappájának elérési
útvonala> [/process=on|off] [/hint=<folyamat futtatható fájljának teljes elérési
útvonala|fájl teljes elérési útvonala>] [/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=<esemény közzétételi dátuma>]
[/channels=<csatornák listája>] [/files=on|off] [/drives=
<összes|rendszer|kritikus|egyedi>] [/excludes=<kizárások listája>][scope=<vizsgálandó
mappák listája>]
```

IOC-fájlok	
<IOC-fájl teljes elérési útja>	A vizsgálathoz használni kívánt IOC-fájl teljes elérési útja. Több IOC-fájlt is megadhat szögzőkökkel elválasztva. Az IOC-fájl teljes elérési útját a /path argumentum nélkül kell megadni. Például C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<IOC-fájlok mappájának elérési útja>	A vizsgálathoz használni kívánt IOC-fájlokat tartalmazó mappa elérési útja. Az <i>IOC-fájlok</i> 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=<folyamat futtatható fájljának teljes elérési útja fájl teljes elérési útja>	Fájladatok elemzése az IOC vizsgálat során (ProcessItem and FileItem kifejezések). Egy fájlt az alábbi módokon választhat ki: <ul style="list-style-type: none"> • <folyamat futtatható fájljának teljes elérési útja> – ProcessItem; • <fájl teljes elérési útja> – FileItem.
/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).

	<p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a Windows rendszerleíró adatbázisát, ha a RegistryItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p> <p>A RegistryItem adattípus esetén a Kaspersky Endpoint Security átvizsgálja a beállítások készletét.</p>
/dnsentry=on off	<p>A helyi DNS-gyorsítótárban lévő rekordok adatainak elemzése az IOC vizsgálat során (DnsEntryItem kifejezés).</p> <p>Ha az argumentum értéke off, a Kaspersky Endpoint Security nem vizsgálja a helyi DNS-gyorsítótárt. Ha az IOC-fájl tartalmazza a DnsEntryItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a helyi DNS-gyorsítótárt, ha a DnsEntryItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>
/arpentry=on off	<p>Az ARP-tábla rekordadatainak elemzése az IOC vizsgálat során (ArpEntryItem kifejezés).</p> <p>Ha az argumentum értéke off, a Kaspersky Endpoint Security nem vizsgálja az ARP-táblát. Ha az IOC-fájl tartalmazza az ArpEntryItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi az ARP-táblát, ha az ArpEntryItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>
/ports=on off	<p>A figyelésre megnyitott portok adatainak elemzése az IOC vizsgálat során (PortItem kifejezés).</p> <p>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).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi az aktív kapcsolatok tábláját, ha a PortItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>
/services=on off	<p>Az eszközre telepített szolgáltatások adatainak elemzése az IOC vizsgálat során (ServiceItem kifejezés).</p> <p>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).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a szolgáltatásadatokat, ha a ServiceItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>

<p>/system=on off</p>	<p>Környezeti adatok elemzése az IOC vizsgálat során (SystemInfoItem kifejezés).</p> <p>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).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a környezeti adatokat, ha a SystemInfoItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>
<p>/users=on off</p>	<p>Felhasználói adatok elemzése az IOC vizsgálat során (UserItem kifejezés).</p> <p>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).</p> <p>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 vizsgálatához biztosított IOC-fájlban.</p>
<p>/volumes=on off</p>	<p>Kötetadatok elemzése az IOC vizsgálat során (VolumeItem kifejezés).</p> <p>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).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a kötetadatokat, ha a VolumeItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>
<p>/eventlog=on off</p>	<p>A Windows Eseménynapló rekordadatainak elemzése az IOC vizsgálat során (EventLogItem kifejezés).</p> <p>Ha az argumentum értéke off, a Kaspersky Endpoint Security nem vizsgálja a Windows Eseménynapló rekordjait. Ha az IOC-fájl tartalmazza az EventLogItem IOC-dokumentumának feltételeit, akkor ezek figyelmen kívül lesznek hagyva (nincs egyezésként észlelve).</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security csak akkor elemzi a Windows Eseménynaplót, ha az EventLogItem IOC-dokumentumának leírása szerepel a vizsgálatához biztosított IOC-fájlban.</p>
<p>/datetime=<esemény közzétételi dátuma></p>	<p>Figyelembe veszi az esemény Windows Eseménynaplóban történő közzétételének dátumát, amikor meghatározza a megfelelő IOC-dokumentumhoz tartozó IOC vizsgálat hatókörét.</p> <p>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.</p> <p>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.</p>

	<p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security minden közzétételi dátumú eseményt megvizsgál. A TaskSettings::BaseSettings::EventLogItem::datetime beállítás nem szerkeszthető.</p> <p>A beállítás csak akkor használható, ha az EventLogItem IOC-dokumentumának leírása szerepel a vizsgálathoz biztosított IOC-fájlban.</p>
<p>/channel=<csatornák listája></p>	<p>Azon csatorna (napló) nevek listája, amelyek esetében IOC vizsgálatot szeretne végezni.</p> <p>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.</p> <p>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 szóközzel elválasztva.</p> <p>Ha az argumentum nincs megadva, a Kaspersky Endpoint Security megvizsgálja az Application, System, Security csatornák rekordjait.</p>
<p>/files=on off</p>	<p>Fájladatok elemzése az IOC vizsgálat során (FileItem kifejezés).</p> <p>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).</p> <p>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.</p>
<p>/drives=<all system critical custom></p>	<p>Az IOC vizsgálat hatókörének beállítása a FileItem IOC-dokumentumadatainak elemzésekor.</p> <p>A következő értékeket állíthatja be a vizsgálat hatóköréhez:</p> <ul style="list-style-type: none"> • <all> az összes rendelkezésre álló fájl hatóköréhez. • <system> azokban a mappákban található fájlhoz, amelyekben az operációs rendszer telepítve van. • <critical> felhasználói és rendszermappákban található ideiglenes fájlhoz. • <custom> a felhasználó által meghatározott hatókörű fájlhoz (/scope=<vizsgálandó mappák listája>). <p>Ha az argumentum nincs megadva, a vizsgálat a kritikus területeken történik.</p>
<p>/excludes=<kizárások listája></p>	<p>Kizárás hatókörének beállítása a FileItem IOC-dokumentumadatainak elemzésekor. Több elérési utat is megadhat szóközzel elválasztva.</p>
<p>/scope=<vizsgálandó mappák listája></p>	<p>Felhasználó által definiált IOC vizsgálati hatókör a FileItem IOC-dokumentumadatainak elemzésekor (/drives=custom). Több elérési utat is megadhat szóközzel elválasztva.</p>

A parancs visszatérési értékei:

- A -1 azt jelenti, hogy a parancsot nem támogatja a Kaspersky Endpoint Agent eszközre telepített 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 fájlal végezhet műveleteket 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](#) talál.

A BLOB fájlokkal végzett műveletekhez rendszergazdai jogosultságra van szükség. A Managed Detection and Response házirendben lévő beállításainak is rendelkezésre kell állniuk szerkesztésre (🔑).

A parancs szintaxisa

```
MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Művelet	
/ADD <fájlnév>	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=<felhasználónév> /password=<jelszó>	Felhasználói fiók bejelentkezési adatai a szükséges Jelszóvédelem jogosultságokkal.

Példa:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

Hibakódok

Hibák akkor léphetnek fel, amikor az alkalmazást a parancssorok keresztül kezeljük. Hiba esetén a Kaspersky Endpoint Security hibaüzenetet jelenít meg, például: **Hiba: Nem lehet elindítani az 'EntAppControl' feladatot.** A Kaspersky Endpoint Security egy kód formájában további információkat is megjelenít, például: **error=8947906D** (lásd az alábbi táblázatot).

Hibakódok

Hibakód	Leírás
09479001	A Kaspersky Endpoint Security licenckulcsa már használatban van ezen a számítógépen.
0947901D	A licenc lejárt. Nem érhető el adatbázisfrissítés.
89479002	Nem található kulcs.
89479003	Nincs digitális frissítés, vagy hibás.
89479004	Fertőzött adat.
89479005	Fertőzött kulcsfájl.
89479006	A licenc vagy a licenckulcs lejárt.
89479007	Nincs megadva kulcsfájl.
89479008	Nem lehet alkalmazni a kulcsfájlt.
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 digitális aláírása nem egyezik meg a Kaspersky digitális aláírásával.
89479015	A kulcsot nem lehet úgy nem kereskedelmi licenchez használni, mint kereskedelmi licenchez.
89479016	Bétalicenc szükséges az alkalmazás bétaverziójának használatához.
89479017	A kulcsfájl nem kompatibilis ezzel az alkalmazással.
89479018	A kulcsot blokkolja a Kaspersky.
89479019	Az alkalmazás már használva volt próbalicenccel. Nem lehet újra próbakulcsot hozzáadni.

8947901A	Fertőzött kulcsfájl.
8947901B	A digitális aláírás hiányzik, fertőzött 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 rendszer dátumát.
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	Hiba a licenckulcs szolgáltatási adataiban.
89479023	Nem lehet érvénytelen kulcsfájllal hozzáadni tartalék kulcsot.
89479025	Nem sikerült kérelmet küldeni az aktivációs kiszolgálóra. Lehetséges okok: internetkapcsolati hiba vagy az aktivációs kiszolgáló átmeneti problémája. Próbálja meg aktiválni az alkalmazást az aktiváló kóddal. Ha a hiba fennáll, lépjen kapcsolatba az internetszolgáltatójával.
89479026	Az aktivációs kiszolgáló válaszadási hibája.
89479027	Nem lehet lekérni a válasz állapotát.
89479028	Hiba az ideiglenes fájl mentése közben.
89479029	A megadott aktiváló kód vagy a rendszer dátuma helytelen. Ellenőrizze a rendszer dátumát a számítógépen.
8947902A	A kulcsfájl nem kompatibilis ezzel az alkalmazással, vagy a licenc lejárt. Nem sikerült aktiválni a Kaspersky Endpoint Security alkalmazást azzal, hogy kulcsfájlt használt egy másik alkalmazáshoz.
8947902B	Nem sikerült lekérni 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	Az aktivációs kiszolgáló a 404-as hibakódot küldte vissza.
89479030	Az aktivációs kiszolgáló a 405-as hibakódot küldte vissza.
89479031	Az aktivációs kiszolgáló a 406-as hibakódot küldte vissza.
89479032	A proxykiszolgáló hitelesítése szükséges. Ellenőrizze a hálózati beállításokat.
89479033	A kérelem várakozási ideje lejárt.
89479034	Az aktivációs kiszolgáló a 409-as hibakódot küldte vissza.
89479035	Az aktivációs kiszolgáló a 410-as hibakódot küldte vissza.
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.

8947903D	A funkció nincs támogatva.
8947903E	Érvénytelen válasz az átjárótól. Ellenőrizze a hálózati beállításokat.
8947903F	A szolgáltatás nem érhető el (HTTP hiba 503).
89479040	Az átjáró válaszüzeje lejárt. Ellenőrizze a hálózati beállításokat.
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 a paraméterek ANSI-karakterlánccá való átalakításakor (URL, mappa, ügynök).
8947904A	Hiba a munkaszál létrehozásakor.
8947904B	A munkaszál már fut.
8947904C	A munkaszál nem fut.
8947904D	Nem található kulcs az aktivációs kiszolgálón.
8947904E	A kulcs blokkolva van.
8947904F	Az aktivációs kiszolgáló belső hibája.
89479050	Nincs elég adat az aktivációs kérelemben.
89479053	A licenckulcs lejárt.
89479054	A számítógépen beállított rendszer dátum érvénytelen.
89479055	A próbalicenc lejárt.
89479056	A licenc lejárt.
89479057	Az alkalmazásaktivációs korlát túl van lépve a megadott kódnál.
89479058	Az aktivációs eljárás rendszerhibával végződött.
89479059	A kulcsot nem lehet úgy nem kereskedelmi licenchez használni, mint kereskedelmi licenchez.
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	Az alkalmazásadatbázis megjelenési dátuma a licenc lejárat dátuma után található.
89479066	Nem lehet lejárt kulccsal lecserélni az aktivációs kulcsot.
89479067	Nem lehet tartalék kulcsot hozzáadni, ha annak lejárat korábbi, mint a jelenlegi licencé.
89479068	A frissített előfizetési kulcs hiányzik.
8947906A	Helytelen aktiváló kód (az ellenőrzőösszeg nem egyezik meg).
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	Az átviteli réteg általános hibája.
89479214	Nem sikerült csatlakozni az aktivációs kiszolgálóhoz.
89479215	Érvénytelen URL-formátum.
89479216	Nem sikerült konvertálni a proxykiszolgáló címét.
89479217	Nem sikerült átalakítani a kiszolgáló címét. Ellenőrizze az internetkapcsolata beállításait.
89479218	Nem sikerült csatlakozni az aktivációs kiszolgálóhoz vagy a proxykiszolgálóhoz.
89479219	Távoli elérés megtagadva.
8947921A	A válaszdő lejárt.
8947921B	Hiba a HTTP-kérelem küldésekor.
8947921C	SSL-kapcsolati hiba.
8947921D	A műveletet visszahívás szakította meg.
8947921E	Túl sok továbbítási próba.
8947921F	A címzett ellenőrzése sikertelen.
89479220	Az aktivációs kiszolgáló válasza üres.
89479221	Hiba az adatok küldésekor.
89479222	Hiba az adatok fogadásakor.
89479223	Helyi SSL-tanúsítvány hiba.
89479224	SSL-titkosítási hiba.
89479225	Kiszolgáló SSL-tanúsítvány hiba.
89479226	A hálózati csomag tartalma érvénytelen.
89479227	Felhasználói hozzáférés megtagadva.
89479228	Érvénytelen SSL-tanúsítvány fájl.
89479229	Nem sikerült SSL-kapcsolatot létrehozni.
8947922A	Nem sikerült hálózati csomagot küldeni vagy fogadni. Kérjük, próbálja újra később.
8947922B	Érvénytelen fájl megvont tanúsítványokkal.
8947922C	SSL-tanúsítvány kérelem hiba.
89479401	Ismeretlen kiszolgáló hiba.
89479402	Belső kiszolgálóhiba.
89479403	Nincs elérhető licenckulcs a megadott aktiváló kódhoz.
89479404	aktiváló kód blokkolva.
89479405	Az alkalmazás aktivációs kérelméhez szükséges paraméterek hiányoznak.
89479406	Érvénytelen felhasználónév vagy jelszó.
89479407	Helytelen aktiváló kód lett elküldve a szerverre.
89479408	Ez az aktiváló kód érvénytelen a Kaspersky Endpoint Security alkalmazáshoz. Nem aktiválhatja a

	Kaspersky Endpoint Security alkalmazást egy ismeretlen alkalmazáshoz tartozó kulcsfájllal.
89479409	A kérelemből hiányzik egy aktiváló kód.
8947940B	A licenc lejárt (az aktivációs kiszolgáló adatai szerint).
8947940C	A kódhoz járó aktivációk száma túllépve.
8947940D	A kérelemazonosító érvénytelen formátuma.
8947940E	Ez az aktiváló kód érvénytelen a Kaspersky Endpoint Security alkalmazáshoz. Az aktiváló kód egy más Kaspersky alkalmazáshoz kell.
8947940F	Nem lehet frissíteni a licenckulcsot.
89479410	Az aktiváló kód érvénytelen ehhez a régióhoz.
89479411	Az aktiváló kód érvénytelen a Kaspersky Endpoint Security nyelvverziójához.
89479412	További hozzáférés szükséges az aktivációs kiszolgálóhoz.
89479413	Az aktivációs kiszolgáló a 643-as hibakódot küldte vissza.
89479414	Az aktivációs kiszolgáló a 644-as hibakódot küldte vissza.
89479415	Az aktivációs kiszolgáló a 645-as hibakódot küldte vissza.
89479416	Az aktivációs kiszolgáló a 646-as hibakódot küldte vissza.
89479417	Az aktiváló kód formátumát nem támogatja az aktivációs kiszolgáló.
89479418	Érvénytelen aktiválókód-formátum.
89479419	A számítógépen beállított rendszeridő érvénytelen.
8947941A	Az aktiváló kód érvénytelen a Kaspersky Endpoint Security verziója számára.
8947941B	Az előfizetés lejárt.
8947941C	Az aktiválások száma túl van lépve ennél a licenckulcsnál.
8947941D	A licenckulcs digitális aláírása érvénytelen.
8947941E	További adat szükséges.
8947941F	Sikertelen felhasználóiadat-hitelesítés.
89479420	Az előfizetés inaktív.
89479421	Az aktivációs kiszolgáló karbantartás alatt áll.
89479501	A Kaspersky Endpoint Security ismeretlen hibája.
89479502	Érvénytelen paraméterek továbbítva (például az aktivációs kiszolgálócímek üres listája).
89479503	Érvénytelen aktiváló kód
89479504	Érvénytelen felhasználónév.
89479505	Érvénytelen felhasználói jelszó.
89479506	Az aktivációs kiszolgáló érvénytelen válasza.
89479507	Az aktivációs kérelem megszakadt.
89479509	Az aktivációs kiszolgáló egy 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`, `EXPORT` és `IMPORT` 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.
- `BehaviorDetection` – Viselkedéselemző.
- `DeviceControl` – Eszközfelügyelő.
- `EntAppControl` – Alkalmazásfelügyelő.
- `File_Monitoring` or `FM` – Fájlvédelem.
- `Firewall` vagy `FW` – Tűzfal.
- `HIPS` – Behatolásmegelőző rendszer.
- `IDS` – Hálózati védelem.
- `IntegrityCheck` – Integritásellenőrző.
- `Mail_Monitoring` or `EM` – Levelezés védelem.
- `Rollback` – visszagörgetés frissítése.
- `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.
- `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 kliens 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 kulchosszal.

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=<Felhasználónév>

A felhasználónév, amivel kezelheti az alkalmazást a REST API-n keresztül. Adja meg a felhasználónevet a következő formátumban: <DOMAIN>\<Felhasználónév> (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 adatcserehez használt port. Opcionális paraméterek. A Port 6782 az alapértelmezett.

- RESTAPI_Certificate=<tanúsítvány útvonala>

Tanúsítvány a kérések azonosítására (pl. RESTAPI_Certificate=C:\cert.pem).

A tanúsítványt az alkalmazás telepítése után telepítheti, vagy a tanúsítvány lejártá 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\Rest

3. Adja meg a tanúsítvány elérési útját, pl. Tanúsítvány = 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-kéréssel 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 beállításában 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-kérélmeket.

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-kérélmekre 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

A Kaspersky Endpoint Security oldal a Kaspersky webhelyen

A [Kaspersky Endpoint Security oldalon](#) megtekintheti az alkalmazásról és funkcióiról szóló általános információkat.

A Kaspersky Endpoint Security oldal hivatkozást tartalmaz az online üzletre. Itt megvásárolhatja vagy megújíthatja az alkalmazást.

A Kaspersky Endpoint Security oldala a Tudásbázisban

A *Tudásbázis* a Terméktámogatás webhely egyik része.

A [Kaspersky Endpoint Security oldalon a Tudásbázisban](#) olvashat olyan cikkeket, amik hasznos információkat, javaslatokat tartalmaznak, valamint válaszokat a vásárlással, telepítéssel és az alkalmazás használatával kapcsolatos gyakori kérdésekre.

A Tudásbázis cikkei nem csak a Kaspersky Endpoint Security alkalmazással kapcsolatos gyakori kérdésekre tudja a választ, hanem egyéb Kaspersky alkalmazásokéra is. A Tudásbázisban lévő cikkek a Terméktámogatástól származó híreket is tartalmazhatnak.

A Kaspersky applications alkalmazásokról szóló beszélgetések a felhasználói közösségben

Ha kérdése nem igényel sürgősen választ, megbeszélheti a Kaspersky szakértőivel és más felhasználókkal a [Közösségünkben](#).

A Közösségben aktuális témákról olvashat, megjegyzéseket fűzhet a beszélgetésekhez és új témákat 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.
- Az egyedi alkalmazásösszetevők beállításainak finomhangolása, melyek a szokásos felhasználói felület elemein keresztül nem érhetők el.
- 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, utasításait 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 törölődnek.

A nyomkövetési fájlok, kivéve a Hitelesítési ügynökben lévő nyomkövetési fájlokat, a %ProgramData%\Kaspersky Lab\KES\Traces mappában vannak tárolva.

A nyomkövetési fájlok a következők: KES<service version number_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 alkalmazás-összetevő.
- Az esemény súlyossági foka (tájékoztató jellegű, figyelmeztetés, kritikus esemény, hiba).
- Az esemény leírása az alkalmazás összetevőjének parancsvégrehajtásával és a végrehajtás eredményével együtt.

A Kaspersky Endpoint Security a nyomkövetési fájlok felhasználói jelszavait csak titkosított formában menti el.

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 fájlnevében szerepel.
- Az Ön e-mail címe vagy fiókja nevét és jelszavát tartalmazó webcím, ha azok az észlelt objektum nevében találhatóak.

- 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 memóriakiírásának 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-nyomonkövetési fájlok a következők: KES<version number_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 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 shelllex.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 találhatóak, 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-<nyomkövetési fájl típusa>.DESKTOP-<fájlfrissítés dátuma>.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 kiszolgálóhoz. ([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 bekövetkezett eseményekről szóló üzenetek részletes nyilvántartása.

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 **Támogatási 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:
 - **Forgatással.** 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 a forgatáshoz szükséges fájlok maximális számát és az egyes fájlok maximális méretét.
 - **Írás egyetlen fájlba.** Egy nyomkövetési fájl mentése (nincs méretkorlát).
5. A **Szint** legördülő listán válassza ki a nyomkövetési szintet.

Ajánlott a szükséges nyomkövetési szintet a Terméktámogatási szolgáltatás szakembereivel tisztázni. Ha nem kap útmutatást a Terméktámogatás szakemberétől, állítsa be a szintet **Normál (500)**-ra.

6. Indítsa újra a Kaspersky Endpoint Security alkalmazást.

7. A nyomkövetési folyamat leállításához térjen vissza a **Támogatás** ablakba, és tiltsa le a nyomkövetést.

Továbbá létrehozhat nyomkövetési fájlokat, ha telepíti az alkalmazást a [parancssorból](#), például a [setup.ini fájl](#) használatával.

Ennek eredményeképpen a teljesítmény nyomonkövetési fájlok a %ProgramData%\Kaspersky Lab\KES\Traces mappában tárolódnak. A nyomkövetési fájl 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 nyomonkövetése* 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 **Támogatási 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:
 - **Forgatással.** 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.
 - **Írás egyetlen fájlba.** 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 nyomkövetési 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 nyomkövetési 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 **Támogatás** ablakba, és tiltsa le a nyomkövetést.

Ennek eredményeképpen a teljesítmény nyomkövetési fájlok a %ProgramData%\Kaspersky Lab\KES\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 törölődnek. A memóriakép kiíratási fájlok a %ProgramData%\Kaspersky Lab\KES\Traces mappában vannak tárolva.

Memóriakép írásának engedélyezése és letiltása:

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

Kiíratási és nyomkövetési fájlok védelmének be- és kikapcsolása:

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

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 beállításai](#)ban.
- 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 az AES titkosítási modul bármely verzióját egy olyan számítógépre próbálja telepíteni, amelyen telepítve van a Kaspersky Endpoint Security for Windows 11.8.0, de nincsenek titkosítási összetevők telepítve, a titkosítási modul telepítése hibaüzenettel fejeződik be, amely azt jelzi, hogy az alkalmazás újabb verziója van telepítve. A Kaspersky Endpoint Security 10 for Windows Service Pack 2 (10.3.0.6294 verzió) verziótól kezdve nincs külön telepítőfájl a Titkosítási modulhoz. A titkosítási könyvtárak az alkalmazás terjesztőcsomagjában találhatóak. A Kaspersky Endpoint Security 11.8.0 nem kompatibilis az AES titkosítási modulokkal. A titkosításhoz szükséges könyvtárak telepítése automatikusan megtörténik, ha a Teljes lemeztitkosítás (FDE) vagy a Fájlszintű titkosítás (FLE) összetevőt választják.
- 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 maradványainak eltávolításához küldjön a helyzet részletes leírását tartalmazó kérelmet a Kaspersky Lab Terméktámogatás részére a [Kaspersky CompanyAccount](#) használatával.
- Ha megszakította az alkalmazás eltávolítását, a számítógép újraindítása után kezdje meg a helyreállítást.
- 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 találhatóak. 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.

- Ha az alkalmazás egy korábbi verzióját frissíti a 11.8.0 verzióra, a Kaspersky Endpoint Agent telepítéséhez indítsa újra a számítógépet, és jelentkezzen be a rendszerbe egy helyi rendszergazdai jogokkal rendelkező felhasználói fiók használatával. Ellenkező esetben a Kaspersky Endpoint Agent nem lesz telepítve a frissítési eljárás során.
- 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 fájljal](#) 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.

[Az alkalmazás frissítése](#)

- Ha a Kaspersky Endpoint Security 10 Service Pack 2 for Windows (10.3.0.6294 számú build) alkalmazásról frissít, akkor a [Behatolásmegelőző rendszer](#) összetevő be van kapcsolva.
- A Kaspersky Endpoint Security 10 for Windows Service Pack 2 (10.3.0.6294 számú build) Kaspersky Endpoint Security 11.3.0 for Windows verzióra történő frissítése esetén a rendszer az alkalmazás korábbi verziójának biztonsági mentésébe vagy karanténjába helyezett fájlokat az alkalmazás új verziójának biztonsági mentésébe helyezi át. Ezek a fájlok nem lesznek átadva a Kaspersky Endpoint Security 10 for Windows Service Pack 2 korábbi verzióinál (10.3.0.6294 számú build). A mentéshez vissza kell állítania a fájlokat a karanténból és a biztonsági mentésből, mielőtt frissítené az alkalmazást. A frissítés befejezése után vizsgálja meg újra a visszaállított fájlokat.
- Az alkalmazás 11.0.0-s verziójától kezdve telepítheti a Kaspersky Endpoint Security for Windows MMC beépülő modul a korábbi verziójú beépülő modulra. Visszatérhet a korábbi verziójú beépülő modulhoz, ha törli az aktuális beépülő modult, és telepíti annak korábbi verzióját.
- A Kaspersky Endpoint Security 11.0.0 vagy 11.0.1 for Windows frissítésekor a *frissítés, a kritikus területek vizsgálata, az egyéni vizsgálat és az Integritás-ellenőrzés helyi feladatütemezési beállításokat* nem menti a rendszer.
- 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.
- Ha az alkalmazás egy korábbi verzióját frissíti a 11.8.0 verzióra, a Kaspersky Endpoint Agent telepítéséhez indítsa újra a számítógépet, és jelentkezzen be a rendszerbe egy helyi rendszergazdai jogokkal rendelkező felhasználói fiók használatával. Ellenkező esetben a Kaspersky Endpoint Agent nem lesz telepítve a frissítési eljárás során.
- Ha a Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 verziót frissíti a Windows 10 1809, 1903 és 1909 verziót futtató számítógépekre telepített Fájlszintű titkosítás (FLE) összetevővel, az FDE illesztőprogramok nem lesznek telepítve a WinRE rendszerképbe.
- 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 *Kritikus* 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.
- Miután az alkalmazást a Kaspersky Endpoint Security 11 for Windows korábbi verziójáról frissítette, a számítógépet újra kell indítani.

- 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 Vírusvizsgálat megfelelően működik.
 - A kiszolgáló víruskeresői ellenőrzésének megkezdése után az iCheckerrel hozzáadott vizsgálati 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.
- A 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 érhetőek el: Web védelem, Levelezés védelem, Webfelügyelő, BadUSB védelem és Anti-Bridging.
 - 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 hajtja végre a telepítést az engedélyezett [Biztosítsa a Citrix PVS szolgáltatásokkal való kompatibilitást 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\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

A Citrix XenDesktoptal 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.

Kompatibilitás a Kaspersky Security Centerrel

- Az Adaptív Anomáiafelügyelő összetevőt csak a Kaspersky Security Center 11-es vagy újabb verziójában kezelheti.
- Előfordulhat, hogy a Kaspersky Security Center 11 fenyegetésjelentése nem jeleníti meg az AMSI védelem által észlelt fenyegetésekkel kapcsolatos intézkedéseket.
- Az AMSI védelem és az Adaptív Anomáiafelügyelő összetevő csak a Kaspersky Security Center 11-es vagy újabb verziójában található meg. A Kaspersky Security Center konzol üzemállapota a számítógép tulajdonságain belül a **Feladatok** részben tekinthető meg. Az ezekről az összetevőkről készített jelentések szintén csak a Kaspersky Security Center version 11-es vagy újabb verziójánál érhetők el.

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 nem aktiválható előfizetősként a Kaspersky Security Center segítségével, ha a licenc lejárt, vagy a próbalicenc aktív a számítógépen. A próbalicenc vagy a hamarosan lejáró licenc előfizetői licenccel történő cseréjéhez [használja a licencterjesztési feladatot](#).
- Az alkalmazás felületén a licenc lejárat 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. Az alkalmazás ugyanis először telepíti és megpróbálja aktiválni a beágyazott próbalicencet, amelynek aktiválásához internet-hozzáférésre van szükség a telepítési eljárás során.
- 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. Az alkalmazás ugyanis ismét telepíti és megpróbálja aktiválni a beágyazott próbalicencet, amelynek aktiválásához internet-hozzáférésre van szükség a frissítés telepítésekor.
- 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 11.8.0-s verzióját használja, előfordulhat, hogy az összetevő-teljesítmény jelentések nem fognak megfelelően működni. 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.

Kármentesítő motor

- Az alkalmazás csak olyan eszközökön állít vissza fájlokat, amiken NTFS vagy FAT32 fájlrendszer van.
- Az alkalmazás a következő kiterjesztésű fájlokat állítja vissza: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsx, 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 fájlmodosításokat, amiket operációs rendszer kernel szintű folyamatok hajtottak végre.
- Az alkalmazás nem figyeli meg a hálózati felületeken történő fájlmodosításokat (például, ha a fájl egy megosztott mappában található, a folyamat pedig egy másik, távoli számítógépről indul el).

Tűzfal

- 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.
- Az alkalmazás 11.0.0 és 11.0.1 verzióiban a meghatározott MAC-címek hibásan vannak alkalmazva. A 11.0.0, 11.0.1 és 11.1.0 vagy újabb verziók MAC-címének beállításai nem kompatibilisek. Miután az alkalmazást vagy a bővítményt ezekről a verziókról a 11.1.0 vagy újabb verzióra frissítette, ellenőriznie kell és újra kell konfigurálnia a Tűzfal szabályokban megadott MAC-címeket.
- Az alkalmazás 11.1.1 és 11.2.0 verziókról 11.8.0 verzióra történő frissítésekor a következő Tűzfal szabályok engedélyeinek jogosultságai nem lesz áttelepítve:
 - Kérések a DNS kiszolgáló számára TCP protokollon keresztül.
 - Kérések a DNS kiszolgáló számára UDP protokollon keresztül.
 - Bármiféle hálózati tevékenység.
 - ICMP cél elérhetetlen bejövő válaszok.
 - Bejövő ICMP adatfolyam.
- 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 paramétercímét 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 beállításában. 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 **Rule type** oszloppal. Hálózati csomagszabály indításakor az **Alkalmazásnév** oszlop értéke üres marad.

[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.

[Alkalmazásfelügyelő](#)

- Csak a 104 MB alatti ZIP-archívumok támogatottak a Kaspersky Security Center Web Console alkalmazásfelügyeleti szabályainak kezelésekor. Más formátumú archívumok, például RAR vagy 7z, nem támogatottak. 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.
- Amikor a progresszív webalkalmazásokat (PWA) blokkolja az Alkalmazásfelügyelő összetevő, akkor az appManifest.xml jelenik meg blokkolt alkalmazásként a jelentésben.
- A szabványos Jegyzetömb 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 Jegyzetömb a következő mappákban található:
 - C:\Windows\notepad.exe
 - C:\Windows\System32\notepad.exe
 - C:\Windows\SysWOW64\notepad.exe

Amikor a Jegyzetömböt hozzáadja egy alkalmazásfelügyeleti szabályhoz, megadhatja például az alkalmazás nevét és a fájl kivonatát a futó alkalmazás tulajdonságaiból.

Eszközfelügyelő

- 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.
- 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.

Webfelügyelő

- Az OGV és WEBM formátumok nem támogatottak.
- Az RTMP protokoll nem támogatott.

Adaptív Anomáiafelügyelő

- 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 Anomáiafelügyeleti szabályok jelentés nem hozható létre](#), ha a minta akár egy olyan eseményt is tartalmaz, amelynek neve meghaladja a 260 karaktert.
- Az Adaptív Anomáiafelügyelő 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 beállításaiiban](#). Kizárást az [Adaptív Anomáiafelügyelő szabályok kiváltásáról szóló jelentésében](#) is hozzáadhat.

Meghajtó titkosítása (FDE)

- Az alkalmazás telepítése után újra kell indítani 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 merevlemez.
- 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 titkosítani a merevlemez.
- 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.
- Az operációs rendszer biztonsági másolatból titkosított GPT-eszközre történő visszaállításával kapcsolatos részletekért keresse fel a [Terméktámogatás tudásbázisát](#).
- Több letöltési ügynök nem lehet egyszerre egy titkosított számítógépen.
- 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 merevlemez.
- 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 < tartomány > / < Windows - fióknév > 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 / Ivanov számítógép 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 merevlemez 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, akkor 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](#) ².

[Fájl szintű titkosítás \(FLE\)](#) ²

- A fájlok és mappák titkosítását a Microsoft Windows Embedded család operációs rendszerei nem támogatják.
- Az alkalmazás telepítése után a fájlok és mappák titkosításának megfelelő működéséhez újra kell indítani az operációs rendszert.
- Ha egy titkosított fájl egy elérhető titkosítási funkciókkal rendelkező számítógépen van tárolva, és a fájl 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 Systemmel 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.
- 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 Fájl szintű 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.

- Fájl titkosítás 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 fájl műveleteket egy harmadik féltől származó alkalmazás végez. Például a fájl másolást a fájlkezelő végzi, nem maga az alkalmazás. Így 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 törölődnek.
- Az offline fájlok Ügyféloldali gyorsítótárazás (CSC) használatával való szinkronizálása nem 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. Az Ügyféloldali gyorsítótárazás (CSC) támogatásáról a titkosítás használatakor lásd a [Terméktámogatási tudásbázist](#).
- [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 fájlserverként 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 fájl szintű 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 természetesemények 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 fájlra a hálózaton, és ehhez fájl-memória leképezési módszerrel működő alkalmazást (például WordPad vagy FAR) és nagy fájlokhoz való használatra tervezett alkalmazásokat (például Notepad ++) használ, 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 találhatóak, 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 fájl szintű titkosítási összetevő telepítésekor a felhasználók és csoportok kezelése WSL módban (Windows rendszer Linux számára) nem működik.
- A fájl szintű titkosító összetevő telepítésekor a fájlok átnevezéséhez és törléséhez a POSIX (hordozható operációs rendszerfelület) 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 elvesz az adat. Az adatvesztés elkerülése érdekében [zárja ki az ideiglenes fájlokat a titkosítási szabályok hatóköréből](#).
- A 11.0.1-es vagy korábbi verziójú Kaspersky Endpoint Security for Windows frissítését követően győződjön meg arról, hogy a Hálózati ügynök fut, hogy a számítógép újraindítása után hozzáférhessen a titkosított fájlokhoz. A Hálózati ügynök késleltetve indul, ezért az operációs rendszer betöltődése után nem fog tudni azonnal hozzáférni a titkosított fájlokhoz. A számítógép következő indítása után nem kell várnia a Hálózati ügynök elindulására.

[Egyéb korlátozások](#)

- 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 működőképés állapotúra visszaállítani, miután frissítette az antivírus adatbázisokat vagy alkalmazta az alkalmazásmodul-frissítéseket.
- Előfordulhat, hogy a [megbízható listához hozzáadott](#) webcímek helytelenül lesznek feldolgozva.
- 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.
- Rendszerfigyelő. A folyamatokkal kapcsolatos összes információ nem jelenik meg.
- 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.
- A levelek [Microsoft Outlook levelezés védelem kiterjesztéssel](#) történő vizsgálatkor javasoljuk, hogy használja a gyorsítótárazott Exchange módot (Gyorsítótárazott Exchange mód használata lehetőség).
- A [Vírusvizsgálat feladat](#) nem támogatja a Microsoft Outlook 64 bites verzióját. Ez azt jelenti, hogy a Kaspersky Endpoint Security akkor sem ellenőrzi a 64 bites verziójú MS Outlook-fájlokat (PST és OST), ha az [e-mailek a vizsgálat hatókörébe tartoznak](#).
- A Kaspersky Security Center alkalmazásban, amikor a globális Kaspersky Security Network használatáról a privát Kaspersky Security Network 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.
- 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 a termékjelentésben és a Kaspersky Security Center jelentésben.
- A [Végponti szenzor](#) összetevő nem telepíthető Microsoft Windows Server 2008 rendszerben.
- 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 Csökkentett módban nem működik.
- Annak érdekében, hogy a Kaspersky Endpoint Security for Windows 11.5.0-s és 11.6.0-s verziója megfelelően működjön a Cisco AnyConnect szoftverrel, telepítenie kell a megfelelőségi modul 4.3.183.2048 vagy újabb verzióját. További tudnivalók a Cisco Identity Services Engine megoldással való kompatibilitásról a [Cisco dokumentációjában](#) található.
- 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 KSN elérhetőség ellenőrzése feladat már nem támogatott.

- „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.
- Az alkalmazás 11.1.0 verzióról 11.8.0 verzióra történő frissítésekor az AMSI védelem beállításai visszaállnak az alapértelmezett értékekre.
- Ha szoftverkorlátozó házirendeket (SRP) használ, előfordulhat, hogy a számítógép betöltése nem sikerül (fekete képernyő). Javasoljuk, hogy változtassa meg az SRP beállításait az alábbiak szerint: a **Szoftverkorlátozások alkalmazása a következő objektumokra** paraméternél állítsa be az **A függvénytárakon (pl. DLL-ek) kívül minden szoftverfájltra** értéket, és adja hozzá az alkalmazásfájlok elérési útjaihoz (C:\Program Files\Common Files\Kaspersky Lab és C:\Program Files\Kaspersky Lab) a **Korlátlan** biztonsági szintet használó szabályokat. Az SRP használatának részleteiért olvassa el a [Microsoft dokumentációját](#).
- Ha a számítógép a Windows csoportházirend-objektum alatt egy tartományhoz tartozik, és a DriverLoadPolicy paramétere 8-ra van állítva (csak Jó), a telepített Kaspersky Endpoint Security-vel rendelkező számítógép újraindítása kékképernyős összeomlást okoz. A hiba megelőzése érdekében a csoportházirendben a korai indítású kártevőirtó paramétereit 1-re kell állítani (Jó és ismeretlen). A korai indítású kártevőirtó beállításai a házirendben találhatóak: **Számítógép konfigurációja** → **Felügyeleti sablonok** → **Rendszer** → **Korai indítású kártevőirtó**.
- Az Outlook bővítmény beállításainak kezelése a Rest API-n keresztül nem támogatott.
- Egy adott felhasználó feladatfuttatási beállításai konfigurációs fájlal 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 [Fájl karanténba helyezése](#) feladat miatt nem vizsgálhat karanténba helyezett objektumot.
- A Kaspersky Endpoint Security nem futtatja az [IOC vizsgálat](#) 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 vizsgálat* feladatokhoz a hálózati meghajtókon. Például \\server\shared_folder.

- 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.
- Ha az *IOC vizsgálat* feladat futtatása során biztonsági sérülési indikátort észlel, az alkalmazás csak a Filetem kifejezésre vonatkozóan helyez egy fájlt karanténba. Fájl karanténba helyezése más kifejezések esetén nem támogatott.
- A 4 MB-nál nagyobb alternatív adatfolyam (ADS) nem helyezhető karanténba. A Kaspersky Endpoint Security a felhasználó értesítése nélkül mellőzi az ilyen alternatív adatfolyamokat.
- Az értesítések részleteinek kezeléséhez a Kaspersky Endpoint Security for Windows 11.7.0 vagy újabb verziójú webes bővítményére van szükség. Az értesítések adataira az [Endpoint Detection and Response](#) megoldásnak (EDR Optimum és EDR Expert) van szüksége. Az észlelés részletei a Kaspersky Security Center Web Console-on és a Kaspersky Security Center Cloud Console-on érhetők el.
- 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).

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 csoportrendszerabályokat 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.

Feladat

A Kaspersky alkalmazásában feladatként végrehajtott funkciók, például: Valós idejű fájlvédelem, Teljes vizsgálat és Adatbázisfrissítés.

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 fájlknál 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.

Hálózati Ügynök

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.

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.

IOC

A 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.

Licenctanúsítvány

Olyan dokumentum, amelyet a Kaspersky a felhasználónak a kulcsfájllal, illetve aktiváló kóddal együtt ad át. A felhasználó részére adott licenccről tartalmaz információkat.

Maszk

Helyettesítő karakterekkel megadott fájlnev 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a `Mappa` nevű mappában és az almappáiban található. 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 `Fo1der` nevű mappában lévő összes olyan fájl elérési útvonalát, aminek TXT-kiterjesztése van és három karakterből áll.

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.

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.

További kulcs

Az a kulcs, amely tanúsítja az alkalmazás használatára vonatkozó jogot, de jelenleg nincs használatban.

Trusted Platform Module (TPM)

Egy biztonsághoz kapcsolódó alapvető funkciók nyújtására (például titkosítási kulcsok tárolására) szolgáló mikrocsip. A Trusted Platform Module általában a számítógép alaplapiján 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 [házi rendet](#), 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 fájlrendszere fertőzéseinek megelőzését. Alapértelmezés szerint a „Fájl védelem” összetevő folyamatosan jelen van a számítógép memóriájában. Az összetevő vizsgálja a fájlokat a számítógép összes meghajtóján, valamint a csatlakoztatott meghajtókon. 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 megkísérel elérni egy olyan fájlt, amelynek tartalmát a OneDrive-felhő tárolja, a Kaspersky Endpoint Security letölti és megvizsgálja a fájl tartalmát.

A Fájl védelem összetevő beállításai

Paraméter	Leírás
Biztonsági szint <i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i>	<p>A Fájl védelemhez a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezek az alkalmazásban tárolt beállításcsoportokat <i>biztonsági szinteknek</i> nevezzük:</p> <ul style="list-style-type: none">• 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 fájltypust 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.
Fájltypusok	Minden fájl. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security kivétel nélkül minden fájlt megvizsgál (formátumtól és kiterjesztéstől függetlenül).

<p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	<p>Formátum alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. Mielőtt egy fájlban megvizsgálná, hogy van-e rosszindulatú kód, elemzi a belső fejléceket a fájlformátum megállapítása céljából (például: .txt, .doc vagy .exe). A vizsgálat bizonyos fájlkiterjesztésekkel rendelkező fájlokat is keres.</p> <p>Kiterjesztés alapján vizsgált fájlok. Ha ez a beállítás van kiválasztva, a Kaspersky Endpoint Security csak a megfertőzhető fájlokat vizsgálja meg. A fájlformátumot a fájl kiterjesztése alapján állapítja meg.</p>
<p>Vizsgálat hatóköre</p>	<p>Azon objektumokat tartalmazza, amelyeket megvizsgál a Fájl védelem összetevő. A vizsgálati objektum lehet merevlemez, cserélhető meghajtó, hálózati meghajtó, mappa, fájl vagy több fájl meghatározó maszk.</p> <p>Alapértelmezés szerint a Fájl védelem összetevő minden, a merevlemezen, a hálózati meghajtókon vagy cserélhető meghajtón elindított fájl megvizsgál. Az ilyen objektumok védelmi hatókörét nem lehet módosítani vagy törölni. Kizárhat objektumot (például cserélhető meghajtót) a vizsgálat alól.</p>
<p>Gépi tanulás és aláírás-elemzés</p> <p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	<p>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.</p> <p>A Kaspersky szakértőinek ajánlásának megfelelően a gépi tanulás és az aláírások elemzése mindig be van kapcsolva.</p>
<p>Heurisztikus elemzés</p> <p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	<p>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.</p> <p>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 alaposága, az operációs rendszer erőforrásainak terhelése, valamint a vizsgálatához szükséges idő közötti egyensúlyt.</p>
<p>Művelet fenyegetés észlelésekor</p>	<p>Vírusmentesítés; törlés, ha a vírusmentesítés nem sikerül. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájl vírusmentesíteni. Ha a vírusmentesítés nem sikerül, a Kaspersky Endpoint Security törli a fájlokat.</p> <p>Vírusmentesítés; blokkolás, ha a vírusmentesítés nem sikerül. Ennek a lehetőségnek a kiválasztása esetén a Kaspersky Endpoint Security automatikusan megpróbálja az összes észlelt fertőzött fájl vírusmentesíteni. Ha a vírusmentesítés nem lehetséges, a Kaspersky Endpoint Security információkat ad hozzá a fertőzött fájlokról az aktív fenyegetések listájához.</p> <p>Blokkolás. Ennek a lehetőségnek a kiválasztása esetén a Fájl védelem összetevő automatikusan blokkolja az összes észlelt fertőzött fájl, anélkül, hogy vírusmentesíteni próbálná őket.</p>

	<p>Mielőtt megpróbál vírusmentesíteni vagy törölni egy fertőzött fájlt, a Kaspersky Endpoint Security létrehozza a fájl egy biztonsági másolatát arra az esetre, ha vissza kell állítani a fájlt, vagy a jövőben az majd vírusmentesíthető lesz.</p>
Csak az 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 tömörített formátumok vizsgálata. A Kaspersky Endpoint Security kiterjesztés és formátum szerint is vizsgálja a tömörített fájlokat.
Terjesztési csomagok vizsgálata	Ez a jelölőnégyzet engedélyezi/letiltja a harmadik féltől származó 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.
Ne csomagoljon ki nagy összetett fájlokat	<p>Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem vizsgálja az összetett fájlokat, ha méretük meghaladja a megadott értéket.</p> <p>Ha a négyzet nincs bejelölve, a Kaspersky Endpoint Security mindenfajta méretű összetett fájlt megvizsgál.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>A Kaspersky Endpoint Security megvizsgálja az archívumokból kibontott nagyobb fájlokat függetlenül attól, hogy be van-e jelölve a jelölőnégyzet.</p> </div>
Összetett fájlok kicsomagolása a háttérben	<p>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.</p> <p>A Kaspersky Endpoint Security csak e fájlok kicsomagolása és vizsgálata után biztosít hozzáférést az ennél kisebb méretű összetett fájlokhoz.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security csak akkor biztosít hozzáférést bármilyen méretű fájlhoz, ha kicsomagolta és átvizsgálta a fájlokat.</p>
Vizsgálat módja <i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A Kaspersky Endpoint Security a felhasználó, az operációs rendszer vagy a felhasználó fiókja alatt futó alkalmazások által elért fájlokat vizsgálja.</p> </div> <p>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 fájl felülíró közttes műveletek nem váltanak ki vizsgálatot.</p> <p>Hozzáféréskor és módosításkor. Ebben a módban a Fájl védelem megnyitási és módosítási kísérletek esetén mindig megvizsgálja az objektumokat.</p>

	<p>Hozzáféréskor. Ebben a módban a Fájlf védelem az objektumokat csak a megnyitási kísérletek esetén vizsgálja meg.</p> <p>Végrehajtáskor. Ebben a módban a Fájlf védelem az objektumokat csak a futtatási kísérletek esetén vizsgálja meg.</p>
<p>iSwift technológia</p> <p><i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i></p>	<p>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.</p>
<p>iChecker technológia</p> <p><i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i></p>	<p>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).</p>
<p>Fájlf védelem szüneteltetése</p> <p><i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i></p>	<p>Ez ideiglenesen és automatikusan szünetelteti a Fájlf védelem működését a megadott időpontban, vagy a megadott alkalmazásokkal való munka során.</p>

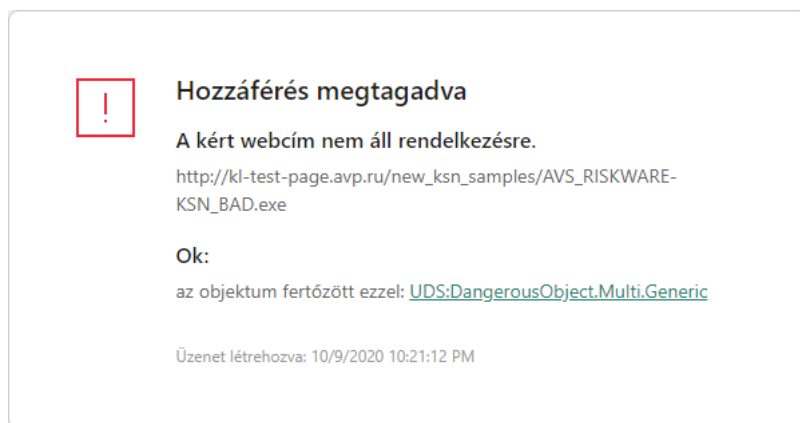
Web védelem

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. Ön [megadhat portokat, amelyeket a Kaspersky Endpoint Security megfigyel](#), vagy kiválaszthatja az összes portot.

A HTTPS forgalom megfigyeléséhez [engedélyeznie kell a titkosított kapcsolatok vizsgálatát](#).

Ha a felhasználó rosszindulatú vagy adathalász weboldalt próbál megnyitni, a Kaspersky Endpoint Security letiltja a hozzáférést és figyelmeztetést jelenít meg (lásd az alábbi ábrát).



A weboldal hozzáféréseinek megtagadásáról szóló üzenet

A Web védelem összetevő beállításai

Paraméter	Leírás
<p>Biztonsági szint</p> <p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	<p>A Web védelemhez a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezek az alkalmazásban tárolt beállítás csoportokat <i>biztonsági szinteknek</i> nevezzük:</p> <ul style="list-style-type: none"> • Magas. Az a biztonsági szint, amely mellett a Web védelem a számítógépre HTTP és FTP protokollon 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. A Kaspersky Endpoint Security teljesítménye és a webes forgalom biztonsága közti optimális egyensúlyt nyújtó 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 közepes vizsgálat szinten üzemel.
<p>Művelet fenygetés észlelésekor</p>	<p>Letöltés blokkolása. 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.</p> <p>Értesítés. 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.</p>
<p>A webcím ellenőrzése a rosszindulatú webcímek adatbázisában</p>	<p>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.</p>

<p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	
<p>Heurisztikus elemzés használata</p> <p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	<p>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.</p> <p>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 alaposága, az operációs rendszer erőforrásainak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.</p>
<p>A webcím ellenőrzése az adathalász webcímek adatbázisában</p> <p>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</p>	<p>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.</p>
<p>Ne vizsgálja a megbízható webcímekről érkező webes forgalmat</p>	<p>Ha a jelölőnégyzet 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.</p>

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

- Microsoft Outlook Express
- Windows Mail

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 támogatja az Outlook 2010, 2013, 2016 és 2019 alkalmazásokkal történő műveleteket.

A „Levelezés védelem” összetevő nem vizsgálja az üzeneteket, ha a levelezési ügyfélprogram böngészőben van megnyitva.

Ha egy mellékletben rosszindulatú fájlt észlel, a Kaspersky Endpoint Security módosítja az üzenet tárgyát a következő módon: [Az üzenet figyelmet kíván a feldolgozás során] <üzenet tárgya> vagy [Üzenet fel lett dolgozva] <üzenet tárgya>.

A Levelezés védelem összetevő beállításai

Paraméter	Leírás
Biztonsági szint <i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i>	<p>A Levelezés védelemhez a Kaspersky Endpoint Security beállítások különböző csoportjait alkalmazza. Ezek az alkalmazásban tárolt beállításcsoportokat <i>biztonsági szinteknek</i> nevezzük:</p> <ul style="list-style-type: none"> • 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 hálózattól. • Ajánlott. A Kaspersky Endpoint Security teljesítménye és az e-mail-biztonság közti optimális egyensúlyt nyújtó 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	<p>Vírusmentesítés, törlés, ha a vírusmentesítés nem sikerül. Ha fertőzött objektumot észlel akár bejövő, akár kimenő üzenetben, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security törli a fertőzött objektumot. A Kaspersky Endpoint Security a végrehajtott művelettel kapcsolatosan információt fűz hozzá az üzenet tárgysorához: [Üzenet fel lett dolgozva] <üzenet tárgysora>.</p>

	<p>Vírusmentesítés, blokkolás, ha a vírusmentesítés nem sikerül. Ha fertőzött objektumot észlel valamely bejövő üzenetben, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. A felhasználó biztonságos melléklettel tudja elérni az üzenetet. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security figyelmeztetést fűz hozzá az üzenet tárgyához: [Az üzenet figyelmet kíván a feldolgozás során] <az üzenet tárgya>. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, a Kaspersky Endpoint Security megkísérli vírusmentesíteni az észlelt objektumot. Ha az objektumot nem lehet vírusmentesíteni, a Kaspersky Endpoint Security letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.</p> <p>Blokkolás. Ha fertőzött objektumot észlel valamely bejövő üzenetben, a Kaspersky Endpoint Security figyelmeztetést fűz hozzá az üzenet tárgysorához: [Az üzenet figyelmet kíván a feldolgozás során] <üzenet tárgya>. A felhasználó az eredeti melléklettel férhet hozzá az üzenethez. Ha fertőzött objektumot észlel valamely kimenő üzenetben, a Kaspersky Endpoint Security letiltja az üzenet továbbítását, a levelezőprogram pedig hibaüzenetet jelenít meg.</p>
<p>Védelem hatóköre</p> <p><i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i></p>	<p>A <i>védelem hatóköre</i> magában foglalja azokat az objektumokat, amelyeket az összetevő a futtatáskor ellenőriz: bejövő és kimenő üzenetek vagy csak bejövő üzenetek.</p> <p>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.</p>
<p>POP3-, SMTP-, NNTP- és IMAP-forgalom vizsgálata</p>	<p>Ez a jelölőnégyzet engedélyezi/letiltja az olyan forgalom Levelezés védelem összetevő általi vizsgálatát, amelynek átvitele POP3, SMTP, NNTP és IMAP protokollal történik.</p>
<p>Microsoft Outlook-bővítmény csatlakoztatása</p>	<p>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.</p> <p>Ha az e-mailek vizsgálata a Microsoft Outlook bővítményével történik, akkor javasoljuk a Gyorsítótárazott Exchange-mód használatát. A gyorsítótáras Exchange móddal kapcsolatban további információ, valamint a használatára vonatkozó ajánlások a Microsoft Tudásbázisban találhatóak.</p>
<p>Heurisztikus elemzés</p> <p><i>(csak az Adminisztrációs Konzolon (MMC) és a Kaspersky Endpoint Security felületén érhető el)</i></p>	<p>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.</p> <p>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 erőforrásainak terhelése, valamint a vizsgálathoz szükséges idő közötti egyensúlyt.</p>
<p>Csatolt archívumok vizsgálata</p>	<p>ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb tömörített formátumok vizsgálata.</p>

	<p>Ha a vizsgálat során a Kaspersky Endpoint Security 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 kicsomagolásra kerül. 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.</p>
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.
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	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A mellékletszűrő nincs alkalmazva a kimenő e-mail-üzenetekre.</p> </div> <p>Szűrés letiltása. Ha ez az opció van kiválasztva, a Levelezés védelem összetevő nem szűri az e-mail üzenetekhez csatolt fájlokat.</p> <p>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.</p> <p>Kiválasztott típusú mellékletek törlése. Ha ez az opció van kiválasztva, a Levelezés védelem összetevő törli az e-mail üzenetekből a megadott típusú mellékelt fájlokat.</p> <p>A fájlmaszkok listájában megadhatja az e-mail üzenetekben átnevezni vagy törölni kívánt csatolt fájlok típusait.</p>

Hálózati védelem

A „Hálózati védelem” összetevő a hálózati támadásokra jellemző bejövő hálózati forgalmat vizsgálja. Ha a Kaspersky Endpoint Security hálózati támadási kísérletet észlel a felhasználó számítógépén, blokkolja a hálózati kapcsolatot a támadást indító számítógép irányában. A Kaspersky Endpoint Security adatbázisai 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
-----------	--------

<p>A portkeresés és hálózati elárasztás támadásként történő kezelése</p>	<p>A <i>hálózati elárasztás</i> 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.</p> <p>A <i>portkereséses támadás</i> 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.</p> <p>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.</p> <p>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.</p>
<p>A támadó számítógép hozzáadása a blokkolt számítógépek listájához N perc</p>	<p>Ha a jelölőnégyzet be van jelölve, 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 32 768 perc.</p> <p>A tiltólistát a Hálózatfigyelő eszköz ablakában tekintheti meg.</p> <div data-bbox="376 1059 1493 1182" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>A Kaspersky Endpoint Security törli a tiltólistát az alkalmazás újraindításakor és a Hálózati védelem beállításainak megváltoztatásakor.</p> </div>
<p>Kizárások</p>	<p>Ez a lista azokat az IP-címeket tartalmazza, amelyeken a Hálózati védelem a hálózati támadásokat nem blokkolja.</p> <p>Az alkalmazás nem naplózza az olyan IP címekről érkező hálózati támadások információit, amik a kizárások listájában szerepelnek.</p>
<p>MAC-cím hamisítása elleni védelem</p>	<p>A <i>MAC-hamisítási támadás</i> 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.</p>

Firewall

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 a következő módon működnek: az alkalmazásokhoz tartozó hálózati szabály a hálózati állapot alapján foglalja magában a hozzáférési szabályokat: *nyilvános, helyi vagy megbízható*. 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 kapcsolatok állapota

A Tűzfal lehetővé teszi Önnek a hálózat tevékenység felügyeletét a hálózati kapcsolat állapotától függően. A Kaspersky Endpoint Security a számítógép operációs rendszerétől kapja meg a hálózati kapcsolatok állapotát. Az operációs rendszerben a hálózati kapcsolat állapotát a felhasználó szabhatja meg a kapcsolat létrehozásakor. Lehetősége van [megváltoztatni a hálózati kapcsolat állapotát a Kaspersky Endpoint Security beállításai között](#). A Tűzfal a hálózati tevékenység nyomon követését a Kaspersky Endpoint Security beállításai alapján végzi, nem az operációs rendszer beállításai szerint.

A hálózati kapcsolat az alábbi állapottípusok egyikével rendelkezhet:

- **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 fájlljaihoz 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* állapotot oszt ki. Az internet állapota nem módosítható.

- **Helyi hálózat.** Hálózat olyan felhasználóknak, akik korlátozott hozzáféréssel rendelkeznek a jelen számítógép fájlljaihoz 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.

Paraméter	Leírás
Hálózati csomagszabályok	<p>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.</p> <p>A táblázatban a Kaspersky által a Microsoft Windows operációs rendszereket futtató számítógépek hálózati forgalmának optimális védelme érdekében ajánlott előre beállított hálózati csomagszabályok szerepelnek.</p> <p>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.</p> <p>A hálózati csomagszabályok prioritása magasabb, mint az alkalmazások hálózati szabályaié.</p>
Hálózati kapcsolatok	<p>Ebben a táblázatban információk találhatóak a Tűzfal által a számítógépen észlelt hálózati kapcsolatokról.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Alapértelmezés szerint az internet <i>Nyilvános hálózat</i> állapotot kap. Az internet állapota nem módosítható.</p> </div>
Hálózati szabályok	<p>Függelék</p> <p>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.</p> <p>Lehetősége van kiválasztani egy alkalmazást a számítógépeken telepített összes alkalmazás egyszerű felsorolásából valamely rendszabály alapján, majd felvenni az alkalmazást egy megbízható csoportba.</p> <p>Hálózati szabályok</p> <p>Valamely megbízható csoportba tartozó alkalmazások hálózati szabályainak táblázata. Ezen szabályoknak megfelelően a Tűzfal szabályozza az alkalmazások hálózati tevékenységét.</p> <p>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.</p>

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.

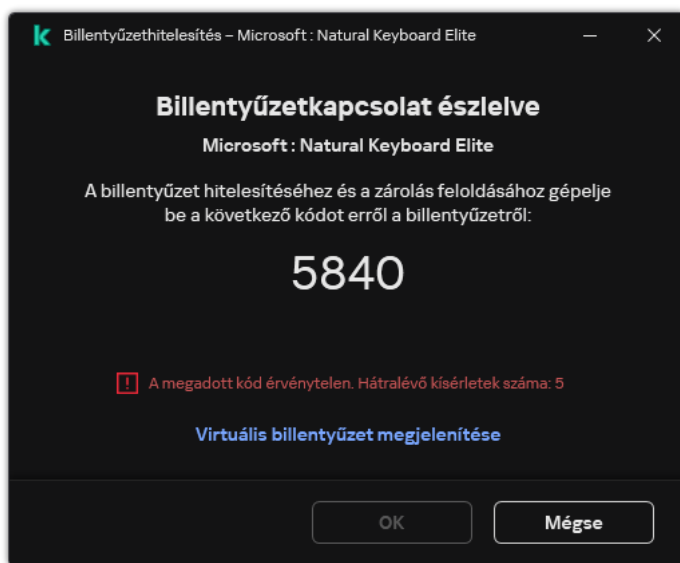
A kód megfelelő beírása esetén az alkalmazás menti az azonosító paramétereket – a billentyűzet VID/PID azonosítóját és a csatlakoztatás portszámát – a hitelesített billentyűzetek listájára. A billentyűzethitelesítést a billentyűzet ismételt csatlakoztatásakor és az operációs rendszer újraindításakor nem kell újra elvégezni.

Ha a hitelesített billentyűzetet a számítógép egy másik USB portjához csatlakoztatja, az alkalmazás ismét megjeleníti a billentyűzet 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 alkalmazás-összetevőket](#) az alkalmazás telepítését után.



Billentyűzethitelesítés

A BadUSB Védelem összetevő beállításai

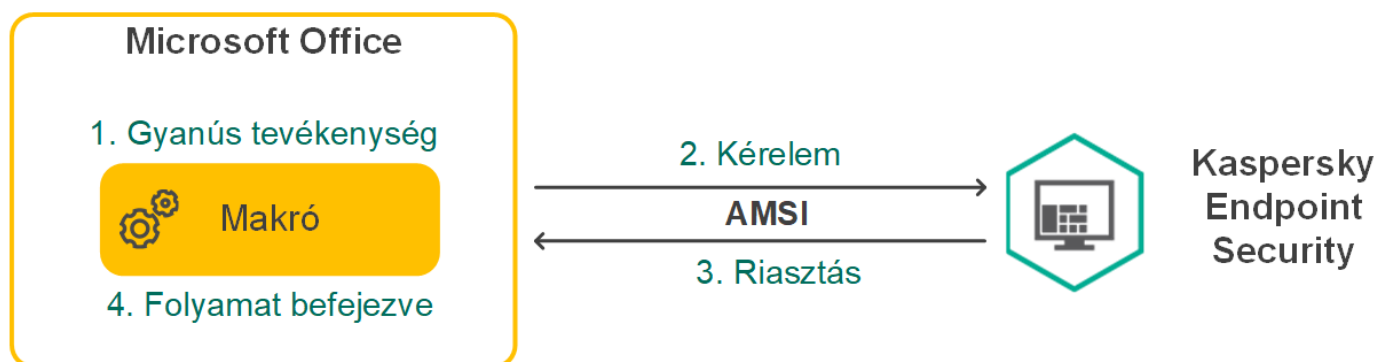
Paraméter	Leírás
Virtuális billentyűzet használatának tiltása az USB-eszközök hitelesítésére	Ha a jelölőnégyzet be van jelölve, az alkalmazás blokkolja a Képernyőn megjelenő billentyűzet használatát olyan USB eszköz hitelesítésénél, amelyen nem lehet megadni hitelesítési kódot
Az USB-készülék-hitelesítési	Automatikusan blokkolja az USB-eszközt, ha a megadott számú alkalommal helytelenül adják meg a hitelesítési kódot. Az érvényes értékek 1 és 10 között vannak.

kísérletek maximális száma	Például, ha 5 kísérletet engedélyez a hitelesítési kód megadására, az USB-eszköz blokkolva lesz az ötödik sikertelen kísérlet után. A Kaspersky Endpoint Security megjeleníti az USB-eszköz blokkolásának időtartamát. Ezen időtartam letelte után 5 alkalommal kísérrelheti meg beírni a hitelesítési kódot.
A próbálkozások maximális számának időkorlátja	Az USB-eszköz blokkolásának időtartama a hitelesítési kód megadott számú sikertelen kísérlet utáni beírásakor. 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 hajthat végre rosszindulatú tevékenységeket (például bezárásokat).



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;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Paraméter	Leírás
Archívumok vizsgálata	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE és egyéb tömörített formátumok vizsgálata.
Terjesztési csomagok vizsgálata	Ez a jelölőnégyzet engedélyezi/letiltja a harmadik féltől származó 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.
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 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 kihasználását megelőző összetevő beállításai

Paraméter	Leírás
Sebezhetőség kihasználásának észlelésekor	Művelet blokkolása. 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. Értesítés. 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.

Viselkedéselemzés

A Viselkedéselemzés összetevő a számítógépen futó alkalmazások műveleteiről fogad adatokat, és a teljesítmény növelése érdekében átadja ezeket az információkat a többi védelmem összetevőinek. A Viselkedéselemzés 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 viselkedésfolyam-aláíráson alapuló funkciói a számítógép számára proaktív védelmet nyújtanak.

A viselkedéselemzés összetevő beállításai

Paraméter	Leírás
<p>Rosszindulatú programtevékenység észlelése esetén</p>	<ul style="list-style-type: none"> • Fájl törlése. 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. • Alkalmazás leállítása. Ha ez az opció van kiválasztva, akkor rosszindulatú tevékenység észlelésekor a Kaspersky Endpoint Security az érintett alkalmazást bezárja. • Értesítés. 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 hozzá az aktív fenyegetések listájához.
<p>A megosztott mappák külső forrásból történő titkosítás elleni védelmének engedélyezése</p>	<p>Ha a kapcsológomb be van kapcsolva, a Kaspersky Endpoint Security elemzi a megosztott mappákban lévő tevékenységet. Ha ez a tevékenység megegyezik a külső titkosításra jellemző viselkedésfolyamat-aláírással, a Kaspersky Endpoint Security végrehajtja a kiválasztott műveletet.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>A Kaspersky Endpoint Security csak azoknak a fájloknak a külső titkosítását akadályozza meg, amelyek NTFS fájlrendszert tartalmazó adathordozón található, és nincsenek EFS rendszerrel titkosítva.</p> </div> <ul style="list-style-type: none"> • Értesítés. Ha ez az opció ki van választva, akkor megosztott mappák fájjai módosítási kísérletének észlelésekor a Kaspersky Endpoint Security információkat ad hozzá az aktív fenyegetések listájához a megosztott mappák fájljainak módosítási kísérletéről. • Kapcsolódás blokkolása N percig. Ha ez az opció be van jelölve, amikor a Kaspersky Endpoint Security a megosztott mappákban lévő fájlok módosítási kísérletét észleli, akkor az alkalmazás blokkolja a fájlok módosítani próbáló számítógép hálózati tevékenységét, és biztonsági másolatot készít a módosított fájlokról. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Ha a Kármentesítő motor összetevő engedélyezve van, és a Kapcsolat blokkolása N percig lehetőség ki van választva, a Kaspersky Endpoint Security visszaállítja a módosított fájlokat a biztonsági mentésből.</p> </div>
<p>Kizárások</p>	<p>Azon külső számítógépek listája, amelyekről a megosztott mappák titkosításának kísérleteit a rendszer nem kíséri figyelemmel.</p>

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](#).

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](#) összetevő 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 [Behatólásmegelőző 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 meglévő alkalmazásjogot. Ha az alkalmazás módosult, a Kaspersky Endpoint Security ugyanúgy végigelemzi, mintha az első elindítására kerülne sor.

A Behatólásmegelőző rendszer összetevő beállításai

Paraméter	Leírás
Alkalmazásjogok	<p>Függelék</p> <p>A „Behatólásmegelőző 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.</p> <p>Lehetősége van kiválasztani egy alkalmazást a számítógépeken telepített összes alkalmazás egyszerű felsorolásából valamely rendszabály alapján, majd felvenni az alkalmazást egy megbízható csoportba.</p> <p>Az alkalmazások hozzáférési jogai a következő táblázatokban szerepelnek:</p> <ul style="list-style-type: none"> • Fájlok és rendszerleíró adatbázis. Ebben a táblázatban szerepelnek egy megbízható csoportba tartozó alkalmazások hozzáférési jogosultságai az operációs rendszer erőforrásaira és személyes adatokra vonatkozóan. • Jogok. Ebben a táblázatban szerepelnek egy megbízható csoportba tartozó alkalmazások hozzáférési jogosultságai az operációs rendszer folyamataira és erőforrásaira 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	<p>Name</p> <p>A táblázat kategorizált számítógépes erőforrásokat tartalmaz. A Behatólásmegelőző rendszer figyeli a többi alkalmazás hozzáférési próbálkozásait a táblázatban található erőforrásokhoz.</p> <p>Az erőforrás lehet egy beállításkategória, fájl, mappa vagy beállításkulcs.</p> <p>Függelék</p> <p>A „Behatólásmegelőző rendszer” összetevő által figyelt alkalmazások táblázata a kijelölt erőforráshoz kapcsolódóan. Az alkalmazások megbízhatósági csoportokba vannak besorolva. A megbízhatósági csoport határozza meg azokat a jogokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére használ.</p>

<p>A Kaspersky Endpoint Security for Windows működésének megkezdése előtt elindított alkalmazások megbízhatósági csoportja</p>	<p>Megbízható csoport, amelybe a Kaspersky Endpoint Security felveszi azokat az alkalmazásokat, amelyek indítására a Kaspersky Endpoint Security indítása előtt kerül sor.</p>
<p>Jogok frissítése a korábban ismeretlen alkalmazásokhoz a KSN-adatbázisokból</p>	<p>Ha a jelölőnégyzet be van jelölve, a Behatolásmegelőző rendszer frissíti a korábban ismeretlen jogokat a Kaspersky Security Network adatbázisai segítségével.</p>
<p>Megbízik a digitálisan aláírt alkalmazásokban</p>	<p>Ha ez a jelölőnégyzet be van jelölve, a Behatolásmegelőző rendszer összetevő a megbízható gyártók digitális aláírásaival rendelkező alkalmazásokat a Megbízható csoportba helyezi.</p> <p><i>A megbízható gyártók olyan szoftvergyártók, amelyekben a Kaspersky megbízik. A gyártói tanúsítványt manuálisan is hozzáadhatja a megbízható tanúsítványtárolóhoz.</i></p> <p>Ha a jelölőnégyzet nincs bejelölve, a Behatolásmegelőző rendszer összetevő nem tekinti megbízhatónak az ilyen alkalmazásokat, és más paraméterek alapján dönti el megbízhatósági csoportjukat.</p>
<p>Azon alkalmazások szabályainak törlése, amelyek inaktívak már több mint ennyi ideje (nap, 1–90.)</p>	<p>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:</p> <ul style="list-style-type: none"> • Ön manuálisan is beteheti az alkalmazást egy megbízhatósági csoportba, és konfigurálhatja a hozzáférési jogait. • Az alkalmazás nem indult el a megadott időtartamon belül. <p>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.</p> <p>Ha legközelebb elindítja az alkalmazást, a Kaspersky Endpoint Security úgy fogja elemezni azt, mintha legelőször indítaná el.</p>
<p>Olyan alkalmazások megbízhatósági csoportja, amelyek nem vehetők fel meglévő csoportokba</p>	<p>Az ezen a legördülő listán lévő elemek szabják meg, melyik megbízhatósági csoportba osztja be a Kaspersky Endpoint Security az ismeretlen alkalmazásokat.</p> <p>Az alábbi elemek közül választhat egyet:</p> <ul style="list-style-type: none"> • Alacsony korlátozás. • Magas korlátozás. • Nem megbízható.

A Kármentesítő motor révén a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben elvégzett 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 fájl visszaállítás 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:

- Megszünteti 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 tevékenység utáni visszagörgetés elindulhat a [Fájl védelem](#) vagy [Viselkedéselemzés](#) összetevővel, illetve a [vírusvizsgálat](#) 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 felhasználoktól 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 részt vesz a Kaspersky Security Networkben, a KSN szolgáltatás megadja a Kaspersky Endpoint Security számára a vizsgált fájlok kategóriáját és hírnevét, valamint a vizsgált webcímek hírnevét.

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](#) található. A Kaspersky Security Network nyilatkozatának szövegét tartalmazó ksn_<nyelv azonosítója>.txt fájl megtalálható az alkalmazás [terjesztőkészletében](#).

A KSN kiszolgálók terhelésének csökkentése érdekében előfordulhat, hogy a Kaspersky szakértők az alkalmazás olyan frissítéseit adja ki, amelyek átmenetileg kikapcsolják vagy részlegesen korlátozzák a Kaspersky Security Network részére küldött kéréseket. Ebben az esetben a KSN-kapcsolat állapota az alkalmazás helyi felületén a következő: *Korlátozásokkal engedélyezve*.

KSN-infrastruktúra

A Kaspersky Endpoint Security a következő KSN-infrastrukturális megoldásokat támogatja:

- *Globális KSN*: a Kaspersky alkalmazások által használt leggyakoribb megoldás. A KSN-részvevők információkat kapnak a Kaspersky Security Networktől, és elküldik a Kaspersky számára a felhasználó számítógépén észlelt objektumokat, hogy a Kaspersky is elemezze azokat, és belevegye a Kaspersky Security Network hírnév- és statisztikai adatbázisába.
- *A Privát KSN* egy olyan megoldás, ami lehetővé teszi a Kaspersky Endpoint Security vagy egyéb Kaspersky alkalmazással rendelkező számítógépek felhasználóinak, hogy hozzáférjenek a Kaspersky Security Network hírnévadatbázisaihoz, valamint egyéb statisztikai adatokhoz anélkül, hogy adatokat küldenének a KSN-re a saját számítógépükről. A privát KSN 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.

Alapértelmezés szerint a Kaspersky Security Center a Globális KSN hálózatot használja. Lehetősége van konfigurálni a privát KSN használatát az adminisztrációs konzolon (MMC), a Kaspersky Security Center Web Console-ban és a [parancssorban](#). A privát KSN használatát nem lehet konfigurálni a Kaspersky Security Center Cloud Console-ban.

A Privát KSN-ről szóló további részletekért lásd a *Kaspersky Private Security Network dokumentációját*.

KSN Proxy

A Kaspersky Security Center felügyeleti kiszolgáló által kezelt felhasználói számítógépek a KSN-nel a KSN Proxyszolgáltatáson keresztül léphetnek interakcióba.

A KSN Proxyszolgáltatás az alábbi lehetőségeket kínálja:

- A felhasználó számítógépe lekérdezheti a KSN-t, és információkat küldhet el részére akár közvetlen internetelés 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.

A KSN Proxy szolgáltatás további részleteiért lásd a [Kaspersky Security Center Súgót](#).

Kaspersky Security Network beállítások

Paraméter	Leírás
Kiterjesztett KSN mód engedélyezése	A <i>Kiterjesztett KSN mód</i> 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	<p>A <i>Felhő mód</i> 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 Security Network letölti az antivírus adatbázisok teljes verzióját a Kaspersky szerverekről.</p> <p>Ha a kapcsológomb be van kapcsolva, a Kaspersky Endpoint Security az antivírus adatbázisok egyszerű verzióit használja, ami csökkenti az operációs rendszer erőforrásainak igénybevetelét.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">A jelölőnégyzet bejelölése után a Kaspersky Endpoint Security a következő frissítés során letölti az antivírus adatbázisok egyszerű verzióját.</div> <p>Ha a kapcsológomb ki van kapcsolva, a Kaspersky Endpoint Security az antivírus adatbázisok teljes verzióját használja.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">A jelölőnégyzet kitörlése után a Kaspersky Endpoint Security a következő frissítés során letölti az antivírus adatbázisok teljes verzióját.</div>
Számítógép státusza, ha a KSN kiszolgálók elérhetetlenek <i>(csak a Kaspersky Security Center konzolon érhető el)</i>	A legördülő listában lévő elemek meghatározzák a számítógép állapotát a Kaspersky Security Centerben, ha a KSN kiszolgálók elérhetetlenek.
KSN Proxy használata	Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a KSN proxykiszolgálót használja. A KSN proxyszolgáltatás beállításait az Adminisztrációs kiszolgáló tulajdonságaiban adhatja meg.

<p>(csak a Kaspersky Security Center konzolon érhető el)</p>	
<p>KSN kiszolgálók használata, amennyiben a KSN Proxy nem érhető el</p> <p>(csak a Kaspersky Security Center konzolon érhető el)</p>	<p>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 (Globális KSN használata esetén) és harmadik felek oldalán (Privát KSN használata esetén).</p>

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 Kaspersky Endpoint Security csak a HTTP és a HTTPS forgalmat figyeli meg.

A HTTPS forgalom megfigyeléséhez [engedélyeznie kell a titkosított kapcsolatok vizsgálatát](#).

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 weboldal adataihoz, elrejthet grafikus 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 „Archívum” adattípusként azonosítja azokat, nem pedig „Grafikus fájlokként”.

- **Egyedi címek.** Megadhat webcímet vagy [használhat maszkokat](#).

Egyszerre több módszert is használhat a weboldalak elérésének szabályozására. Például, ha korlátozhatja az „Office fájlok” adattípus elérést a „Webalapú e-mail” weboldalkategória 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.



A kért weboldal nem jeleníthető meg.

Cím: <http://kaspersky.ru/>.

A weboldalt a(z) test_block szabály blokkolta.

Ok: a webes erőforrás a(z) Nem megadott tartalomkategóriá(k)ba és a(z) Nem megadott adattípus kategóriá(k)ba tartozik.

Ez a webes erőforrás tiltva van a vállalatnál. Ha Ön szerint a blokkolás téves vagy mindenképp hozzá kell férnie ehhez a webes erőforráshoz, lépjen kapcsolatba a vállalati helyi hálózat rendszergazdjával ([Hozzáférés kérése](#)).

Üzenet létrehozva: 10/29/2020 4:58:30 AM



Elképzelhető, hogy a kért weboldal nem biztonságos, vagy tiltja a vállalat szabályzata.

Cím: <http://kaspersky.com/>.

A weboldalt a(z) test_warning szabály blokkolta.

Ok: a webes erőforrás a(z) Nem megadott tartalomkategóriá(k)ba és a(z) Nem megadott adattípus kategóriá(k)ba tartozik.

Kattintson a(z) <http://kaspersky.com/> hivatkozásra a kért weboldal megnyitásához.

Ha azon teljes webhely tartalmához szeretne hozzáférni, amelyen a kért weboldal található, kattintson a(z) http://kaspersky.com/* hivatkozásra.

Ha a "*" szimbólummal megjelölt tartománynévnel alacsonyabb vagy azzal azonos minden létező tartományhoz szeretne hozzáférni, kattintson a(z) */*.kaspersky.com/* hivatkozásra.

A hozzáférés a fenti webes erőforrásokhoz az alkalmazás jelenlegi munkamenetének idejére érvényes.

Ha a figyelmeztetés téves, lépjen kapcsolatba a vállalati helyi hálózat rendszergazdjával ([Hozzáférés kérése](#)).

Üzenet létrehozva: 10/29/2020 5:00:10 AM

Webfelügyelő üzenet

A Webfelügyelő összetevő beállításai

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 <i>Alapértelmezett szabály</i> azt a webes erőforráshoz hozzáférő szabályt jelenti, amire nem vonatkozik egyetlen más szabály sem. A következők közül választhat: <ul style="list-style-type: none">• 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.

<p>Üzenetsablonok</p>	<ul style="list-style-type: none"> • 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 hozzáféréseinek 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.
<p>Az engedélyezett oldalak megnyitásának naplózása</p>	<p>A Kaspersky Endpoint Security naplózza a weboldalak látogatását, köztük az engedélyezett weboldalakat 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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Az internettevékenység megfigyelése több számítógépes erőforrást vehet igénybe HTTPS-forgalom visszafejtése során.</p> </div>

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 védje számítógépét a fertőzésektől, ha ilyen eszközök vannak csatlakoztatva, valamint megelőzi az adatvesztés- vagy szivárgást.


Eszközhozzáférési szintek

Az Eszközfelügyelő a következő szinteken felügyeli a hozzáférést:



- **Eszköztípus.** Például nyomtatók, cserélhető meghajtók és CD/DVD meghajtók.

Az eszköz hozzáféréseinek beállításait az alábbiak szerint lehet megadni:

- Engedélyezés – ✓.
- Blokkolás – ⛔.
- A csatlakozóbusztól függ (kivéve a Wi-Fi-hez) – 🌐.

- Blokkolás kivételekkel (csak Wi-Fi) – .
- **Csatlakozási busz.** A *csatlakozási busz* egy felület, amivel csatlakoztatni lehet eszközöket a számítógéphez (például USB vagy FireWire). Ennek megfelelően például USB-n keresztül is korlátozhatja az eszközök kapcsolatát.



Az eszköz hozzáféréseinek 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 beállításaiiban meg vannak adva.

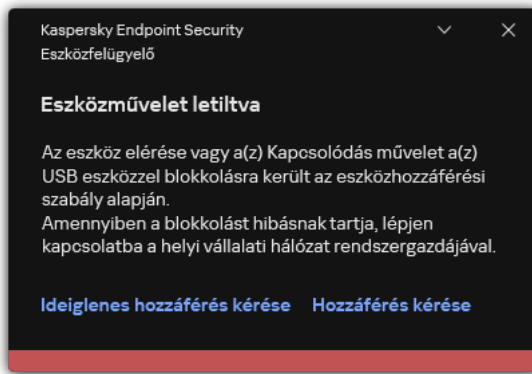
Az alábbi adatok alapján hozzáadhat megbízható eszközöket:

- **Eszközök azonosító alapján.** Minden eszköz egyedi azonosítóval rendelkezik (Hardverazonosítóval, azaz HWID-vel). Megtekintheti az azonosítót az eszköz tulajdonságaiban, ha operációsrendszer-eszközöket használ. Eszközazonosító példája:
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 azonosítomaszk 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.

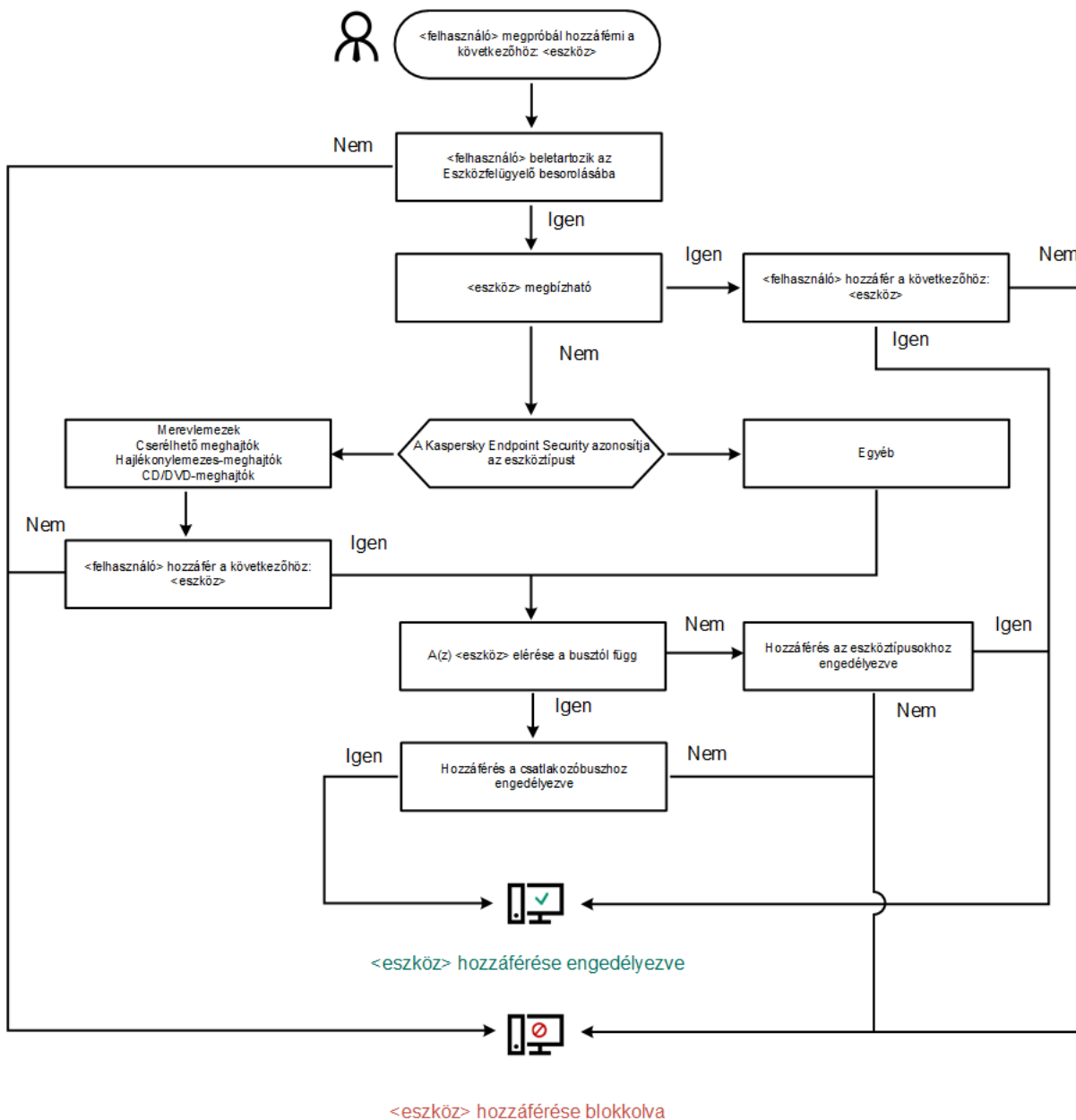
Ha egy olyan eszköz csatlakozik a számítógéphez, ami blokkolva van az Eszközfelügyelő által, akkor a Kaspersky Endpoint Security blokkolja az elérést, és megjelenít egy értesítést (lásd az alábbi ábrát).



Eszközfelügyelő értesítés

Eszközfigyelő műveleti algoritmus

A Kaspersky Endpoint Security döntést hoz az eszközök hozzáféréseinek 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](#).

Az Eszközfelügyelő összetevő beállításai

Paraméter	Leírás
Ideiglenes hozzáférési kérelem engedélyezése <i>(csak a Kaspersky Security Center konzolon érhető el)</i>	<p>Ha a jelölőnégyzet be van jelölve, a Hozzáférés kérése gombra használható a Kaspersky Endpoint Security helyi felületén. Erre a gombra kattintva megnyílik a Hozzáférés kérése az eszközhöz ablakot. Ebben az ablakban a felhasználó ideiglenes hozzáférést kérhet egy blokkolt eszközhöz.</p>
Készülékek és Wi-Fi hálózatok	<p>Ez a táblázat tartalmazza az összes lehetséges eszköztípust az Eszközfelügyelő összetevő osztályozásának megfelelően, ideértve hozzáférési állapotukat is.</p>
Csatlakozási buszok	<p>Az összes rendelkezésre álló csatlakozási busz listája az Eszközfelügyelő összetevő osztályozásának megfelelően, ideértve hozzáférési állapotukat is.</p>
Megbízható eszközök	<p>A megbízható eszközök listája, valamint a felhasználók, akik hozzáférést adtak ezekhez az eszközökhöz.</p>
Anti-Bridging	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Az Anti-Bridging a következő típusú eszközökön támogatja a műveletet: hálózati adapter, Wi-Fi és modem.</p>
Üzenetsablonok	<ul style="list-style-type: none"> • 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 létrehozása érdekében a következő feltételeket használhatja: KL kategória (például *Böngészők*), fájlkivonat, alkalmazásforgalmazó 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”.

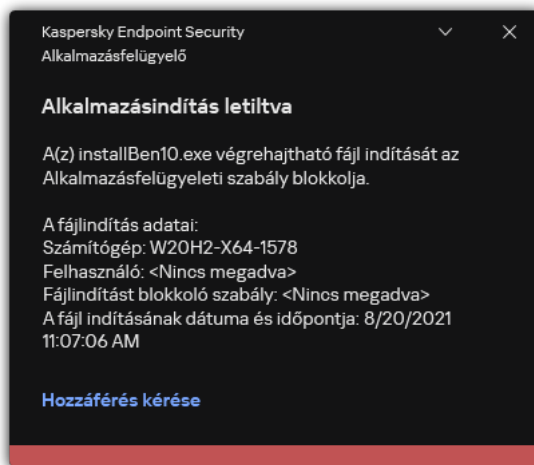
3. [Az Alkalmazásfelügyelő módjának kiválasztása](#).

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.
- **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.

Eloolvhatja 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.

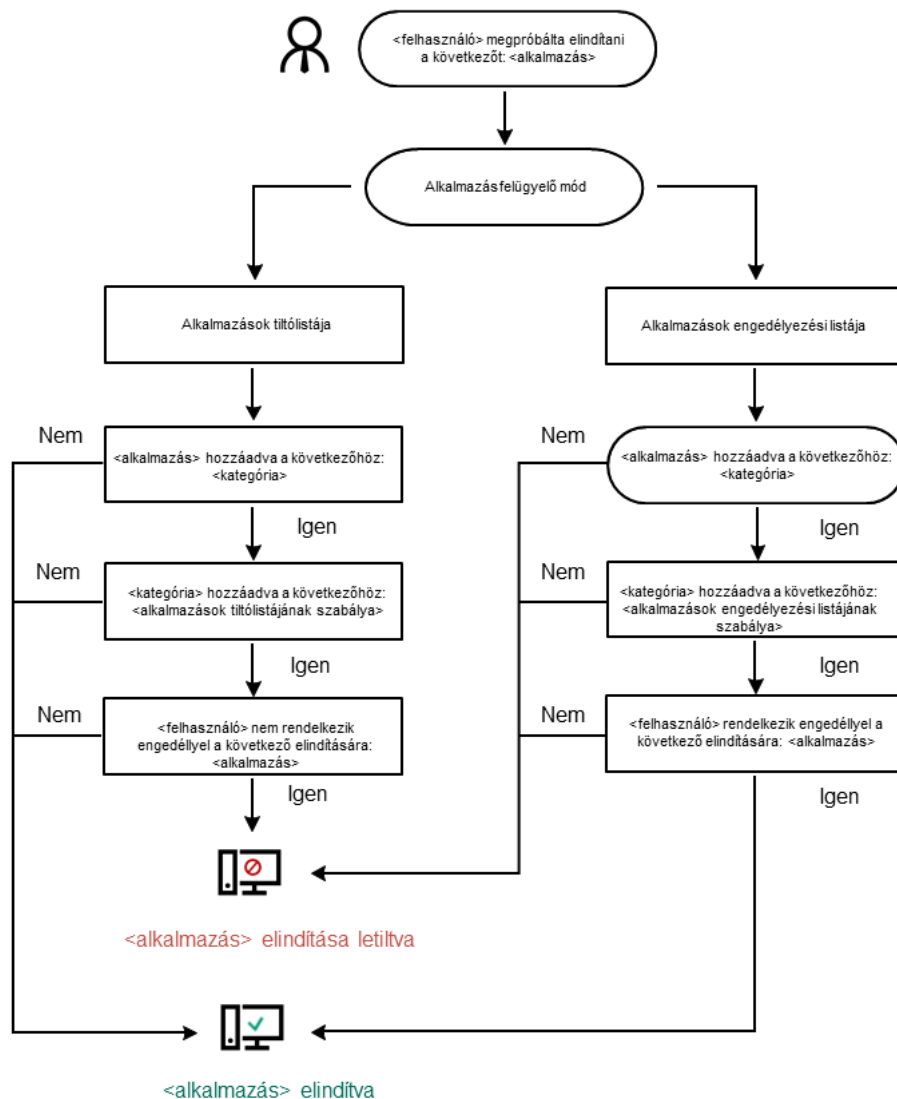
A Kaspersky Security Center azonban olyan eszközöket is kínál, amelyek a Kaspersky Endpoint Security helyi felületén nem találhatóak meg, köztük az alábbi feladatokhoz szükséges eszközöket:

- [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 algoritmus

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
Test mode	Ha a kapcsológomb be van kapcsolva, a Kaspersky Endpoint Security lehetővé teszi az Alkalmazásfelügyelő jelenlegi módjában blokkolt alkalmazás elindítását, azonban az indítás információit a jelentésben rögzíti.
Application Control Mode	<p>Az alábbi opciók közül választhat:</p> <ul style="list-style-type: none"> 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. <p>Ha az Engedélyezési lista mód van kiválasztva, két Alkalmazásfelügyeleti szabály automatikusan létrejön:</p> <ul style="list-style-type: none"> Golden Image.

	<ul style="list-style-type: none"> • Megbízható frissítéstelepítők. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Az automatikusan létrehozott szabályok nem törölhetők, és beállításaik nem szerkeszthetők. A szabályok letilthatók és engedélyezhetők.</p> </div>
<p>Control DLL modules load (significantly increases the load on the system)</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security szabályozza a DLL modulok betöltését, ha a felhasználó alkalmazásokat próbál elindítani. A DLL modulral és az azt betöltő alkalmazással kapcsolatos információk bekerülnek a jelentésbe.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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 Megbízható tanúsítványok 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.</p> </div> <p>A Kaspersky Endpoint Security kizárólag a jelölőnégyzet bejelölését követően betöltött DLL modulokat és illesztőprogramokat figyel. 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.</p>
<p>Message templates</p>	<p>Message about blocking. Az üzenet sablonja, amely akkor jelenik meg, ha kiváltódik egy Alkalmazásfelügyeleti szabály, amely egy alkalmazás indítását blokkolja.</p> <p>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. Miután a felhasználó hozzáférést kér, a Kaspersky Endpoint Security eseményt küld a Kaspersky Security Center számára: Alkalmazásindítás hozzáféréseinek 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.</p>

Adaptív Anomália felügyelő

Ez az összetevő csak a Kaspersky Endpoint Security for Business Advanced és a Kaspersky Total Security for Business termékben érhető el. A Kaspersky Endpoint Security for Business további részleteiért látogasson el a [Kaspersky webhelyére](#).

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 Anomáiafelügyelő összetevő megfigyeli és letiltja azokat a tevékenységeket, amelyek nem megszokottak a cég hálózatán található számítógépeken. Az Adaptív Anomáiafelügyelő egy szabálycsoport alapján követi nyomon a nem megszokott viselkedést (például a *Microsoft PowerShell indítása egy Office-alkalmazásból* szabályt). A szabályokat a Kaspersky szakemberei állították össze a rosszindulatú tevékenységek tipikus forgatókönyvei alapján. Konfigurálhatja, hogy az Adaptív Anomáiafelügyelő 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 Anomáiafelügyelő beállításai

Az Adaptív Anomáiafelügyelő beállításai a következő lépésekből állnak:

1. Az Adaptív Anomáiafelügyelő betanítása.

Miután engedélyezte az Adaptív Anomáiafelügyelőt, a szabályok *tanuló módban* vannak. A tanulás során az Adaptív Anomáiafelügyelő 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 Anomáiafelügyelő 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 **Triggering of rules in Smart Training state** gyűjteményben.

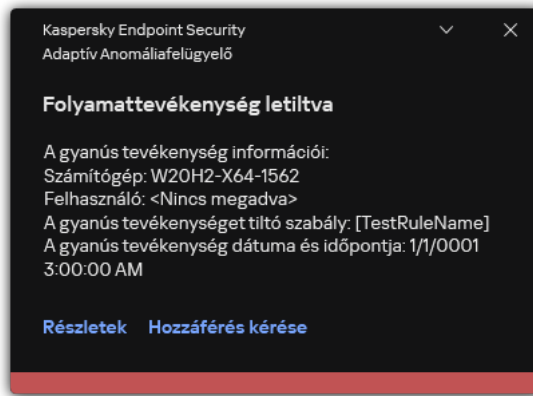
2. A szabálykiváltó jelentés értelmezése.

A [szabálykiváltó jelentést](#) vagy a **Triggering of rules in Smart Training state** gyűjteményt a rendszergazdának kell értelmezni. A rendszergazda ezt követően kiválaszthatja az Adaptív Anomáiafelügyelő 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 Anomáiafelügyelő konfigurálása valós időben történik. Az Adaptív Anomáiafelügyelő konfigurálása a következő csatornákon történik:

- Az Adaptív Anomáiafelügyelő 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 Anomáiafelügyelő működését, hogy áttekintette a szabálykiváltó jelentést és a **Triggering of rules in Smart Training state** gyűjtemény tartalmát. Javasoljuk, hogy ellenőrizze a szabálykiváltó jelentést és a **Triggering of rules in Smart Training state** gyűjtemény tartalmát.

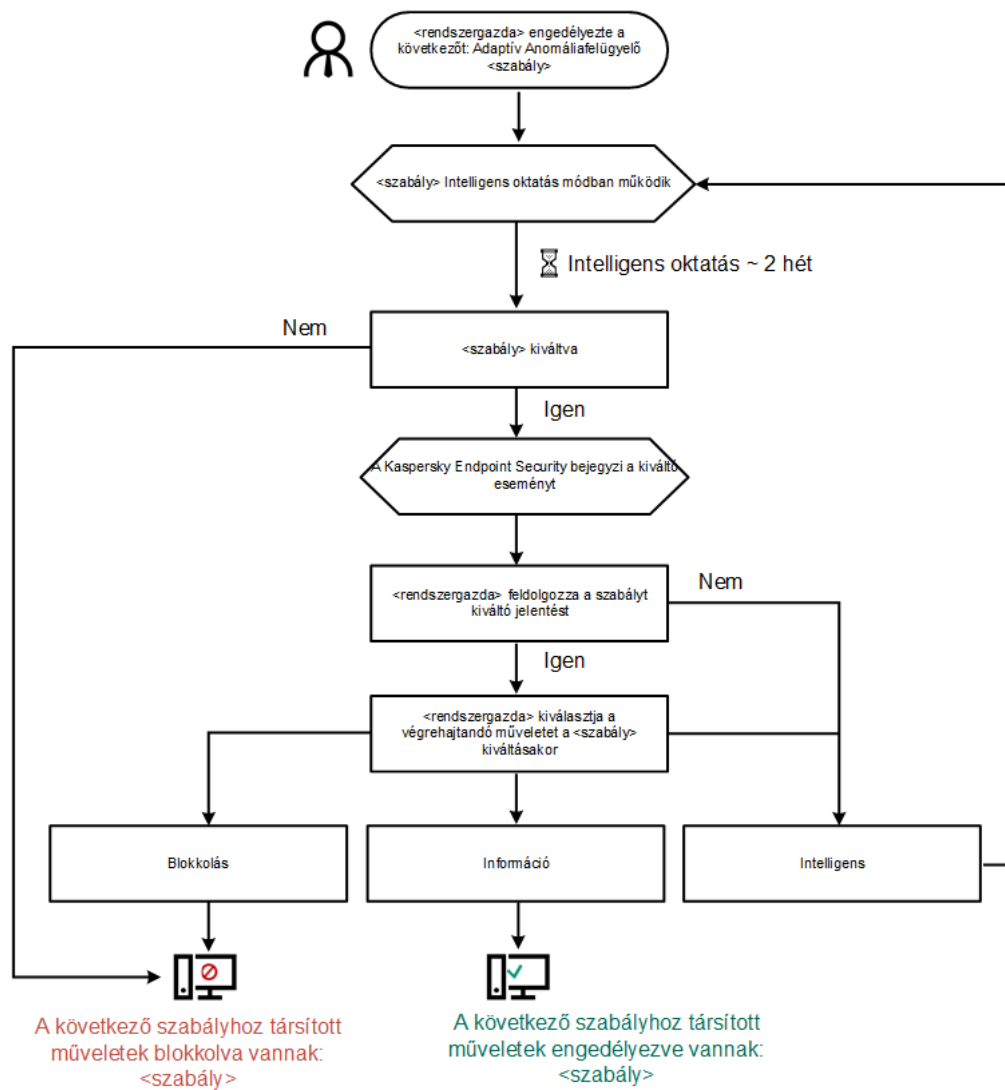
Amikor egy rosszindulatú alkalmazás megpróbál műveletet végrehajtani, a Kaspersky Endpoint Security letiltja a műveletet és értesítést jelenít meg (lásd az alábbi ábrát).



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
Report on	Ez a jelentés az Adaptív Anomáliafelügyeleti szabályészleléseinek állapotáról tartalmaz

<p>Adaptive Anomaly Control rules state</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>információkat (például <i>Kikapcsolva</i> vagy <i>Letiltva</i>). A jelentés minden rendszergazdai csoport számára létrejön.</p>
<p>Report on triggered rules of Adaptive Anomaly Control</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>Ez a jelentés tartalmazza az Adaptív Anomáiafelügyelő által észlelt gyanús tevékenységek információit. A jelentés minden rendszergazdai csoport számára létrejön.</p>
<p>Szabályok</p>	<p>Adaptív Anomáiafelügyeleti szabályok táblázata A szabályokat a Kaspersky szakemberei hozták létre, a potenciálisan kártékony tevékenységek jellemző forgatókönyvei alapján.</p>
<p>Sablonok</p>	<ul style="list-style-type: none"> • Üzenet a blokkolásról. Üzenetsablon, ami akkor jelenik meg a felhasználónak, amikor aktiválódik az Adaptív Anomáiafelügyelő 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.

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-Célzott-Támadások-Elleni-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 Célzott Támadások Elleni Platform két blokkot foglal magába: Kaspersky Célzott Támadások Elleni Platform (a továbbiakban „KATA”) és a Kaspersky Endpoint Észlelés és válasz (a továbbiakban „KEDR”). A KEDR külön vásárolható meg. A megoldás részleteivel kapcsolatos információért lásd a [Kaspersky Célzott Támadások Elleni 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 súgóikkében 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. Ezekon 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 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 Célzott Támadások Elleni Platform súgót](#).

Kaspersky Sandbox

A Kaspersky Endpoint Security 11.7.0 mostantól beépített ügynököt tartalmaz a Kaspersky Sandbox megoldással való integrációhoz. A *Kaspersky Sandbox megoldás* észleli és automatikusan blokkolja a speciális fenyegetéseket a számítógépeken. A Kaspersky Sandbox az objektumok viselkedésének elemzésével észleli a rosszindulatú tevékenységeket és a vállalat informatikai infrastruktúrája elleni célzott támadásokra jellemző műveleteket. A Kaspersky Sandbox a Microsoft Windows operációs rendszerek telepített virtuális képeivel speciális kiszolgálókon elemzi és vizsgálja az objektumokat (Kaspersky Sandbox-kiszolgálók). A megoldás részleteit a [Kaspersky Sandbox súgóban](#) találja.

Az összetevőt csak a Kaspersky Security Center Web Console használatával lehet felügyelni. Ezt az összetevőt nem felügyelheti az Adminisztrációs Konzol (MMC) használatával.

A Kaspersky Sandbox összetevő beállításai

Paraméter	Leírás
Kiszolgálói TLS-tanúsítvány hibája	Ha megbízható kapcsolatot szeretne konfigurálni a Kaspersky Sandbox kiszolgálóival, elő kell készítenie egy TLS-tanúsítványt. Ezután hozzá kell adnia a tanúsítványt a Kaspersky Sandbox-kiszolgálókhoz és a Kaspersky Endpoint Security házirendjéhez. A tanúsítvány előkészítéséről és a tanúsítványnak a kiszolgálókhoz való hozzáadásáról részletesen lásd a Kaspersky Sandbox súgót .
Időtűllépés	A Kaspersky Sandbox-kiszolgáló kapcsolódási időtűllépése. A beállított időtűllépés letelte után a Kaspersky Endpoint Security kérést küld a következő kiszolgálónak. Növelheti a Kaspersky Sandbox kapcsolódási időtűllépését, ha a kapcsolat sebessége alacsony, vagy ha a kapcsolat instabil. A kérések ajánlott időtűllépése 0,5 másodperc vagy kevesebb.
A Kaspersky Sandbox kérési várólistája	A kérési várólista mappájának mérete. Amikor a számítógépen hozzáfér egy objektumhoz (futtatható fájl indítása vagy egy dokumentum – például DOCX vagy PDF formátumú fájl – megnyitása), a Kaspersky Endpoint Security képes elküldeni az objektumot vizsgálatra a Kaspersky Sandbox számára. Több kérés esetén a Kaspersky Endpoint Security létrehoz egy kérési várólistát. Alapértelmezés szerint a kérési várólista mappamérete 100 MB-ra van korlátozva. A maximális méret elérése után a Kaspersky 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.
Kaspersky Sandbox-kiszolgálók	A Kaspersky 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.
Művelet fenyegetés észlelésekor	<p>Másolat áthelyezése a karanténba, objektum törlése. 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.</p> <p>Kritikus területek vizsgálatának futtatása. Ha ezt az opciót választja, a Kaspersky Endpoint Security futtatja a Kritikus területek vizsgálata feladatot. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.</p> <p>IOC vizsgálati feladat létrehozása. Ha ezt az opciót választja, a Kaspersky Endpoint Security automatikusan létrehozza az IOC vizsgálati feladatot (<i>autonóm IOC vizsgálati feladat</i>). Ehhez a feladathoz konfigurálhatja a futásmódot, a vizsgálat hatókörét és az IOC észlelési műveletet: objektum törlése, a <i>Kritikus területek vizsgálata</i> feladat futtatása. Az <i>IOC vizsgálat</i> feladat beállításainak módosításához nyissa meg a feladat beállításait.</p>
IOC vizsgálat hatóköre	<p>Kritikus fájlterületek. Ha ezt az opciót választja, a Kaspersky Endpoint Security csak a számítógép kritikus fájlterületein végez IOC vizsgálatot: rendszermag memóriája és rendszerindítási szektorok.</p> <p>Fájlterületek a számítógép rendszer meghajtóin. Ha ez az opció van kiválasztva, a Kaspersky Endpoint Security IOC vizsgálatot végez a számítógép rendszer meghajtóján.</p>

IOC vizsgálati feladat futtatása	<p>Manually. A futásmód, amelyben elindíthatja az <i>IOC vizsgálat</i> feladatot manuálisan az Ön által választott időpontban.</p> <p>Fenyegetés észlelése után. A futásmód, amelyben a Kaspersky Endpoint Security automatikusan futtatja az <i>IOC vizsgálat</i> feladatot, amikor fenyegetést észlel.</p> <p>Csak akkor fusson, ha a számítógép üresjáratban van. A futásmód, amelyben a Kaspersky Endpoint Security futtatja az <i>IOC vizsgálat</i> 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.</p>
---	---

Endpoint Detection and Response

A Kaspersky Endpoint Security 11.7.0 beépített ügynökkel rendelkezik a Kaspersky Endpoint Detection and Response Optimum megoldáshoz (a továbbiakban: „EDR Optimum”). A Kaspersky Endpoint Security 11.8.0 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. 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.

Az EDR Optimum összetevőt a Web Console-on és a Cloud Console-on konfigurálhatja. Az EDR Expert összetevő beállításai csak a Cloud Console-on érhetők el.

Az Endpoint Detection and Response beállításai

Paraméter	Leírás
Hálózatelkülönítés	<p>A számítógép automatikus leválasztása a hálózatról válaszul az észlelt fenyegetésekre.</p> <p>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:</p> <ul style="list-style-type: none"> • A Hálózatelkülönítés kizárásaiban felsorolt kapcsolatok. • A Kaspersky Endpoint Security szolgáltatásai által kezdeményezett kapcsolatok. • A Kaspersky Security Center Felügyeleti ügynök által kezdeményezett kapcsolatok.
Az elkülönített számítógép automatikus	<p>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.</p>

<p>feloldása N óra múlva</p>	
<p>Network isolation exclusions</p>	<p>A hálózatelkülönítési kizárásokhoz tartozó szabályok listája. Az e szabályoknak megfelelő hálózati kapcsolatok nincsenek blokkolva a számítógépeken, ha a Hálózatelkülönítés be van kapcsolva.</p> <p>A Hálózatelkülönítés kizárásainak konfigurálásához használhatja a <i>szabványos hálózati profilok</i> listáját. Alapértelmezés szerint a kizárások közé tartoznak azok a hálózati profilok, amelyek a DNS-/DHCP-kiszolgálóval és a DNS-/DHCP-ügyszerep körrel rendelkező eszközök zavartalan működését biztosító szabályokat tartalmazzák. Módosíthatja a szabványos hálózati profilok beállításait, vagy manuálisan is megadhat kizárásokat.</p> <div style="border: 1px solid #f08080; padding: 10px; margin-top: 10px;"> <p>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 manuálisan kapcsolják be.</p> </div>
<p>Végrehajtás megelőzése</p>	<p>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.</p>
<p>Action on execution or opening of forbidden object</p>	<p>Block and write to report. 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.</p> <p>Log events only. 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.</p>
<p>A végrehajtás megakadályozásának szabályai</p>	<p>Az objektumvégrehajtás megakadályozási szabályainak listája. A <i>végrehajtás-megakadályozási szabály</i> olyan feltételkészletnek minősül, amelyet figyelembe kell venni a blokkolásakor. Az alkalmazás elérési utak vagy az MD5 és SHA256 kivonatolási algoritmusokkal kiszámított ellenőrzőösszegek alapján azonosítja a fájlokat.</p>

Teljes lemeztitkosítás

Kiválaszthatja a titkosítási technológiát: Kaspersky lemeztitkosítás vagy BitLocker meghajtótitkosítás (a továbbiakban egyszerűen „BitLocker” is).

Kaspersky lemeztitkosítás

A rendszermerevlemezek titkosítását követően a számítógép legközelebbi indításakor a felhasználónak a [Hitelesítési ügynök](#) segítségével hitelesítést kell végeznie, mielőtt hozzáférhetne a merevlemezekhez, és betölthető 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 felhasználónevet és jelszavát. Ezek a fiókok azon Microsoft Windows fiókokon alapulnak, amelyekkel a felhasználó az operációs rendszerbe bejelentkezik. Emellett [használhatja az egyszerű bejelentkezés \(SSO\) 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 felhasználónevet és jelszavát.
- Adja meg a token vagy a számítógéphez csatlakoztatott okoskártya jelszavát.

Akkor lehet token 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 Security Centeren keresztül 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 BitLocker egy Trusted Platform Module segítségével a hozzáférési kulcsok biztonságos tárolását biztosítja. A *Trusted Platform Module (TPM)* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapiján 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 rendszerintegritáció-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.

A meghajtó titkosítása után a BitLocker főkulcsot hoz létre. A Kaspersky Endpoint Security elküldi a főkulcsot a Kaspersky Security Center számára, hogy Ön [vissza tudja állítani a lemez hozzáférést](#), például akkor, ha a felhasználó elfelejtette a jelszót.

Ha a felhasználó BitLocker használatával titkosítja a lemezt, a Kaspersky Endpoint Security elküldi a [lemeztitkosítás információit a Kaspersky Security Center számára](#). A Kaspersky Endpoint Security azonban nem küldi el a főkulcsot a Kaspersky Security Center számára, szóval a Kaspersky Security Center használatával nem lehet visszaállítani a lemezhez való hozzáférést. Ahhoz, hogy a BitLocker megfelelően működjön a Kaspersky Security Center alkalmazással, [fejtse vissza a meghajtót](#), majd [titkosítsa újra](#) rendszabállyal. Meghajtót helyileg, illetve házirenddel is titkosíthat.

Miután titkosítja a rendszer merevlemezeit, a felhasználónak végig kell mennie a BitLocker hitelesítések, hogy elindítsa az operációs rendszert. A BitLocker a hitelesítést követően lehetővé teszi a felhasználó bejelentkezését. A BitLocker nem támogatja az egyszerű bejelentkezési technológiát (SSO).

Ha Windows csoportrendszabályokat használ, kapcsolja ki a BitLocker kezelést a rendszabály-beállításokban. A Windows rendszabály-beállítások összeférhetetlenek lehetnek a Kaspersky Endpoint Security rendszabály-beállításával. Meghajtó titkosításakor hiba léphet fel.

A Kaspersky lemeztitkosítási összetevő beállításai

Paraméter	Leírás
Titkosítási mód	<p>Összes merevlemez titkosítása. Ha ez az elem ki van választva, az alkalmazás a rendszabály alkalmazásakor titkosítja az összes merevlemezt.</p> <div style="border: 1px solid #f08080; padding: 5px; margin: 10px 0;"> <p>Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak az az operációs rendszer tölthető be, amelyeken az alkalmazás telepítve van.</p> </div> <p>Összes merevlemez visszafejtése. Ha ez az elem ki van választva, az alkalmazás a rendszabály alkalmazásakor visszafejti az összes korábban titkosított merevlemezt.</p> <p>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.</p>
A titkosítás során Hitelesítési ügynöki fiókok automatikus létrehozása Windows-felhasználóknak	<p>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.</p>
Hitelesítési ügynök fióklétrehozási beállítások	<p>A számítógépen lévő összes fiók. Ha ez a jelölőnégyzet be van jelölve, akkor a teljes lemeztitkosítási feladat során a Kaspersky Endpoint Security Hitelesítési ügynök-fiókokat hoz létre a számítógép minden olyan fiókja számára, amely valaha is aktív volt.</p> <p>A számítógépen lévő összes tartományfiók. Ha ez a jelölőnégyzet be van jelölve, akkor a teljes lemeztitkosítási feladat során a Kaspersky Endpoint Security Hitelesítési ügynök-fiókokat hoz létre egy adott tartományhoz tartozó összes olyan számítógépes fiók számára, amely valaha is aktív volt.</p> <p>A számítógépen lévő összes helyi fiók. Ha ez a jelölőnégyzet be van jelölve, akkor a teljes lemeztitkosítási feladat során a Kaspersky Endpoint Security Hitelesítési ügynök-fiókokat hoz létre a helyi számítógép minden olyan fiókja számára, amely valaha is aktív volt.</p> <p>Helyi rendszergazda. Ha ez a jelölőnégyzet be van jelölve, akkor a teljes lemeztitkosítási feladat során a Kaspersky Endpoint Security helyi rendszergazdai fiókot hoz létre.</p> <p>Számítógép kezelője Ha ez a jelölőnégyzet be van jelölve, akkor a teljes lemeztitkosítási feladat során a Kaspersky Endpoint Security Hitelesítési ügynök-fiókokat hoz létre azon fiók számára, amely az Active Directoryban szereplő tulajdonságai alapján kezelői fiók.</p> <p>Aktív fiók. Ha ez a jelölőnégyzet be van jelölve, akkor a teljes lemeztitkosítási feladat során a Kaspersky Endpoint Security automatikusan Hitelesítési ügynök-fiókokat hoz létre a titkosítási feladat közben aktív számítógépes fiók számára.</p>
Hitelesítési ügynöki fiókok automatikus létrehozása a számítógép összes	<p>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</p>

<p>felhasználójának bejelentkezéskor</p>	<p>hitelesítéskor. Ezért a már titkosított meghajtókkal rendelkező számítógépek esetében nem kell manuálisan hozzáadnia Hitelesítési ügynöki fiókokat a <i>Hitelesítési ügynöki fiókok kezelése</i> feladattal.</p>
<p>Hitelesítési ügynökben megadott felhasználónév mentése</p>	<p>Ha a jelölőnégyzet ki van jelölve, az alkalmazás elmenti a Hitelesítési ügynök fiókjának nevét. Ily módon nem szükséges a fióknevet a legközelebbi alkalommal megadni, amikor ugyanabban a fiókban a Hitelesítési ügynökben hitelesítést szeretne végezni.</p>
<p>Csak a használt lemezterület titkosítása</p>	<p>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.</p> <div data-bbox="416 555 1493 745" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>A Csak a felhasznált lemezterület titkosítása (Windows 8 és újabb verziók) funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemez visszafejtése. A titkosítás megkezdése előtt kell a jelölőnégyzetet bejelölni, illetve törölni.</p> </div> <p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a teljes merevlemez titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit.</p> <div data-bbox="416 1016 1493 1240" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Ez a lehetőség új merevlemezeken javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha már használatban lévő merevlemezeken alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről – azokról is, amelyeket már letörölt, de még visszakereshető információkat tartalmaznak.</p> </div> <p>Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.</p>
<p>Örökölt USB-támogatás használata</p>	<p>Ez a jelölőnégyzet be/kikapcsolja a Legacy USB Support funkciót. A <i>Legacy USB Support</i> 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.</p> <p>Ha a jelölőnégyzet be van jelölve, engedélyezve van az USB eszközök támogatása a számítógép indulásakor.</p> <div data-bbox="416 1664 1493 1854" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f9e7e7;"> <p>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, amelyekben fennáll a probléma.</p> </div>
<p>Jelszóbeállítások</p>	<p>A Hitelesítési ügynök-fiók jelszóerősségi beállításai. Lehetősége van engedélyezni az egyszeri bejelentkezés (SSO) technológia használatát is.</p> <p>Az SSO technológia révén ugyanazon hitelesítési adatokkal férhet hozzá a titkosított merevlemezhez és jelentkezhet be az operációs rendszerbe.</p>

	<p>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.</p> <p>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.</p>
Súgószövegek	<p>Hitelesítés. Súgószöveg, amely a fiók bejelentkezési adatainak megadásakor jelenik meg a Hitelesítési ügynök ablakában.</p> <p>Jelszó módosítása. Súgószöveg, amely a Hitelesítési ügynök-fiók jelszavának módosításakor jelenik meg a Hitelesítési ügynök ablakában.</p> <p>Jelszó visszaállítása. Súgószöveg, amely a Hitelesítési ügynök-fiók jelszavának visszaállításakor jelenik meg a Hitelesítési ügynök ablakában.</p>

A BitLocker meghajtótitkosítás összetevő beállításai

Paraméter	Leírás
Titkosítási mód	<p>Összes merevlemez titkosítása. Ha ez az elem ki van választva, az alkalmazás a rendszabály alkalmazásakor titkosítja az összes merevlemez.</p> <div style="background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>Ha a számítógépen több operációs rendszer van telepítve, akkor a titkosítás után csak az az operációs rendszer tölthető be, amelyeken az alkalmazás telepítve van.</p> </div> <p>Összes merevlemez visszafejtése. Ha ez az elem ki van választva, az alkalmazás a rendszabály alkalmazásakor visszafejti az összes korábban titkosított merevlemez.</p> <p>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.</p>
Rendszerindítás előtt, billentyűzetten keresztül történő BitLocker hitelesítés bekapcsolása táblagépeken	<p>Ez a jelölőnégyzet engedélyezi/letiltja az adatbevitt igénylő hitelesítést rendszerindítás előtti környezetben, még akkor is, ha a platformon nem lehetséges a bevitel rendszerindítás előtt (például táblagépek érintőképernyős billentyűzetei esetén).</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>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.</p> </div> <p>Ha a jelölőnégyzet be van jelölve, a rendszerindítás előtti bevitt 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.</p> <p>Ha a jelölőnégyzet üres, a BitLocker meghajtótitkosítás nem érhető el táblagépeken.</p>
Hardveres titkosítás használata	<p>Ha a jelölőnégyzet be van jelölve, az alkalmazás hardveres titkosítást használ. Ennek köszönhetően felgyorsul a titkosítás, és kevesebb számítógépes erőforrást vesz igénybe.</p>
Csak a felhasznált lemezterület titkosítása	<p>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.</p>

(Windows 8 és újabb verziók)

A Csak a felhasznált lemezterület titkosítása (Windows 8 és újabb verziók)
funkció engedélyezése vagy letiltása a titkosítás elindítása után nem módosítja ezt a beállítást, amíg meg nem történik a merevlemez 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 merevlemezeken esetén javasolt, melyeknél még nem történt adatmódosítás és -törlés. Ha már használatban lévő merevlemezeken alkalmaz titkosítást, akkor javasolt az egész meghajtót titkosítani. Ez gondoskodik az összes adat védelméről – azokról is, amelyeket már törölt, de még visszakereshető információkat tartalmaznak.

Alapértelmezés szerint a jelölőnégyzet nincs bejelölve.

Hitelesítési beállítások

Jelszó használata (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) használata

Ha ez a lehetőség van kiválasztva, a BitLocker Trusted Platform Module-t (TPM) használ.

A *Trusted Platform Module (TPM)* egy mikrocsip, amely alapvető biztonsági funkciók nyújtására (például titkosítási kulcsok tárolására) szolgál. A Trusted Platform Module általában a számítógép alaplapiján 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:

- **Use PIN for TPM.** Ezzel a jelölőnégyzettel 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.

Engedélyezheti a felhasználónak a bővített PIN-kód használatát. A *bővített PIN-kód* lehetővé teszi a számokon kívül más karakterek használatát is: latin nagy- és kisbetűket, speciális karaktereket és szóközöket.

- **A Trusted Platform Module (TPM) használata; ha nem érhető el - használja a jelszót.** Ha a jelölőnégyzet be van jelölve, 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.

Fájl szintű titkosítás

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 fejtí 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.

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 fejtí 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 fejtí 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 fájl szintű titkosítási összetevő beállításai

Paraméter	Leírás
Titkosítási mód	<p>Maradjon változatlan. Ha ez az elem ki van választva, a Kaspersky Endpoint Security a fájlokat és mappákat titkosítás és visszafejtés nélkül változatlanul hagyja.</p> <p>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.</p> <p>Összes visszafejtése. Ha ez az elem ki van választva, a Kaspersky Endpoint Security az összes titkosított fájlt és mappát visszafejti.</p>
Titkosítási szabályok	<p>Ezen a lapon a helyi meghajtókon tárolt fájlok titkosítási szabályai láthatók. Fájlt a következőképpen lehet hozzáadni:</p> <ul style="list-style-type: none"> • Előre megadott mappák. A Kaspersky Endpoint Security a következő területek hozzáadását teszi lehetővé: <ul style="list-style-type: none"> Dokumentumok. Az operációs rendszer szokványos <i>Dokumentumok</i> mappájában, valamint az azon belüli almappákban található fájlok. Kedvencek. Az operációs rendszer szokványos <i>Kedvencek</i> mappájában, valamint az azon belüli almappákban található fájlok. Asztal. Az operációs rendszer szokványos <i>Asztal</i> 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: <ul style="list-style-type: none"> Használjon környezeti változót (például: %FOLDER%\UserFolder\). Egy környezeti változót csak egyszer lehet használni, és kizárólag az elérési út kezdetén. Ne használjon relatív útvonalat. Használhatja a \ . . \ karakterláncot (pl. C:\Users\ . . \UserFolder\). A \ . . \ karakterlánc a szülőkönyvtárra való áttérést jelöli. 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 <i>Archívumok</i> kiterjesztéscsoportot. Lehetősége van kézzel is hozzáadni fájlkiterjesztést.
Visszafejtési szabályok	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 csomag jelszóbeállításai	Jelszóerősség követelményei a titkosított csomag létrehozásánál.

Cserélhető meghajtók titkosítása

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:

- Teljes lemeztitkosítás (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 vállalati hálózaton belül sem lehetséges, ha a számítógép nincs csatlakoztatva a Kaspersky Security Centerhez (pl „vendég” számítógépen).

- Fájl szintű titkosítás (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

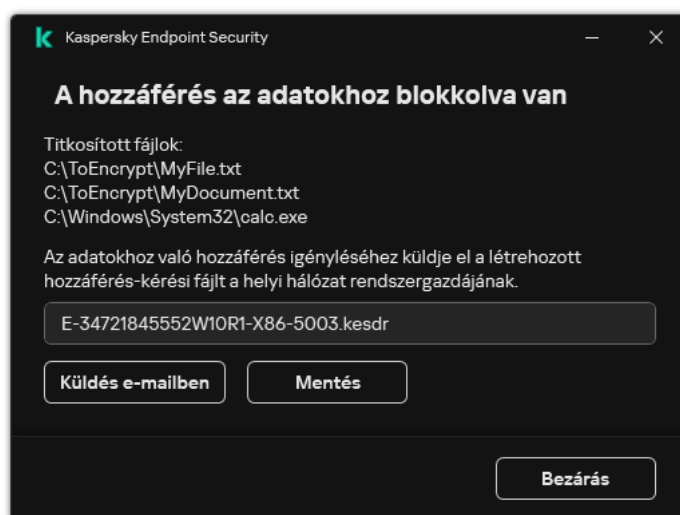
Paraméter	Leírás
Titkosítás kezelése	<p>Teljes cserélhető meghajtó titkosítása. E lehetőség kiválasztása esetén a rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtókat fájlrendszerükkel együtt szektoronként titkosítja.</p> <p>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 hozzáférhetőek maradnak.</p>

	<p>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. Így 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.</p> <p>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 fájlrendszerével együtt, ha azok titkosítására korábban sor került.</p> <p>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.</p>
<p>Hordozható mód</p>	<p>Ez a jelölőnégyzet engedélyezi/letiltja a cserélhető meghajtók előkészítését, ami lehetővé teszi a cserélhető meghajtón lévő fájlokhoz való hozzáférést a vállalati hálózaton kívüli számítógépeken.</p> <p>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.</p> <p>A hordozható mód az Összes fájl titkosítása és a Csak az új fájlok titkosítása beállításához érhető el.</p>
<p>Csak a használt lemezterület titkosítása</p>	<p>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.</p> <p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a teljes meghajtó titkosítására sor kerül, ideértve a korábban törölt és módosított fájlok megmaradt töredékeit.</p> <p>A csak a foglalt terület titkosításának képessége kizárólag a Teljes cserélhető meghajtó titkosítása módban áll rendelkezésre.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>
<p>Titkosítási mód a kiválasztott eszközökhöz</p>	<p>Ez a táblázat azokat az eszközöket tartalmazza, amelyekhez egyéni visszafejtési szabályok vannak megadva. Lehetősége van létrehozni titkosítási szabályokat az egyes cserélhető meghajtókhoz a következő módokon:</p> <ul style="list-style-type: none"> • Adjon hozzá egy cserélhető meghajtót az Eszközfelügyelő megbízható eszközeinek listájáról.

	<ul style="list-style-type: none"> • Kézzel adjon hozzá cserélhető meghajtót: <ul style="list-style-type: none"> • Eszközazonosító alapján (hardverazonosító vagy HWID) • Eszközmodell alapján: gyártóazonosító (VID) és termékazonosító (PID)
Cserélhető meghajtók titkosításának engedélyezése offline módban	<p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem titkosítja a cserélhető meghajtókat, ha nincs kapcsolat a Kaspersky Security Centerrel.</p>
Hordozható mód jelszavának beállításai	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 jelteni 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.
- **Üzenet.** 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 házi rendben található általános megbízható zóna mellett létrehozhatják a kizárásokra és megbízható alkalmazásokra vonatkozó saját listájukat is.

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 jogszerű szoftverek részleteiért, amelyekkel a bűnözők károsíthatják a számítógépet vagy a személyes adatokat, keresse fel a [Kaspersky IT Encyclopedia webhelyet](#) ².

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:

- [Viselkedéselemzés.](#)
- [Biztonsági rések kihasználásának megelőzése.](#)
- [Behatolásmegelőző rendszer.](#)
- [Fájl védelem.](#)
- [Web védelem.](#)

- [Levelezés védelem.](#)
- [Vizsgálati feladatok.](#)

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 megvizsgálja a megnyitott, végrehajtott vagy bármilyen alkalmazásfolyamat által mentett objektumokat, és felügyeli az összes alkalmazás tevékenységét és az általuk generált hálózati forgalmat. A megbízható alkalmazások listájához hozzáadott alkalmazást azonban a Kaspersky Endpoint Security kizárja a vizsgálatokból.


Ha például úgy véli, hogy a szokásos Microsoft Windows Jegyzettömb alkalmazás vizsgálat nélkül is biztonságos, azaz megbízik ebben az alkalmazásban, akkor a Microsoft Windows Jegyzettömböt felveheti a megbízható alkalmazások listájára. Ekkor a vizsgálat kihagyja azokat az objektumokat, amelyeket ez az alkalmazás használ.

Ezenkívül bizonyos, a Kaspersky Endpoint Security által gyanúsként osztályzott műveletek számos alkalmazás funkcióinak kontextusában biztonságos lehet. A billentyűzetten begépelte 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 vizsgálatokból való kizárásával elkerülhetők a kompatibilitási ütközések a Kaspersky Endpoint Security és más programok között (pl. a hálózati forgalom kettős vizsgálata harmadik fél számítógépén a Kaspersky Endpoint Security alkalmazással és más víruskereső alkalmazással is), ezenkívül növeli a számítógép teljesítményét, ami kiszolgálók alkalmazásai esetén kritikus fontosságú lehet.

A megbízható alkalmazás végrehajtható fájljában és folyamatában ugyanakkor továbbra is sor kerül a vírusok és egyéb rosszindulatú programok jelenlétének vizsgálatára. Az alkalmazásokat a Kaspersky Endpoint Security vizsgálataiból teljes körűen vizsgálatból való kizárásokkal lehet kizárni.

Kizárások beállításai

Paraméter	Leírás
Észlelt objektumok típusai	<p>A megadott alkalmazásbeállításoktól függetlenül a Kaspersky Endpoint Security mindig észleli és blokkolja a vírusokat, férgeket és trójaiakat. Ezek jelentős károkat okozhatnak a számítógépen.</p> <ul style="list-style-type: none"> • Vírusok és férgek 

Alkategória: vírusok és férgek (Viruses_and_Worms)

Fenyegetési szint: 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 *felülíró* vírusok saját kódjukkal felülírják a fertőzött fájlt, így törölve annak tartalmát. A fertőzött fájl működése leáll, így nem lehet helyreállítani. A *parazita* vírusok csak módosítják a fájlokat, azokat teljesen vagy részlegesen működőképessé állapotban hagyva. A *társító* vírusok 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: *hivatkozásvírusok*, *OBJ-vírusok*, *LIB-vírusok*, *forráskódú* vírusok és számos egyéb.

Férgék

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.

		<p>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 megkezd a rosszindulatú műveleteket. Ezután megkezd lemásolni saját magát, újabb e-mail címek keresésébe kezd, és terjeszteni kezdi a fertőzött üzeneteket.</p>
IM-féreg	IM kliens férgek	<p>Azonnali üzenetküldőkön keresztül terjednek.</p> <p>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.</p>
IRC-féreg	Internetes csevegési férgek	<p>Ezek olyan internetes csevegő szolgáltatásokon keresztül terjednek, amelyek valós idejű kommunikációt biztosítanak az interneten keresztül.</p> <p>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.</p>
Hálózati féreg	Hálózati férgek	<p>Ezek a férgek számítógépes hálózatokon terjednek.</p> <p>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.</p>
P2P-féreg	Fájlcsere hálózati férgek	<p>Fájlcsere (Peer-to-Peer) hálózatokon keresztül terjednek.</p> <p>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.</p>

		A kifinomultabb férgek adott P2P-hálózat protokollját is képesek emulálni: ezek pozitív válaszokat küldenek a keresésekre, majd felajánlják saját másolataikat letöltésre.
Férgek	Egyéb típusú férgek	<p>Az egyéb típusú férgek a következők lehetnek:</p> <ul style="list-style-type: none"> • 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 megkísérik 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

Fenyegetési szint: 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, weboldalnak 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
Trójai 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.
Hátsó kapu	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.

Trójai	Trójai programok	<p>Ez a kategória az alábbi rosszindulatú alkalmazásokat tartalmazza:</p> <ul style="list-style-type: none"> • 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.
Váltságdíj-trójai	Váltságdíj trójai	<p>Ezek a felhasználó adatait „túszul ejtik”, módosítva vagy blokkolva azt, esetleg meggátolják a számítógép működését, hogy a felhasználó számára elveszenek az adatok. A betolakodó váltságdíjat követel a felhasználótól, azt ígérve, hogy küld egy alkalmazást, amellyel visszaállítható a számítógép normál állapota az elveszett adatokkal együtt.</p>
Trójai-kattintó	Trójai kattintók	<p>Ezek a felhasználó számítógépéről weboldalakat látogatnak meg, saját maguk utasítva a webböngészőt, vagy módosítva az operációs rendszer fájljaiban megadott webcímet.</p> <p>Az ilyen programokkal a betolakodó hálózati támadást indíthat, valamint webhelyek látogatottságát növelheti, hogy a reklámcsíkhirdetések megjelenítésének a száma növekedjen.</p>
Trójai-letöltő	Trójai-letöltők	<p>Ezek a betolakodó weboldaláról további</p>

		rosszindulatú alkalmazásokat töltenek le és telepítenek a felhasználó számítógépére. A letöltendő rosszindulatú alkalmazás fájlnevét tartalmazhatják, illetve megkaphatják a meglátogatott weboldalról is.
Trójaitelepítő	Trójaitelepítők	<p>Más trójai programokat tartalmaznak, melyeket a számítógép merevlemezére mentenek, majd telepítenek.</p> <p>A betolakodók a telepítő típusú trójai programokat az alábbi célokból használhatják:</p> <ul style="list-style-type: none"> • 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.
Trójai-értesítő	Trójai-értesítők	<p>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.</p> <p>Ezek a programok gyakran több trójai programból álló programcsomag részét képezik. Ezek értesítik a betolakodót a többi trójai program sikeres telepítéséről.</p>
Trójai-proxy	Trójai-proxyk	Segítségükkel a betolakodó névtelenül érhet el weboldalakat a felhasználó számítógépéről; gyakran

		alkalmazzák őket levélszemét küldésére.
Trójai-PSW	Jelszólopó programok	<p>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.</p> <p>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).</p>
Trójai-kém	Trójai-kémek	<p>Ezek kémkednek a felhasználó után, információkat gyűjtenek az általa a számítógépen végzett műveletekről. Eltéríthetik a felhasználó által a billentyűzeten begépelte 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.</p>
Trójai-DDoS	Trójai hálózattámadók	<p>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</p>

		<p>párhuzamos támadást indíthassanak egyetlen kiszolgáló ellen.</p> <p>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.</p>
Trójai-IM	Azonnali üzenetküldő ügyfelek felhasználótól adatokat lopó trójai programok	Ellopják az azonnali üzenetküldők felhasználóinak számlaszámait és jelszavait. Az információkat eljuttatják a betolakodónak e-mail, FTP útján, a weboldalt 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.
Trójai-SMS	SMS-üzenetek formájában megjelenő trójai programok	Ezek mobiltelefonokat fertőznek meg, SMS-üzeneteket küldve fizetős telefonszámokra.
Trójai GameThief	Online játékok felhasználótól adatokat lopó trójai programok	Ezek online játékok résztvevőitől lopnak fiókbejelentkezéseket, aztán eljuttatják a betolakodónak e-mailben, FTP-n, a weboldala meglátogatásával vagy más módon.
Trójai bankár	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.
Trójai 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
Konstruktor	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).
Biztonsági rés	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” weboldalnak.

		<p>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.</p> <p>A hálózati férgek a hálózaton exploitok segítségével terjednek. A <i>Nuker</i> exploitok számítógépeket leállító hálózati csomagok.</p>
Fájltitkosító	Titkosítók	Ezek más rosszindulatú alkalmazásokat titkosítanak, hogy elrejtse azokat a víruskereső alkalmazások elől.
Elárasztó	Hálózatokat „szennyező” programok	<p>Ezek nagy mennyiségű üzenetet küldenek hálózati csatornákon. Az ilyen eszközök között található az internetes csevegéseket szennyező programok is.</p> <p>Az elárasztó eszközök nem tartalmazzák 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.</p>
HackTool	Hackelő eszközök	<p>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 elrejtve 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.</p>

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.
Hamisító	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 elrejtsek azokat víruskereső alkalmazások előtt.
E-mail-elárasztó	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-elárasztó	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-elárasztó	A forgalmat SMS üzenetekkel „szennyező” programok	Ezek nagy mennyiségű SMS-üzenetet küldenek a mobiltelefonra.

- [Reklámprogram](#) 

Alkategória: hirdetési szoftver (reklámprogram);

Fenyegetési szint: 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: jogszerű szoftverek, amelyekkel a bűnözők károsíthatják a számítógépét vagy személyes adatait

Veszély szintje: közepes

A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetnek 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
Kliens 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.
Tárcsázó	Autotárcsázók	Ezek modemen keresztül rejtve hoznak létre kapcsolatot.
Letöltő	Letöltéshez használható programok	Ezek rejtve töltenek le fájlokat különböző weboldalokról.
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

		<p>monitorozása és felügyelése céljából. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal: a távoli számítógép monitorozása és felügyelete céljából.</p> <p>A legális távfelügyeleti programok különböznek a hátsó kapu típusú trójai távfelügyeleti programoktól. A trójai programok jellegzetessége, hogy függetlenül bejutnak az operációs rendszerbe, és magukat fellepipítik; a jogszerű programok nem rendelkeznek ilyen funkcióval.</p>
Kiszolgáló FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Kiszolgáló proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Kiszolgáló Telnet	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Kiszolgáló Web	Web kiszolgálók	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 rejtetheti el, és aktív folyamatokat állíthat le.
NetTool	Hálózati eszközök	A felhasználó számára

		<p>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.</p>
Kliens P2P	P2P-hálózati kliensek	<p>Segítségükkel a felhasználó fájlcsere (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.</p>
Kliens SMTP	SMTP-kliensek	<p>E-mail üzeneteket küldenek a felhasználó tudta nélkül. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.</p>
WebToolbar	Webes eszköztárak	<p>Ezek eszköztárakkal egészítik ki más alkalmazások kezelőfelületeit, keresőmotorok elérését megkönnyítve.</p>
FraudTool	Pszudoprogramok	<p>Ezek más programoknak adják ki magukat. Lehetnek például pszeudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.</p>

- [Egyéb olyan szoftverek észlése, amelyekkel a behatolók károsíthatják a számítógépét vagy személyes adatait](#) 

Alkategória: jogszerű szoftverek, amelyekkel a bűnözők károsíthatják a számítógépét vagy személyes adatait

Veszély szintje: közepes

A legtöbb ilyen alkalmazás hasznos, így a legtöbb felhasználó igénybe veszi őket. Ezek az alkalmazások lehetnek 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
Kliens 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.
Tárcsázó	Autotárcsázók	Ezek modemen keresztül rejtve hoznak létre kapcsolatot.
Letöltő	Letöltéshez használható programok	Ezek rejtve töltenek le fájlokat különböző weboldalokról.
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

		<p>monitorozása és felügyelése céljából. A betolakodók titokban telepítik ezeket a felhasználó számítógépére ugyanilyen céllal: a távoli számítógép monitorozása és felügyelete céljából.</p> <p>A legális távfelügyeleti programok különböznek a hátsó kapu típusú trójai távfelügyeleti programoktól. A trójai programok jellegzetessége, hogy függetlenül bejutnak az operációs rendszerbe, és magukat fellepipítik; a jogszerű programok nem rendelkeznek ilyen funkcióval.</p>
Kiszolgáló FTP	FTP-kiszolgálók	Ezek FTP-kiszolgálóként funkcionálnak. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy FTP-n keresztül távoli elérést nyissanak hozzá.
Kiszolgáló proxy	Proxykiszolgálók	Ezek proxykiszolgálóként funkcionálnak. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.
Kiszolgáló Telnet	Telnet-kiszolgálók	Ezek Telnet kiszolgálóként működnek. A betolakodók ezeket azért telepítik a felhasználó számítógépére, hogy Telneten keresztül távoli elérést nyissanak hozzá.
Kiszolgáló Web	Web kiszolgálók	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 rejtetheti el, és aktív folyamatokat állíthat le.
NetTool	Hálózati eszközök	A felhasználó számára

		<p>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.</p>
Kliens P2P	P2P-hálózati kliensek	<p>Segítségükkel a felhasználó fájlcsere (Peer-to-Peer) hálózatokon dolgozhat. A betolakodó rosszindulatú programok terjesztésére használhatja.</p>
Kliens SMTP	SMTP-kliensek	<p>E-mail üzeneteket küldenek a felhasználó tudta nélkül. A betolakodó azért telepíti a felhasználó számítógépére, hogy a nevében kéretlen leveleket küldjön.</p>
WebToolbar	Webes eszköztárak	<p>Ezek eszköztárakkal egészítik ki más alkalmazások kezelőfelületeit, keresőmotorok elérését megkönnyítve.</p>
FraudTool	Pszudoprogramok	<p>Ezek más programoknak adják ki magukat. Lehetnek például pszeudovírusirtók, amelyek képernyőüzeneten közlik, hogy rosszindulatú programot észleltek. Valójában azonban nem találnak és nem vírusmentesítenek semmit.</p>

- [Csomagolt objektumok, melyek tömörítése felhasználható károkozásra képes kód védelmére](#) 

A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található csomagolt objektumokat és az önkicsomagoló modult is ellenőrzi.

A veszélyes programoknak a víruskereső alkalmazások elől való elrejtéséhez a betolakodók különleges csomagolók segítségével tömörítik azokat, vagy többszörösen tömörített fájlokat hoznak létre.

A Kaspersky víruselemzői azonosították a hackerek által leggyakrabban alkalmazott tömörítőprogramokat.

Ha a Kaspersky Endpoint Security egy fájlban ilyen tömörítőt talál, az nagy valószínűséggel rosszindulatú alkalmazást vagy olyan alkalmazást tartalmaz, amelyet a betolakodó a számítógép vagy az adatok ellen felhasználhat.

A Kaspersky Endpoint Security az alábbi programokat választja ki:

- *Esetleg kárt okozó csomagolt fájlok* – rosszindulatú programok, például vírusok, férgek és trójaiak becsomagolására kerülnek használatra.
- *Többszörösen csomagolt fájlok* (közepes fenyegetettségi szint) – a fájl háromszorosan be van csomagolva egy vagy több tömörített fájlba.

• [Többszörösen csomagolt objektumok](#)

A Kaspersky Endpoint Security az SFX (önkicsomagoló) archívumokban található csomagolt objektumokat és az önkicsomagoló modult is ellenőrzi.

A veszélyes programoknak a víruskereső alkalmazások elől való elrejtéséhez a betolakodók különleges csomagolók segítségével tömörítik azokat, vagy többszörösen tömörített fájlokat hoznak létre.

A Kaspersky víruselemzői azonosították a hackerek által leggyakrabban alkalmazott tömörítőprogramokat.

Ha a Kaspersky Endpoint Security egy fájlban ilyen tömörítőt talál, az nagy valószínűséggel rosszindulatú alkalmazást vagy olyan alkalmazást tartalmaz, amelyet a betolakodó a számítógép vagy az adatok ellen felhasználhat.

A Kaspersky Endpoint Security az alábbi programokat választja ki:

- *Esetleg kárt okozó csomagolt fájlok* – rosszindulatú programok, például vírusok, férgek és trójaiak becsomagolására kerülnek használatra.
- *Többszörösen csomagolt fájlok* (közepes fenyegetettségi szint) – a fájl háromszorosan be van csomagolva egy vagy több tömörített fájlba.

Kizárások

Ez a táblázat a vizsgálati kizárásokkal kapcsolatos adatokat tartalmaz.

A következő módszerekkel kizárhat objektumokat a vizsgálat alól:

- A fájl vagy mappa elérési útjának megadása.
- Az objektum ellenőrzőösszeg megadása.
- maszkok használata:

	<ul style="list-style-type: none"> • 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 minden olyan TXT kiterjesztésű fájlhoz vezető útvonalat magába foglal, mely a Mappa nevű mappában és az almappáiban található. 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. • Adja meg az objektumtípus nevét a Kaspersky Encyclopedia osztályozási rendszerének megfelelően (például e-mail-féreg, 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.
<p>Megbízható alkalmazások</p>	<p>Ebben a táblázatban azoknak a megbízható alkalmazásoknak a listája található, amelyeknek a tevékenységét a Kaspersky Endpoint Security működése közben nem figyeli.</p> <p>Az Alkalmazásfelügyelő összetevő szabályozza az egyes alkalmazások elindulását, függetlenül attól, hogy az adott alkalmazás szerepel-e a megbízható alkalmazások listáján.</p>
<p>Értékek egyesítése örökléskor</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Ha a gyermek- és szülőházirend listák elemei egyeznek, ezek az elemek a szülőházirend ugyanazon elemeként jelennek meg.</p> <p>Ha a jelölőnégyzet nincs bejelölve, akkor a lista elemeit nem egyesíti a rendszer, amikor a Kaspersky Security Center házirendek beállításainak öröklése zajlik.</p>
<p>Helyi kizárások használatának engedélyezése/Helyi megbízható</p>	<p><i>Helyi kizárások és helyi megbízható alkalmazások (helyi megbízható zóna)</i> – 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</p>

<p>alkalmazások használatának engedélyezése</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>alkalmazásokat. Így a felhasználók a házirendben található általános megbízható zóna mellett létrehozhatják a kizárásokra és megbízható alkalmazásokra vonatkozó saját listájukat is.</p> <p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a felhasználó csak a házirendben létrehozott vizsgálati kizárások általános listájához és megbízható alkalmazások általános listájához férhet hozzá. Ha helyi listákat hoztak létre, a funkció letiltása után a Kaspersky Endpoint Security továbbra is kizárja a felsorolt objektumokat a vizsgálatokból.</p>
<p>Megbízható rendszertanúsítvány tárhelye</p>	<p>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 <i>Megbízható</i> csoporthoz.</p> <p>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.</p>

Alkalmazásbeállítások

A következő általános beállításokat adhatja meg az alkalmazáshoz:

- Működési mód
- Önvédelem
- Teljesítmény
- Hibakeresési adatok
- A számítógép állapota a beállítások alkalmazásakor

Alkalmazásbeállítások

Paraméter	Leírás
<p>A Kaspersky Endpoint Security for Windows indítása a számítógép bekapcsolásával egy időben</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security az operációs rendszer betöltését követően elindul, és a teljes munkamenet során védi a számítógépet.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem indul el az operációs rendszer indításakor, amíg a felhasználó kézikézik el nem indítja. A számítógép védelme le van tiltva, és a felhasználói adatok fenyegetéseknek lehetnek kitéve.</p>
<p>Fejlett vírusmentesítő technológia használata (jelentős számítógépes erőforrásokat igényel)</p>	<p>Ha a jelölőnégyzet be van jelölve, a képernyőn előugró értesítés jelenik meg, ha az operációs rendszerben rosszindulatú tevékenység észlelhető. Az értesítésben a Kaspersky Endpoint Security felajánlja a számítógép Fejlett vírusmentesítésének elvégzését. Miután a felhasználó jóváhagyja az eljárást, a</p>

	<p>Kaspersky Endpoint Security semlegesíti a fenyegetést. A fejlett vírusmentesítési eljárás végeztével a Kaspersky Endpoint Security újraindítja a számítógépet. A fejlett vírusmentesítő technológia jelentős számítógépes erőforrásokat vesz igénybe, amitől a többi alkalmazás lelassulhat.</p> <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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 a felhasználó 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 <i>Vírusvizsgálat</i> feladat beállításában. Ezután el kell indítania a <i>Vírusvizsgálat</i> feladatot.</p> </div>
<p>A Kaspersky Security Center használata proxykiszolgálóként az aktiváláshoz</p> <p><i>(csak a Kaspersky Security Center konzolon érhető el)</i></p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Security Center felügyeleti kiszolgáló proxykiszolgálóként szolgál az alkalmazás aktiválásakor.</p>
<p>Önvédelem engedélyezése</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security megakadályozza a merevlemezen lévő alkalmazásfájlok, a memóriafolyamatok és a beállításjegyzék bejegyzései módosítását és törlését.</p>
<p>A Kaspersky Endpoint Security beállításainak távoli vezérlőalkalmazásokból való kezelésének engedélyezése</p>	<p>Ha a jelölőnégyzet be van jelölve, a megbízható távoli adminisztrációs alkalmazások (mint a TeamViewer, a LogMeIn Pro vagy a Remotely Anywhere) módosíthatják a Kaspersky Endpoint Security beállításait.</p> <p>A nem megbízható távoli adminisztrációs alkalmazások akkor sem módosíthatják a Kaspersky Endpoint Security beállításait, ha a jelölőnégyzet be van jelölve.</p>
<p>Külső szolgáltatásvezérlés engedélyezése</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security engedélyezi a távoli számítógépekről az alkalmazásslolgáltatások kezelését. Az alkalmazásslolgáltatások távoli kezelésére tett kísérlet esetén a Microsoft Windows tálcán az alkalmazás ikonja fölött értesítés jelenik meg (kivéve, ha az értesítési szolgáltatást a felhasználó letiltotta).</p>
<p>Ütemezett feladatok elhalasztása, amíg a számítógép akkumulátorról üzemel</p>	<p>Ha a jelölőnégyzet be van jelölve, az energiatakarékos mód engedélyezett. A Kaspersky Endpoint Security elhalasztja az ütemezett feladatokat. Szükség esetén kézzel indíthatja el a vizsgálati és frissítési feladatokat.</p>
<p>Erőforrások adása más alkalmazásoknak</p>	<p>Amikor a Kaspersky Endpoint Security ütemezett feladatokat futtat, a CPU és a lemez alrendszer terhelése megnőhet, ami lelassítja a többi alkalmazás teljesítményét.</p> <p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security felfüggeszti az ütemezett feladatokat, ha megnövekedett terhelést észlel, és felszabadítja az operációs rendszer erőforrásait a felhasználói alkalmazások számára.</p>
<p>Memóriakép írásának engedélyezése</p>	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security</p>

	<p>összeomláskor kiíratási fájlt ír.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem ír kiíratási fájlt. Az alkalmazás a számítógép merevlemezén található kiíratási fájlokat is törli.</p>
<p>Kiíratási és nyomkövetési fájlok védelmének engedélyezése</p>	<p>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.</p> <p>Ha a jelölőnégyzet nincs bejelölve, bármely felhasználó hozzáférhet a kiíratási és nyomkövetési fájlokhoz.</p>
<p>A számítógép állapota a beállítások alkalmazásakor (csak a Kaspersky Security Center konzolon érhető el)</p>	<p>A Kaspersky Endpoint Security alkalmazást telepített ügyfélszámítógépek állapotának megjelenítésének beállításai a Webfelügyelőben, ha hiba lép fel a rendszabály alkalmazása vagy feladat végrehajtása közben. Az <i>OK</i>, <i>Figyelmeztetés</i> és a <i>Kritikus</i> állapotok érhetőek el</p>

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\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 másolatait különleges formátumban vannak tárolva, és nem jelentenek fenyegetést.

A fájlok biztonsági másolatait a C:\ProgramData\Kaspersky Lab\KES\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, ahová a vírusokkal vagy nem fertőtleníthető fájlokkal fertőzött fájlokat helyezi át az alkalmazás. A karanténba helyezett fájlok titkosított állapotban vannak tárolva, és nem veszélyeztetik a készülék biztonságát. A Kaspersky Endpoint Security csak akkor használja a Karantént, ha a Kaspersky Sandbox és a Kaspersky Endpoint Detection and Response megoldásokkal dolgozik együtt. Más esetekben a Kaspersky Endpoint Security a megfelelő fájlt a [Biztonsági mentésbe](#) helyezi. A megoldások részeként a karantén kezelésével kapcsolatos részletekért lásd a [Kaspersky Sandbox súgót](#), a [Kaspersky Endpoint Detection and Response Optimum súgót](#) és a [Kaspersky Endpoint Detection and Response Expert 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
Jelentések tárolása legfeljebb ennyi ideig N nap	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 jelentésfájlból lévő legrégebbi bejegyzéseket.
Jelentésfájl méretének korlátozása N MB-ra	Ha a jelölőnégyzet be van jelölve, a maximális jelentésfájlméretet a megadott érték korlátozza. Alapértelmezés szerint a maximális fájl méret 1024 MB. A jelentésfájlok maximális méretének túllépését elkerülendő a Kaspersky Endpoint Security automatikusan törli a jelentésfájlok legrégebbi bejegyzéseit a maximális méret elérésekor.
Objektumok tárolása legfeljebb ennyi ideig N nap	Ha a jelölőnégyzet be van jelölve, a maximális fájl tárolási időtartamot a meghatározott időintervallum korlátozza. A fájlok maximális tárolási időtartama alapértelmezett esetben 30 nap. A maximális tárolási időtartam lejáratát követően a Kaspersky Endpoint Security törli a legrégebbi fájlokat a Biztonsági mentésből.
Limit the size of Backup to N MB-ra	Ha a jelölőnégyzet be van jelölve, a maximális tárhelyet a meghatározott érték korlátozza. Alapértelmezés szerint a maximális méret 100 MB. A tárhely maximális méretének túllépését elkerülve a Kaspersky Endpoint Security automatikusan törli a tárhely legrégebbi fájljait a maximális méret elérésekor.
A karantén méretének korlátozása: N MB <i>(csak a Web Console-ban érhető el)</i>	Maximális karanténméret MB-ban. Például beállíthatja a maximális karanténméretet 200 MB-ra. Amikor a karantén eléri a maximális méretet, a Kaspersky Endpoint Security elküldi a megfelelő 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.
Értesítés, ha a karanténtár mérete N százalékhoz ér <i>(csak a Web Console-ban érhető el)</i>	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.
Adatátvitel az adminisztrációs kiszolgálóra	Az események kategóriája az ügyfélszámítógépen, amik információit el kell küldeni az Adminisztrációs kiszolgálóra.

(csak a
Kaspersky
Security
Centeren
érhető el)

Hálózati beállítások

Megadhatja az internethez való csatlakozáshoz és az antivírus adatbázisok frissítéséhez használt proxykiszolgálót, kiválaszthatja a hálózati port figyelő módját, megadhat titkosítottkapcsolat-vizsgálatokat.

Hálózati opciók

Paraméter	Leírás
Forgalom csökkentése díjköteles kapcsolatoknál	<p>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.</p> <p>A Költségtudatos hálózati figyelés a Windows 8 vagy újabb rendszert futtató számítógépeken működik.</p>
Szkript beillesztése a webforgalomba a weboldallal való interakcióhoz	<p>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.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"><p>A Kaspersky szakértői azt javasolják, hogy a Webfigyelő helyes működésének biztosítása érdekében injektálja be a weboldal-interakciós parancsfájlt a forgalomba.</p></div>
Proxykiszolgáló	<p>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.</p> <p>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, a Kaspersky Endpoint Security a Microsoft Internet Explorer böngészőbeállításában megadott proxykiszolgáló címét használja fel.</p>
Proxykiszolgáló kihagyása helyi címek esetén	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security nem használ proxykiszolgálót megosztott mappából történő frissítéshez.</p>
Figyelt portok	<p>Minden hálózati port figyelése. Ebben a hálózati portmegfigyelési módban a védelmi összetevők (Fájl védelem, Web védelem, Levelezés védelem) a számítógép minden nyitott hálózati portján továbbított adatfolyamot figyelnek.</p> <p>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.</p>

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 kapcsolat 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 Fájlfédelem, a Levelezés védelem vagy a Webfelügyelő összetevő ezt kéri.
- **Mindig vizsgálja a titkosított kapcsolatokat.** A Kaspersky Endpoint Security akkor is vizsgálja 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.

Nem megbízható tanúsítvánnyal rendelkező tartomány meglátogatása esetén

- **Engedélyezés.** Ha ez az opció van kijelölve, akkor 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. 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.

	<p>Kapcsolat blokkolása. Ha ez az opció van kijelölve, akkor 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.</p>
<p>Ha a titkosított kapcsolat vizsgálatakor hiba lép fel</p>	<ul style="list-style-type: none"> • Kapcsolat blokkolása. Ha ez az elem van kijelölve, és egy titkosított kapcsolat vizsgálata közben hiba történik, akkor a Kaspersky Endpoint Security blokkolja a hálózati kapcsolatot. • Tartomány hozzáadása a kizárásokhoz Ha ez az elem van kijelölve, és egy titkosított kapcsolat vizsgálata közben hiba történik, akkor a Kaspersky Endpoint Security hozzáadja a hibát okozó tartományt a tartományok vizsgálati hibákkal listájához, és nem figyeli a titkosított hálózati forgalmat ennek a tartománynak a felkeresésekor. Azoknak a tartományoknak a listáját, amelyeknél a titkosított kapcsolatok vizsgálata során hiba jelentkezett, csak az alkalmazás helyi felületén lehet megtekinteni. A lista törléséhez ki kell választania a Kapcsolat blokkolása lehetőséget.
<p>SSL 2.0 kapcsolatok blokkolása (ajánlott)</p>	<p>Ha a jelölőnégyzet be van jelölve, akkor a Kaspersky Endpoint Security blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat.</p> <p>Ha a jelölőnégyzet nincs bejelölve, akkor a Kaspersky Endpoint Security nem blokkolja az SSL 2.0 protokollon keresztül létrehozott hálózati kapcsolatokat, és nem figyeli kapcsolatokon keresztül küldött hálózati forgalmat.</p>
<p>Titkosított kapcsolatok visszafejtése EV-tanúsítványt használó webhelyeken</p>	<p>Az EV-tanúsítványok (Extended Validation Certificates) 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.</p> <p>Ha van jelölés ebben a jelölőnégyzetben, a Kaspersky Endpoint Security visszafejti és figyeli az EV-tanúsítványt használó rendelkező webhelyeket.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem fér hozzá a HTTPS-forgalom tartalmához. Ezen okokból az alkalmazás csak a webcím alapján figyeli meg a HTTPS-forgalmat, például: <code>https://google.com</code>.</p> <p>Ha először nyit meg egy EV-tanúsítvánnyal rendelkező weboldalt, a titkosított kapcsolat attól függetlenül vissza lesz fejtve, hogy Ön kijelölte-e a jelölőnégyzetet.</p>
<p>Megbízható címek</p>	<p>Olyan webcímeknek a listáját használja, amelyeknél a Kaspersky Endpoint Security nem vizsgálja a hálózati kapcsolatokat. Megadhat egy tartománynevet vagy egy IP-címet. A Kaspersky Endpoint Security támogatja a * karaktert maszk megadásához a tartománynévben.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>A Kaspersky Endpoint Security nem támogatja a IP-címmaszkokat. Az alkalmazás helyi felületén megadhat egy IP-címtartományt (például 198.51.100.0/24). A Kaspersky Security Center konzolban nem adhat meg IP-címtartományt.</p> </div> <p>Példák:</p> <ul style="list-style-type: none"> • <code>domain.com</code> – a rekord a következő címeket tartalmazza: <code>https://domain.com</code>, <code>https://www.domain.com</code>, <code>https://domain.com/page123</code>. A rekord nem tartalmaz altartományt (pl. <code>subdomain.domain.com</code>).

	<ul style="list-style-type: none"> • <code>subdomain.domain.com</code> – a rekord a következő címeket tartalmazza: https://subdomain.domain.com, https://subdomain.domain.com/page123. A rekord nem tartalmaz <code>domain.com</code> tartományt. • <code>*.domain.com</code> – a rekord a következő címeket tartalmazza: https://movies.domain.com, https://images.domain.com/page123. A rekord nem tartalmaz <code>domain.com</code> tartományt.
Megbízható alkalmazások	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 <code>*</code> és <code>?</code> karaktereket egy maszk megadásakor.
Használja a kiválasztott tanúsítványtárolót a titkosított kapcsolatok vizsgálatához a Mozilla-alkalmazásokban <i>(csak a Kaspersky Endpoint Security felületen érhető el)</i>	<p>Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security megvizsgálja a titkosított forgalmat a Mozilla Firefox böngészőben és a Thunderbird levelezőprogramban. Néhány webhely HTTPS-protokollon keresztüli elérése blokkolva lehet.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>A Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmának vizsgálatához engedélyeznie kell a Titkosított kapcsolatok vizsgálatát. Ha a Titkosított kapcsolatok vizsgálata le van tiltva, a Kaspersky Endpoint Security nem vizsgálja a Mozilla Firefox böngésző és a Thunderbird levelezőprogram forgalmát.</p> </div> <p>A Kaspersky Endpoint Security a Kaspersky főtanúsítványát használja a titkosított forgalom visszafejtésére és elemzésére. Kiválaszthatja azt a tanúsítványtárolót, amely a Kaspersky főtanúsítványt tartalmazza.</p> <ul style="list-style-type: none"> • Windows tanúsítványtároló használata (ajánlott). A Kaspersky főtanúsítvány bekerül ebbe a tárolóba a Kaspersky Endpoint Security telepítése során. • Mozilla tanúsítványtároló használata. 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 beállításában.

Felület

Megadhatja az alkalmazás felületének beállításait.

Felület beállítások

Paraméter	Leírás
Interakció a felhasználóval	<p>With simplified interface. 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 értesítéseket is megjelenít az alkalmazásikon felett.</p>

<p>(csak a Kaspersky Security Center konzolon érhető el)</p>	<p>Teljes felületen. 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 alkalmazásokon felett.</p> <p>Az Alkalmazástevékenység-figyelő szakaszának elrejtése. Az ügyfélszámítógépen a Kaspersky Endpoint Security főablakában az Alkalmazástevékenység-figyelő gombja nem érhető el. Az <i>Alkalmazástevékenység-figyelő</i> egy olyan eszköz, amellyel valós időben tekinthetők meg a felhasználó számítógépén futó alkalmazások tevékenységével kapcsolatos információk.</p> <p>No interface. Az ügyfélszámítógépen nincs jelen a Kaspersky Endpoint Security működésének. A Windows értesítési sávon lévő ikon és az értesítések nem érhetőek el.</p>
<p>Értesítési beállítások</p>	<p>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.</p>
<p>E-mail értesítési beállítások</p>	<p>Az SMTP szerver beállításai az alkalmazás működése során regisztrált események értesítéseinek biztosításához.</p>
<p>Az alkalmazás állapotának megjelenítése az értesítési területen</p>	<p>Alkalmazásesemények kategóriája, amik miatt a Kaspersky Endpoint Security ikon megváltozott a Microsoft Windows feladatsáv értesítési területén (🔔 vagy 📧), előbukkanó értesítést eredményezve.</p>
<p>Helyi vírusadatbázis állapotáról szóló értesítések</p>	<p>Az alkalmazás által használt elavult antivírus adatbázisok értesítéseinek beállításai.</p>
<p>Jelszóvédelem</p>	<p>Ha a kapcsológomb be van kapcsolva, a Kaspersky Endpoint Security jelszót kér a felhasználtól, 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.</p> <p>A Jelszóvédelem engedélyezése után a Kaspersky Endpoint Security egy jelszó megadását kéri a műveletek végrehajtásához.</p>
<p>Technical Support web resources</p> <p>(csak a Kaspersky Security Center konzolon érhető el)</p>	<p>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.</p>
<p>Message to user</p>	<p>Az üzenet, ami a Kaspersky Endpoint Security Támogatás ablakában jelenik meg.</p>

(csak a Kaspersky Security Center konzolon érhető el)

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 Center 12-n keresztül telepíti egy [telepítőcsomaggal](#). Az alapértelmezett beállításokat bármikor visszaállíthatja.

Az alkalmazáskonfigurációs kezelési beállítások csak a Kaspersky Endpoint Security felületen érhetőek 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	Bármikor visszatérhet az Endpoint Security alkalmazás Kaspersky által ajánlott beállításaihoz. 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.

A rendszeres frissítéshez működő licenc szükséges. Ha nincs aktuális licence, csak egyetlen alkalommal végezhet frissítést.

A Kaspersky Endpoint Security fő frissítésforrását a Kaspersky frissítéskiszolgálói jelentik.

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 elfogadják 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.

Az alkalmazásmodulok frissítéseivel együtt a helyi súgófájlok is frissülhetnek.

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.

Alkalmazásmodul- és adatbázis-frissítési beállítások

Paraméter	Leírás
Adatbázis-frissítés ütemezése	<p>Automatikus. Ebben a módban a Kaspersky Endpoint Security 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.</p> <p>Manually. A frissítési feladatok ezen futásmódjában a frissítési feladatokat manuálisan lehet elindítani.</p> <p>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 kézilleg is elindítható.</p>
Kihagyott feladatok futtatása	<p>Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a kihagyott frissítési feladatot azonnal elindítja, amint lehetségessé válik. A frissítési feladat például akkor hagyható ki, ha a számítógép a frissítési feladat indítási időpontjában ki volt kapcsolva.</p> <p>Ha a jelölőnégyzet nincs bejelölve, a Kaspersky Endpoint Security nem indítja el a kihagyott frissítési feladatokat. Ehelyett a következő frissítési feladatot a jelenlegi ütemezésnek megfelelően futtatja.</p>
Frissítésforrás	<p>A <i>frissítésforrás</i> a Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítéseit tartalmazó erőforrás.</p>

A frissítési források közé a Kaspersky Security Center kiszolgálója, a Kaspersky frissítési kiszolgálói, valamint hálózati vagy helyi mappák tartoznak.

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.

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. A Kaspersky Endpoint Security beállításában megadhat egy olyan felhasználót, aki rendelkezik ezekkel a jogosultságokkal, és a Kaspersky Endpoint Security frissítési feladatát elindíthatja ennek a felhasználói fióknak a nevében.

Alkalmazásmodulok frissítéseinek letöltése

Ez a jelölőnégyzet engedélyezi/letiltja az alkalmazásmodulok frissítéseinek letöltését a víruskereső adatbázis frissítéseivel együtt.

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 licen szerződés feltételeit, akkor az alkalmazás csak ennek megtörténte után telepíti a frissítéseket.

Alapértelmezésben a négyzet be van jelölve.

Frissítések

Ha ez a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a frissítési

másolása mappába	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\Update distribution\.
Frissítési proxykiszolgáló <i>(csak a Kaspersky Endpoint Security felületen érhető el)</i>	<p>A kliensszámítógépek felhasználóinak internet-hozzáférése vonatkozó proxykiszolgáló-beállítások az alkalmazásmodulok és adatbázisok frissítéséhez.</p> <p>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, a Kaspersky Endpoint Security a Microsoft Internet Explorer böngészőbeállításáiban megadott proxykiszolgáló címét használja fel.</p>
Proxykiszolgáló kihagyása helyi címek esetén <i>(csak a Kaspersky Endpoint Security felületen érhető el)</i>	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 fájllokba beépített szkript

wsh – Microsoft Windows Script Host fájl

wsf – Microsoft Windows szkript

the – Microsoft Windows 95 asztali háttérkép-fájl

hlp – Win súgó fájl

eml – Microsoft Outlook Express e-mail üzenet

nws – új Microsoft Outlook Express e-mail üzenet

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, xslm 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 fájlformátumok

Megjegyzés: előfordulhat, hogy egy fájl tényleges formátuma nem egyezik a fájlnev 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 fájllokba beépített szkript

wsh – Microsoft Windows Script Host fájl

wsf – Microsoft Windows szkript

the – Microsoft Windows 95 asztali háttérkép-fájl

hlp – Win súgó fájl

eml – Microsoft Outlook Express e-mail üzenet

nws – új Microsoft Outlook Express e-mail üzenet

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, xslm 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 a következő hálózati beállításokat használja a külső szolgáltatásokkal való interakcióhoz.

Hálózati beállítások

Cím	Leírás
activation- v2.kaspersky.com/activation-service/activation-service.svc Protokoll: HTTPS Port: 443	Alkalmazás aktiválása
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	Adatbázisok és alkalmazásmodulok frissítése

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

downloads.upd.kaspersky.com

Protokoll: HTTPS

Port: 443

- Adatbázisok és alkalmazásmodulok frissítése
- Annak ellenőrzése, hogy a Kaspersky-kiszolgálók elérhetőek-e. 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).

	<p>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.</p>
<p>touch.kaspersky.com Protokoll: HTTP</p>	<ul style="list-style-type: none"> • Megbízható idő fogadása a tanúsítvány érvényességi idejének ellenőrzéséhez (TLS-kapcsolat). • Figyelmeztetés webes erőforráshoz való hozzáférés megtagadásáról a böngészőben (Web védelem és Webfelügyelő)
<p>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</p>	<p>Adatbázisok és alkalmazásmodulok frissítése</p>

<p>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</p> <p>Protokoll: HTTP Port: 80</p>	
<p>ds.kaspersky.com</p> <p>Protokoll: HTTPS Port: 443</p>	A Kaspersky Security Network használata.
<p>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</p> <p>Protokoll: Any Port: 443, 1443</p>	A Kaspersky Security Network használata.
<p>click.kaspersky.com redirect.kaspersky.com</p> <p>Protokoll: HTTPS</p>	Kövesse a felület hivatkozásait
<p>cr1.kaspersky.com ocsp.kaspersky.com</p> <p>Protokoll: HTTP Port: 80</p>	Public Key Infrastructure (PKI)

6. melléklet Alkalmazásesemények a Windows eseménynaplójában

A Kaspersky Endpoint Security egyes összetevőinek működésére, az adattitkosítási eseményekre, az egyes vizsgálati feladatok, frissítési feladatok és integritás-ellenőrzési feladatok teljesítményére, valamint az alkalmazás általános működésére vonatkozó információk bekerülnek a Windows eseménynaplójába.

[Rendszer-felülvizsgálat](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
201		Végfelhasználói licencszerződés megsértve.	✓
203		A licenc majdnem lejárt.	–
206		Hiányoznak vagy sérültek az adatbázisok.	–
207		Az adatbázisok rendkívül elavultak.	–
209		Az alkalmazás automatikus indítása le van tiltva.	–
229		Aktiválási hiba.	✓
231		Aktív fenyegetés észlelve. El kell indítani a Fejlett vírusmentesítést.	✓
2023		A KSN kiszolgálói nem érhetőek el.	–
343		Nincs elegendő hely a karanténként szolgáló tárhelyen.	✓
346		Karanténból nem visszaállított objektum.	✓
348		Karanténból nem törölt objektum.	✓
212		A feladat nem hajtható végre.	–
237		Az alkalmazás összeomlott az előző munkamenetben.	✓
204		A licenc hamarosan lejár.	–
208		Az adatbázisok elavultak.	–
210		Az automatikus frissítések le vannak tiltva.	–
211		Az Önvédelem le van tiltva.	–
214		A védelem összetevői le vannak tiltva.	–
215		A számítógép csökkentett módban működik.	–
216		Feldolgozatlan fájlok találhatóak.	–
219		Csoportházirend alkalmazva.	✓
222		A feladat leállt.	–
224		Indítsa újra az alkalmazást a frissítés befejezéséhez.	–
225		A számítógép újraindítása szükséges.	✓
226		A licenc lehetővé teszi olyan összetevők használatát, amelyek még nincsenek telepítve.	–
232		Elindult a Fejlett vírusmentesítés.	–
233		Befejeződött Fejlett vírusmentesítés.	–
230		Hibás tartalék kulcs.	–
240		Az előfizetés hamarosan lejár.	✓
336		Az objektum nem állítható vissza a biztonsági mentésből.	–
2001		Gyanús hálózati tevékenység észlelve.	–

250	⚠	A titkosított kapcsolat megszakadt.	✓
2021	⚠	A KSN-ben való részvétel le van tiltva.	–
245	⚠	Az operációs rendszer egyes funkciói le vannak tiltva.	✓
344	⚠	A karanténként szolgáló tárhely majdnem megtelt.	✓
235	🕒	Az alkalmazás elindult.	✓
236	🕒	Az alkalmazás leállt.	✓
213	🕒	Az alkalmazás-erőforrásokkal végzett műveletet az Önvédelem blokkolja.	–
217	🕒	Jelentés törölve.	✓
220	🕒	Csoportházirend letiltva.	–
218	🕒	Az alkalmazás beállításai módosultak.	✓
221	🕒	A feladat elindult.	–
223	🕒	A feladat befejeződött.	–
227	🕒	A licencben meghatározott összes alkalmazás-összetevő telepítve van és normál módban fut.	–
238	🕒	Az előfizetés beállításai megváltoztak.	✓
239	🕒	Az előfizetés megújult.	✓
335	🕒	Az objektum visszaállítva a biztonsági mentésből.	–
2000	🕒	Felhasználónév és jelszó megadása.	–
2020	🕒	A KSN-ben való részvétel engedélyezve van.	–
2022	🕒	A KSN kiszolgálói elérhetőek.	–
2024	🕒	Az alkalmazás a vonatkozó törvények szerint működik és dolgozza fel az adatokat, és a megfelelő infrastruktúrát használja.	✓
345	🕒	Az objektum a karanténból visszaállítva.	✓
347	🕒	Karanténból törölt objektum.	✓

Viselkedéselemzés

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	–
313		Nem lehet törölni.	–
452		Folyamat megszakítva.	–
453		Nem lehet megszakítani a folyamatot.	–
455		A visszagörgetés befejeződött.	–
331		Blokkolva.	–
307		Objektum törölve.	–
323		Az objektum az újraindításkor törlődik.	–
311		Nem lehet biztonsági másolatot létrehozni.	–
303		Legitim szoftver észlelve, amellyel a behatólók károsíthatják a számítógépét vagy személyes adatait.	–
457		Fájl visszaállítva.	–
308		Létrejött az objektum biztonsági másolata.	–
458		A beállításkulcs értéke visszaállítva.	–
459		A beállításkulcs értéke törölve.	–
329		Objektum átnevezve.	–

[Biztonsági rések kihasználásának megelőzése](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	–
331		Blokkolva.	–
455		A visszagörgetés befejeződött.	–
307		Objektum törölve.	–
323		Az objektum az újraindításkor törlődik.	–
457		Fájl visszaállítva.	–
458		A beállításkulcs értéke visszaállítva.	–
459		A beállításkulcs értéke törölve.	–
329		Objektum átnevezve.	–

[Behatólasmegelőző rendszer](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	
312		A vírusmentesítés nem lehetséges.	–
313		Nem lehet törölni.	–
317		Feldolgozási hiba.	–
452		Folyamat megszakítva.	–
453		Nem lehet megszakítani a folyamatot.	–
310		Nem lehet biztonsági másolatot létrehozni.	–
314		Az objektum nincs feldolgozva.	–
320		Objektum titkosítva.	–
321		Sérült objektum.	–
323		Az objektum az újraindításkor törlődik.	–
324		Az objektum az újraindításkor lesz vírusmentesítve.	–
303		Legitim szoftver észlelve, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.	–
336		Az objektum nem állítható vissza a biztonsági mentésből.	–
307		Objektum törölve.	–
306		Objektum vírusmentesítve.	–
301		Objektum feldolgozva.	–
308		Létrejött az objektum biztonsági másolata.	–
315		Az objektum kihagyva.	–
318		Archívum észlelve.	–
319		Csomagolt objektum észlelve.	–
327		Egy korábban vírusmentesített másolat által felülírva.	–
332		Információ az észlelt objektumról.	–
322		Jelszóval védett archívum észlelve.	–
335		Az objektum visszaállítva a biztonsági mentésből.	–
401		Az alkalmazás a megbízható csoportba került.	–
402		Az alkalmazás korlátozott csoportba került.	–
403		A Behatolásmegelőző rendszer sikeresen aktiválva.	–
340		Az objektum a privát KSN engedélyezési listáján található.	

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	✓
312		A vírusmentesítés nem lehetséges.	–
313		Nem lehet törölni.	–
317		Feldolgozási hiba.	✓
452		Folyamat megszakítva.	–
453		Nem lehet megszakítani a folyamatot.	–
310		Nem lehet biztonsági másolatot létrehozni.	–
314		Az objektum nincs feldolgozva.	–
320		Objektum titkosítva.	–
321		Sérült objektum.	–
323		Az objektum az újraindításkor törlődik.	–
324		Az objektum az újraindításkor lesz vírusmentesítve.	–
303		Legitim szoftver észlelve, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.	–
336		Az objektum nem állítható vissza a biztonsági mentésből.	–
307		Objektum törölve.	–
306		Objektum vírusmentesítve.	–
455		A visszagörgetés befejeződött.	–
301		Objektum feldolgozva.	–
308		Létrejött az objektum biztonsági másolata.	–
315		Az objektum kihagyva.	–
318		Archívum észlelve.	–
319		Csomagolt objektum észlelve.	–
325		Egy korábban vírusmentesített másolat által felülírva.	–
322		Jelszóval védett archívum észlelve.	–
332		Információ az észlelt objektumról.	–
335		Az objektum visszaállítva a biztonsági mentésből.	–
340		Az objektum a privát KSN engedélyezési listáján található.	✓

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	✓
362		Veszélyes hivatkozás blokkolva.	✓
363		Veszélyes hivatkozás megnyitva.	✓
1201		Korábban megnyitott veszélyes hivatkozás észlelve.	✓
317		Feldolgozási hiba.	✓
303		Legitim szoftver észlelve, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.	–
331		Blokkolt	–
341		Az objektum letöltése blokkolva.	–
321		Sérült objektum.	–
301		Objektum feldolgozva.	–
301		Hivatkozás feldolgozva.	–
332		Információ az észlelt objektumról.	–
319		Csomagolt objektum észlelve.	–
318		Archívum észlelve.	–
322		Jelszóval védett archívum észlelve.	–
370		A hivatkozás a privát KSN engedélyezési listáján található.	✓
370		Az objektum a privát KSN engedélyezési listáján található.	✓

[Levelezés védelem](#) 

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	✓
312		A vírusmentesítés nem lehetséges.	–
317		Feldolgozási hiba.	✓
314		Az objektum nincs feldolgozva.	–
303		Legitim szoftver észlelve, amellyel a behatolók károsíthatják a számítógépét.	–
321		Sérült objektum.	–
336		Az objektum nem állítható vissza a biztonsági mentésből.	–
307		Objektum törölve.	–
342		Az objektum törlése a beállításoknak megfelelően megtörtént.	–
306		Objektum vírusmentesítve.	–
301		Objektum feldolgozva.	–
308		Létrejött az objektum biztonsági másolata.	–
318		Archívum észlelve.	–
319		Csomagolt objektum észlelve.	–
329		Objektum átnevezve.	–
332		Információ az észlelt objektumról.	–
322		Jelszóval védett archívum észlelve.	–
335		Az objektum visszaállítva a biztonsági mentésből.	–
340		Az objektum a privát KSN engedélyezési listáján található.	✓


Firewall

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
602		Hálózati tevékenység blokkolva.	✓
601		Hálózati tevékenység engedélyezve.	–




Hálózati védelem

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
651		Hálózati támadás észlelve.	–



[BadUSB védelem](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2051		A billentyűzet nem hitelesített.	✓
2052		Billentyűzethitelesítési hiba.	✓
2050		Billentyűzet hitelesítve.	–

[AMSI védelem](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	✓
2200		AMSI-kérés blokkolva.	✓
317		Feldolgozási hiba.	✓
314		Az objektum nincs feldolgozva.	–
320		Objektum titkosítva.	–
321		Sérült objektum.	–
303		Legitim szoftver észlelve, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.	–
1512		Az objektum vizsgálati eredménye el lett küldve egy külső alkalmazásnak.	–
301		Objektum feldolgozva.	–
315		Az objektum kihagyva.	–
318		Archívum észlelve.	–
319		Csomagolt objektum észlelve.	–
322		Jelszóval védett archívum észlelve.	–
332		Információ az észlelt objektumról.	–
340		Az objektum a privát KSN engedélyezési listáján található.	✓

[Alkalmazásfelügyelő](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
702		Az alkalmazás indítása tiltva.	–
710		Tiltott folyamat indult el a Kaspersky Endpoint Security for Windows indítása előtt.	–
707		Hiba a feladat beállításában. A feladat beállításai nem kerültek alkalmazásra.	–
708		Feladatbeállítások sikeresen alkalmazva.	–
701		Az alkalmazás indítása engedélyezve.	–
703		Az alkalmazás indítása tesztelési módban tiltva.	–
704		Az alkalmazás indítása tesztelési módban engedélyezve.	–

[Eszközfelügyelő](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
802		Működés a készülékkel tiltva.	–
809		Hálózati kapcsolat blokkolva.	–
803		A készülékhez való ideiglenes hozzáférés aktiválva.	✓
801		Működés a készülékkel engedélyezve.	–
808		Fájlművelet végrehajtva.	–




[Webfelügyelő](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
752		Hozzáférés megtagadva.	–
753		Figyelmeztetés nemkívánatos tartalomról.	–
754		Nemkívánatos tartalomhoz való hozzáférés történt figyelmeztetés után.	–
751		Hozzáférés engedélyezve.	–
751		Engedélyezett oldal megnyitva.	–

[Adaptív Anomáliafelügyelő](#)

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2200		Folyamatművelet blokkolva.	
2201		Folyamatművelet kihagyva.	–

[Adattitkosítás](#) 

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
904		Hiba történt a fájltitkosítási/-visszafejtési szabályok alkalmazásakor.	✓
912		Fájltitkosítási/-visszafejtési hiba.	✓
940		Fájlhozzáférés blokkolva.	✓
951		Hiba történt a hordozható mód engedélyezésekor.	✓
953		Hiba történt a hordozható mód letiltásakor.	✓
931		Hiba történt a titkosított csomag létrehozásakor.	✓
1305		Hiba történt a készülék titkosításakor/visszafejtésekor.	✓
1311		Nem sikerült betölteni a titkosítási modult.	✓
1340		A Hitelesítési ügynöki fiókok kezelésének feladata hibával zárult.	✓
1312		A házirend nem alkalmazható.	✓
1342		Az FDE frissítése nem sikerült.	✓
1344		A Teljes lemeztitkosítás frissítési visszaállítása hibával végződött.	✓
903		Megszakadt a fájltitkosítási/-visszafejtési szabályok alkalmazása.	–
914		A fájltitkosítás/-visszafejtés megszakadt.	–
1303		A készülék titkosítása/visszafejtése megszakadt.	–
1306		A felhasználó elutasította a titkosítási házirendet.	–
1345		Nem sikerült telepíteni vagy frissíteni a Kaspersky lemeztitkosítás illesztőprogramjait a WinRE lemezképben.	✓
901		Megkezdődött a fájltitkosítási/-visszafejtési szabályok alkalmazása.	–
902		Fájltitkosítási/visszafejtési szabályok alkalmazása befejezve.	–
905		Folytatódott a fájltitkosítási/-visszafejtési szabályok alkalmazása.	–
910		A fájltitkosítás/-visszafejtés elindult.	–
911		A fájltitkosítás/-visszafejtés befejeződött.	–
913		A fájl nem lett titkosítva, mert kizárásnak minősül.	–
950		Hordozható mód engedélyezve.	–
952		Hordozható mód blokkolva.	–
1301		A készülék titkosítása/visszafejtése elindult.	–
1302		A készülék titkosítása/visszafejtése befejeződött.	–
1304		A készülék titkosítása/visszafejtése folytatódott.	–

1310	①	Titkosítási modul betöltve.	–
1307	①	A készülék nincs titkosítva.	–
1308	①	A készülék titkosítási/visszafejtési folyamata aktív módra váltott.	–
1309	①	A meghajtó titkosítási/visszafejtési folyamata passzív módra váltott.	–
1330	①	Új Hitelesítési ügynöki fiók létrehozva.	–
1331	①	Hitelesítési ügynöki fiók törölve.	–
1332	①	A Hitelesítési ügynöki fiók jelszava megváltozott.	–
1333	①	Sikeres Hitelesítési ügynöki bejelentkezés.	–
1334	①	Sikertelen Hitelesítési ügynöki bejelentkezési kísérlet.	–
1335	①	A merevlemez elérése sikerült a titkosított eszközökhöz való hozzáférés kérésének eljárásával.	–
1336	①	Nem sikerült elérni a merevlemez a titkosított eszközökhöz való hozzáférés kérésének eljárásával.	–
1337	①	A fiók nem lett hozzáadva. Ez a fiók már létezik.	–
1338	①	A fiók nem lett módosítva. Ez a fiók nem létezik.	–
1339	①	A fiók nem lett törölve. Ez a fiók nem létezik.	–
1341	①	Az FDE frissítése sikerült.	✓
1343	①	Az FDE frissítésének visszaállítása sikerült.	✓
1346	①	Nem sikerült eltávolítani a Kaspersky lemeztitkosítás illesztőprogramjait a WinRE lemezképből.	✓
1370	①	A BitLocker visszaállítási kulcsa megváltozott.	✓
1371	①	A BitLockerhez tartozó jelszó/PIN-kód megváltozott.	✓
1372	①	A BitLocker visszaállítási kulcsa mentve lett a cserélhető meghajtóra.	✓

Végponti szenzor

Az események kódjai


Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2100		A Kaspersky Célzott Támadások Elleni Platform kiszolgálója nem érhető el.	–
2105		Alkalmazás indítása blokkolva.	✓
2106		Dokumentum megnyitása blokkolva.	✓
2112		A fájlképből vagy adatfolyamból indított összes folyamat leállt.	✓
2113		Az alkalmazás elindult.	✓
2111		A fájlt vagy adatfolyamot a Kaspersky Célzott Támadások Elleni Platform kiszolgáló rendszergazdája törölte.	✓
2110		A fájlt a rendszergazda karanténból visszaállította a Kaspersky Célzott Támadások Elleni Platform kiszolgálóján.	✓
2109		A fájlt a rendszergazda karanténba helyezi a Kaspersky Célzott Támadások Elleni Platform kiszolgálóján.	✓
2107		Minden harmadik féltől származó alkalmazás hálózati tevékenysége blokkolva.	✓
2108		Nem blokkolt hálózati támadás.	✓
2104		A Kaspersky Célzott Támadások Elleni Platform kiszolgálójának feladatai feldolgozás alatt állnak.	–
2103		A Kaspersky Célzott Támadások Elleni Platform kiszolgálói feladatainak feldolgozása inaktív.	–
2101		A végponti szenzorok csatlakoztatva a kiszolgálóhoz.	–
2102		Helyreállt a kapcsolat a Kaspersky Célzott Támadások Elleni Platform kiszolgálójával.	–

[Vírusvizsgálat](#) 

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
302		Rosszindulatú objektum észlelve.	✓
312		A vírusmentesítés nem lehetséges.	–
313		Nem lehet törölni.	–
317		Feldolgozási hiba.	–
452		Folyamat megszakítva.	–
453		Nem lehet megszakítani a folyamatot.	–
310		Nem lehet biztonsági másolatot létrehozni.	–
314		Az objektum nincs feldolgozva.	–
320		Objektum titkosítva.	–
321		Sérült objektum.	–
323		Az objektum az újraindításkor törlődik.	–
324		Az objektum az újraindításkor lesz vírusmentesítve.	–
303		Legitim szoftver észlelve, amellyel a behatolók károsíthatják a számítógépét vagy személyes adatait.	–
336		Az objektum nem állítható vissza a biztonsági mentésből.	✓
307		Objektum törölve.	–
306		Objektum vírusmentesítve.	–
455		A visszagörgetés befejeződött.	–
301		Objektum feldolgozva.	–
308		Létrejött az objektum biztonsági másolata.	–
315		Az objektum kihagyva.	–
318		Archívum észlelve.	–
319		Csomagolt objektum észlelve.	–
327		Egy korábban vírusmentesített másolat által felülírva.	–
332		Információ az észlelt objektumról.	–
322		Jelszóval védett archívum észlelve.	–
335		Az objektum visszaállítva a biztonsági mentésből.	✓
329		Objektum átnevezve.	–
340		Az objektum a privát KSN engedélyezési listáján található.	✓

Az események kódjai




Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2002		A rendszermodul aláírás-ellenőrzése nem sikerült.	–

[Adatbázis-frissítés](#) 

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
1011		Hiba történt az összetevő frissítésekor.	–
1012		Hiba történt az összetevői frissítések terjesztésekor.	–
1014		Helyi frissítési hiba.	–
1015		Hálózati frissítési hiba.	–
1017		Két feladat nem indítható el egyidejűleg.	–
1018		Hiba történt az alkalmazás adatbázisainak és moduljainak ellenőrzésekor.	–
1019		Hiba történt a Kaspersky Security Centerrel való kommunikáció során.	–
1021		Nem minden összetevő frissült.	–
1023		A frissítés sikeresen befejeződött, a frissítés terjesztése nem sikerült.	–
101		Belső hiba történt.	✓
2153		A javítás telepítése nem sikerült.	–
2156		A javítás visszagörgetése nem sikerült.	–
1016		A műveletet a felhasználó megszakította.	–
1001		Frissítésforrás kijelölve.	–
1002		Proxykiszolgáló kijelölve.	–
1003		Fájl letöltése.	–
1004		Fájl letöltve.	–
1005		Fájl telepítve.	–
1006		Fájl frissítve.	–
1007		Fájl frissítési hiba miatt visszagördítve.	–
1008		Fájlok frissítése.	–
1009		Frissítések terjesztése.	–
1010		Fájlok visszagörgetése.	–
1013		A letöltendő fájlok listájának létrehozása.	–
1020		Nincs elérhető frissítés.	–
1022		A frissítés terjesztése sikeresen befejeződött.	–
2150		Javítások letöltése.	–
2151		Javítások telepítése.	–
2152		Javítás telepítve.	–
2154		Javítás visszagörgetése.	–
2155		Javítás visszagörgetve.	–

Adatok törlése [?]

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2252		Nem lehet törölni.	–
2253		Törlési feladat statisztikái.	–
2251		Objektum törölve.	–

Endpoint Detection and Response [?]

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2551		Az objektum indítása blokkolva.	✓
2552		A folyamat indítása blokkolva.	✓
2559		A parancsfájl végrehajtása blokkolva.	✓
2556		Karanténba nem helyezett objektum (Endpoint Detection and Response).	✓
2651		IOC észlelve.	✓
2553		Az objektum indítása engedélyezve. Az esemény naplózva.	✓
2554		A folyamat indítása engedélyezve. Az esemény naplózva.	✓
2560		A parancsfájl végrehajtása engedélyezve. Az esemény naplózva.	✓
2558		Újraindítás után az objektum törölve lesz (Endpoint Detection and Response).	✓
2700		Hálózatelkülönítés	✓
2701		Hálózatelkülönítés megszakítása	✓
2555		Karanténba helyezett objektum (Endpoint Detection and Response)	✓
2557		Az objektum törölve (Endpoint Detection and Response)	✓
2652		Az IOC-vizsgálat elkezdődött	✓
2653		Az IOC-vizsgálat befejeződött	✓

Kaspersky Sandbox [?]

Az események kódjai

Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
2603		Karanténba nem helyezett objektum (Kaspersky Sandbox).	✓
2607		Belső hiba történt.	✓
2611		Hiba történt a vizsgálati feladat Kaspersky Sandboxba történő küldése során.	✓
2613		Érvénytelen a Kaspersky Sandbox kiszolgálói tanúsítványa.	✓
2614		A Kaspersky Sandbox-csomópont nem érhető el.	✓
2615		Fenyegetést észleltünk az aszinkron feladatfeldolgozás során.	✓
2617		Nem sikerült feldolgozni egy objektumot a Kaspersky Sandboxban.	✓
2618		Túllépte a Kaspersky Sandbox maximális terhelési értékét.	✓
2651		IOC észlelve.	✓
2620		A Kaspersky Sandbox-licenc ellenőrzése nem sikerült.	✓
2605		Újraindítás után az objektum törölve lesz (Kaspersky Sandbox).	✓
2612		A vizsgálati feladatok teljes mérete túllépte a korlátértéket.	✓
308		Létrejött az objektum biztonsági másolata.	–
2602		Karanténba helyezett objektum (Kaspersky Sandbox).	✓
2604		Az objektum törölve (Kaspersky Sandbox).	✓
2606		Úgy döntött, hogy elküldi a vizsgálati feladatot a Kaspersky Sandboxba.	✓
2609		A helyi gyorsítótár ki lett ürítve.	✓
2610		A vizsgálati feladat el lett küldve a Kaspersky Sandboxba.	✓
2616		Nem találtunk fenyegetéseket az aszinkron feladatfeldolgozás során.	✓
2652		Az IOC-vizsgálat elkezdődött.	✓
2653		Az IOC-vizsgálat befejeződött.	✓
2608		Gyorsítótárazott eredmény található a szinkron objektumfeldolgozás során	✓

7. melléklet Alkalmazásesemények a Kaspersky Security Center eseménynaplójában

A Kaspersky Endpoint Security egyes összetevőinek működésére, az adattitkosítási eseményekre, az egyes vizsgálati feladatok, frissítési feladatok és integritás-ellenőrzési feladatok befejezésére, valamint az alkalmazás általános működésére vonatkozó információk bekerülnek a Kaspersky Security Center eseménynaplójába.

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 – Tájékoztató üzenet (i), 2 – Figyelmeztetés (⚠), 3 – Működési hiba (⚠), 4 – Kritikus (⚠).
- EVENT_TYPE_DISPLAY_NAME: az esemény címe.
- TASK_DISPLAY_NAME: az eseményt kiváltó alkalmazás-összetevő 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.

[A Kaspersky Endpoint Security for Windows specifikus eseményeinek listája](#) 





















Esemény azonosítója		Leírás	Alapértelmezés szerint engedélyezve
00000065		Belső műveleti hiba.	–
000000cb		A licenc majdnem lejárt.	–
000000cc		A licenc hamarosan lejár.	✓
000008cd		Törlési feladat statisztikái.	✓
000000ce		Hiányoznak vagy sérültek az adatbázisok.	–
000000cf		Az adatbázisok rendkívül elavultak.	✓
000000d0		Az adatbázisok elavultak.	✓
000000d1		Az alkalmazás automatikus indítása le van tiltva.	✓
000000d2		Az automatikus frissítések le vannak tiltva.	✓
000000d3		Az Önvédelem le van tiltva.	✓
000000d4		A feladat nem hajtható végre.	✓
000000d5		Az alkalmazás-erőforrásokkal végzett műveletet az Önvédelem blokkolja.	✓
000000d6		A védelem összetevői le vannak tiltva.	✓
000000d7		A számítógép csökkentett módban működik.	–
000000d8		Feldolgozatlan fájlok találhatóak.	✓
000000d9		Jelentés törölve.	✓
000000da		Az alkalmazás beállításai módosultak.	✓
000000db		Csoportházirend alkalmazva.	✓
000000dc		Csoportházirend letiltva.	✓
000000dd		A feladat elindult.	✓
000000de		A feladat leállt.	✓
000000df		A feladat befejeződött.	✓
000000e1		A számítógép újraindítása szükséges.	✓
000000e2		A licenc lehetővé teszi olyan összetevők használatát, amelyek még nincsenek telepítve.	✓
000000e3		A licencben meghatározott összes alkalmazás-összetevő telepítve van és normál módban fut.	–
000000e6		Hibás tartalék kulcs.	✓
000000e7		Aktív fenyegetés észlelve. El kell indítani a Fejlett vírusmentesítést.	✓
000000e8		Elindult a Fejlett vírusmentesítés.	✓
000000e9		Befejeződött Fejlett vírusmentesítés.	✓
000000ee		Az előfizetés beállításai megváltoztak.	✓
000000ef		Az előfizetés megújult.	✓

000000f0		Az előfizetés hamarosan lejár.	✓
000000f5		Az operációs rendszer egyes funkciói le vannak tiltva.	✓
00000134		Létrejött az objektum biztonsági másolata.	✓
00000136		Nem lehet biztonsági másolatot létrehozni.	✓
00000139		Nem lehet törölni.	✓
0000013a		Az objektum nincs feldolgozva.	✓
0000013d		Feldolgozási hiba.	✓
00000140		Objektum titkosítva.	–
00000141		Sérült objektum.	–
00000143		Az objektum az újraindításkor törlődik.	✓
00000144		Az objektum az újraindításkor lesz vírusmentesítve.	✓
00000147		Egy korábban vírusmentesített másolat által felülírva.	–
00000149		Objektum átnevezve.	✓
0000014c		Információ az észlelt objektumról.	✓
0000014f		Az objektum visszaállítva a biztonsági mentésből.	✓
00000150		Az objektum nem állítható vissza a biztonsági mentésből.	✓
00000154		Az objektum a privát KSN engedélyezési listáján található.	✓
00000157		Nincs elegendő hely a karanténként szolgáló tárhelyen.	✓
00000158		A karanténként szolgáló tárhely majdnem megtelt.	✓
00000159		Az objektum a karanténból visszaállítva.	✓
0000015a		Karanténból nem visszaállított objektum.	✓
0000015b		Karanténból törölt objektum.	✓
0000015c		Karanténból nem törölt objektum.	✓
00000172		A hivatkozás a privát KSN engedélyezési listáján található.	✓
00000191		Az alkalmazás a megbízható csoportba került.	✓
00000192		Az alkalmazás korlátozott csoportba került.	✓
00000193		A Behatolásmegelőző rendszer sikeresen aktiválva.	✓
000001c4		Folyamat megszakítva.	✓
000001c5		Nem lehet megszakítani a folyamatot.	–
000001c7		A visszagörgetés befejeződött.	✓
000001c9		Fájl visszaállítva.	✓
000001ca		A beállításkulcs értéke visszaállítva.	✓
000001cb		A beállításkulcs értéke törölve.	–
000002c3		Hiba a feladat beállításában. A feladat beállításai nem kerültek alkalmazásra.	✓
000002c4		Feladatbeállítások sikeresen alkalmazva.	✓

000002c6		Tiltott folyamat indult el a Kaspersky Endpoint Security for Windows indítása előtt.	✓
000002f2		Nemkívánatos tartalomhoz való hozzáférés történt figyelmeztetés után.	–
000002f4		Engedélyezett oldal megnyitva.	–
00000321		Működés a készülékkel engedélyezve.	–
00000323		A készülékhez való ideiglenes hozzáférés aktiválva.	✓
00000329		Hálózati kapcsolat blokkolva.	✓
00000385		Megkezdődött a fájltitkosítási/-visszafejtési szabályok alkalmazása.	✓
00000386		Fájltitkosítási/visszafejtési szabályok alkalmazása befejezve.	✓
00000388		Hiba történt a fájltitkosítási/-visszafejtési szabályok alkalmazásakor.	✓
000003a3		Hiba történt a titkosított csomag létrehozásakor.	✓
000003b7		Hiba történt a hordozható mód engedélyezésekor.	✓
000003b9		Hiba történt a hordozható mód letiltásakor.	✓
000003f3		Hiba történt az összetevő frissítésekor.	✓
000003f4		Hiba történt az összetevői frissítések terjesztésekor.	–
000003f7		Hálózati frissítési hiba.	–
000003f8		A műveletet a felhasználó megszakította.	✓
000003f9		Két feladat nem indítható el egyidejűleg.	✓
000003fa		Hiba történt az alkalmazás adatbázisainak és moduljainak ellenőrzésekor.	✓
000003fb		Hiba történt a Kaspersky Security Centerrel való kommunikáció során.	✓
000003fc		Nincs elérhető frissítés.	–
000003fd		Nem minden összetevő frissült.	✓
000003fe		A frissítés terjesztése sikeresen befejeződött.	–
000003ff		A frissítés sikeresen befejeződött, a frissítés terjesztése nem sikerült.	–
00000519		Hiba történt a készülék titkosításakor/visszafejtésekor.	✓
0000051a		A felhasználó elutasította a titkosítási házirendet.	✓
0000051e		Titkosítási modul betöltve.	–
0000051f		Nem sikerült betölteni a titkosítási modult.	✓
00000520		A házirend nem alkalmazható.	✓
00000532		Új Hitelesítési ügynöki fiók létrehozva.	–
00000533		Hitelesítési ügynöki fiók törölve.	–
00000534		A Hitelesítési ügynöki fiók jelszava megváltozott.	–

00000535		Sikeres Hitelesítési ügynöki bejelentkezés.	–
00000536		Sikertelen Hitelesítési ügynöki bejelentkezési kísérlet.	–
00000539		A fiók nem lett hozzáadva. Ez a fiók már létezik.	–
0000053a		A fiók nem lett módosítva. Ez a fiók nem létezik.	–
0000053b		A fiók nem lett törölve. Ez a fiók nem létezik.	–
0000053c		A Hitelesítési ügynöki fiókok kezelésének feladata hibával zárult.	✓
0000053d		Az FDE frissítése sikerült.	✓
0000053e		Az FDE frissítése nem sikerült.	✓
0000053f		Az FDE frissítésének visszaállítása sikerült.	✓
00000540		A titkosítás frissítési visszaállítása hibával fejeződött be (további részletekért lásd a Kaspersky Endpoint Security for Windows online súgóját).	✓
00000541		Nem sikerült telepíteni vagy frissíteni a Kaspersky lemeztitkosítás illesztőprogramjait a WinRE lemezképben.	✓
00000542		Nem sikerült eltávolítani a Kaspersky lemeztitkosítás illesztőprogramjait a WinRE lemezképből.	✓
0000055a		A BitLocker visszaállítási kulcsa megváltozott.	✓
0000055b		A BitLockerhez tartozó jelszó/PIN-kód megváltozott.	✓
0000055c		A BitLocker visszaállítási kulcsot egy cserélhető meghajtóra mentették.	✓
00000579		Hiba az alkalmazás összetevőinek módosítása közben.	✓
0000057a		Alkalmazás összetevői sikeresen módosítva.	✓
0000057b		Újraindítás szükséges a feladat befejezéséhez.	✓
000007d0		Felhasználónév és jelszó megadása.	✓
000007d1		Gyanús hálózati tevékenység észlelve.	✓
000007d2		A rendszermodul aláírás-ellenőrzése nem sikerült.	✓
000007d3		A titkosított kapcsolat megszakadt.	–
000007e4		A KSN-ben való részvétel engedélyezve van.	✓
000007e5		A KSN-ben való részvétel le van tiltva.	✓
000007e6		A KSN kiszolgálói elérhetőek.	✓
000007e7		A KSN kiszolgálói nem érhetőek el.	✓
000007e8		Az alkalmazás a vonatkozó törvények szerint működik és dolgozza fel az adatokat, és a megfelelő infrastruktúrát használja.	✓
00000802		Billentyűzet hitelesítve.	✓
00000803		A billentyűzet nem hitelesített.	✓
00000804		Billentyűzethitelesítési hiba.	✓
00000834		A Kaspersky Célzott Támadások Elleni Platform kiszolgálója nem érhető el.	✓




00000835		A végponti szenzor csatlakoztatva a kiszolgálóhoz.	
00000836		Helyreállt a kapcsolat a Kaspersky Célzott Támadások Elleni Platform kiszolgálójával.	
00000837		A Kaspersky Célzott Támadások Elleni Platform kiszolgálói feladatainak feldolgozása inaktív.	
00000838		A Kaspersky Célzott Támadások Elleni Platform kiszolgálójának feladatai feldolgozás alatt állnak.	
00000839		Alkalmazás indítása blokkolva.	
0000083a		Dokumentum megnyitása blokkolva.	
0000083b		Minden harmadik féltől származó alkalmazás hálózati tevékenysége blokkolva.	
0000083c		Nem blokkolt hálózati támadás.	
0000083d		A fájlt a rendszergazda karanténba helyezi a Kaspersky Célzott Támadások Elleni Platform kiszolgálóján.	
0000083e		A fájlt a rendszergazda karanténból visszaállította a Kaspersky Célzott Támadások Elleni Platform kiszolgálóján.	
0000083f		A fájlt vagy adatfolyamot a Kaspersky Célzott Támadások Elleni Platform kiszolgáló rendszergazdája törölte.	
0000083e		A fájlt a rendszergazda karanténból visszaállította a Kaspersky Célzott Támadások Elleni Platform kiszolgálóján.	
00000840		A fájlképből vagy adatfolyamból indított összes folyamat leállt.	
00000841		Az alkalmazás elindult.	
00000869		A javítás telepítése nem sikerült.	
0000086c		A javítás visszagörgetése nem sikerült.	
00000898		AMSI-kérés blokkolva.	
000008cc		Hiba történt egy objektum törlése során.	
000009f8		A folyamat futtatása engedélyezett, esemény naplózva.	
000009f9		Az objektum indítása blokkolva.	
000009fa		Az objektum futtatása engedélyezett, esemény naplózva.	
000009fb		Karanténba helyezett objektum (Endpoint Detection and Response).	
000009fc		Karanténba nem helyezett objektum (Endpoint Detection and Response).	
000009fd		Az objektum törölve (Endpoint Detection and Response).	
000009fe		Újraindítás után az objektum törölve lesz (Endpoint Detection and Response).	
00000a2a		Karanténba helyezett objektum (Kaspersky Sandbox).	
00000a2b		Karanténba nem helyezett objektum (Kaspersky Sandbox).	
00000a2d		Újraindítás után az objektum törölve lesz (Kaspersky Sandbox).	
00000a2f		Belső hiba történt.	



00000a34		A vizsgálati feladatok teljes mérete túllépte a korlátértéket.	
00000a35		Érvénytelen a Kaspersky Sandbox kiszolgálói tanúsítványa.	
00000a36		A Kaspersky Sandbox-csomópont nem érhető el.	
00000a39		Nem sikerült feldolgozni egy objektumot a Kaspersky Sandboxban.	
00000a3c		A Kaspersky Sandbox-licenc ellenőrzése nem sikerült.	
00000a5b		IOC észlelve.	
00000a5c		Az IOC-vizsgálat elkezdődött.	
00000a5d		Az IOC-vizsgálat befejeződött.	
00000a8c		Hálózatelkülönítés.	
00000a8d		Hálózatelkülönítés megszakítása.	


[Általános események listája](#)




Esemény azonosítója		Leírás	
GNRL_EV_VIRUS_FOUND	❗	Rosszindulatú objektum észlelve.	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_VIRUS_FOUND_BY_KSN	❗	Rosszindulatú objektum észlelve (KSN).	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_VIRUS_FOUND_AND_BLOCKED	❗	Veszélyes hivatkozás	

		blokkolva (Web védelem).	<ul style="list-style-type: none"> • GNRL_EA_PAI útja. • GNRL_EA_PAI Kaspersky be • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetésé: [?]. A Privát KSN (denylist):
GNRL_EV_VIRUS_FOUND_AND_REPORTED		Veszélyes hivatkozás megnyitva (Web védelem).	<ul style="list-style-type: none"> • GNRL_EA_PAI útja. • GNRL_EA_PAI Kaspersky be • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetésé: [?]. A Privát KSN (denylist):
GNRL_EV_VIRUS_FOUND_AND_PASSED		Korábban megnyitott veszélyes hivatkozás észlelve (Web védelem).	<ul style="list-style-type: none"> • GNRL_EA_PAI útja. • GNRL_EA_PAI Kaspersky be • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI az észlelt objekt Alkalmazásös Fenyegetésé: [?].

			A Privát KSN (denylist):
GNRL_EV_SUSPICIOUS_OBJECT_FOUND		Legitim szoftver észlelve, amellyel a bűnözők károsíthatják a számítógépét vagy személyes adatait	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware
GNRL_EV_OBJECT_CURED		Objektum vírusmentesítve.	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI létrehozásán • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_OBJECT_DELETED		Objektum törölve.	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI létrehozásán • GNRL_EA_PAI Kaspersky be







			<p>Test-File.</p> <ul style="list-style-type: none"> • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_OBJECT_NOTCURED		A vírusmentesítés nem lehetséges.	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI létrehozásána • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_OBJECT_BLOCKED		Az objektum letöltése blokkolva.	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár






			<ul style="list-style-type: none"> • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_OBJECT_REPORTED		<p>Az objektum nincs feldolgozva (Levelezés védelem).</p> <p>Az objektum vizsgálati eredménye el lett küldve egy külső alkalmazásnak (AMSI védelem).</p>	<ul style="list-style-type: none"> • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI • GNRL_EA_PAI Kaspersky be Test-File. • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI pl. Trojware • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (denylist): EDR verzió. Fenyegetés a Az objektum l
GNRL_EV_PASSWD_ARCHIVE_FOUND		Jelszóval védett archívum észlelve.	<ul style="list-style-type: none"> • GNRL_EA_PAI • GNRL_EA_PAI létrehozásána • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI észlelt objekt Alkalmazásös Fenyegetés: [?]. A Privát KSN (tiltólista): tru
GNRL_EV_ATTACK_DETECTED		Hálózati támadás észlelve (Hálózati védelem).	<ul style="list-style-type: none"> • GNRL_EA_PAI

			<ul style="list-style-type: none"> • GNRL_EA_PAI • GNRL_EA_PAI forrásaként s Az IP-cím a ga van megadva. 172.16.0.20 • GNRL_EA_PAI • GNRL_EA_PAI 12B012B012I • GNRL_EA_PAI célpontjának Az IP-cím a ga van megadva. 172.16.0.20
GNRL_EV_LICENSE_EXPIRATION		Végfelhasználói licenszerződés megsértve.	
GNRL_EV_APPLICATION_LAUNCHED		Alkalmazásindítás engedélyezve (Alkalmazásfelügyelő).	<ul style="list-style-type: none"> • GNRL_EA_PAI indításának id Security Cen • GNRL_EA_PAI indításának te • GNRL_EA_PAI azonosítója (S • GNRL_EA_PAI alkalmazáskat (opcionális). • GNRL_EA_PAI felhasználójár
GNRL_EV_APPLICATION_LAUNCH_DENIED		Az alkalmazásindítás letiltva (Alkalmazásfelügyelő).	<ul style="list-style-type: none"> • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI manuálisan lé • GNRL_EA_PAI alkalmazáskat (opcionális). • GNRL_EA_PAI aláírására von • GNRL_EA_PAI futtatható fá chrome.exe).

			<ul style="list-style-type: none"> • GNRL_EA_PAI elérési útja. • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI futtatni kíván
GNRL_EV_APP_INCIDENT_OCCURED	ⓘ	A Kaspersky Sandbox aszinkron riasztása.	<ul style="list-style-type: none"> • GNRL_EA_PAI Sandbox-öss • GNRL_EA_PAI útja. • GNRL_EA_PAI azonosítója. • GNRL_EA_PAI (SHA256).
GNRL_EV_APP_LAUNCH_TESTED_DENIED	ⓘ	Az alkalmazásindítás letiltva teszt üzemmódban (Alkalmazásfelügyelő).	<ul style="list-style-type: none"> • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI manuálisan lé • GNRL_EA_PAI azonosítója (S • GNRL_EA_PAI aláírására von • GNRL_EA_PAI futtatható fá chrome.exe). • GNRL_EA_PAI elérési útja. • GNRL_EA_PAI (SHA256). • GNRL_EA_PAI futtatni kíván
GNRL_EV_APP_LAUNCH_TESTED_ALLOW	ⓘ	Az alkalmazásindítás engedélyezve teszt üzemmódban (Alkalmazásfelügyelő).	<ul style="list-style-type: none"> • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI manuálisan lé • GNRL_EA_PAI azonosítója (S • GNRL_EA_PAI alkalmazáskat

			(opcionális).
GNRL_EV_AC_USER_REQUEST		Az alkalmazásindítás hozzáféréseinek blokkolására vonatkozó üzenet az adminisztrátornak (Alkalmazásfelügyelő).	<ul style="list-style-type: none"> • GNRL_EA_DE: felhasználónak • GNRL_EA_PA felhasználójár • GNRL_EA_PA futtatható fá chrome.exe). • GNRL_EA_PA elérési útja. • GNRL_EA_PA (SHA256). • GNRL_EA_PA futtatni kíván
GNRL_EV_WEB_URL_BLOCKED		Hozzáférés megtagadva (Web Control).	<ul style="list-style-type: none"> • GNRL_EA_PA • GNRL_EA_PA felhasználójár • GNRL_EA_PA szabály neve.
GNRL_EV_WEB_URL_BLOCKED_BY_KSN		A KSN megtagadta a hozzáférést (Webfelügyelő).	<ul style="list-style-type: none"> • GNRL_EA_PA • GNRL_EA_PA felhasználójár • GNRL_EA_PA szabály neve.
GNRL_EV_WEB_URL_WARNING		Figyelmeztetés nemkívánatos tartalomra (Web Control).	<ul style="list-style-type: none"> • GNRL_EA_PA • GNRL_EA_PA felhasználójár • GNRL_EA_PA szabály neve.
GNRL_EV_WC_USER_REQUEST		Weboldal hozzáféréseinek blokkolására vonatkozó üzenet az adminisztrátornak (Web Control).	<ul style="list-style-type: none"> • GNRL_EA_DE: felhasználónak • GNRL_EA_PA • GNRL_EA_PA felhasználójár
GNRL_EV_DC_USER_REQUEST		Eszközhozzáférés blokkolására vonatkozó üzenet az adminisztrátornak (Eszközfelügyelő).	<ul style="list-style-type: none"> • c_er_descrn • GNRL_EA_PA (HWID).

			<ul style="list-style-type: none"> GNRL_EA_PAI felhasználójár
GNRL_EV_DEVCTRL_DEV_PLUGGED		Az eszköz csatlakoztatva van (Eszközfelügyelő).	<ul style="list-style-type: none"> GNRL_EA_PAI (HWID). GNRL_EA_PAI felhasználójár
GNRL_EV_DEVCTRL_DEV_UNPLUGGED		Az eszköz nincs csatlakoztatva (Eszközfelügyelő).	<ul style="list-style-type: none"> GNRL_EA_PAI (HWID). GNRL_EA_PAI felhasználójár
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		A csatlakoztatott eszköz blokkolva van (Eszközfelügyelő).	<ul style="list-style-type: none"> GNRL_EA_PAI (HWID). GNRL_EA_PAI felhasználójár
GNRL_EV_ADSEC_DETECT	 / 	Folyamattevékenység letiltva/Folyamattevékenység kihagyva (Adaptív Anomáiafelügyelő).	<ul style="list-style-type: none"> GNRL_EA_PAI Anomáiafelüg GNRL_EA_PAI azonosítója. GNRL_EA_PAI felhasználójár GNRL_EA_PAI GNRL_EA_PAI GNRL_EA_PAI GNRL_EA_PAI GNRL_EA_PAI észlelt objekt A forrásfolyar célfolyamat/- összegei. Folyamat blok igaz vagy ha Felhasználó b
GNRL_EV_ADSEC_USER_REQUEST		Alkalmazástevékenység hozzáféréseinek blokkolására vonatkozó üzenet az adminisztrátornak (Adaptív Anomáiafelügyelő).	<ul style="list-style-type: none"> GNRL_EA_DE: felhasználón GNRL_EA_PAI Anomáiafelüg GNRL_EA_PAI azonosítója.

			<ul style="list-style-type: none"> • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI • GNRL_EA_PAI • GNRL_EA_PAI • GNRL_EA_PAI • GNRL_EA_PAI észlelt objekt A forrásfolyar célfolyamat/-összegei. Folyamat blok igaz vagy ha Felhasználó b
GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION		Fájlhozzáférés blokkolva.	<ul style="list-style-type: none"> • GNRL_EA_PAI • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI próbáló alkaln neve (például:
GNRL_EV_ENCRYPTION_ERROR		Fájltitkosítási/-visszafejtési hiba.	<ul style="list-style-type: none"> • GNRL_EA_PAI • GNRL_EA_PAI • GNRL_EA_PAI
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		Működés a készülékkel tiltva	<ul style="list-style-type: none"> • GNRL_EA_PAI (HWID). • GNRL_EA_PAI felhasználójár
GNRL_EV_USB_FILE_OPERATION		Fájlművelet végrehajtva (Device Control).	<ul style="list-style-type: none"> • GNRL_EA_PAI vagy törlés). • GNRL_EA_PAI • GNRL_EA_PAI • GNRL_EA_PAI felhasználójár • GNRL_EA_PAI (HWID).
GNRL_EV_HST_CMD_RESULT		Feladateredmények.	<ul style="list-style-type: none"> • GNRL_EA_PAI azonosítója.

- | | | | |
|--|--|--|--|
| | | | <ul style="list-style-type: none">• GNRL_EA_PAI végrehajtási é
Az 1 azt jelen
végre lett haj
A 2 azt jelent
végrehajtva
A 3 azt jelent
törölve lett
A 4 azt jelent
törölve• GNRL_EA_PAI
eredményéne |
|--|--|--|--|

A harmadik féltől származó kódra vonatkozó információk

A harmadik féltől származó kódra vonatkozó információkat az alkalmazás telepítési mappájában található `legal_notices.txt` fájl 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 Systems Incorporated bejegyzett védjegye vagy védjegye az Egyesült Államokban és/vagy más országokban.

Az Apple, FireWire, iTunes és a Safari az Apple Inc. bejegyzett védjegyei az Egyesült Államokban és 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.

Az Android és a Google Chrome a Google, Inc. védjegye.

A Citrix és a Citrix Provisioning Services és a XenDesktop a Citrix Systems, Inc. és/vagy egy vagy több leányvállalata védjegye, és az Egyesült Államok szabadalmi hivatalában vagy más országokban lehet bejegyezve.

A Dell a Dell, Inc. vagy leányvállalatai védjegye.

A dBase a dataBased Intelligence, Inc. védjegye.

Az EMC az EMC Corporation védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Radmin a Famatech bejegyzett védjegye.

Az IBM az International Business Machines Corporation védjegye, mely a világ számos jogrendszerében be van jegyezve.

Az ICQ az ICQ LLC védjegye és / vagy szolgáltatási védjegye.

Az Intel az Intel Corporation védjegye az Egyesült Államokban és/vagy más országokban.

Az IOS a Cisco Systems, Inc. és/vagy leányvállalatai bejegyzett védjegye az Egyesült Államokban és más országokban.

A Lenovo és a 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 is a Mail.Ru, LLC. bejegyzett védjegye.

A McAfee a McAfee, Inc. védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft, az Access, az Active Directory, az ActiveSync, a BitLocker, az Excel, az Internet Explorer, a LifeCam Cinema, az MSDN, a MultiPoint, az Outlook, a PowerPoint, a PowerShell, a Visual Basic, a Visual FoxPro, a Windows, a Windows PowerShell, a Windows Server, a Windows Store, az MS-DOS, a Surface és a Hyper-V a Microsoft Corporation védjegyei az Egyesült Államokban és más országokban.

A Mozilla, a Firefox és a Thunderbird a Mozilla Foundation védjegyei.

A Java és a JavaScript az Oracle és/vagy leányvállalatai bejegyzett védjegyei.

A VERISIGN a VeriSign, Inc. és leányvállalatainak védjegye vagy bejegyzett védjegye az Egyesült Államokban és más országokban.

A VMware és a VMware ESXi a VMware, Inc. bejegyzett védjegyei vagy védjegyei az Egyesült Államokban és/vagy más jogrendszerekben,

A Thawte a Symantec Corporation vagy leányvállalatai védjegye vagy bejegyzett védjegye az Egyesült Államokban és más országokban.

SAMSUNG a SAMSUNG bejegyzett védjegye az Egyesült Államokban és más országokban.