kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Tartalmat

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Ez a rész ismerteti a Kaspersky Endpoint Security funkcióit, összetevőit és forgalmazási csomagját, és felsorolja a Kaspersky Endpoint Security hardver- és szoftverkövetelményeit.

Újdonságok

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows az alábbi funkciókat és továbbfejlesztéseket kínálja:

1. Alkalmazásindítás-felügyelő:
    - Támogatja a kiszolgálók operációs rendszereit.
    - Felügyeli a DLL modulok és az illesztőprogramok letöltését.
    - Kezeli a leltári feladatban szereplő objektumok (DLL modulok és szkriptfájlok) listáját
    - Az objektumokat egy új feltétel, a digitális aláírás tanúsítványainak attribútumai alapján felügyeli.
    - A blokkolt alkalmazások tesztindításairól szóló jelentést készít.
    - Két üzemmódot támogat az Alkalmazásindítás-felügyelőnél: a feketelistát és a fehérlistát.
    - A SHA256 ellenőrzőösszeget használja az objektumok felügyeletéhez és leltározásához.
    - A PowerShell értelmezőből származó szkriptek futtatását felügyeli.
    - Megbízható rendszertanúsítványok tárolóját használja.
2. A Microsoft BitLocker adminisztráció lehetővé teszi a merevlemezek titkosítását a Microsoft BitLocker technológiájának segítségével:
    - Titkosítás távoli kezelése.
    - Titkosított eszközök figyelése.
    - Eszköztitkosítási jelentések készítése.
    - Titkosított eszközökhöz való hozzáférés visszaállítása.
3. Kaspersky lemeztitkosítás:
    - Támogatja a Hitelesítési ügynök rendszerindítás előtti környezetében a hitelesítési adatok virtuális billentyűzettel történő bevitelét.
    - Támogatja a csak az eszközön foglalt terület titkosítását elvégző titkosítási módot.
    - Titkosítás támogatása táblagépeken (MS Surface 3 és 4 verzió).
4. Alkalmazásjogosultság-felügyelő:
    - Felügyeli az alkalmazások hang- és videórögzítő eszközökhöz való hozzáférését.

5. Webfelügyelő:

   - Beállítja a webes erőforrásokhoz való hozzáférés szabályait a webes erőforrások további kategóriáinál.

6. Eszközfelügyelő:

   - Az USB eszközön lévő fájlok törléséhez és mentéséhez kapcsolódó események naplózása.
   - Listakészítés a megbízható Wi-Fi hálózatokról az alábbi beállítások alapján: név, titkosítás típusa és hitelesítési típus.
   - A felhasználók hozzáférési jogainak kezelése CD-/DVD-lemezek fájlolvasási és -írási műveletek vonatkozásában.

7. Levél víruskereső:

   - A Levél víruskereső által vizsgált archívumokon belüli adott típusú fájlok törölhetők és átnevezhetők.

8. Kaspersky Security Network:

   - Megjeleníti a Kaspersky Endpoint Security jelentésekben és a Kaspersky Security Center jelentésekben a KSN-t annak a döntésnek az okaként, amely az objektum feldolgozási módszerére vonatkozik.
   - Lekérdezést küld a KSN részére a kiválasztott fájl reputációjára vonatkozóan.
   - Megjeleníti a KSN kiszolgálók elérhetőségi állapotát az olyan ügyfélszámítógépeken, amelyeken telepítve van a Kaspersky Endpoint Security.

Forgalmazási készlet

A Kaspersky Endpoint Security terjesztőkészlete az alábbi fájlokat tartalmazza:

- Az alkalmazás telepítéséhez szükséges fájlok az igénybe vehető módszerek mindegyike esetén:
- Az alkalmazás telepítése során használt frissítési csomagfájlok.
- A klcfginst.msi fájl, mely a Kaspersky Endpoint Security adminisztrációs bővítmény Kaspersky Security Centeren keresztül történő telepítésére szolgál.
- A ksn_<language ID>.txt fájl, amelyben megtekintheti a Kaspersky Security Network való részvétel feltételeit.
- A license.txt fájl, amelyben megtekintheti a Végfelhasználói licencszerződést.
- Az incompatible.txt fájl, melyben inkompatibilis szoftverek listája látható.
- Az installer.ini file, amely a terjesztőkészlet belső beállításait tartalmazza.

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

A fájlokhoz való hozzáféréshez ki kell csomagolni a terjesztőkészletet.

A Kaspersky Endpoint Security for Windows névjegye

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.

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

Az alábbi alkalmazásösszetevők tartoznak a felügyeleti összetevők közé:

- **Alkalmazásfelügyelő**. Ez az összetevő nyilvántartja a felhasználó alkalmazások indítására tett próbálkozásait, és szabályozza az alkalmazások indítását.
- **Eszközfelügyelő**. Ez az összetevő lehetővé teszi rugalmas hozzáférési korlátozások konfigurálását az adattároló eszközökhöz (így a merevlemezek, cserélhető meghajtók, és CD-/DVD-lemezek), adatátviteli berendezésekhez (így a modemek), az információkból papíralapú példányt előállító berendezésekhez (így a nyomtatók), illetve az eszközök számítógéphez csatlakoztatására szolgáló felületekhez (így az USB, Bluetooth és infravörös) való hozzáférés tekintetében.
- **Webfelügyelő**. Ez az összetevő lehetővé teszi rugalmas szabályok felállítását különböző felhasználói csoportok számára a webes erőforrások hozzáférésének korlátozása céljából.
- **Adaptív Anomáliafelügyelő**. Ez az összetevő megfigyeli és felügyeli a potenciálisan káros tevékenységeket, amik nem megszokottak a védett számítógépnél.

A felügyeleti összetevők működése az alábbi szabályokon alapszik:

- Az Alkalmazásfelügyelő az Alkalmazásfelügyeleti szabályokat használja.
- Az Eszközfelügyelő az eszközhozzáférési szabályokat és a csatlakozóbusz-hozzáférési szabályokat használja.
- A Webfelügyelő a webes erőforrások hozzáférési szabályait használja.
- Az Adaptív AnomáliafelügyelőAdaptív Anomáliafelügyeleti szabályokat használ.

Az alábbi alkalmazásösszetevők tartoznak a védelmi összetevők közé:

- **Viselkedéselemzés**. Ez az összetevő a számítógépen futó alkalmazások műveleteiről kap adatokat, és a védelem fokozása érdekében átadja ezeket az információkat a többi összetevőnek.
- **Biztonsági rések kihasználásának megelőzése**. Ez az összetevő követi a sebezhető alkalmazások által futtatott végrehajtható fájlokat. Ha a Kaspersky Endpoint Security egy sebezhető alkalmazásból származó végrehajtható fájl futtatására irányuló kísérletet észlel, amelyet nem a felhasználó kezdeményezett, akkor blokkolja a fájl indítását.
- **Behatolásmegelőző rendszer**. Ez az összetevő rögzíti az operációs rendszerben lévő alkalmazások tevékenységeit, és az adott alkalmazások megbízhatósági csoportja alapján szabályozza az alkalmazások tevékenységét. Minden egyes alkalmazáscsoportra külön szabálykészlet vonatkozik. Ezek a szabályok határozzák meg az alkalmazások felhasználói adatokhoz és az operációs rendszer erőforrásaihoz való hozzáférését. Ezek közé az adatok közé tartoznak a felhasználói fájlok (Saját dokumentumok mappa, cookie-k, felhasználói tevékenység naplófájljai) és az olyan fájlok, mappák és beállításjegyzékkulcsok, amelyek a leggyakrabban használt alkalmazások beállításait és fontos adatait tartalmazzák.
- **Kármentesítő motor**. Ezzel az összetevővel a Kaspersky Endpoint Security képes a rosszindulatú programok által az operációs rendszerben elvégzett műveleteket visszagörgetni.

- **Fájl védelem**. Ez az összetevő védi a számítógép fájlrendszerét a fertőzésektől. Az összetevő a Kaspersky Endpoint Security alkalmazás indítása után azonnal elindul, folyamatosan aktív marad a számítógép RAM-jában, és vizsgálja a számítógépen és az összes csatlakoztatott tárolóeszközön megnyitott, mentett és elindított összes fájlt. Ez az összetevő észlel minden, a fájlokhoz való hozzáférésre irányuló kísérletet, és ellenőrzi, hogy nincsenek-e ismert vírusok és egyéb fenyegetések a fájlokban.

- **Web védelem**. Ez az összetevő vizsgálja a felhasználó számítógépére HTTP és FTP protokollokon keresztül érkező forgalmat, és ellenőrzi, hogy a webcímek rosszindulatúak vagy adathalászok-e.

- **Levelezés védelem**. Ez az összetevő a bejövő és kimenő e-mail üzenetekben vizsgálja a vírusokat és egyéb fenyegetéseket.

- **Hálózati védelem**. Ez az összetevő a hálózati támadásokra jellemző tevékenységet keresve vizsgálja a bejövő forgalmat. Hálózati támadásra irányuló próbálkozás észlelésekor a Kaspersky Endpoint Security blokkolja a hálózati tevékenységet, így az nem tudja megtámadni a számítógépet.

- **Tűzfal**. Ez az összetevő védelmet nyújt a számítógépen lévő adatok számára, és blokkolja az operációs rendszerre leselkedő fenyegetések legtöbb lehetséges típusát, miközben a számítógép az internethez vagy helyi hálózathoz csatlakozik. Az összetevő kétféle szabálytípussal szűri az összes hálózati tevékenységet: hálózati alkalmazásszabályokkal és hálózati csomagszabályokkal.

- **BadUSB védelem**. Ez az összetevő megakadályozza azt, hogy a billentyűzetet emuláló fertőzött USB eszközök a számítógéphez csatlakozzanak.

- **AMSI Védelmi szolgáltató**. Ez az összetevő megvizsgálja az objektumokat harmadik fél alkalmazásainak kérelmére, és értesíti a kérelmező alkalmazást a vizsgálat eredményéről.

Az alkalmazás összetevői biztosította valós idejű védelem mellett is javasoljuk, hogy rendszeresen végezze el vírusok és egyéb fenyegetések *vizsgálatát* a számítógépen. Ezzel megelőzheti a rosszindulatú programok terjedését, amiket például az alacsony biztonsági szint miatt nem észleltek a védelmi összetevők.

A számítógépes védelem naprakész állapotban tartásához *frissíteni* kell az alkalmazás által használt adatbázisokat és alkalmazásmodulokat. Az alkalmazás frissítésére alapértelmezés szerint automatikusan sor kerül, szükség esetén azonban az adatbázisokat és az alkalmazásmodulokat kézileg is frissítheti.

A Kaspersky Endpoint Security a következő feladatokat kínálja:

- **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.

- **Teljes vizsgálat**. A Kaspersky Endpoint Security megvizsgálja az operációs rendszert a kernelmemóriával együtt, az operációs rendszer indításakor betöltődő objektumokat, a lemez rendszerindító szektorait, az operációs rendszer biztonsági mentési tárterületét, valamint az összes merevlemezt és cserélhető meghajtót.

- **Egyéni vizsgálat**. A Kaspersky Endpoint Security a felhasználó által kiválasztott objektumokat vizsgálja.

- **Kritikus területek vizsgálata**. A Kaspersky Endpoint Security megvizsgálja a kernelmemóriát, az operációs rendszer indításakor betöltődő objektumokat, a lemez rendszerindító szektorait.

- **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.

- **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.

Távoli adminisztráció a Kaspersky Security Centeren keresztül

A Kaspersky Security Center lehetővé teszi, hogy távolról indíthassa el vagy állíthassa le a Kaspersky Endpoint Security alkalmazást a számítógépen, kezelhessen feladatokat, konfiguráljon alkalmazás beállításokat, valamint fájltitkosítást és teljes lemeztitkosítást végezhessen.

A fájltitkosítási funkció révén a számítógép helyi meghajtóin lévő fájlokat és mappákat titkosíthatja. A teljes lemeztitkosítás funkcióval merevlemezeket és cserélhető meghajtókat titkosíthat.

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.

- **Adattárolás**. 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.

- **Értesítési szolgáltatás**. 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.

Ha az alkalmazás hibákat jelez vagy működés közben lefagy, előfordulhat, hogy automatikusan újraindul.

Ha az alkalmazás visszatérő hibákkal találkozik, melyek miatt összeomlik, az alábbi műveleteket végzi el:

1. Letiltja a felügyeleti és védelmi funkciókat (a titkosítási funkciók bekapcsolva maradnak).

2. Értesíti a felhasználót a funkciók letiltásáról.

3. Megpróbálja az alkalmazást működőképes állapotúra visszaállítani, miután frissítette az antivírus adatbázisokat vagy alkalmazta az alkalmazásmodul-frissítéseket.

Az alkalmazás információkat fogad a visszatérő, összeomlást eredményező hibákról a Kaspersky szakértői által külön erre a célra kifejlesztett algoritmusok segítségével. Ez az információ az alkalmazás visszaállítás érdekében szükséges.

Hardveres és szoftveres rendszerkövetelmények

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

Minimális általános követelmények:

- 2 GB szabad lemezterület a merevlemezen
- 1 GHz-es órajelű processzor (támogatja az SSE2 utasításkészletet)
- RAM:
  - 32 bites operációs rendszer esetén – 1 GB
  - 64 bites operációs rendszer esetén – 2 GB

Támogatott operációs rendszerek személyi számítógépek esetén:

- Windows 7 Home / Professional / Enterprise Service Pack 1 vagy frissebb;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

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

Támogatott operációs rendszerek fájlkiszolgálók esetén:

- Windows Small Business Server 2008 Standard / Premium (64-bit);
- Windows Small Business Server 2011 Essentials / Standard (64-bit);
- Windows MultiPoint Server 2011 (64-bit);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 vagy frissebb;
- 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.

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

Az alkalmazás telepítése és eltávolítása

Ez a rész végigvezeti a Kaspersky Endpoint Security számítógépen történő telepítésén, a kezdeti beállítás elvégzésén, az alkalmazás korábbi verziójáról történő frissítésen, valamint az alkalmazás számítógépről való eltávolításán.

Az alkalmazás telepítése

Ez a rész ismerteti a Kaspersky Endpoint Security számítógépen történő telepítésének menetét, és az alkalmazás kezdeti beállításának elvégzését.

Az alkalmazás telepítésének módjai

A Kaspersky Endpoint Security 10 for Windows telepíthető helyileg (közvetlenül a felhasználó számítógépén) vagy távolról a rendszergazda munkaállomásáról.

A Kaspersky Endpoint Security 10 for Windows helyi telepítését az alábbi módok egyikén lehet elvégezni:

- Interaktív módban az Alkalmazástelepítő varázslóval.

  Interaktív módban a telepítési folyamat során a felhasználó beavatkozása szükséges.

- Csendes módban a parancssorból.

  A telepítés csendes módban való elindítását követően a felhasználónak nem szükséges beavatkoznia a telepítési folyamatba.

Az alkalmazás hálózati számítógépeken távolról telepíthető az alábbiakkal:

- Kaspersky Security Center szoftvercsomag (lásd: *Kaspersky Security Center megvalósítási útmutató*).
- A Microsoft Windows Group Policy Editora (lásd az operációs rendszer súgófájljait).
- Rendszerközpont beállításkezelő.

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

Az alkalmazás telepítése a Telepítővarázsló segítségével

A Telepítővarázsló alkalmazás felülete az alkalmazás telepítési lépéseinek megfelelő ablakok sorozatából áll. A Telepítővarázsló oldalai között a **Vissza** és a **Tovább** gombokkal lépkedhet. A Telepítővarázsló bezárására feladata befejezése után a **Megszakítás** gomb szolgál. A Telepítővarázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

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

1. Futtassa a forgalmazási készletben lévő setup.exe fájlt.

Elindul a Telepítővarázsló.

2. Kövesse a Telepítővarázsló utasításait.

A setup.exe fájl indításakor a Kaspersky Endpoint Security ellenőrzi, hogy a számítógépen nincsenek-e inkompatibilis szoftverek. Alapértelmezés szerint inkompatibilis szoftverek észlelése esetén a telepítési folyamat megszakad, és megjelenik a képernyőn a Kaspersky Endpoint Security alkalmazással inkompatibilis alkalmazások listája. A telepítés folytatásához távolítsa el a számítógépről ezeket az alkalmazásokat.

1. lépés. Annak ellenőrzése, hogy a számítógép megfelel-e a telepítés követelményeinek

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

- Az operációs rendszer és a szervizcsomagok megfelelnek-e az termektelepítési szoftverkövetelményeknek.
- 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 kézileg.

Ha az észlelt alkalmazások között megtalálhatók a Kaspersky Endpoint Security korábbi verziói, akkor minden áttelepíthető adat (így az aktiválási adatok és az alkalmazás beállításai) a Kaspersky Endpoint Security 11.1.1 for Windows telepítése során megőrződik és felhasználásra kerül, és az alkalmazás korábbi verziója automatikusan törlődik. Ez az alábbi alkalmazásverziókra vonatkozik:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (build 10.2.2.10535).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (build 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (build 10.2.5.3201).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (build 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (build 10.3.3.275).
- Kaspersky Endpoint Security 11.0.0 for Windows (build 11.0.0.6499).
- Kaspersky Endpoint Security for Windows 11.0.1 (build 11.0.1.90).
- Kaspersky Endpoint Security for Windows 11.1.0 (build 11.1.0.15919).

2. lépés. A telepítési eljárás üdvözlő oldala

Ha az alkalmazás telepítésének összes követelménye teljesül, a telepítőcsomag indítása után üdvözlő oldal jelenik meg. Az üdvözlő oldal bejelenti a Kaspersky Endpoint Security telepítésének megkezdését a számítógépen.

A Telepítővarázsló folytatásához kattintson a **Tovább** gombra.

3. lépés. A Licencszerződés és Adatvédelmi szabályzat megtekintése

A Beállítás varázsló ezen lépésénél alaposan el kell olvasnia az Ön és a Kaspersky között megkötendő Végfelhasználói licencszerződést és Adatvédelmi szabályzatot.

Kérjük, olvassa el alaposan a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot. Ha elfogadja a Végfelhasználói licencszerződés és az Adatvédelmi szabályzat összes feltételét, jelölje ki a **Megerősítem, hogy teljesen elolvastam, megértettem és elfogadom a következőt** részben következő jelölőnégyzeteket:

- **ennek a Végfelhasználó licencszerződésnek a feltételei**
- **az adatok kezelését leíró Adatvédelmi szabályzat**

Az alkalmazás telepítése a jelölőnégyzetek kijelölése után folytatódik.

Ha nem fogadja el a Végfelhasználói licencszerződést és az Adatvédelmi szabályzatot, megszakíthatja a telepítést a **Mégse** gomb megnyomásával.

4. lépés. A telepítés típusának kiválasztása

Ennél a lépésnél kiválaszthatja a Kaspersky Endpoint Security legalkalmasabb típusú telepítését:

- **Alapszintű telepítés**. Ezt a lehetőséget választva a BadUSB védelem kivételével a védelem minden összetevője feltelepül a számítógépre, a Kaspersky szakértői által javasolt beállításokkal.
- **Normál telepítés**. Ezt a lehetőséget választva a BadUSB védelem kivételével a védelem és felügyelet minden összetevője feltelepül a számítógépre, a Kaspersky szakértői által javasolt beállításokkal.
- **Egyéni telepítés**. Ezt a lehetőséget választva a rendszer felkéri, hogy válassza ki a telepíteni kívánt összetevőket és adja meg az alkalmazás célmappáját.

  Ennél a telepítéstípusnál telepítheti az alapszintű és normál telepítésben nem szereplő összetevőket.

Alapértelmezés szerint a normál telepítés van kiválasztva.

A Telepítővarázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Telepítővarázsló folytatásához kattintson a **Tovább** gombra. A Telepítővarázsló leállításához kattintson a **Mégse** gombra.

5. lépés. A telepíteni kívánt alkalmazásösszetevők kiválasztása

Erre a lépésre akkor kerül sor, ha az alkalmazás *Egyéni telepítés* lehetőségét választja.

Ebben a lépésben kiválaszthatja a Kaspersky Endpoint Security telepíteni kívánt összetevőit. A Fájl víruskereső kötelezően telepítendő összetevő. Telepítését nem lehet törölni.

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

- BadUSB védelem.
- Meghajtótitkosítás.
- Fájltitkosítás.
- Microsoft BitLocker kezelő.
- KATA végponti érzékelő.

A *Microsoft BitLocker kezelő* az alábbi funkciókat látja el:

- Kezeli a Windows operációs rendszerbe beépített BitLocker titkosítást.
- Megadja a titkosítási rendszabály beállításait, és ellenőrzi, hogy alkalmazhatók-e a kezelt számítógépre.
- Elindítja a titkosítási és visszafejtési folyamatot.
- Figyelemmel kíséri a titkosítási állapotot a kezelt számítógépen.
- Központilag tárolja a visszaállítási kulcsokat a Kaspersky Security Center Adminisztrációs Kiszolgálón.

A *KATA végponti érzékelő* a Kaspersky Anti Targeted Attack Platform egyik összetevője. Ez a megoldás különféle fenyegetések – például célzott támadások – gyors észlelésére szolgál. Az összetevő folyamatosan figyeli a folyamatokat, az aktív hálózati kapcsolatokat és a módosított fájlokat, és mindezen információkat továbbítja a Kaspersky Anti Targeted Attack Platform részére.

Az összetevő telepítésre kiválasztásához nyissa meg a helyi menüt az összetevő neve melletti ikonra kattintva, és válassza ki **A szolgáltatás a helyi merevlemezre lesz telepítve** lehetőséget. A kiválasztott összetevő által elvégzett feladatok körére és az összetevő által igényelt lemezterület nagyságára vonatkozó részletekért tekintse meg az aktuális Telepítővarázsló-oldal alsó részét.

A helyi merevlemezeken rendelkezésre álló terület részletes adatainak megtekintéséhez kattintson a **Kötet** gombra. Az információk a megnyíló **Rendelkezésre álló lemezterület** ablakban jelennek meg.

Az összetevő telepítésének törléséhez válassza ki a helyi menüben a **Funkció nem lesz elérhető** lehetőséget.

A telepítendő összetevők alapértelmezett listájához való visszatéréshez kattintson az **Visszaállítás** gombra.

A Telepítővarázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Telepítővarázsló folytatásához kattintson a **Tovább** gombra. A Telepítővarázsló leállításához kattintson a **Mégse** gombra.

6. lépés. A célmappa kiválasztása

Ez a lépés akkor válik elérhetővé, ha az alkalmazásnál az *Egyéni telepítés* lehetőséget választotta.

Ebben a lépésben adhatja meg az alkalmazás telepítési célmappájának elérési útját Az alkalmazás célmappájának kiválasztásához kattintson a **Tallózás** gombra.

A helyi merevlemezeken rendelkezésre álló terület adatainak megtekintéséhez kattintson a **Kötet** gombra. Az információk a megnyíló **Lemezterület követelményei** ablakban jelennek meg.

A Telepítővarázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Telepítővarázsló folytatásához kattintson a **Tovább** gombra. A Telepítővarázsló leállításához kattintson a **Mégse** gombra.

7. lépés. A vizsgálatból való kizárások hozzáadása

Ez a lépés akkor válik elérhetővé, ha az alkalmazásnál az *Egyéni telepítés* lehetőséget választotta.

Ekkor megadhatja a kizárásokat a vizsgálatból, melyeket hozzá kíván adni az alkalmazás beállításaihoz.

A Microsoft által javasolt területek kizárása a vizsgálat hatóköréből / **A Kaspersky által javasolt területek kizárása a vizsgálat hatóköréből** jelölőnégyzetek kizárják a megbízható zónából, illetve beveszik oda a Microsoft vagy a Kaspersky által javasolt területeket.

Ha valamelyik jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security a megbízható zónába beleveszi a Microsoft, illetve a Kaspersky által javasolt területeket. A Kaspersky Endpoint Security az ilyen területeken nem vizsgálja a vírusok és egyéb fenyegetések jelenlétét.

A Microsoft által javasolt területek kizárása a vizsgálat hatóköréből jelölőnégyzet akkor használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

A Telepítővarázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Telepítővarázsló folytatásához kattintson a **Tovább** gombra. A Telepítővarázsló leállításához kattintson a **Mégse** gombra.

8. lépés. Előkészítés az alkalmazás telepítésére

A telepítési folyamatot javasolt megvédeni, mivel a számítógép rosszindulatú programokkal fertőződhetett meg, amelyek megzavarhatják a Kaspersky Endpoint Security 10 for Windows telepítését.

A telepítési folyamat védelme alapértelmezés szerint engedélyezve van.

Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni. Ilyenkor szakítsa meg a telepítést, és indítsa újra az Alkalmazástelepítő varázslót. Az „Alkalmazás telepítésének előkészítése" lépésnél törölje a **Telepítési folyamat védelme** jelölőnégyzetet.

A **Citrix PVS-kompatibilitás biztosítása** jelölőnégyzet engedélyezi/letiltja az illesztőprogramokat Citrix PVS kompatibilitási módban telepítő funkciót.

Csak akkor jelölje be ezt a jelölőnégyzetet, ha Citrix Provisioning Services szolgáltatással dolgozik.

Adja hozzá az avp.com fájl elérési útját a %PATH% rendszerváltozóhoz jelölőnégyzet engedélyezi/letiltja azt a lehetőséget, amely hozzáadja az avp.com fájl elérési útját a %PATH% rendszerváltozóhoz.

Ha a jelölőnégyzet be van jelölve, a Kaspersky Endpoint Security vagy bármely feladata parancssorban történő elindításakor nem szükséges a végrehajtható fájl elérési útját begépelni. Az adott feladat indításához elegendő begépelni a végrehajtható fájl nevét és a parancsot.

A Telepítővarázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A program telepítéséhez kattintson a **Telepítés** gombra. A Telepítővarázsló leállításához kattintson a **Mégse** gombra.

Előfordulhat, hogy az aktuális hálózati kapcsolatok megszakadnak az alkalmazás számítógépen való telepítése közben. A legtöbb megszakadt hálózati kapcsolat alkalmazás telepítésének befejeztével visszaáll

9. Lépés. Az alkalmazás telepítése

Az alkalmazás telepítése némi időt igénybe vesz. Várja meg, amíg befejeződik.

Ha az alkalmazás korábbi verzióját frissíti, akkor ehhez a lépéshez hozzátartozik a beállítások áttelepítése és az alkalmazás korábbi verziójának eltávolítása is.

A Kaspersky Endpoint Security telepítésének befejeztét követően elindul a Kezdeti beállító varázsló.

Az alkalmazás telepítése a parancssorból

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.

Az alkalmazás telepítéséhez vagy az alkalmazásverzió frissítéséhez:

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|0] [/pADDLOCAL=<összetevő>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/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] [ADDLOCAL=<összetevő>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<felhasználónév> KLPASSWD=<jelszó> KLPASSWDAREA=<jelszó hatóköre>] [ENABLETRACES=1|0 TRACESLEVEL=<nyomkövetési szint>] /qn
   ```

`EULA`	A Végfelhasználói licencszerződés feltételeinek elfogadása vagy elutasítása. Választható értékek: • `1` – a Végfelhasználói licencszerződés feltételeinek elfogadása. • `0` – a Végfelhasználói licencszerződés feltételeinek elutasítása.	

	A Licencszerződés szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. A Végfelhasználói licencszerződés feltételeit az alkalmazás telepítéséhez, illetve verziójának frissítéséhez kötelező elfogadni.
PRIVACYPOLICY	Az Adatvédelmi szabályzat elfogadása vagy elutasítása. Választható értékek: • 1 – az Adatvédelmi szabályzat elfogadása. • 0 – az Adatvédelmi szabályzat elutasítása. Az Adatvédelmi irányelv szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. Az alkalmazás telepítéséhez, vagy a verziója frissítéséhez el kell fogadnia az Adatvédelmi irányelvet.
KSN	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: • 1 – a KSN-ben való részvétel elfogadása. • 0 – a KSN-ben való részvétel elutasítása (alapértelmezett érték). A Kaspersky Endpoint Security terjesztőcsomag a with Kaspersky Security Networkkel való használatra van optimalizálva. Ha úgy döntött, hogy nem vesz részt a Kaspersky Security Networkben, a telepítés befejezését követően azonnal frissítenie kell a Kaspersky Endpoint Security rendszert.
ALLOWREBOOT	A számítógép automatikus újraindítása, ha szükséges az alkalmazás telepítése vagy frissítése után. Választható értékek: • 1 – automatikus számítógép-újraindítás, szükség esetén. • 0 – az automatikus számítógép-újraindítás le van tiltva (alapértelmezett érték). Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.
ADDLOCAL	Válassza ki a telepíteni kívánt kiegészítő összetevőket. Alapértelmezés szerint az alábbi összetevők kivételével az összes alkalmazásösszetevő telepítése ki van választva: BadUSB védelem, Fájlszintű titkosítás, Teljes lemeztitkosítás, BitLocker kezelés és KATA végponti érzékelő. Választható értékek: • MSBitLockerFeature. A BitLocker Manager összetevő telepítésre kerül. • AntiAPTFeature. A KATA végponti érzékelő összetevő telepítésre kerül.
SKIPPRODUCTCHECK	Inkompatibilis szoftver keresése. Azon inkompatibilis szoftverek listája, amik elérhetőek a terjesztőkészletben lévő incompatible.txt fájlban. Választható értékek:

	• `1` – az inkompatibilis szoftverek keresése engedélyezve van (alapértelmezett érték). • `0` – az inkompatibilis szoftverek keresése ki van kapcsolva.
`SKIPPRODUCTUNINSTALL`	Az észlelt, inkompatibilis szoftver automatikus eltávolítása. Választható értékek: • `1` – A Kaspersky Endpoint Security megpróbálja eltávolítani az inkompatibilis szoftvert (az alapértelmezett érték). • `0` – az inkompatibilis szoftver automatikus eltávolítása le van tiltva.
`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. Az alapértelmezett felhasználónév KLAdmin.
`KLPASSWD`	A Kaspersky Endpoint Security funkcióihoz és beállításaihoz való hozzáférés jelszavának megadása (a jelszót a `KLLOGIN` és a `KLPASSWDAREA` paraméterekkel együtt kell megadni). Ha a `KLLOGIN` paraméternél jelszót megadott, de felhasználónevet nem, alapértelmezés szerint a rendszer a KLAdmin felhasználónevet használja.
`KLPASSWDAREA`	A Kaspersky Endpoint Security-hez való hozzáférési jelszó hatókörének megadása. Ha a felhasználó megpróbál végrehajtani egy olyan tevékenységet, ami beletartozik ebbe a hatókörbe, a Kaspersky Endpoint Security kérni fogja a felhasználó fiókjának bejelentkezési adatait (`KLLOGIN` és `KLPASSWD` paraméterek). Használja a „`;`” karaktert több érték megadásához. Választható értékek: • `SET` – az alkalmazásbeállítások módosítása. • `EXIT` – kilépés az alkalmazásból. • `DISPROTECT` – védelem összetevőinek letiltása és a vizsgálati feladatok leállítása. • `DISPOLICY` – a Kaspersky Security Center rendszabályának letiltása. • `UNINST` – az alkalmazás eltávolítása a számítógépről. • `DISCTRL` – a felügyeleti összetevők kikapcsolása. • `REMOVELIC` – a kulcs eltávolítása. • `REPORTS` – a jelentések megtekintése.
`ENABLETRACES`	Az alkalmazások nyomkövetésének engedélyezése vagy kikapcsolása. Indulás után a Kaspersky Endpoint Security elmenti a nyomkövetési fájlokat a %ProgramData%/Kaspersky Lab mappába. Választható értékek: • `1` – a nyomkövetés engedélyezve van. • `0` – a nyomkövetés ki van kapcsolva (alapértelmezett érték).
	A nyomkövetések részleteinek szintje. Választható értékek:

TRACESLEVEL	• 100 (kritikus). Csak a kritikus hibaüzenetek. • 200 (magas). Minden hibáról szóló üzenet, köztük a súlyos hibáké. • 300 (diagnosztika). Minden hibáról szóló üzenet, és bizonyos figyelmeztetéseket tartalmazó üzenetek. • 400 (fontos). Minden figyelmeztetés és szokásos és kritikus hibákról szóló üzenet és a további információkat tartalmazó üzenetek egy része. • 500 (normális). Minden tájékoztató üzenet, figyelmeztetés és a szokásos és kritikus hibákról szóló üzenetek, valamint az alkalmazás szokásos módban való működéséről szóló részletesebb információkat tartalmazó üzenetek (alapértelmezett érték). • 600 (alacsony). Minden lehetséges üzenet.

Példa:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Rendszergazda KLPASSWD=Jelszó
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Az alkalmazás telepítése után a Kaspersky Endpoint Security aktiválja a próbalicencet, ha nem adott meg aktiváló kódot a setup.ini fájlban. A próbalicenc általában rövid ideig érvényes. A próbalicenc lejárata után a Kaspersky Endpoint Security minden funkciója letiltásra kerül. Az alkalmazás további használatához aktiválni kell egy kereskedelmi licencet.

Ha az alkalmazás telepítését vagy verziójának frissítését csendes módban végzi, az alábbi fájlok használata támogatott:

- setup.ini – az alkalmazás általános telepítési beállításait tartalmazza
- install.cfg – a Kaspersky Endpoint Security helyi beállításai
- setup.reg – beállításkulcsok

  A setup.reg fájl beállításkulcsai csak akkor lesznek 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 fájlnak 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.

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 **Alkalmazáskezelés** részben válassza ki a **Csomagok** lehetőséget.
3. A vezérlőpulton lévő konzol felső részén kattintson a **Csomag létrehozása** 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 terjesztőkészletét tartalmazó mappa elérési útját.
   b. Az **Alkalmazás típusa** részben válassza ki a **Szokásos alkalmazás** lehetőséget.
   c. A **Szokásos alkalmazás** részben:
      - Írja be a **Név** mezőbe a telepítőcsomag egyedi nevét (például az alkalmazás nevét a verzióval együtt).
      - Adja meg a **Parancssor** mezőben a Kaspersky Endpoint Security parancssori telepítési beállításait.
      - Kattintson a **Tallózás** gombra az alkalmazás végrehajtható fájlja elérési útjának megadásához.
      - Győződjön meg arról, hogy a **Végrehajtási mód** listán ki van választva a **Futtatás rendszergazdai jogokkal** elem.
   d. A **Követelmények** részben:
      - Jelölje be az **Előbb másik alkalmazás indítása** 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 alkalmazást csak a megadott platformokon lehet elindítani** lehetőséget a **Platform követelményei** részben, ha azt szeretné, hogy az alkalmazást csak a meg adott operációs rendszereken lehessen telepíteni.
        Jelölje be a lenti listán a jelölőnégyzeteket azokkal az operációs rendszerekkel szemben, amelyeken a Kaspersky Endpoint Security telepíthető lesz.

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

   A létrehozott telepítőcsomag felbukkan a rendelkezésre álló telepítőcsomagok listáján a **Csomagok** részben.
5. A telepítőcsomag helyi menüjében válassza ki az **Üzembehelyezés** elemet.
   Ezzel elindul az *Üzembehelyezési varázsló*.

6. Az Üzembehelyezési varázslóban:

   a. Az **Általános** részben:

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

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

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

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

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

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

A setup.ini fájl telepítései beállításainak leírása

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

A setup.ini 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.
- `[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
`[Beállítás]`	`InstallDir`	Az alkalmazás telepítési mappájának elérési útja.
	`ActivationCode`	Kaspersky Endpoint Security aktiváló kód.
	`Eula`	A Végfelhasználói licencszerződés feltételeinek elfogadása vagy elutasítása. Választható értékek:

		• `1` – a Végfelhasználói licencszerződés feltételeinek elfogadása. • `0` – a Végfelhasználói licencszerződés feltételeinek elutasítása. A Licencszerződés szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. A Végfelhasználói licencszerződés feltételeit az alkalmazás telepítéséhez, illetve verziójának frissítéséhez kötelező elfogadni.
	`PrivacyPolicy`	Az Adatvédelmi szabályzat elfogadása vagy elutasítása. Választható értékek: • `1` – az Adatvédelmi szabályzat elfogadása. • `0` – az Adatvédelmi szabályzat elutasítása. Az Adatvédelmi irányelv szövege megtalálható a Kaspersky Endpoint Security terjesztőkészletében. Az alkalmazás telepítéséhez, vagy a verziója frissítéséhez el kell fogadnia az Adatvédelmi irányelvet.
	`KSN`	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: • `1` – a KSN-ben való részvétel elfogadása. • `0` – a KSN-ben való részvétel elutasítása (alapértelmezett érték). A Kaspersky Endpoint Security terjesztőcsomag a with Kaspersky Security Networkkel való használatra van optimalizálva. Ha úgy döntött, hogy nem vesz részt a Kaspersky Security Networkben, a telepítés befejezését követően azonnal frissítenie kell a Kaspersky Endpoint Security rendszert.
	`Login`	Állítsa be a felhasználónevet a Kaspersky Endpoint Security funkcióinak és beállításainak eléréséhez (a Jelszóvédelem összetevő). A felhasználónevet a `Password` és a `PasswordArea` paraméterekkel együtt kell megadni. Alapértelmezetten a KLAdmin felhasználónév van használva.
	`Jelszó`	A Kaspersky Endpoint Security funkcióihoz és beállításaihoz való hozzáférés jelszavának megadása (a jelszót a `Login` és a `PasswordArea` paraméterekkel együtt kell megadni). Ha a `Bejelentkezés` paraméternél jelszót megadott, de felhasználónevet nem, alapértelmezés szerint a rendszer a KLAdmin felhasználónevet használja.
	`PasswordArea`	A Kaspersky Endpoint Security-hez való hozzáférési jelszó hatókörének megadása. Ha a felhasználó

		megpróbál végrehajtani egy olyan tevékenységet, ami beletartozik ebbe a hatókörbe, a Kaspersky Endpoint Security kérni fogja a felhasználó fiókjának bejelentkezési adatait (`Login` és `Password` paraméterek). Használja a „`;`" karaktert több érték megadásához. Választható értékek: • `SET` – az alkalmazásbeállítások módosítása. • `EXIT` – kilépés az alkalmazásból. • `DISPROTECT` – védelem összetevőinek letiltása és a vizsgálati feladatok leállítása. • `DISPOLICY` – a Kaspersky Security Center rendszabályának letiltása. • `UNINST` – az alkalmazás eltávolítása a számítógépről. • `DISCTRL` – a felügyeleti összetevők kikapcsolása. • `REMOVELIC` – a kulcs eltávolítása. • `REPORTS` – a jelentések megtekintése.
	`SelfProtection`	Az alkalmazástelepítés védelmi mechanizmusának engedélyezése és letiltása. Választható értékek: • `1` – az alkalmazástelepítés védelmi mechanizmusa engedélyezve van. • `0` – az alkalmazástelepítés védelmi mechanizmusa nincs engedélyezve. Kikapcsolhatja a telepítési védelmet. A telepítési védelembe tartozik a terjesztőcsomagok rosszindulatú programokkal való kicserélése, a Kaspersky Endpoint Security telepítési mappái elérésének blokkolása, valamint az alkalmazáskulcsokat tartalmazó beállításjegyzék részek elérésének blokkolása elleni védelem. Ha azonban az alkalmazást nem lehet telepíteni (például a Windows Remote Desktop segítségével végzett távoli telepítés esetén), akkor javasolt a telepítési folyamat védelmét kikapcsolni.
	`Reboot`	A számítógép automatikus újraindítása, ha szükséges az alkalmazás telepítése vagy frissítése után. Választható értékek: • `1` – automatikus számítógép-újraindítás, szükség esetén. • `0` – az automatikus számítógép-újraindítás le van tiltva (alapértelmezett érték).

		Nem szükséges újraindítás a Kaspersky Endpoint Security telepítésekor. Csak akkor szükséges újraindítás, ha inkompatibilis alkalmazásokat kellett eltávolítania a telepítés előtt. Újraindításra lehet szükség, ha frissíti az alkalmazás verzióját.
	`AddEnvironment`	Kiegészíti a %PATH% rendszerváltozót a Kaspersky Endpoint Security telepítési mappájában lévő végrehajtható fájlok elérési útjával. Választható értékek: • `1` – ta %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 szolgáltatás védelmét az AM-PPL technológiával (Antimalware Protected Process Light). Választható értékek: • `1` – a Kaspersky Endpoint Security szolgáltatás AM-PPL technológiával történő védelme engedélyezve van. • `0` – a Kaspersky Endpoint Security szolgáltatás AM-PPL technológiával történő védelme ki van kapcsolva.
	`SetupReg`	Engedélyezi a beállításkulcsok írását a setup.reg fájlból a beállításjegyzékbe. `SetupReg: a setup.reg` paraméter értéke.
	`EnableTraces`	Az alkalmazástelepítések nyomkövetésének engedélyezése vagy kikapcsolása. A Kaspersky Endpoint Security elmenti a nyomkövetési fájlokat a %ProgramData%/Kaspersky Lab mappában. Választható értékek: • `1` – az alkalmazástelepítések nyomkövetése engedélyezve van. • `0` – az alkalmazástelepítések nyomkövetése ki van kapcsolva (alapértelmezett érték).
	`TracesLevel`	A nyomkövetések részleteinek szintje. Választható értékek: • `100` (kritikus). Csak a súlyos hibákról szóló üzenetek. • `200` (magas). Minden hibáról szóló üzenet, köztük a súlyos hibáké. • `300` (diagnosztika). Minden hibáról szóló üzenet, és bizonyos figyelmeztetéseket tartalmazó üzenetek.

		• `400` (fontos). Minden figyelmeztetés és szokásos és kritikus hibákról szóló üzenet és a további információkat tartalmazó üzenetek egy része. • `500` (normális). A normális és súlyos hibákról szóló minden figyelmeztetés, valamint a normális működés részletes információit tartalmazó üzenetek (alapértelmezett érték). • `600` (alacsony). Minden lehetséges üzenet.
`[Összetevők]`	`MIND`	Az összes összetevő telepítése. Az `1` paraméterérték megadása esetén minden összetevő telepítésére sor kerül, függetlenül az egyedi összetevők telepítési beállításaitól.
	`MailThreatProtection`	Levelezés védelem.
	`WebThreatProtection`	Web védelem.
	`AMSI`	AMSI Védelmi szolgáltató.
	`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 Anomáliafelügyelő.
	`FileEncryption`	Fájl szintű titkosítás könyvtárak.
	`DiskEncryption`	Teljes lemeztitkosítás rész.
	`BadUSBAttackPrevention`	BadUSB védelem.
	`AntiAPT`	Végponti szenzor.
	`AdminKitConnector`	Hálózati Ügynök Csatoló az alkalmazás távoli adminisztrációjához a Kaspersky Security Centeren keresztül. Választható értékek: • `1` – a Hálózati Ügynök Csatoló telepítésre kerül. • `0` – a Hálózati Ügynök Csatoló nem kerül telepítésre.
`[Tasks]`	`ScanMyComputer`	Teljes vizsgálat feladat. Választható értékek: • `1` – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára.

		• `0` – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.
	`ScanCritical`	Kritikus területek vizsgálata feladat. Választható értékek: • `1` – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • `0` – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.
	`Updater`	Frissítési feladat. Választható értékek: • `1` – a feladat felkerül a Kaspersky Endpoint Security feladatainak listájára. • `0` – a feladat nem kerül fel a Kaspersky Endpoint Security feladatainak listájára.

Kezdeti beállító varázsló

A Kaspersky Endpoint Security Kezdeti beállító varázslója az alkalmazástelepítési eljárást követően indul el. A Kezdeti beállító varázsló lehetővé teszi az alkalmazás aktiválását, és adatokat gyűjt az operációs rendszeren található alkalmazásokról. Ezek az alkalmazások a megbízható alkalmazások listájára kerülnek, amelyekre nem vonatkoznak az operációs rendszeren végzett műveleteiket érintő korlátozások.

A Kezdeti beállító varázsló felülete oldalak (lépések) sorozatából áll. A Kezdeti beállító varázsló oldalai között a **Vissza** és a **Tovább** gombokkal lépkedhet. A Kezdeti beállító varázsló befejezéséhez kattintson a **Megszakítás** gombra. A Kezdeti beállító varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

Ha a Kezdeti beállító varázsló valamilyen okból megszakad, a már megadott beállításokat nem menti. Az alkalmazás használatának legközelebbi kísérlete során a Kezdeti beállító varázsló ismét elindul, és a beállításokat az alapoktól kezdve meg kell adni.

Alkalmazás aktiválása

Az alkalmazást a jelenlegi rendszerdátumot és -időt tartalmazó számítógépen kell aktiválni. Ha az alkalmazás aktiválását követően a rendszerdátum és -idő megváltozik, a kulcs működésképtelenné válik. Az alkalmazás frissítések nélküli üzemmódba vált, és a Kaspersky Security Network nem használható. A kulcsot az operációs rendszer újratelepítésével lehet ismét működőképessé tenni.

Ebben a lépésben válasszon egyet a Kaspersky Endpoint Security alábbi aktiválási lehetőségei közül:

- **Aktiválás aktiváló kóddal**. Az alkalmazás aktiváló kóddal történő aktiválásához válassza ezt a lehetőséget, és adja meg az aktiváló kódot.
- **Aktiválás kulcsfájllal**. Válassza ezt a lehetőséget az alkalmazás kulcsfájllal történő aktiválásához.

- **Próbaverzió aktiválása**. Az alkalmazás próbaverziójának aktiválásához válassza ezt a lehetőséget. Az alkalmazás próbaverziója esetén a felhasználó teljesen működőképes verziót használhat a licenc által korlátozott ideig. A licenc lejártát követően az alkalmazás funkciói leblokkolnak, és a próbaverzió többé nem aktiválható.

- **Aktiválás később**. Válassza ezt a lehetőséget, ha ki szeretné hagyni a Kaspersky Endpoint Security aktiválási szakaszát. A felhasználó ekkor csak a Fájl víruskereső és a Tűzfal összetevőket használhatja. A víruskereső adatbázisok és a Kaspersky Endpoint Security modulok frissítésére a telepítés után csak egyszer lesz lehetősége. Az **Aktiválás később** lehetőség csak a Kezdeti beállító varázsló első indításakor elérhető, közvetlenül az alkalmazás telepítése után.

Az alkalmazás próbaverziójának aktiválásához, illetve az alkalmazás aktiváló kóddal történő aktiválásához internetkapcsolat szükséges.

A Kezdeti beállító varázsló folytatásához válasszon egy aktiválási lehetőséget, majd kattintson a **Tovább** gombra. A Kezdeti beállító varázsló leállításához kattintson a **Mégse** gombra.

2. lépés. Aktiválás aktiváló kóddal

Ez a lépés csak akkor áll rendelkezésre, ha az alkalmazást aktiváló kóddal aktiválja. Ez a lépés kimarad, ha az alkalmazás próbaverzióját aktiválja, illetve ha az alkalmazást kulcsfájllal aktiválja.

Ebben a lépésben a Kaspersky Endpoint Security adatokat küld az aktiválási kiszolgálónak, hogy ellenőrizze a megadott aktiváló kódot:

- Ha az aktiváló kód ellenőrzése sikeres, a Kezdeti beállító varázsló automatikusan a következő ablakra lép.

- Ha az aktiváló kód ellenőrzése nem sikerül, megjelenik egy erről tájékoztató üzenet. Ilyenkor kérjen tanácsot azzal a szoftverforgalmazótól, akitől a Kaspersky Endpoint Security licencét vásárolta.

- Ha az aktiválások száma meghaladta az aktiválási kód által engedélyezett értéket, megjelenik egy erről tájékoztató értesítés. A Kezdeti beállító varázsló megszakad, az alkalmazás pedig azt javasolja, hogy lépjen kapcsolatba a Kaspersky Terméktámogatásával.

A Kezdeti beállító varázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Kezdeti beállító varázsló leállításához kattintson a **Mégse** gombra.

Aktiválás kulcsfájllal

Ez a lépés csak akkor áll rendelkezésre, ha az alkalmazást kulcsfájllal aktiválja.

Ebben a lépésben adja meg a kulcsfájl elérési útját. Ehhez kattintson a **Tallózás** gombra, majd válassza ki a `<Fájlazonosító>.key` formátumú kulcsfájlt.

A kulcsfájl kiválasztását követően az ablak alsó részében az alábbi adatok jelennek meg.

- Kulcs

- Licenc típusa (kereskedelmi vagy próbaverzió) és a licenc által lefedett számítógépek száma
- Az alkalmazás aktiválásának dátuma a számítógépen
- Előfizetés lejárati dátuma
- Alkalmazás licenc alapján igénybe vehető funkciói
- Kulcs problémáival kapcsolatos értesítések, ha vannak. Például: *Kulcsok feketelistája megsérült*.

A Kezdeti beállító varázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Kezdeti beállító varázsló folytatásához kattintson a **Tovább** gombra. A Kezdeti beállító varázsló leállításához kattintson a **Mégse** gombra.

Aktiválandó funkciók kiválasztása

Ez a lépés csak az alkalmazás próbaverziójának aktiválása után elérhető.

Ebben a lépésben kiválaszthatja az alkalmazás aktiválását követően elérhetővé váló funkciókat:

- **Alapszintű telepítés**. Ezt a lehetőséget választva a védelmi összetevők, az Alkalmazásjogosultság-felügyelő és a Sebezhetőség-figyelő áll rendelkezésre az alkalmazás aktiválását követően.
- **Normál telepítés**. Ezt a lehetőséget választva csak az alkalmazás védelmi és felügyeleti összetevői állnak rendelkezésre az alkalmazás aktiválását követően.
- **Teljes telepítés**. Ezt a lehetőséget választva az alkalmazás összes telepített összetevője – köztük az adattitkosítási funkciók is – rendelkezésre áll az alkalmazás aktiválását követően.

Ha telepítés közben a beszerzett licenc által lehetővé tettnél több összetevőt választott ki, akkor az alkalmazás aktiválását követően a licenc alapján nem használható összetevők telepítése megtörténik, ám nem lesznek működőképesek. Ha a megvásárolt licenc a jelenleg telepítetteknél több összetevő használatát teszi lehetővé, akkor az alkalmazás aktiválását követően a nem telepített összetevők felsorolása megtalálható a **Licencelés** részben.

Alapértelmezés szerint a normál telepítés van kiválasztva.

A Kezdeti beállító varázsló előző lépésére való visszalépéshez kattintson a **Vissza** gombra. A Kezdeti beállító varázsló folytatásához kattintson a **Tovább** gombra. A Kezdeti beállító varázsló leállításához kattintson a **Mégse** gombra.

Az aktiválás befejezése

Ebben a lépésben a Kezdeti beállító varázsló tájékoztatja a Kaspersky Endpoint Security sikeres aktiválásáról. Az alábbi licenccel kapcsolatos információk jelennek meg:

- Licenc típusa (kereskedelmi vagy próbaverzió) és a licenc által lefedett számítógépek száma
- Előfizetés lejárati dátuma

- Alkalmazás licenc alapján igénybe vehető funkciói

A Kezdeti beállító varázsló folytatásához kattintson a **Tovább** gombra. A Kezdeti beállító varázsló leállításához kattintson a **Mégse** gombra.

Az operációs rendszer elemzése

Ebben a lépésben kerül sor az adatgyűjtésre az operációs rendszeren található alkalmazásokról. Ezek az alkalmazások a megbízható alkalmazások listájára kerülnek, amelyekre nem vonatkoznak az operációs rendszeren végzett műveleteiket érintő korlátozások.

A többi alkalmazás elemzésére azt követően kerül sor, hogy a Kaspersky Endpoint Security telepítése után először elindulnak.

A Kezdeti beállító varázsló leállításához kattintson a **Mégse** gombra.

Az alkalmazás kezdeti beállításának befejezése

A Kezdeti beállító varázsló befejező ablaka információkat tartalmaz a Kaspersky Endpoint Security telepítési folyamat befejezéséről.

Ha el szeretné indítani a Kaspersky Endpoint Security alkalmazást, kattintson a **Befejezés** gombra.

Ha a Kaspersky Endpoint Security elindítása nélkül ki szeretne lépni a Kezdeti beállító varázslóból, törölje a **Kaspersky Endpoint Security 10 for Windows indítása** jelölőnégyzetet, és kattintson a **Befejezés** gombra.

Kaspersky Security Network Nyilatkozat

Ennél a lépésnél felkérést kap a Kaspersky Security Network való részvételre.

Tekintse meg a Kaspersky Security Network nyilatkozatát.

- Ha elfogadja az összes feltételt, jelölje be az **Elfogadom a Kaspersky Security Network részvételi feltételeit** jelölőnégyzetet a Kezdeti beállító varázsló ablakában.
- Ha nem fogadja el a Kaspersky Security Network részvételi feltételeit, jelölje be az **Nem fogadom el a Kaspersky Security Network részvételi feltételeit** jelölőnégyzetet a Kezdeti beállító varázsló ablakában.

A Kezdeti beállító varázsló folytatásához kattintson az **OK** gombra.

A régi alkalmazásverziók frissítésének módjai

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows alkalmazás korábbi verziójának frissítéséhez fejtse vissza az összes titkosított merevlemezt.

Az alábbi alkalmazásokat lehet a Kaspersky Endpoint Security 10 Service Pack 2 for Windows alkalmazásra frissíteni:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (build 6.0.4.1424), MP4 CF2 (build 6.0.4.1611)

- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (build 6.0.4.1424) / MP4 CF2 (build 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (build 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (build 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (build 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (build 10.2.5.3201).

Ha a fent felsorolt alkalmazások közül valamelyiket a Kaspersky Endpoint Security 10 Service Pack 2 for Windows alkalmazásra frissíti, a Karantén és másolattároló tartalma nem adódik át.

Az alkalmazás régi verzióját az alábbiak szerint frissítheti:

- Helyileg, interaktív módban, a Alkalmazástelepítő varázslóval.
- Helyileg, nem interaktív módban, a Telepítővarázslóval
- Távolról, a Kaspersky Security Center szoftvercsomaggal (lásd: *Kaspersky Security Center megvalósítási útmutató*)
- Távolról, a Microsoft Windows Group Policy Editora segítségével (lásd az operációs rendszer súgófájljait)

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows korábbi verziójáról történő frissítéskor az alkalmazás korábbi verzióját nem szükséges eltávolítani. A korábbi alkalmazásverzió frissítése előtt javasoljuk, hogy lépjen ki minden aktív alkalmazásból.

Az alkalmazás eltávolítása

Ez a rész ismerteti a Kaspersky Endpoint Security számítógépről történő eltávolítását.

Az alkalmazás eltávolításának módjai

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

A Kaspersky Endpoint Security több módon eltávolítható a számítógépről:

- Helyileg, interaktív módban, a Telepítővarázslóval
- Helyileg, nem interaktív módban, a Telepítővarázslóval
- Távolról, a Kaspersky Security Center szoftvercsomaggal (részletekért lásd: *Kaspersky Security Center megvalósítási útmutató*)

- Távolról, a Microsoft Windows Group Policy Editora segítségével (lásd az operációs rendszer súgófájljait)

Az alkalmazás eltávolítása a Telepítővarázsló segítségével

A Kaspersky Endpoint Security eltávolítása a Telepítővarázsló segítségével:

1. Válassza ki a **Start** menüben az **Alkalmazások→ Kaspersky Endpoint Security 10 for Windows → Módosítás, Javítás vagy Eltávolítás** lehetőséget.

   Elindul a Telepítővarázsló.

2. A Telepítővarázsló **Alkalmazás módosítása, javítása vagy eltávolítása** ablakában kattintson a **Eltávolítás** gombra.

3. Kövesse a Telepítővarázsló utasításait.

1. lépés. Az alkalmazás adatainak jövőbeni használatra való elmentése

Ebben a lépésben megadhatja, hogy az alkalmazás által használt adatok közül melyeket szeretné megtartani az alkalmazás következő telepítésekor való további használatra (pl. újabb verzió telepítésekor). Ha nem ad meg adatokat, az alkalmazás teljes mértékben törlődik.

Az alkalmazás adatainak jövőbeni használatra való elmentéséhez tegye a következőket:

jelölje be a menteni kívánt adattípusok melletti jelölőnégyzeteket:

- **Aktiválási adatok** – az alkalmazás jövőbeni aktiválását szükségtelenné tevő adatok. Az aktiválásra automatikusan sor kerül a jelenlegi licenccel, feltéve, hogy az a telepítés idején még nem járt le.
- **Biztonsági mentés fájljai** – az alkalmazás által vizsgált, és a Karanténba helyezett fájlok.

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

  Ha az alkalmazás eltávolítása után Biztonsági mentésbe helyezett objektumokat használni szeretné, akkor az alkalmazás eltávolítása előtt vissza kell állítani ezeket az objektumokat a tárhelyükről. 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 tárolása** – az alkalmazás eltávolítása előtt titkosított fájlokhoz és eszközökhöz közvetlen hozzáférést nyújtó adatok. A titkosított fájlokhoz és meghajtókhoz közvetlenül hozzá lehet férni az alkalmazás titkosítási funkciókkal való újratelepítését követően.

  Alapértelmezés szerint a jelölőnégyzet be van jelölve.

A Telepítővarázsló folytatásához kattintson a **Tovább** gombra. A Telepítővarázsló leállításához kattintson a **Mégse** gombra.

2. lépés Az alkalmazás eltávolításának megerősítése

Mivel az alkalmazás eltávolítása veszélyezteti a számítógép biztonságát, meg kell erősítenie az alkalmazás eltávolítására irányuló szándékát. Ehhez kattintson az **Eltávolítás** gombra.

Az alkalmazás eltávolításának leállításához a **Mégse** gombra kattintva bármikor megszakíthatja ezt a műveletet.

3. lépés. Az alkalmazás eltávolítása. Eltávolítás befejezése

A Telepítővarázsló ennél a lépésnél távolítja el az alkalmazást a számítógépről. Várja meg, amíg az alkalmazás eltávolítása befejeződik.

Az alkalmazás eltávolításakor elképzelhető, hogy az operációs rendszert újra kell indítani. Ha úgy dönt, hogy nem indítja újra azonnal a számítógépet, az alkalmazás eltávolításának befejezése áttevődik arra az alkalomra, amikor az operációs rendszer újraindul, vagy a számítógépet kikapcsolja és bekapcsolja.

Az alkalmazás eltávolítása a parancssorból

Az alkalmazás eltávolítási folyamata a parancssorból is elindítható. Az eltávolítás interaktív vagy csendes módban (az Alkalmazástelepítő varázsló elindítása nélkül) történik.

Az alkalmazás eltávolítási folyamatának indítása interaktív módban:

Gépelje be a parancssorban a következőt: `setup.exe /x` vagy `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Elindul a Telepítővarázsló. Kövesse a Telepítővarázsló utasításait.

Az alkalmazás eltávolítási folyamatának indítása csendes módban:

Gépelje be a parancssorban a következőt: `setup.exe /s /x` vagy `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Ezzel az alkalmazás eltávolítási folyamata elindul csendes módban (a Telepítővarázsló elindítása nélkül).

Ha az alkalmazás eltávolítási művelete jelszóval védett, akkor a parancssorban meg kell adni a felhasználónevet és a hozzá tartozó jelszót.

Az alkalmazás eltávolítása a parancssorban interaktív módban, ha a Kaspersky Endpoint Security eltávolításához, módosításához és javításához felhasználónév és jelszó van beállítva:

Gépelje be a parancssorban a következőt: `setup.exe /pKLLOGIN=<felhasználónév> /pKLPASSWD=***** /x` vagy

```
msiexec.exe KLLOGIN=<felhasználónév> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}.
```

Elindul a Telepítővarázsló. Kövesse a Telepítővarázsló utasításait.

Az alkalmazás eltávolítása a parancssorban csendes módban, ha a Kaspersky Endpoint Security eltávolításához, módosításához és javításához felhasználónév és jelszó van beállítva:

Gépelje be a parancssorban a következőt: `setup.exe /pKLLOGIN=<felhasználónév> /pKLPASSWD=***** /s /x` vagy

```
msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<felhasználónév>
KLPASSWD=***** /qn.
```

A Hitelesítési ügynök tesztműködése után megmaradt 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 kétféleképpen távolíthatja el:

- A Kaspersky Security Center rendszabállyal.
- A Visszaállító segédprogrammal.

A Hitelesítési ügynök tesztműködése után megmaradt objektumok és adatok eltávolítása Kaspersky Security Center rendszabállyal:

1. Alkalmazzon a számítógépen olyan Kaspersky Security Center rendszabályt, amely úgy van beállítva, hogy a számítógép összes merevlemezét visszafejti.
2. Indítsa el a Kaspersky Endpoint Security alkalmazást.

A Hitelesítési ügynök tesztműködése után megmaradt objektumok és adatok eltávolítása a Visszaállító segédprogrammal:

1. Indítsa el a Visszaállító segédprogramot a Kaspersky Endpoint Security segítségével létrehozott fdert.exe végrehajtható fájl futtatásával azon a számítógépen, amelyhez csatlakoztatva van a hitelesítési ügynök tesztműködése után visszamaradt objektumokat és adatokat tartalmazó rendszermerevlemez.
2. A Visszaállító segédprogram ablakának **Eszköz kiválasztása** legördülő listáján válassza ki az eltávolítani kívánt objektumokat és adatokat tartalmazó rendszermerevlemezt.
3. Kattintson a **Vizsgálat** gombra.
4. Kattintson a **AA objektumok és adatok törlése** gombra.

Ezzel elindul a Hitelesítési ügynök tesztműködése után megmaradt objektumok és adatok eltávolítási folyamata.

A Hitelesítési ügynök tesztműködése után megmaradt objektumok és adatok eltávolítását követően szükség lehet az alkalmazás Hitelesítési ügynökkel való inkompatibilitására vonatkozó adatok eltávolítására is.

Az alkalmazás Hitelesítési ügynökkel való inkompatibilitására vonatkozó adatok eltávolítása:

Gépelje be a parancssorba az `avp pbatestreset` parancsot.

Az `avp pbatestreset` parancs végrehajtásához telepítve kell lenniük a titkosítási összetevőknek.

Az alkalmazás felülete

Ez a rész ismerteti az alkalmazás felületének alapszintű elemeit.

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.

Alkalmazástevékenység jelzése

Az alkalmazásikon az alkalmazástevékenységet jelzi:

- A védelem engedélyezve van ikon az alkalmazás összes védelmi összetevőjének engedélyezett állapotát jelzi.
- A újra kell indítani a számítógépet ikon azt jelzi, hogy figyelmet igénylő fontos események történtek a Kaspersky Endpoint Security működése során. Például a Fájl védelem összetevő letiltásra került vagy az alkalmazásadatbázisok elavultak.
- A hiba történt ikon azt jelzi, hogy kritikus fontosságú események történtek a Kaspersky Endpoint Security működése során. Például egy összetevő működése során meghibásodás történt, vagy megsérültek az alkalmazás adatbázisai.

Az alkalmazás ikonjának helyi menüje

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.
- **Beállítások**. Megnyitja a **Beállítások** ablakot. A **Beállítások** lapon lehet az alkalmazás alapértelmezett beállításait módosítani.
- **Védelem és felügyelet szüneteltetése** / **Védelem és felügyelet folytatása**. Átmenetileg szünetelteti, illetve folytatja a védelmi és felügyeleti összetevők működését. Ez a helyi menüelem nem befolyásolja a frissítési feladatot és a vizsgálati feladatokat, mivel csak akkor használható, ha a Kaspersky Security Center rendszabály le van tiltva.

  A Kaspersky Security Network a Kaspersky Endpoint Security által van használva, függetlenül attól, hogy a védelem és felügyelet összetevők működése szünetel vagy fut.

- **Szabályzat letiltása** / **Szabályzat engedélyezése**. Letiltja, illetve engedélyezi a Kaspersky Security Center rendszabályát. Ez a helyi menüelem akkor használható, ha rendszabály van érvényben egy olyan számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, és be van állítva jelszó a Kaspersky Security Center rendszabály letiltásához.

- **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

Az alkalmazásikon helyi menüjét úgy nyithatja meg, ha a mutatót a Microsoft Windows tálca értesítési területén látható alkalmazásikon fölé viszi, majd kattint a jobb egérgombbal.

Fő alkalmazásablak

A Kaspersky Endpoint Security főablaka a felhasználói felület azon elemeit tartalmazza, amelyekkel elérhetők az alkalmazás fő funkciói.

A fő alkalmazásablakban az alábbi elemek találhatók:

- Hivatkozás a **Kaspersky Endpoint Security for Windows** alkalmazásra. Erre a hivatkozásra kattintva megnyílik a **Névjegy** ablak, amely tájékoztatást nyújt az alkalmazásverzióról.

- Gomb Súgó ikon. Erre a gombra kattintva megnyílik a Kaspersky Endpoint Security súgórendszere.

- **Fenyegetésészlelő technológiák** rész. Ez a rész a következő információkat tartalmazza:

  - A rész bal oldala megjeleníti a fenyegetésészlelési technológiák listáját. Az egyes fenyegetésészlelési technológiák nevétől jobbra jelenik meg az adott technológia által azonosított fenyegetések száma.

  - Az aktív fenyegetések jelenlététől függően a rész közepén a következő feliratok egyike látható:

    - **Nincsenek fenyegetések**. Ha ez a felirat látszik, akkor a **Fenyegetésészlelő technológiák** részre kattintva megnyílik a **Fenyegetésészlelő technológiák** ablak, amely rövid leírást ad a fenyegetésészlelő technológiákról, valamint a Kaspersky Security Network felhőszolgáltatás infrastruktúrájának állapotáról és globális statisztikáiról.

    - **N aktív fenyegetések**. Ha ez a felirat jelenik meg, akkor a **Fenyegetésészlelő technológiák** részre kattintva megnyílik az **Aktív fenyegetések** ablak, melyben a valamilyen okból fel nem dolgozott fertőzött fájlokhoz kapcsolódó események listája látható.

- A **Védelem összetevői** rész. Erre a részre kattintva megnyílik a **Védelem összetevői** ablak. Ebben az ablakban megtekintheti a telepített összetevők működési állapotát. Ebben az ablakban megnyithatja továbbá a **Beállítások** ablak egy alszakaszát, melyben a titkosítási összetevőkön kívüli telepített összetevők beállításai találhatók.

- **Feladatok** rész. Erre a részre kattintva megnyílik a **Feladatok** ablak. Ebben az ablakban kezelheti a Kaspersky Endpoint Security feladatainak működését, melyek az alkalmazásmodulok és az adatbázisok frissítésére, a

vírusok és egyéb rosszindulatú programok keresésére, valamint az integritási ellenőrzés futtatására szolgálnak.

- **Jelentések** gomb. Erre a gombra kattintva megnyílik a **Jelentések** ablak, melyben általában az alkalmazás, illetve külön összetevői működése vagy a feladatok elvégzése során történt eseményekről szóló információk találhatók.
- **Tárhelyek** gomb. Erre a gombra kattintva megnyílik a **Biztonsági mentés** ablak. Ebben az ablakban látható az alkalmazás által törölt fertőzött fájlok példányainak listája.
- **Támogatás** gomb. Erre a gombra kattintva megnyílik a **Támogatás** ablak, amely információkat jelenít meg az operációs rendszerről, a Kaspersky Endpoint Security jelenlegi verziójáról, és hivatkozásokat tartalmaz a Kaspersky információs erőforrásaira.
- **Beállítások** gomb. Erre a gombra kattintva megnyílik a **Beállítások** ablak, melyben az alkalmazás alapértelmezett beállításait lehet módosítani.
- Gomb / / . Erre a gombra kattintva megnyílik az **Események** ablak, amely információkat tartalmaz a rendelkezésre álló frissítésekről, valamint a titkosított fájlokhoz és eszközökhöz való hozzáférési kérésekről.
- **Licenc** hivatkozás. Erre a hivatkozásra kattintva megnyílik a **Licencelés** ablak, amely tájékoztatást nyújt az aktuális licencről.

Fő alkalmazásablak

A Kaspersky Endpoint Security főablakának megnyitásához hajtsa végre a következő műveletek valamelyikét:

- Kattintson az alkalmazás Microsoft Windows tálca értesítési területén lévő ikonjára.
- Válassza a **Kaspersky Endpoint Security for Windows** elemet az alkalmazásikon helyi menüjében.

Alkalmazásbeállítások ablak

A Kaspersky Endpoint Security beállításainak ablakában megadhatja az alkalmazás általános beállításait, valamint az egyedi összetevők, jelentések és tárhelyek, vizsgálati és frissítési feladatok és a Kaspersky Security Network kiszolgálóival való kommunikáció beállításait.

Az alkalmazás beállításainak ablaka két részből áll (lásd a következő ábrát):

- A bal oldali részen találhatók az alkalmazásösszetevők, a feladatok és a több alrészből álló speciális beállítási rész.
- A jobb oldali részen vezérlőelemek találhatók, melyek segítségével megadhatja az ablak bal oldali részén kiválasztott összetevő vagy feladat beállításait, valamint a speciális beállításokat.

Alkalmazásbeállítások ablak

Az alkalmazás beállítási ablakának megnyitásához hajtsa végre a következő műveletek valamelyikét:

- A fő alkalmazásablakban válassza ki a **Beállítások** lapot.
- Az alkalmazásikon helyi menüjében válassza ki a **Beállítások** elemet.

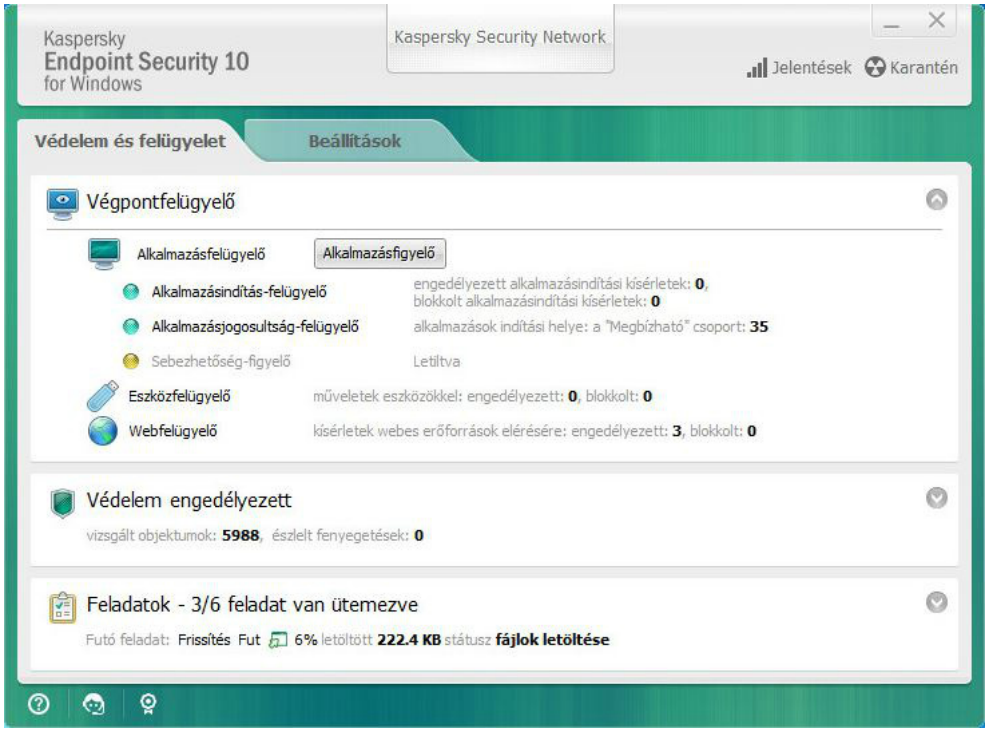
Alkalmazás Védelem és felügyelet lapja

A Kaspersky Endpoint Security Védelem és felügyelet lapja az összes feladat teljesítményére és az összes alkalmazásösszetevő működésére vonatkozó általános információk nyújtására szolgál. Ezen a lapon szabályozható az összetevők működése és a feladatok teljesítménye is.

Az Alkalmazásvédelem és -felügyelet lap három részből áll (lásd a lenti ábrát):

- A **Végpontfelügyelő** rész a felügyeleti összetevők listáját tartalmazza.
- A **Védelem kezelése** rész a Vírusvédelem összetevőinek listáját tartalmazza.
- A **Feladatok** részben a számítógépen futó helyi feladatok listája található.

Minden rész vezérlőelemeket tartalmaz, melyek segítségével egy-egy összetevő működését be- vagy kikapcsolhatja, a kiválasztott összetevő vagy feladat beállításaihoz léphet, illetve megtekintheti működési statisztikáját.



Alkalmazás Védelem és felügyelet lapja

Az Alkalmazásvédelem és -felügyelet lap megnyitásához hajtsa végre a következő műveletek valamelyikét:

- A fő alkalmazásablakban válassza ki a **Védelem és felügyelet** lapot.
- Kattintson az alkalmazás Microsoft Windows tálca értesítési területén lévő ikonjára.
- Válassza a **Kaspersky Endpoint Security 10 for Windows** elemet az alkalmazásikon helyi menüjében.

Az alkalmazás licencelése

Ez a rész tájékoztatást nyújt az alkalmazás licencelésével kapcsolatos általános fogalmak tekintetében.

A végfelhasználói licencszerződés

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. A dokumentum megtalálható az alkalmazás terjesztőkészletében.

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.

Az érvényes licenccel rendelkező felhasználók a következő típusú szolgáltatásokra jogosultak:

- Az alkalmazás használata a Végfelhasználói licencszerződés feltételeinek megfelelően.
- Terméktámogatás.

A szolgáltatások köre és valamint az alkalmazás használatának időtartama az alkalmazás aktiválásához használt licenc típusától függ.

Az alábbi licencek biztosítottak:

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

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

  Mindössze egyszer aktiválhatja az alkalmazást próbalicenccel.

- *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:

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

Az előfizetés

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

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

Korlátozott előfizetés esetén a lejáratot követően türelmi időszakot kaphat az előfizetés megújítására, melynek során az alkalmazás megőrzi funkcióit. A türelmi időszak megadásáról és időtartamáról a szolgáltató dönt.

A Kaspersky Endpoint Security előfizetéses használatához a szolgáltatótól kapott aktiváló kódot kell alkalmaznia. Az aktiváló kód alkalmazását követően sor kerül az aktív kulcs telepítésére. Az aktív kulcs határozza meg az alkalmazás előfizetés alapján történő használatának licencét. További kulcsot kizárólag aktiváló kód segítségével lehet telepíteni, kulcsfájllal vagy előfizetés alapján nem.

Az alkalmazás előfizetés alapján használható funkciói megfelelnek az alkalmazásfunkcióknak a következő kereskedelmi licenctípusoknál: Szokásos, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Az ilyen típusú licencek fájlkiszolgálók, munkaállomások és mobileszközök védelmére szolgálnak, és támogatják a felügyeleti összetevők használatát munkaállomásokon és mobileszközökön.

Az előfizetés kezelésének lehetséges opciói szolgáltatónként változhatnak. Előfordulhat, hogy a szolgáltató nem kínál fel olyan türelmi időszakot az előfizetés megújítására, amelynek folyamán az alkalmazás összes funkciója működik.

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

Az aktiváló kód

Az *aktiváló kód* egy egyedi, húsz latin betűből és számjegyből álló alfanumerikus karaktersorozat, amelyet a Kaspersky Endpoint Security kereskedelmi licencének megvásárlásakor kap.

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

Az alkalmazás aktiváló kóddal történő aktiválásakor sor kerül az aktív kulcs telepítésére. További kulcsot kizárólag aktiváló kód segítségével lehet telepíteni, kulcsfájllal vagy előfizetés alapján nem.

Ha az alkalmazás aktiválását követően elveszti az aktiváló kódot, a kódot visszaállíthatja. Az aktiváló kód például Kaspersky CompanyAccount fiók regisztrálásakor szükséges. Az aktiváló kód visszaállításához kapcsolatba kell lépnie a Kaspersky Terméktámogatással.

A kulcs

A *kulcs* egy egyedi alfanumerikus sorozat. A kulcs révén lehetséges az alkalmazás használata a Licenctanúsítványban szereplő feltételeknek megfelelően (licenc típusa, licenc érvényességi időszaka, licenc korlátozásai).

Az előfizetés alapján telepített kulcshoz nem jár licenctanúsítvány.

Kulcsot aktiváló kód vagy kulcsfájl segítségével lehet hozzáadni alkalmazáshoz.

Kulcsokat lehetséges hozzáadni, szerkeszteni és törölni. A kulcsot a végfelhasználói licencszerződés feltételeinek megsértése esetén a Kaspersky blokkolhatja. Ha a kulcs feketelistára került, az alkalmazás további használatához másik kulcsra van szükség.

Ha egy lejárt licenc kulcsát törli, az alkalmazás funkciói nem érhetők el. A törlést követően ilyen kulcsot többé nem lehet hozzáadni.

A kulcsnak két típusa van: aktív és további kód.

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 *további kulcs* lehetővé teszi a felhasználó számára az alkalmazás használatát, de aktuálisan nincs használatban. A további kulcs automatikusan aktívvá válik az aktuális aktív kulcs lejártával. További kulcs csak abban az esetben hozzáadható, ha van elérhető aktív kulcs.

A próbaverziós licenckulcs csak aktív kulcsként adható meg. Nem lehet kiegészítő kulcsként megadni. A próbaverziós licenckulcs nem válthatja fel kereskedelmi licenc aktív kulcsát.

Ha egy kulcs feketelistára kerül, alkalmazásnak az aktiválásához használt licenc által megszabott funkciói nyolc napig maradnak használhatóak. A Kaspersky Security Network, valamint adatbázis- és alkalmazásmodul-frissítések korlátozások nélkül igénybe vehetők. Az alkalmazás értesíti a felhasználót, hogy a kulcs feketelistára került. Nyolc nap elteltével alkalmazás funkciói arra a szintre korlátozódnak, amely a licencidőszak lejárta után áll rendelkezésre: az alkalmazás frissítések nélkül működik, a Kaspersky Security Network pedig nem használható.

A kulcsfájl

A *kulcsfájl* egy .key kiterjesztésű fájl, melyet a Kaspersky Endpoint Security megvásárlását követően kap meg a Kaspersky vállalattól. A kulcsfájl célja az alkalmazást aktiváló kulcs megadása.

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

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

Kulcsfájl visszaállításához tegye az alábbiak valamelyikét:

- Lépjen kapcsolatba a licenc eladójával.
- Kulcsfájl beszerzése a Kaspersky webhelyen a meglévő aktiváló kód alapján.

Az adatszolgáltatás

Ha egy aktiváló kód használatával aktiválja a Kaspersky Endpoint Security-t, beleegyezik a következő információk automatikus továbbításába 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 aktívkulcs-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 előállítása érdekében.

Aktiváló kód használatával beleegyezik a fent felsorolt adatok automatikus továbbításába. Ha nem egyezik bele az információ továbbításába a Kaspersky felé, használjon egy kulcsfájlt a Kaspersky Endpoint Security aktiválásához.

A Végfelhasználói licencszerződés elfogadásával beleegyez a következő információk automatikus továbbításába:

- Kaspersky Endpoint Security frissítése közben:
  - A Kaspersky Endpoint Security verziója
  - A Kaspersky Endpoint Security azonosítója
  - Aktív kulcs
  - A frissítés indításának egyedi azonosítója
  - A Kaspersky Endpoint Security telepítés egyedi azonosítója
- Ha a Kaspersky Endpoint Security felületen lévő következő hivatkozások:
  - A Kaspersky Endpoint Security verziója
  - Az operációs rendszer verziója
  - A Kaspersky Endpoint Security aktiválásának dátuma
  - Előfizetés lejárati 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 hash kódja, és neve a Kaspersky osztályozás alapján
  - Kaspersky Endpoint Security aktiválási hiba kategóriája
  - Kaspersky Endpoint Security aktiválási hibakód
  - A kulcs lejártáig hátralévő napok száma
  - A kulcs hozzáadása óta eltelt napok száma
  - A licenc lejárta óta eltelt napok száma
  - A számítógépek száma, melyeken az aktív licenc alkalmazva van
  - Aktív kulcs
  - Kaspersky Endpoint Security licenc feltétel
  - A licenc jelenlegi állapota

- Az aktív licenc típusa
- Alkalmazástípus
- A frissítés indításának egyedi azonosítója
- A Kaspersky Endpoint Security telepítés egyedi azonosítója
- A szoftver telepítés egyedi azonosítója a számítógépen
- A Kaspersky Endpoint Security felületének nyelve

A kapott adatokat a Kaspersky a törvénynek és a Kaspersky vonatkozó követelményeinek és előírásainak megfelelően védi.

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.

A licencadatok megtekintése

Információk megtekintése a licencről:

kattintson a fő alkalmazásablak alsó részén található license_expired / main_license lehetőségre.

Megnyílik a **Licencelés** ablak. Az ablak megjeleníti a licenc információit (lásd az alábbi ábrát).


KES11_License_info

Licencelés ablak

A következő információt tartalmazza a **Licencelés** ablak:

- **Kulcs állapota**. Számoskulcs tárolható a számítógépen. A kulcsnak két típusa van: aktív és további kód. Az alkalmazásban csak egy aktív kulcs lehet. Egy másik kulcs csak akkor lehet aktív, ha az aktív kulcs lejár vagy akkor, ha törölte az aktív kulcsot a component_malfunction gomb használatával.
- **Kulcs**. A *kulcs* egy egyedi alfanumerikus sorozat, ami az aktiváló kódból vagy a kulcsfájlból van létrehozva.
- **Licenctípus**. A következő típusú licencek érhetőek el: próba és kereskedelmi.
- **Alkalmazásnév**. A megvásárolt Kaspersky termék teljes neve.
- **Funkció**. A licence alatt elérhető alkalmazásfunkciók. A funkciók közé tartozhat a Védelem, a Biztonsági felügyelet, az Adattitkosítás, a Végponti szenzor és egyebek. Az elérhető funkciók listáját megtekintheti a Licenctanúsítványban is.
- **További információk a licencről**. Licenctípus, a licenc által fedezett számítógépek száma, a licenc indít és lejárati dátuma (csak az aktív kulcshoz).

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

A Licencelés ablakban az alábbiak egyikét is megteheti:

- **Licencvásárlás** / **Licenc megújítás**. 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 alapján**. Elindítja az Alkalmazás aktiválása varázslót. Ebben a Varázslóban hozzáadhat egy kulcsot az aktiváló kód vagy a kulcsfájl használatával. Az Alkalmazás Aktiváló Varázsló lehetővé teszi, hogy hozzáadjon egy aktív kulcsot és egy további kulcsot.

Licencvásárlás

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

Licencvásárlás:

1. Kattintson a fő alkalmazásablakban a main_license / license_expired gombra.

   Megnyílik a **Licencelés** ablak.

2. A **Licencelés** ablakban 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.

Licenc megújítása

Ha a licenc lejáratához közeledik, megújíthatja. Ily módon a számítógép védelme fennmarad a jelenlegi licenc lejártát követően is, és amíg az alkalmazást új licenc alapján nem aktiválja.

Licenc megújítása:

1. Szerezzen be új alkalmazásaktiváló kódot vagy kulcsfájlt.
2. Adjon meg további kulcsot a kapott aktiváló kóddal vagy a kulcsfájllal.

Ennek eredményeképpen további kulcs megadására kerül sor. A licenc lejártakor aktívvá válik.

A Kaspersky aktiválási kiszolgálói közti terheléselosztás miatt eltarthat egy ideig, amíg a kulcs a továbbiról az aktívra frissül.

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 lejártát követő türelmi időszak, melynek során az előfizetés meghosszabbítható) lejártának napján a Kaspersky Endpoint Security erre utaló értesítést jelenít meg, és felhagy az előfizetés automatikus meghosszabbítási kísérletével. Ilyenkor a Kaspersky Endpoint Security ugyanúgy viselkedik, mint amikor az alkalmazás kereskedelmi licence jár le: az alkalmazás frissítések nélkül működik, a Kaspersky Security Network pedig nem használható.

Az előfizetést automatikusan megújíthatja a szolgáltató weboldalán.

Az előfizetés állapotát kézileg frissítheti a **Licencelés** ablakban. Erre akkor lehet szükség, ha az előfizetést a türelmi időszak lejárta után hosszabbította meg, és az alkalmazás nem frissítette automatikusan az előfizetés állapotát.

A szolgáltató webhelyének felkeresése

A szolgáltató webhelyének felkeresése az alkalmazás felületéről:

1. Kattintson a fő alkalmazásablakban a main_license / license_expired gombra.

   Megnyílik a **Licencelés** ablak.

2. Kattintson a **Licencelés** ablakban a **Lépjen kapcsolatba az előfizetési szolgáltatójával** lehetőségre.

Az alkalmazás aktiválási módjai

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

Az alkalmazást az alábbi módokon aktiválhatja:

- A Kezdeti beállító varázsló használatával történő alkalmazás telepítéskor. Ily módon az aktív kulcsot is megadhatja.
- Helyileg az alkalmazás felhasználói felületén az Aktiválási varázslóval. Ily módon az aktív és a további kulcsot egyaránt megadhatja.
- Távolról a Kaspersky Security Center szoftvercsomaggal kulcshozzáadási feladat létrehozásával, majd elindításával. Ily módon az aktív és a további kulcsot egyaránt megadhatja.
- Távolról a Kaspersky Security Center Administration Server kulcstárban tárolt kulcsok és aktiváló kódok ügyfélszámítógépek részére történő szétosztásával (további információért lásd a Kaspersky Security Center Súgót). Ily módon az aktív és a további kulcsot egyaránt 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 terheléselosztás miatt. Ha az alkalmazást azonnal aktiválni szeretné, megszakíthatja a folyamatban lévő aktiválási eljárást, és elkezdheti az aktiválást az Aktiválási varázslóval.

Az Aktiválási varázslóval aktiválhatja az alkalmazást.

A Kaspersky Endpoint Security aktiválása az Aktiválási varázsló segítségével:

1. Kattintson a fő alkalmazásablak alsó részén található license_expired / main_license gombra.

   Megnyílik a **Licencelés** ablak.

2. A **Licencelés** ablakban kattintson az **Alkalmazás aktiválása új licenccel** gombra.

   Elindul az Alkalmazás aktiválása varázsló.

3. Kövesse az Aktiválási varázsló utasításait.

Az alkalmazás aktiválási eljárásával kapcsolatos információ a Kezdeti beállító varázsló részben található.

Az alkalmazás aktiválása a parancssorból

Az alkalmazás aktiválása a parancssorból:

Gépelje be a parancssorba a következőt: `avp.com license /add <aktiváló kód vagy kulcsfájl> /password=<jelszó>`.

Az alkalmazás indítása és leállítása

Ez a rész ismerteti, hogyan lehet az alkalmazás automatikus indítását beállítani, kézileg elindítani és leállítani az alkalmazást, illetve a védelmi és felügyeleti összetevőket szüneteltetni és újraindítani.

Az alkalmazás automatikus indításának engedélyezése és letiltása

Az automatikus indítás azt jelenti, hogy a Kaspersky Endpoint Security az operációs rendszer indulása után felhasználói beavatkozás nélkül azonnal elindul. Alapértelmezés szerint ez az alkalmazásindítási lehetőség van engedélyezve.

A telepítést követően az első alkalommal a Kaspersky Endpoint Security automatikusan elindul. Ezt követően az alkalmazás az operációs rendszer indítását követően automatikusan elindul.

A Kaspersky Endpoint Security víruskereső adatbázisainak letöltése az operációs rendszer elindulását követően a számítógép képességeitől függően akár két percig is eltarthat. Eközben a számítógép védelmi szintje csökken. A víruskereső adatbázisok letöltése a Kaspersky Endpoint Security már betöltött operációs rendszeren történő elindítása esetén nem csökkenti a számítógép védelmének szintjét.

Az alkalmazás automatikus indításának engedélyezése és letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. Végezze el az alábbiak egyikét:

   - Ha engedélyezni szeretné az alkalmazás automatikus futását, jelölje be a **Kaspersky Endpoint Security 10 for Windows elindítása a számítógép indításakor** jelölőnégyzetet.
   - Ha le szeretné tiltani az alkalmazás automatikus futását, törölje a **Kaspersky Endpoint Security 10 for Windows elindítása a számítógép indításakor** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az alkalmazás kézi elindítása és leállítása

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 Kaspersky Endpoint Security alkalmazást akkor kell kézileg elindítani, ha korábban letiltotta az alkalmazás automatikus indítását.

Az alkalmazás kézi indítása:

Válassza ki a **Start** menüben az **Alkalmazások** →Κασπερσκψ Ενδποιντ Σεχυριτψ φορ Ωινδοωσ elemet.

Az alkalmazás kézi leállítása:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.
2. A helyi menüben válassza a **Kilépés** elemet.

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 hiba történt ikon azt jeleni, hogy a számítógép védelme és felügyelete szünetel.
- A védelem engedélyezve van ikon azt jeleni, hogy a számítógép védelme és felügyelete ki van kapcsolva.

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

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

A számítógép védelmének és felügyeletének szüneteltetése és folytatása:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.
2. A helyi menüjében válassza a **Védelem és felügyelet szüneteltetése** elemet.

   Megnyílik a **Védelem szüneteltetése** ablak.
3. Válassza ki az alábbi lehetőségek egyikét:

   - **Szüneteltetés a megadott időre** – a számítógép védelme és felügyelete a lenti legördülő listán megadott idő leteltekor folytatódik.
   - **Szüneteltetés újraindításig** – A számítógép védelme és a felügyelet azt követően kapcsol vissza, hogy kilép az alkalmazásból, és ismét megnyitja, illetve újraindítja az operációs rendszert. A lehetőség használatához engedélyezni kell az alkalmazás automatikus indítását.
   - **Szüneteltetés** – a számítógép védelme és felügyelete akkor folytatódik, ha Ön úgy dönt, hogy visszakapcsolja.
4. Ha az előző lépésben a **Szüneteltetés a megadott időre** lehetőséget választotta, akkor válassza ki a legördülő listán a szükséges időközt.

A számítógép védelmének és felügyeletének folytatása:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.

2. A helyi menüjében válassza a **Védelem és felügyelet folytatása** elemet.

A számítógép védelmét és felügyeletét attól függetlenül bármikor folytathatja, hogy korábban milyen felfüggesztési lehetőséget választott ki.

A számítógép fájlrendszerének védelme. Fájl víruskereső

Ez a rész tájékoztatást nyújt a Fájl víruskeresővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Fájl víruskereső

A Fájl víruskereső megakadályozza a számítógép fájlrendszerének megfertőződését. Alapértelmezés szerint a Fájl víruskereső a Kaspersky Endpoint Security alkalmazással együtt indul el, folyamatosan aktív marad a számítógép memóriájában, és vizsgálja a számítógépen és a hozzá csatlakoztatott összes csatlakoztatott meghajtón a megnyitott, mentett és elindított összes fájlban a vírusok és egyéb fenyegetések jelenlétét.

Ha egy fájlban fenyegetést észlel, a Kaspersky Endpoint Security az alábbiakat végzi el:

1. Észleli a fájlban talált objektum típusát (például *vírus* vagy *trójai*).
2. A fájlt *valószínűleg fertőzöttként* címkézi meg, ha a vizsgálat során nem tudja megállapítani, hogy a fájl fertőzött-e. A fájl valószínűleg egy vírus vagy egyéb rosszindulatú program tipikus kódrészletét vagy egy ismert vírus módosított kódját tartalmazza.
3. Az alkalmazás megjelenít egy értesítést a fájlban észlelt rosszindulatú objektumról (ha be vannak állítva értesítések), és feldolgozza a fájlt a Fájl víruskereső beállításaiban megadott műveletet elvégezve.

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 védelem szükség esetén kikapcsolható.

A Fájl védelem engedélyezése és letiltása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Fájl védelem** lehetőséget.
   Az ablak jobb oldali részén megjelennek a Fájl védelem összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Ha be szeretné kapcsolni a Fájl védelem összetevőt, jelölje be a **Fájl védelem** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Fájl védelem összetevőt, törölje a **Fájl védelem** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Fájl védelem automatikus szüneteltetése

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

A Fájl védelem szüneteltetését csak végső megoldásként szabad igénybe venni, ha alkalmazásokkal ütközik. Ha egy összetevő működése során ütközés lép fel, javasoljuk, hogy forduljon a Kaspersky Terméktámogatáshoz (https://companyaccount.kaspersky.com). A terméktámogatási szakemberek segítséget nyújtanak a Fájl védelem összetevő beállításában, így az más alkalmazásokkal egy időben is futhat.

A Fájl védelem automatikus szüneteltetésének beállítása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Fájl védelem** lehetőséget.

   Az ablak jobb oldali részén megjelennek a **Fájl védelem** összetevő beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Fájl védelem** ablak.
4. A **Fájl védelem** ablakban válassza ki az **További** lapot.
5. A **Feladat szüneteltetése** részben:
   - A Fájl védelem adott időpontban történő automatikus felfüggesztésének beállításához jelölje be az **Ütemezés szerint** jelölőnégyzetet, és kattintson az **Ütemezés** gombra.

     Megnyílik a **Feladat szüneteltetése** ablak.
   - A Fájl védelem adott alkalmazás elindításakor történő automatikus felfüggesztésének beállításához jelölje be az **Az alkalmazás indításakor** jelölőnégyzetet, és kattintson a **Kijelölés** gombra.

     Megnyílik az **Alkalmazások** ablak.
6. Végezze el az alábbiak egyikét:
   - Ha a Fájl védelem adott időpontban történő automatikus felfüggesztését állítja be, akkor a **Feladat szüneteltetése** ablakban adja meg a **Feladat szüneteltetése** és **Feladat folytatása** mezőkben azt az időszakot (ÓÓ:PP formátumban), amikor a Fájl védelem fel van függesztve. Kattintson az **OK** gombra.
   - Ha a Fájl védelem adott alkalmazás elindításakor történő automatikus felfüggesztését állítja be, akkor a **Hozzáadás**, **Szerkesztés** és **Eltávolítás** gombokkal készítsen egy listát az **Alkalmazások** ablakban azokról az alkalmazásokról, amelyek működése közben a Fájl védelem szünetel. Kattintson az **OK** gombra.
7. A **Fájl védelem** ablakban kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Fájl védelem beállításai

A Fájl védelem összetevő beállítása érdekében a következő műveleteket végezheti el:

- A biztonsági szint módosítása.

  Kiválaszthatja az előre beállított biztonsági szintek egyikét, de kézileg is megadhatja a beállításokat. Ha módosítja a biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.
- A Fájl védelem összetevő által fertőzött fájl észlelésekor elvégzett művelet módosítása.

- A Fájl védelem összetevő védelmi hatókörének kialakítása.

  A védelem hatókörét kiterjesztheti vagy szűkítheti a vizsgálandó objektumok hozzáadásával és eltávolításával, vagy a vizsgálandó fájlok típusának módosítása révén.

- Heurisztikus elemző beállítása.

  A Fájl védelem összetevő egy Gépi tanulás és aláíráselemzés nevű vizsgálati technikát alkalmaz. Az aláírások elemzése során a Fájl védelem összetevő az észlelt objektumot összeveti az alkalmazás antivírus adatbázisaiban 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. A heurisztikus elemzés során a Fájl védelem összetevő elemzi az objektumok tevékenységét az operációs rendszerben. A heurisztikus elemzés képes az olyan rosszindulatú objektumokat észlelni, amelyeknek még nem szerepel bejegyzése az alkalmazás víruskereső adatbázisaiban.

- Vizsgálat optimalizálás.

  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.

- Az összetett fájlok vizsgálatának beállítása.

- A fájlvizsgálati mód módosítása.

A biztonsági szint módosítása

A számítógép fájlrendszerének védelme érdekében a Fájl védelem összetevő különféle beállításcsoportokat alkalmaz. Ezeket a beállításcsoportokat *biztonsági szinteknek* nevezzük. Három előre beállított biztonsági szint létezik: **Magas**, **Ajánlott** és **Alacsony**. Az **Ajánlott** biztonsági szint beállításai tekinthetők optimálisnak, és a Kaspersky szakértői is ezeket ajánlják.

Biztonsági szint módosítása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Fájl védelem** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Fájl védelem összetevő beállításai.
3. A **Biztonsági szint** részben végezze el az alábbiak egyikét:

   - Ha valamelyik előtelepített biztonsági szintet (**Magas**, **Ajánlott** vagy **Alacsony**) szeretné beállítani, válassza ki a csúszkával.

   - Ha egyéni fájlbiztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, majd a megnyíló **Fájl védelem** ablakban adja meg az egyéni beállításokat.

     Egyéni biztonsági szint beállítását követően a biztonsági szint neve a **Biztonsági szint** részben **Egyéni** értékre vált.

   - Ha a biztonsági szintet **Ajánlott** értékre szeretné módosítani, kattintson az **Alapértelmezett** gombra.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Fájl víruskereső által a fertőzött fájlokon végrehajtandó művelet módosítása

A Fájl víruskereső által a fertőzött fájlokon végrehajtandó művelet módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.
   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.
3. Válassza ki a kívánt lehetőséget a **Művelet fenyegetés észlelésekor** részben:
   - **Művelet automatikus kiválasztása**.
   - **Művelet végrehajtása: Vírusmentesítés. Törlés, ha a vírusmentesítés nem sikerül**.
   - **Művelet végrehajtása: Vírusmentesítés**.

     A Kaspersky Endpoint Security a **Eltávolítás** műveletet a lehetőség kiválasztása esetén is elvégzi azokon a fájlokon, amelyek a Windows Store alkalmazás részei.

   - **Művelet végrehajtása: Eltávolítás**.
   - **Művelet végrehajtása: Blokkolás**.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Fájl víruskereső védelmi hatókörének szerkesztése

A védelmi hatókör azon objektumok körére utal, amelyeket az összetevő vizsgál, ha engedélyezve van. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak. A vizsgálandó fájlok helye és típusa a Fájl víruskereső védelmi hatókörének tulajdonságai. Alapértelmezés szerint a Fájl víruskereső a merevlemezeken, a hálózati meghajtókon és a cserélhető adathordozón csak a megfertőzhető fájlokat vizsgálja.

A védelem hatókörének létrehozása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.
   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
   Megnyílik a **Fájl víruskereső** ablaka.
4. A **Fájl víruskereső** ablakban válassza ki az **Általános** lapot.

5. A **Fájltípusok** részben adja meg azokat a fájltípusokat, amelyeket a Fájl víruskeresőnek meg kell vizsgálnia:

   - Ha minden fájlt vizsgálni kíván, válassza a **Minden fájl** lehetőséget.
   - Ha a fertőzés által leginkább veszélyeztetett formátumú fájlokat szeretné vizsgálni, válassza a **Formátum alapján vizsgált fájlok** lehetőséget.
   - Ha a fertőzés által leginkább veszélyeztetett kiterjesztésű fájlokat szeretné vizsgálni, válassza a **Kiterjesztés alapján vizsgált fájlok** lehetőséget.

   A vizsgálandó fájltípusok kiválasztásakor tartsa észben az alábbi tudnivalókat:

   - A rosszindulatú kódok behatolási és későbbi aktiválódási valószínűsége bizonyos fájlformátumok (például .txt) esetén meglehetősen alacsony. Más formátumok (például .exe, .dll és .doc) ugyanakkor végrehajtható kódot tartalmaz(hat)nak. A rosszindulatú kódok behatolásának és aktiválódásának kockázata az ilyen fájloknál meglehetősen magas.
   - Egy behatoló vírust vagy egyéb rosszindulatú programot küldhet a számítógépre olyan végrehajtható fájlban, amelyet .txt kiterjesztésűre nevezett át. Ha a fájlok kiterjesztés alapján történő vizsgálatát választja, az ilyen fájlok kimaradnak a vizsgálatból. Ha a formátum alapján történő vizsgálat van kiválasztva, a Fájl víruskereső kiterjesztéstől függetlenül elemzi a fájl fejlécét. Ez az elemzés felfedheti, hogy a fájl valójában .exe fájl. Az ilyen fájlt alaposan megvizsgálja vírusok és egyéb rosszindulatú programok szempontjából.

6. A **Védelem hatóköre** listán hajtsa végre a következő műveletek valamelyikét:

   - Ha egy új objektumot szeretne hozzáadni a vizsgálat hatóköréhez, kattintson a **Hozzáadás** gombra.
   - Ha meg szeretné változtatni egy objektum helyét, válassza ki a vizsgálat hatókörében, és kattintson a **Szerkesztés** gombra.

   Megnyílik a **Vizsgálat hatókörének kiválasztása** ablak.

   - Ha törölni kíván egy objektumot a vizsgálandó objektumok listájáról, válasszon ki egyet a listáról, és kattintson a **Eltávolítás** gombra.

     A törlés megerősítésére szolgáló ablak megnyílik.

7. Végezze el az alábbiak egyikét:

   - Ha egy új objektumot kíván felvenni, illetve módosítani szeretné egy objektum helyét a vizsgálandó objektumok listáján, jelöljön ki egyet a **Vizsgálat hatókörének kiválasztása** ablakban, és kattintson a **Hozzáadás** gombra.

     A **Vizsgálat hatókörének kiválasztása** ablakban kiválasztott összes objektum megjelenik a **Fájl víruskereső** ablakában a **Védelem hatóköre** listán.

     Kattintson az **OK** gombra.

   - Ha el szeretne távolítani egy objektumot, kattintson az eltávolítást megerősítő ablakban az **Igen** gombra.

8. Ha szükséges, ismételje meg a 6–7. lépést a vizsgálandó objektumok listáján objektumok hozzáadásához, áthelyezéséhez vagy törléséhez.

9. Törölje az objektum neve melletti jelölőnégyzet bejelölését a **Védelem hatóköre** listán, ha ki szeretné zárni az objektumot a vizsgálandó objektumok listájából. Az objektum a vizsgálandó objektumok listáján marad, de a Fájl víruskereső kizárja a vizsgálatból.

10. A **Fájl víruskereső** ablakban kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Heurisztikus elemző alkalmazása a Fájl víruskereső működése során

A Heurisztikus elemző Fájl víruskereső működése során történő használatának beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Fájl víruskereső** ablaka.
4. A **Fájl víruskereső** ablakban válassza ki a **Teljesítmény** lapot.
5. A **Vizsgálatmódok** részben:

   - Ha azt szeretné, hogy a Fájl víruskereső heurisztikus elemzést alkalmazzon, jelölje be a **Heurisztikus elemzés** jelölőnégyzetet, és a csúszkával állítsa be a heurisztikus elemzés szintjét: **Egyszerű vizsgálat**, **Közepes vizsgálat** vagy **Alapos vizsgálat**.
   - Ha nem szeretné, hogy a Fájl víruskereső heurisztikus elemzést alkalmazzon, törölje a **Heurisztikus elemzés** jelölőnégyzetet.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Vizsgálati technológiák alkalmazása a Fájl víruskereső működése során

A vizsgálati technológiák Fájl víruskereső működése során történő használatának beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Fájl víruskereső** ablaka.
4. A **Fájl víruskereső** ablakban válassza ki a **További** lapot.
5. A **Vizsgálati technológiák** részben:

   - Jelölje be a jelölőnégyzeteket azoknak a technológiáknak a nevével szemben, amelyeket a Fájl víruskereső működése során alkalmazni szeretne.

- Törölje a jelölőnégyzeteket azoknak a technológiáknak a nevével szemben, amelyeket a Fájl víruskereső működése során nem szeretne alkalmazni.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A fájlvizsgálat optimalizálása

A fájlvizsgálat optimalizálása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.

3. Kattintson a **Beállítások** gombra.

   Megnyílik a **Fájl víruskereső** ablaka.

4. A **Fájl víruskereső** ablakban válassza ki a **Teljesítmény** lapot.

5. A **Vizsgálat optimalizálás** részben jelölje be a **Csak az új és módosult fájlok vizsgálata** jelölőnégyzetet.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az összetett fájlok vizsgálata

A vírusok és egyéb rosszindulatú programok álcázásának gyakori módja az összetett fájlokba, pl. archívumokba, adatbázisokba stb. 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 készletét, így felgyorsíthatja a vizsgálatot.

A fertőzött összetett fájl feldolgozásának módszere (vírusmentesítés vagy törlés) a fájl típusától függ.

A Fájl víruskereső virusmentesíti a RAR, ARJ, ZIP, CAB és LHA formátumokban lévő összetett fájlokat, az összes többi formátumban lévő fájlokat pedig törli (kivéve a levelezési adatbázisokat).

Az összetett fájlok vizsgálatának beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.

3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Fájl víruskereső** ablaka.

4. A **Fájl víruskereső** ablakban válassza ki a **Teljesítmény** lapot.

5. Adja meg az **Összetett fájlok vizsgálata** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, telepítőcsomagok, illetve Office formátumú fájlok.

6. Ha csak az új és megváltozott fájlokat szeretné vizsgálni, jelölje be a **Csak az új és módosult fájlok vizsgálata** jelölőnégyzetet.

   A Fájl víruskereső mindenfajta típusból csak az új és megváltozott fájlokat vizsgálja.

7. Kattintson a **További** gombra.

   Megnyílik az **Összetett fájlok** ablak.

8. A **Vizsgálat a háttérben** részben végezze el az alábbiak egyikét:

   - Ha meg szeretné akadályozni, hogy a Fájl víruskereső a háttérben kicsomagolja az összetett fájlokat, törölje az **Összetett fájlok kicsomagolása a háttérben** jelölőnégyzetet.

   - Ha engedélyezni szeretné, hogy a Fájl víruskereső a háttérben kicsomagolja az összetett fájlokat, jelölje be az **Összetett fájlok kicsomagolása a háttérben** jelölőnégyzetet, és adja meg a szükséges értéket a **Minimális fájlméret** mezőben.

9. A **Méretkorlát** részben végezze el az alábbiak egyikét:

   - Ha meg szeretné akadályozni, hogy a Fájl víruskereső kicsomagolja a nagy méretű összetett fájlokat, jelölje be az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet, és adja meg a szükséges értéket a **Maximális fájlméret** mezőben. A Fájl víruskereső nem csomagolja ki a megadott értéknél nagyobb összetett fájlokat.

   - Ha engedélyezni szeretné, hogy a Fájl víruskereső kicsomagolja a nagy méretű összetett fájlokat, törölje az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet.

     A fájlok akkor számítanak nagy méretűnek, ha méretük meghaladja a **Maximális fájlméret** mezőben megadott értéket.

   A Fájl víruskereső 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. A **Fájl víruskereső** ablakban kattintson az **OK** gombra.

12. A módosítások mentéséhez kattintson a **Mentés** gombra.

Vizsgálatmód megváltoztatása

A *Vizsgálat módja* olyan feltételt jelent, amely szerint a Fájl víruskereső elkezdi a fájlok vizsgálatát. A Kaspersky Endpoint Security alapértelmezés szerint okos módban vizsgálja a fájlokat. Ebben a fájlvizsgálati módban a Fájl víruskereső 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. E kettő között a fájlt felülíró semmilyen művelet nem váltja ki a fájl vizsgálatát.

A fájlvizsgálati mód módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Fájl víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Fájl víruskereső összetevő beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Fájl víruskereső** ablaka.
4. A **Fájl víruskereső** ablakban válassza ki a **További** lapot.
5. A **Vizsgálat módja** részben válassza ki a kívánt módot:
   - **Okos mód**.
   - **Hozzáféréskor és módosításkor**.
   - **Hozzáféréskor**.
   - **Végrehajtáskor**.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

E-mail védelem. Levél víruskereső

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt a Levél víruskeresővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Levél víruskereső

A Levél víruskereső a bejövő és kimenő e-mail üzenetekben vizsgálja a vírusokat és egyéb fenyegetéseket. A Kaspersky Endpoint Security alkalmazással együtt indul el, folyamatosan aktív marad a számítógép memóriájában, és vizsgálja az összes POP3, SMTP, IMAP, MAPI és NNTP protokoll segítségével küldött és fogadott üzenetet. Ha az üzenetben nem észlelhető fenyegetés, hozzáférhetővé válik és / vagy sor kerül feldolgozására.

Ha egy e-mail üzenetben fenyegetést észlel, a Levél víruskereső az alábbiakat végzi el:

1. Azonosítja az e-mail üzenetben talált objektum típusát (például *trójai*).
2. Az e-mail üzenetek az alábbi állapotok egyikét kapják:
   - *Valószínűleg fertőzött*. Ezt az állapotot a rendszer akkor adja, ha a vizsgálat során nem tudja megállapítani, hogy az e-mail üzenet fertőzött-e. Az e-mail üzenetbe valószínűleg egy vírus vagy egyéb rosszindulatú program tipikus kódrészletét vagy egy ismert vírus módosított kódját tartalmazza.
   - *Fertőzött*. Ezt az állapotot az olyan objektumok kapják, amelyeknél az adott e-mail üzenet vizsgálata a Kaspersky Endpoint Security víruskereső adatbázisaiban szereplő ismert vírus kódrészletét találja.
   - *Nem található*. Ezt az állapotot az olyan objektumok kapják, amelyeknél az adott e-mail üzenet vizsgálata nem észlel vírust és egyéb fenyegetést.

Az alkalmazás ekkor blokkolja az e-mailt, egy értesítést jelenít meg a képernyőn az észlelt objektumról (ha ez van megadva az értesítési beállításokban), és végrehajtja a Levél víruskereső beállításaiban megadott műveletet.

Ez az összetevő együttműködik a számítógépen telepített levelezőprogramokkal. Rendelkezésre áll egy beágyazható kiterjesztés a Microsoft Office Outlook® levelezőprogramhoz, melynek segítségével elvégezheti az üzenetek vizsgálati beállításainak finomhangolását. A Levél víruskereső kiterjesztés beágyazása a Microsoft Office Outlook levelezőprogramba a Kaspersky Endpoint Security telepítése során történik.

A Levél víruskereső működését a tálca értesítési területén található alkalmazásikon jelzi. Miközben a Levél víruskereső e-mail üzenetet vizsgál, az alkalmazás ikonja a következőre változik:  .

A Levelezés védelem engedélyezése és letiltása

A Levelezés védelem összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. Szükség esetén letilthatja a Levelezés védelem összetevőt.

A Levelezés védelem összetevő be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.

2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Levelezés védelem** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Levelezés védelem összetevő beállításai.

3. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni a Levelezés védelem összetevőt, jelölje be a **Levelezés védelem** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Levelezés védelem összetevőt, törölje a **Levelezés védelem** jelölőnégyzetet.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Levelezés védelem beállításai

A Levelezés védelem összetevő beállítása érdekében a következő műveleteket végezheti el:

- Az e-mailek biztonsági szintjének módosítása.

  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 Kaspersky Endpoint Security által fertőzött üzeneteken elvégzett művelet módosítása.

- A Levelezés védelem összetevő védelmi hatókörének kialakítása.

- Az e-mail üzenetekhez mellékelt összetett fájlok vizsgálatának beállítása.

  Bekapcsolhatja vagy kikapcsolhatja az üzenetek mellékleteinek vizsgálatát, és beállíthat egy maximális mérethatárt az üzenetek mellékleteinek vizsgálatához, és korlátozhatja az üzenetek mellékletei vizsgálatának maximális időtartamát.

- A szűrés beállítása az e-mail üzenetek mellékleteinek típusa szerint.

  Az üzenetek mellékleteinek típus szerinti szűrésével az adott típusú fájlokat automatikusan átnevezheti vagy törölheti.

- Heurisztikus elemző beállítása.

  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 az üzenetekben, amelyeknek még nem szerepel bejegyzése a Kaspersky Endpoint Security adatbázisaiban.

- E-mailek vizsgálatának beállítása a Microsoft Office Outlookban.

  Rendelkezésre áll egy beágyazható kiterjesztés a Microsoft Office Outlook levelezőprogramhoz, mely lehetővé teszi az e-mailek vizsgálati beállításainak kényelmes beállítását.

  Más levelezőprogramok – mint például Microsoft Outlook Express®, Windows Mail, és Mozilla™ Thunderbird™ – esetén a Levelezés védelem összetevő az SMTP, POP3, IMAP és NNTP levelezési protokollok forgalmát vizsgálja.

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 áthelyezésre kerülnek a **Bejövő üzenetek** mappából.

Az e-mailek biztonsági szintjének módosítása

A Levelezés védelem összetevő az e-mailek védelme érdekében különböző beállításcsoportokat alkalmaz. Ezeket a beállításcsoportokat *e-mail-biztonsági szinteknek* nevezzük. Három e-mail-biztonsági szint létezik: **Magas**, **Ajánlott** és **Alacsony**. Az **Ajánlott** fájlbiztonsági szint tekinthető optimális beállításnak, és a Kaspersky is ezt javasolja.

Az e-mail-biztonsági szint módosítása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Levelezés védelem** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Levelezés védelem összetevő beállításai.
3. A **Biztonsági szint** részben végezze el az alábbiak egyikét:

   - Ha valamelyik előtelepített e-mail-biztonsági szintet (**Magas**, **Ajánlott** vagy **Alacsony**) szeretné telepíteni, válassza ki a csúszkával.
   - Ha egyéni fájlbiztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, majd a megnyíló **Levelezés védelem** ablakban adja meg az egyéni beállításokat.

     Egyéni e-mail-biztonsági szint beállítását követően a biztonsági szint neve a **Biztonsági szint** részben **Egyéni** értékre vált.
   - Ha az e-mail-biztonsági szintet **Ajánlott** értékre szeretné módosítani, kattintson az **Alapértelmezett** gombra.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A fertőzött e-mail üzeneteken végrehajtandó művelet módosítása

A fertőzött e-mail üzeneteken végrehajtandó művelet módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Levél víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Levél víruskereső összetevő beállításai.
3. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security fertőzött üzenet észlelése esetén végez.

   - **Művelet automatikus kiválasztása**.
   - **Művelet végrehajtása: Vírusmentesítés. Törlés, ha a vírusmentesítés nem sikerül**.

- **Művelet végrehajtása: Vírusmentesítés**.
- **Művelet végrehajtása: Eltávolítás**.
- **Művelet végrehajtása: Blokkolás**.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Levél víruskereső védelmi hatókörének szerkesztése

A védelmi hatókör azon objektumok körére utal, amelyeket az összetevő aktív állapotában vizsgál. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak. A Levél víruskereső védelmi hatókörének tulajdonságai közé a Levél víruskereső levelezőprogramokba való integrációjának beállításai, valamint az e-mail üzenetek típusainak és azon e-mail protokolloknak a beállításai tartoznak, amelyeknek forgalmát a Levél víruskereső 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 Levél víruskereső védelmi hatókörének létrehozása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Levél víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Levél víruskereső összetevő beállításai.
3. Kattintson a **Beállítások** gombra.

   Megnyílik a **Levél víruskereső** ablaka.
4. Válassza ki az **Általános** lapot.
5. A **Védelem hatóköre** részben hajtsa végre a következő műveletek valamelyikét:
   - Ha azt szeretné, hogy a Levél víruskereső a számítógépen az összes bejövő és kimenő üzenetet vizsgálja, válassza a **Bejövő és kimenő üzenetek** lehetőséget.
   - Ha azt szeretné, hogy a Levél víruskereső a számítógépen csak a bejövő üzenetet vizsgálja, válassza a **Csak bejövő üzenetek** lehetőséget.

     Ha úgy fönt, hogy csak a bejövő üzeneteket vizsgálja, javasoljuk, hogy egyszer vizsgálja meg az összes kimenő üzenetet is, mivel fennáll a veszélye, hogy a számítógépen e-mail férgek találhatók, melyek e-mailben terjednek. Ezzel elkerülheti az olyan problémákat, amelyeket az Ön számítógépéről érkező ellenőrizetlen tömeges fertőzött üzenetek okozhatnak.
6. A **Csatlakozás** részben végezze el az alábbiak egyikét:
   - Ha azt szeretné, hogy a Levél víruskereső megvizsgálja a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzeneteket, mielőtt azok megérkeznek a számítógépre, jelölje be a **POP3 / SMTP / NNTP / IMAP forgalom** jelölőnégyzetet.

Ha nem szeretné, hogy a Levél víruskereső megvizsgálja a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzeneteket, mielőtt azok megérkeznek a számítógépre, törölje a **POP3 / SMTP / NNTP / IMAP forgalom** jelölőnégyzetet. Ilyenkor a Levél víruskereső Microsoft Office Outlook levelezőprogramba beépült kiterjesztése azután vizsgálja az e-mail üzeneteket, hogy azok a felhasználó számítógépére letöltődtek, ha be van jelölve a **További: Microsoft Office Outlook kiterjesztés** jelölőnégyzet.

Ha a Microsoft Office Outlooktól eltérő levelezőprogramot használ, akkor a Levél víruskereső nem vizsgálja a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzeneteket, ha a **POP3 / SMTP / NNTP / IMAP forgalom** jelölőnégyzet nincs bejelölve.

- Ha a Microsoft Office Outlookból hozzá szeretne férni a Levél víruskereső beállításaihoz, és be szeretné kapcsolni a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzenetek vizsgálatát a Microsoft Office Outlookba beépülő kiterjesztéssel, miután megérkeztek a számítógépre, jelölje be a **További: Microsoft Office Outlook kiterjesztés** jelölőnégyzetet.

  Ha a Microsoft Office Outlookból blokkolni szeretné a Levél víruskereső beállításait, és ki szeretné kapcsolni a POP3, SMTP, NNTP és IMAP protokollokon keresztül továbbított üzenetek vizsgálatát a Microsoft Office Outlookba beépülő kiterjesztéssel, miután megérkeztek a számítógépre, törölje a **További: Microsoft Office Outlook kiterjesztés** jelölőnégyzetet.

  A Levél víruskereső kiterjesztés beágyazása a Microsoft Office Outlook levelezőprogramba a Kaspersky Endpoint Security telepítése során történik.

7. Kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az e-mail üzenetekhez mellékelt összetett fájlok vizsgálata

Az e-mail üzenetekhez mellékelt összetett fájlok vizsgálatának beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Levél víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Levél víruskereső összetevő beállításai.
3. Kattintson a **Beállítások** gombra.

   Megnyílik a **Levél víruskereső** ablaka.
4. Válassza ki az **Általános** lapot.
5. Végezze el az alábbiakat az **Összetett fájlok vizsgálata** részben:

   - Ha azt szeretné, hogy a Levél víruskereső kihagyja az üzenetekhez mellékelt archívumokat, törölje a **Csatolt archívumok vizsgálata** jelölőnégyzetet.
   - Ha azt szeretné, hogy a Levél víruskereső kihagyja azokat az üzenetekhez mellékelt archívumokat, amelyek mérete meghaladja az N megabájtot, jelölje be a **Hagyja ki az archívumot, ha annak mérete nagyobb, mint N MB** jelölőnégyzetet. Ha bejelöli ezt a jelölőnégyzetet, adja meg a nevével szemben lévő mezőben az archívumok maximális méretét.

- Ha azt szeretné, hogy a Levél víruskereső kihagyja azokat az üzenetekhez mellékelt archívumokat, amelyek vizsgálata N másodpercnél tovább tart, jelölje be a **Az archívumok ellenőrzése ne tartson tovább, mint N másodperc** jelölőnégyzetet.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Mellékletek szűrése az e-mail üzenetekben

A rosszindulatú programok 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 programok automatikus végrehajtása ellen.

A mellékletek szűrésének beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Levél víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Levél víruskereső összetevő beállításai.

3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Levél víruskereső** ablaka.

4. A **Levél víruskereső** ablakban válassza ki a **Mellékletszűrő** lapot.

5. Végezze el az alábbiak egyikét:

   - Ha nem szeretné, hogy a Levél víruskereső szűrje az üzenetek mellékleteit, válassza a **Szűrés letiltása** lehetőséget.

   - Ha azt szeretné, hogy a Levél víruskereső átnevezze az **adott típusú** üzenetmellékleteket, válassza az **Megadott melléklettípusok átnevezése** lehetőséget.

Megjegyzés: előfordulhat, hogy egy fájl tényleges formátuma nem egyezik a fájlnév kiterjesztésével.

Ha bekapcsolja az e-mail üzenetekhez csatolt objektumok szűrését, a Levél víruskereső az alábbi kiterjesztéssel rendelkező fájlokat átnevezheti vagy törölheti:

com – 64 KB-nál nem nagyobb az alkalmazás végrehajtható fájlja

exe – végrehajtható fájl vagy önkicsomagoló archívum

sys – Microsoft Windows rendszerfájl

prg – dBase™, Clipper vagy Microsoft Visual FoxPro® programszöveg, illetve WAVmaker program

bin – bináris fájl

bat – kötegfájl

cmd – Microsoft Windows NT (a DOS bat fájlhoz hasonló) vagy OS/2 parancsfájl

dpl – tömörített Borland Delphi könyvtár

dll – dinamikus csatolású könyvtár

scr – Microsoft Windows üdvözlő képernyő

cpl – Microsoft Windows vezérlőpult-modul

ocx – Microsoft OLE (Object Linking and Embedding) objektum

tsp – felosztott idejű módban futó program

drv – eszköz illesztőprogramja

vxd – Microsoft Windows virtuális eszközillesztő

pif – programinformációs fájl

lnk – Microsoft Windows hivatkozásfájl

reg – Microsoft Windows beállításkulcsfájl

ini – Microsoft Windows, Windows NT és egyes alkalmazások konfigurációs adatait tartalmazó konfigurációs fájl

cla – Java osztály

vbs – Visual Basic® szkript

vbe – BIOS videokiterjesztés

js, jse – JavaScript forrásszöveg

htm – hiperszöveg dokumentum

htt – Microsoft Windows hiperszöveg fejléc

hta – hiperszöveg program a Microsoft Internet Explorer® részére

asp – Active Server Pages szkript

chm – lefordított HTML fájl

pht – beépített PHP szkripteket tartalmazó HTML fájl

php – HTML fájlokba beépített szkript

wsh – Microsoft Windows Script Host fájl

wsf – Microsoft Windows szkript

the – Microsoft Windows 95 asztali háttérkép-fájl

hlp – Win súgófájl

eml – Microsoft Outlook Express üzenet

nws – új Microsoft Outlook Express e-mail üzenet

msg – Microsoft Mail e-mail üzenet

plg – e-mail üzenet

mbx – mentett Microsoft Office Outlook e-mailek kiterjesztése

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. A Microsoft Windows OS metafájljainak következő generációja. Az EMF fájlokat a 16 bites Microsoft Windows nem támogatja.

ico – objektum ikonfájlja

ov? – Microsoft Office Word végrehajtható fájlok

xl* – Microsoft Office Excel dokumentumok és fájlok, például: xla, a Microsoft Office Excel kiterjesztése, xlc grafikonoknál, xlt dokumentumsablonoknál, xlsx Microsoft Office Excel 2007 munkafüzeteknél, xltm Microsoft Office Excel 2007 munkafüzeteknél makrótámogatással, xlsb Microsoft Office Excel 2007 bináris (nem XML) formátumú munkafüzeteknél, xltx Microsoft Office Excel 2007 sablonoknál, xlsm Microsoft Office Excel 2007 sablonoknál makrótámogatással, és xlam Microsoft Office Excel 2007 bővítményeknél makrótámogatással

pp* – Microsoft Office PowerPoint® dokumentumok és fájlok, például: pps Microsoft Office PowerPoint diáknál, ppt bemutatóknál, pptx Microsoft Office PowerPoint 2007 bemutatóknál, pptm Microsoft Office PowerPoint 2007 bemutatóknál makrótámogatással, potx Microsoft Office PowerPoint 2007 bemutatósablonoknál, potm Microsoft Office PowerPoint 2007 bemutatósablonoknál makrótámogatással, ppsx Microsoft Office PowerPoint 2007 diavetítéseknél, ppsm Microsoft Office PowerPoint 2007 diavetítéseknél makrótámogatással, és ppam Microsoft Office PowerPoint 2007 bővítményeknél makrótámogatással

md* – Microsoft Office Access® dokumentumok és fájlok, például: mda Microsoft Office Access munkacsoportoknál és mdb adatbázisoknál

sldx – Microsoft PowerPoint 2007 dia

sldm – Microsoft PowerPoint 2007 dia makrótámogatással

thmx – Microsoft Office 2007 téma

- Ha azt szeretné, hogy a Levél víruskereső törölje az adott típusú üzenetmellékleteket, válassza az **Megadott melléklettípusok törlése** lehetőséget.

6. Ha az előző lépésben az **Megadott melléklettípusok átnevezése** vagy **Megadott melléklettípusok törlése** lehetőséget választotta, jelölje be a kívánt fájltípusokkal szemben lévő jelölőnégyzeteket.

   A fájltípusok listáját a **Hozzáadás**, **Szerkesztés** és **Eltávolítás** gombokkal módosíthatja.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

E-mailek vizsgálata a Microsoft Office Outlookban

A Kaspersky Endpoint Security telepítése során a Levél víruskereső kiterjesztése beágyazódik a Microsoft Office Outlookba (a továbbiakban: Outlook is). Ennek segítségével a Microsoft Office Outlookból megnyithatja a Levél víruskereső beállításait, és megadhatja, hogy keressen-e az e-mail üzenetekben vírusokat és más fenyegetéseket. Az Outlook Levél víruskereső kiterjesztése a POP3, SMTP, NNTP, IMAP és MAPI protokollok segítségével küldött és fogadott bejövő és kimenő üzeneteket képes vizsgálni.

A Levél víruskereső beállításait akkor lehet közvetlenül az Outlookban megadni, ha be van jelölve a **További: Microsoft Office Outlook kiterjesztés** jelölőnégyzet a Kaspersky Endpoint Security felületén.

Az Outlookban a bejövő üzeneteket először a Levél víruskereső (ha be van jelölve a **POP3 / SMTP / NNTP / IMAP forgalom** jelölőnégyzet a Kaspersky Endpoint Security felületén), majd az Outlook Levél víruskereső kiterjesztése vizsgálja. Ha a Levél víruskereső egy üzenetben rosszindulatú objektumot észlel, értesítést jelenít meg erről.

Az értesítési ablakban kiválasztható műveletek határozzák meg, melyik összetevő szünteti meg a fenyegetést az üzenetben: a Levél víruskereső vagy az Outlook Levél víruskereső kiterjesztése.

- Ha az értesítési ablakban a **Vírusmentesítés** vagy **Eltávolítás** műveletet választja ki, akkor a fenyegetést a Levél víruskereső szünteti meg.
- Ha az értesítési ablakban a **Átugrás** műveletet választja ki, akkor a fenyegetést az Outlook Levél víruskereső kiterjesztése szünteti meg.

A kimenő üzeneteket először az Outlook Levél víruskereső kiterjesztése, majd a Levél víruskereső vizsgálja meg.

E-mailek vizsgálatának beállítása az Outlookban

Az e-mailek vizsgálatának beállítása az Outlook 2007-ben:

1. Nyissa meg az Outlook 2007 főablakát.
2. Válassza ki a menüsorban a **Szolgáltatás** → **Beállítások** lehetőséget.
   Megnyílik a **Beállítások** ablak.
3. A **Beállítások** ablakban válassza ki az **E-mail védelem** lapot.

Az e-mailek vizsgálatának beállítása az Outlook 2010/2013-ban:

1. Nyissa meg az Outlook főablakát.
   Válassza ki a bal felső sarokban a **Fájl** lapot.
2. Kattintson a **Beállítások** gombra.
   Megnyílik az **Outlook beállításai** ablak.
3. Válassza ki a **Bővítmények** részt.
   Az Outlookba beágyazott bővítmények beállításai az ablak jobb oldalán jelennek meg.
4. Kattintson a **Bővítmények beállításai** gombra.

Az e-mailek vizsgálatának beállítása a Kaspersky Security Center segítségével

Ha az e-mailek vizsgálata az Outlook Levél víruskereső kiterjesztésével történik, akkor javasoljuk a Gyorsítótárazott Exchange-mód használatát. Az Exchange gyorsítótárazási módjával kapcsolatban további információ, valamint a használatára vonatkozó ajánlások a Microsoft Tudásbázisban találhatók: https://technet.microsoft.com/en-us/library/cc179175.aspx.

Az Outlook Levél víruskereső kiterjesztés üzemmódjának beállítása a Kaspersky Security Center segítségével:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani az e-mail vizsgálatát.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. A **Vírusvédelem** részben válassza ki a **Levél víruskereső** alrészt.
7. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.
   Megnyílik a **Levél víruskereső** ablaka.
8. A **Csatlakozás** részben kattintson a **Beállítások** gombra.
   Megnyílik az **E-mail védelem** ablak.
9. Az **E-mail védelem** ablakban:
   - Jelölje be a **Vizsgálat fogadáskor** jelölőnégyzetet, ha azt szeretné, hogy az Outlook Levél víruskereső kiterjesztés a bejövő üzeneteket megvizsgálja, amint a postaládába megérkeznek.
   - Jelölje be a **Vizsgálat olvasás közben** jelölőnégyzetet, ha azt szeretné, hogy az Outlook Levél víruskereső kiterjesztés a bejövő üzeneteket akkor vizsgálja meg, amikor a felhasználó megnyitja őket.
   - Jelölje be a **Vizsgálat küldéskor** jelölőnégyzetet, ha azt szeretné, hogy az Outlook Levél víruskereső kiterjesztés a kimenő üzeneteket megvizsgálja, amint elküldésre kerülnek.
10. Az **E-mail védelem** ablakban kattintson az **OK** gombra.
11. A **Levél víruskereső** ablakban kattintson az **OK** gombra.
12. Alkalmazza a rendszabályt.

A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

A számítógép védelme az interneten. Webes víruskereső

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt a Webes víruskeresővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Webes víruskereső

Az interneten töltött idő minden percében vírusoknak és egyéb rosszindulatú programoknak teszi ki a számítógépen tárolt adatokat. Ezek akkor szivároghatnak a számítógépére, amikor a felhasználó ingyenes szoftvert tölt le, vagy olyan webhelyeket látogat meg, amelyeket hackertámadás ért. A hálózati férgek azonnal behatolhatnak a számítógépbe, amint internetkapcsolatot létesít, még mielőtt megnyitna egy weboldalt vagy letöltene egy fájlt.

A Webes víruskereső védi a számítógépen HTTP és FTP protokollokon keresztül küldött és fogadott bejövő és kimenő adatokat, és ellenőrzi az URL-eket a rosszindulatú és adathalász webcímek listáján.

A Webes víruskereső elfogja a felhasználó vagy egy program által HTTPS- vagy FTP-protokollon elért összes oldalt és fájlt, és vírusokat és egyéb fenyegetéseket keres bennük. Ezután az alábbiak történnek:

- Ha az oldalon vagy fájlban nem található rosszindulatú kód, a felhasználó azonnal hozzáférhet.
- Ha a felhasználó rosszindulatú kódot tartalmazó weboldalhoz vagy fájlhoz fér hozzá, az alkalmazás elvégzi a Webes víruskereső beállításaiban megadott műveletet.

A Web védelem engedélyezése és letiltása

A Web védelem összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. Szükség esetén letilthatja a Web védelem összetevőt.

A Web védelem összetevő be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Web védelem** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Web védelem összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Ha be szeretné kapcsolni a Web védelem összetevőt, jelölje be a **Web védelem** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Web védelem összetevőt, törölje a **Web védelem** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Webes víruskereső beállítása

A Webes víruskereső beállítását az alábbi módokon végezheti:

- Webes forgalom biztonsági szintjének megváltoztatása.

  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 Kaspersky Endpoint Security által a webes forgalomban észlelt rosszindulatú objektumokon elvégzett művelet módosítása.

  Ha egy HTTP-objektum elemzésekor kiderül, hogy rosszindulatú kódot tartalmaz, a Webes víruskereső reakciója a megadott művelettől függ.

- Annak beállítása, hogy a Webes víruskereső ellenőrizze az URL-eket az adathalász és rosszindulatú webcímek adatbázisai alapján.

- A heurisztikus elemzés alkalmazásának beállítása a webes forgalom vírusokat és egyéb rosszindulatú programokat kereső vizsgálata közben.

  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 weboldalak adathalászati szempontból való vizsgálatakor aktiválódó heurisztikus elemzés használatának beállítása.

- A z HTTP és FTP protokollon keresztül küldött és fogadott webes forgalom Webes víruskereső által végzett vizsgálatának optimalizálása.

- Megbízható URL-ek listájának létrehozása.

  Létrehozhatja azon URL-ek listáját, amelyeknek a tartalmában megbízik. A Webes víruskereső nem elemzi a megbízható URL-címekről érkező információkban a vírusok és egyéb fenyegetések jelenlétét. Ez a lehetőség akkor lehet hasznos például, ha a Webes víruskereső zavarja egy fájl letöltését egy ismert webhelyről.

  Az URL egy adott weboldal vagy egy webhely címe lehet.

A webes forgalom biztonsági szintjének módosítása

A HTTP és FTP protokollokon keresztül fogadott és továbbított adatok védelme érdekében a Web védelem összetevő különböző beállításcsoportokat alkalmaz. Ezeket a beállításcsoportokat *webes forgalmi biztonsági szinteknek* nevezzük. Három előtelepített webes forgalmi biztonsági szint létezik: **Magas**, **Ajánlott** és **Alacsony**. Az **Ajánlott** webes forgalmi biztonsági szint tekinthető optimális beállításnak, és a Kaspersky is ezt javasolja.

A webes forgalom biztonsági szintjének módosítása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.

2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Web védelem** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Web védelem összetevő beállításai.

3. A **Biztonsági szint** részben végezze el az alábbiak egyikét:

   - Ha valamelyik előtelepített webes forgalmi biztonsági szintet (**Magas**, **Ajánlott** vagy **Alacsony**) szeretné telepíteni, válassza ki a csúszkával.
   - Ha egyéni webes forgalmi biztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, majd a megnyíló **Web védelem** ablakban adja meg a beállításokat.

     Egyéni webes forgalmi biztonsági szint beállítását követően a biztonsági szint neve a **Biztonsági szint** részben **Egyéni** értékre vált.
   - Ha a webes forgalmi biztonsági szintet **Ajánlott** értékre szeretné módosítani, kattintson az **Alapértelmezett** gombra.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A webes forgalomban észlelt rosszindulatú objektumokon végrehajtandó művelet módosítása

A webes forgalomban észlelt rosszindulatú objektumokon végrehajtandó művelet módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Webes víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Webes víruskereső összetevő beállításai.

3. Válassza ki a **Művelet fenyegetés észlelésekor** részben azt a műveletet, amelyet a Kaspersky Endpoint Security a webes forgalomban észlelt rosszindulatú objektumokon végez:

   - **Művelet automatikus kiválasztása**.
   - **Letöltés blokkolása**.
   - **Letöltés engedélyezése**.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az URL-ek Webes víruskereső által végzett ellenőrzése az adathalász és rosszindulatú webcímek adatbázisai alapján

A hivatkozások vizsgálata az adathalász webcímek listáján lehetővé teszi az *adathalász támadások* elkerülését. Az adathalász támadás álcázható például egy banktól érkező e-mail üzenetként is, amely 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 Webes víruskereső 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 Webes víruskereső ellenőrizze az URL-eket az adathalász és rosszindulatú webcímek adatbázisai alapján:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Webes víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Webes víruskereső összetevő beállításai.
3. Kattintson a **Beállítások** gombra.

   Megnyílik a **Webes víruskereső** ablaka.
4. A **Webes víruskereső** ablakban válassza ki az **Általános** lapot.
5. Végezze el az alábbiakat:

   - Ha azt szeretné, hogy a Webes víruskereső az URL-eket ellenőrizze a rosszindulatú webcímek adatbázisai alapján, akkor a **Vizsgálatmódok** részben jelölje be az **Ellenőrzés, hogy a hivatkozások szerepelnek-e a rosszindulatú hivatkozások adatbázisában** jelölőnégyzetet.
   - Ha azt szeretné, hogy a Webes víruskereső az URL-eket ellenőrizze az adathalász webcímek adatbázisai alapján, akkor az **Adathalászat-blokkoló beállításai** részben jelölje be az **Ellenőrzés, hogy a hivatkozások szerepelnek-e az adathalász hivatkozások adatbázisában** jelölőnégyzetet.

   A hivatkozásokat ellenőrizheti a Kaspersky Security Network reputációs adatbázisai alapján is.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Heurisztikus elemző alkalmazása a Webes víruskereső működése során

A heurisztikus elemzés beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Webes víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek a Webes víruskereső összetevő beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Webes víruskereső** ablaka.

4. Válassza ki az **Általános** lapot.

5. Ha azt szeretné, hogy a Webes víruskereső a vírusok és egyéb rosszindulatú programok webes forgalomban való vizsgálata során heurisztikus elemzést alkalmazzon, jelölje be a **Vizsgálatmódok** részben a **Heurisztikus elemzés vírusok észlelésére** jelölőnégyzetet, és a csúszkával állítsa be a heurisztikus elemzés szintjét: **Egyszerű vizsgálat**, **Közepes vizsgálat** vagy **Alapos vizsgálat**.

6. Ha azt szeretné, hogy a Webes víruskereső az adathalász hivatkozások weboldalakon történő vizsgálata során heurisztikus elemzést alkalmazzon, akkor az **Adathalászat-blokkoló beállításai** részben jelölje be a **Heurisztikus elemzés adathalász hivatkozások észlelésére** jelölőnégyzetet.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Megbízható URL-ek listájának szerkesztése

Megbízható URL-ek listájának létrehozása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Webes víruskereső** alrészt.
   Az ablak jobb oldali részén megjelennek a Webes víruskereső összetevő beállításai.

3. Kattintson a **Beállítások** gombra.
   Megnyílik a **Webes víruskereső** ablaka.

4. Válassza ki a **Megbízható URL-ek** lapot.

5. Jelölje be a **Ne vizsgálja a megbízható webcímekről érkező webes forgalmat** jelölőnégyzetet.

6. Hozzon létre egy listát olyan URL-ekről/weboldalakról, amelyek tartalmában megbízik. Lista létrehozása:

   a. Kattintson a **Hozzáadás** gombra.
      Megnyílik a **Webcím / Webcímmaszk** ablak.

   b. Adja meg a webhely/weboldal címét vagy címmaszkját.

   c. Kattintson az **OK** gombra.
      Megjelenik egy új bejegyzés a megbízható URL-ek listáján.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az IM-ügyfelek forgalmának védelme. IM víruskereső

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt az IM víruskeresővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

Az IM víruskereső

Az IM víruskereső az azonnali üzenetküldő ügyfelek (más néven *IM ügyfelek*) forgalmát vizsgálja.

Az IM víruskereső a titkosított csatornákon továbbított üzeneteket nem vizsgálja.

Az IM ügyfeleken keresztül küldött üzenetek az alábbi típusú biztonsági fenyegetéseket tartalmazhatják:

- A számítógépre rosszindulatú programot letölteni próbáló URL-ek
- A betolakodók által adathalász támadásokhoz használt rosszindulatú programok és webhelyek URL-jei

  Az adathalász támadások célja a személyes adatok ellopása a felhasználóktól – ilyen adatok a bankkártyák számai, az útlevelek adatai, a banki fizetési rendszerek és egyéb online szolgáltatások (például a közösségi oldalak és e-mail-fiókok) jelszavai.

Az IM ügyfeleken keresztül fájlokat is továbbítani lehet. Amikor a felhasználó menteni próbálja ezeket a fájlokat, a Fájl víruskereső összetevő megvizsgálja őket.

Az IM víruskereső a felhasználó által IM ügyfélen keresztül küldött és fogadott összes üzenetet elfogja, és megvizsgálja, hogy nincsenek-e benne a számítógép biztonságát esetleg fenyegető hivatkozások:

- Ha az üzenetben nem észlelhetők veszélyes URL-ek, a felhasználó megtekintheti.
- Ha az üzenetben veszélyes hivatkozások észlelhetők, az IM víruskereső az üzenetet a fenyegetésre vonatkozó információkkal cseréli le az aktív IM ügyfél üzenetablakában.

Az IM víruskereső be- és kikapcsolása

Az IM víruskereső alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. Szükség esetén letilthatja az IM víruskeresőt.

Az összetevő kétféle módon engedélyezhető és tiltható le:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

Az IM víruskereső be- és kikapcsolása a Védelem és felügyelet lapon a fő alkalmazásablakban:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Védelem** részre.
   Megnyílik a **Védelem** rész.
4. Kattintson a jobb egérgombbal az **IM víruskereső** sorra az összetevő műveletei helyi menüjének megnyitásához.
5. Végezze el az alábbiak egyikét:
   - Az IM víruskereső bekapcsolásához válassza ki a helyi menüben az **Indítás** lehetőséget.
     Az összetevő állapotikonja , mely az **IM víruskereső** sorában a bal oldalon látható, átvált ikonra.
   - Az IM víruskereső kikapcsolásához válassza ki a helyi menüben az **Leállítás** lehetőséget.
     Az összetevő állapotikonja , mely az **IM víruskereső** sorában a bal oldalon látható, átvált ikonra.

Az IM víruskereső be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki az **IM víruskereső** alrészt.
   Az ablak jobb oldali részén megjelennek az IM víruskereső összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Ha be szeretné kapcsolni az IM víruskeresőt, jelölje be az **IM víruskereső engedélyezése** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni az IM víruskeresőt, törölje az **IM víruskereső engedélyezése** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az IM víruskereső beállítása

Az IM víruskereső beállítását az alábbi műveletekkel végezheti:

- A védelem hatókörének beállítása.
  A vizsgálandó IM-ügyfélüzenetek típusának megváltoztatása révén bővítheti és szűkítheti a védelem hatókörét.
- Az IM-ügyfelek üzeneteiben lévő hivatkozások IM víruskereső által végzett, adathalász és rosszindulatú webcímek adatbázisai alapján történő ellenőrzésének beállítása.

IM víruskereső védelmi hatókörének létrehozása

A védelmi hatókör azon objektumok körére utal, amelyeket az összetevő vizsgál, ha engedélyezve van. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak. Az IM ügyfelek bejövő, illetve kimenő vizsgált üzeneteinek típusa az IM víruskereső védelmi hatókörének jellemzője. Az IM víruskereső alapértelmezés szerint a bejövő és kimenő üzeneteket egyaránt vizsgálja. A kimenő üzenetek vizsgálatát kikapcsolhatja.

A védelem hatókörének létrehozása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki az **IM víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek az IM víruskereső összetevő beállításai.
3. A **Védelem hatóköre** részben hajtsa végre a következő műveletek valamelyikét:

   - Ha azt szeretné, hogy az IM víruskereső a számítógépen az IM ügyfelek összes bejövő és kimenő üzenetét vizsgálja, válassza a **Bejövő és kimenő üzenetek** lehetőséget.
   - Ha azt szeretné, hogy az IM víruskereső a számítógépen csak az IM ügyfelek bejövő üzeneteit vizsgálja, válassza a **Csak bejövő üzenetek** lehetőséget.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az URL-ek vizsgálata a rosszindulatú és adathalász URL-ek adatbázisai alapján az IM víruskeresővel

Annak beállítása, hogy az IM víruskereső ellenőrizze az URL-eket a rosszindulatú és adathalász webcímek adatbázisai alapján:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki az **IM víruskereső** alrészt.

   Az ablak jobb oldali részén megjelennek az IM víruskereső összetevő beállításai.
3. A **Vizsgálatmódok** részben válassza ki az IM víruskereső által használandó módszereket:

   - Ha az IM-ügyfelek üzeneteiben lévő hivatkozásokat ellenőrizni szeretné a rosszindulatú webcímek adatbázisai alapján, akkor jelölje be a **Ellenőrzés, hogy a hivatkozások szerepelnek-e a rosszindulatú hivatkozások adatbázisában** jelölőnégyzetet.
   - Ha az IM-ügyfelek üzeneteiben lévő hivatkozásokat ellenőrizni szeretné az adathalász webcímek adatbázisai alapján, akkor jelölje be az **Ellenőrzés, hogy a hivatkozások szerepelnek-e az adathalász hivatkozások adatbázisában** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Rendszerfigyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt a Rendszerfigyelővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Rendszerfigyelő

A Rendszerfigyelő a számítógépen futó alkalmazások műveleteiről gyűjt adatokat, és a védelem fokozása érdekében átadja ezeket az információkat a többi összetevőnek.

Viselkedésfolyam-aláírások

A Viselkedésfolyam-aláírások (BSS) az alkalmazásműveletek olyan sorozatait tartalmazzák, amelyeket a Kaspersky Endpoint Security veszélyesként sorol be. Ha egy alkalmazás aktivitása megegyezik egy viselkedésfolyam-aláírással, a Kaspersky Endpoint Security végrehajtja a megadott műveletet. A Kaspersky Endpoint Security viselkedésfolyam-aláíráson alapuló funkciói a számítógép számára proaktív védelmet nyújtanak.

Ha egy alkalmazás tevékenysége megfelel egy viselkedésfolyam-aláírásnak, akkor alapértelmezés szerint a Rendszerfigyelő az adott alkalmazás végrehajtható fájlját a Karanténba helyezi.

A rosszindulatú programok által végzett műveletek visszagörgetése

A Rendszerfigyelő által gyűjtött információk alapján a Kaspersky Endpoint Security képes **a rosszindulatú programok által az operációs rendszerben elvégzett műveleteket visszagörgetni** a vírusmentesítés folyamán.

A rosszindulatú programok operációs rendszerben végzett tevékenységeinek visszagörgetésekor a Kaspersky Endpoint Security a rosszindulatú programok alábbi típusú tevékenységein végez műveleteket:

- Fájl tevékenysége.

  A Kaspersky Endpoint Security a hálózati meghajtók kivételével minden adathordozón törli a rosszindulatú program által létrehozott fájlokat.

  A Kaspersky Endpoint Security törli az olyan program által létrehozott fájlokat, amelyekbe a rosszindulatú program bejutott.

  A Kaspersky Endpoint Security nem állítja helyre a módosult, illetve törölt fájlokat.

- Beállításjegyzék-tevékenység.

  A Kaspersky Endpoint Security törli a rosszindulatú programok által létrehozott partíciókat és beállításkulcsokat.

  A Kaspersky Endpoint Security nem állítja helyre a módosult, illetve törölt partíciókat és beállításkulcsokat.

- Rendszertevékenység.

  A Kaspersky Endpoint Security megszakítja a rosszindulatú program által indított folyamatokat.

  A Kaspersky Endpoint Security megszakítja azokat a folyamatokat, amelyekbe a rosszindulatú program bejutott.

  A Kaspersky Endpoint Security nem indítja újra a rosszindulatú program által leállított folyamatokat.

- Hálózati tevékenység.

  A Kaspersky Endpoint Security blokkolja a rosszindulatú programok hálózati tevékenységét.

  A Kaspersky Endpoint Security blokkolja azoknak a folyamatoknak a hálózati tevékenységét, amelyekbe a rosszindulatú program bejutott.

A rosszindulatú tevékenység utáni visszagörgetést elindíthatja a Fájl víruskereső, illetve elindulhat 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 Rendszerfigyelő engedélyezése és letiltása

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

Ha nem feltétlenül szükséges, nem javasolt kikapcsolni a Rendszerfigyelőt, mivel kihat a védelmi összetevők teljesítményére. A védelmi összetevők a Rendszerfigyelő által gyűjtött adatokat kikérhetik, hogy segítségükkel pontosabban azonosíthassák az észlelt fenyegetéseket.

A Rendszerfigyelő kétféle módon kapcsolhat be és ki:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban

- Az alkalmazás beállításai ablakból

*A Rendszerfigyelő be- és kikapcsolása a **Védelem és felügyelet** lapon a fő alkalmazásablakban:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Védelem** részre.

   Megnyílik a **Védelem** rész.
4. Kattintson a jobb egérgombbal a helyi menü megjelenítéséhez a Rendszerfigyelő összetevőre vonatkozó adatokat tartalmazó sorban.

   Megnyílik az összetevő műveleteinek kiválasztására szolgáló menü.
5. Végezze el az alábbiak egyikét:
   - A Rendszerfigyelő bekapcsolásához válassza ki az **Indítás** lehetőséget.

     Az összetevő állapotikonja , mely a **Rendszerfigyelő** sorában a bal oldalon látható, átvált ikonra.
   - A Rendszerfigyelő kikapcsolásához válassza ki az **Leállítás** lehetőséget.

     Az összetevő állapotikonja , mely a **Rendszerfigyelő** sorában a bal oldalon látható, átvált ikonra.

A Rendszerfigyelő be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Rendszerfigyelő** alrészt.

   Az ablak jobb oldali részén megjelennek a **Rendszerfigyelő** összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Ha be szeretné kapcsolni a Rendszerfigyelőt, jelölje be a **Rendszerfigyelő bekapcsolása** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Rendszerfigyelőt, törölje a **Rendszerfigyelő bekapcsolása** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Rendszerfigyelő beállítása

A Rendszerfigyelő beállítása érdekében a következő műveleteket végezheti el:

- biztonsági rések kihasználása elleni védelem be- és kikapcsolása;
- rosszindulatú tevékenység programban való észlelése esetén végzendő művelet kiválasztása;
- Rosszindulatú programok műveletei vírusmentesítés során történő visszagörgetésének be- és kikapcsolása.

Biztonsági rések kihasználása elleni védelem be- és kikapcsolása

A biztonsági rések kihasználása elleni védelem be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Rendszerfigyelő** alrészt.

   Az ablak jobb oldali részén megjelennek a **Rendszerfigyelő** összetevő beállításai.
3. Végezze el az alábbiak egyikét:

   - Jelölje be a **Biztonsági rések kihasználása elleni védelem** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security figyelje a sebezhető programok által használt fájlokat indításukkor.

     Ha a Kaspersky Endpoint Security azt észleli, hogy egy sebezhető program által használt fájlt a felhasználótól eltérő entitás indítja el, akkor aszerint jár el, ami a **Művelet fenyegetés észlelésekor** előugró listán ki van választva.

   - Jelölje be a **Biztonsági rések kihasználása elleni védelem** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security figyelje a sebezhető programok által használt fájlokat indításukkor.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Rosszindulatú tevékenység programban való észlelése esetén végzendő művelet kiválasztása

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

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Rendszerfigyelő** alrészt.

   Az ablak jobb oldali részén megjelennek a **Rendszerfigyelő** összetevő beállításai.
3. Válassza ki a **Művelet fenyegetés észlelésekor** részben a **Rosszindulatú program tevékenységének észlelése esetén** előugró listán az alábbi műveletet:

   - **Művelet automatikus kiválasztása**.
   - **Fájl áthelyezése a Karanténba**.
   - **A rosszindulatú program bezárása**.
   - **Átugrás**.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Rosszindulatú programok műveletei vírusmentesítés során történő visszagörgetésének be- és kikapcsolása

Rosszindulatú programok műveletei vírusmentesítés során történő visszagörgetésének be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Rendszerfigyelő** alrészt.

   Az ablak jobb oldali részén megjelennek a **Rendszerfigyelő** összetevő beállításai.
3. Végezze el az alábbiak egyikét:

   - Ha azt szeretné, hogy a Kaspersky Endpoint Security a vírusmentesítés során görgesse vissza azokat a műveleteket, amelyeket az operációs rendszerben rosszindulatú programok végeztek, jelölje be a **Rosszindulatú programok tevékenységeinek visszagörgetése a vírusmentesítés során** jelölőnégyzetet.
   - Ha azt szeretné, hogy a Kaspersky Endpoint Security a vírusmentesítés során hagyja figyelmen kívül azokat a műveleteket, amelyeket az operációs rendszerben rosszindulatú programok végeztek, törölje a **Rosszindulatú programok tevékenységeinek visszagörgetése a vírusmentesítés során** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Tűzfal

Ez a rész tájékoztatást nyújt a Tűzfallal kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Tűzfal

A számítógép helyi hálózaton és az interneten történő használat során ki van téve a vírusoknak és egyéb rosszindulatú programoknak, valamint az operációs rendszer és a szoftverek sebezhetőségeit kiaknázó különféle támadásoknak.

A Tűzfal védelmet nyújt a felhasználó számítógépén lévő személyes adatok számára, és blokkolja az operációs rendszerre leselkedő lehetséges fenyegetések legtöbb típusát, miközben a számítógép az internethez vagy helyi hálózathoz csatlakozik. A Tűzfal észleli a felhasználó számítógépén az összes hálózati kapcsolatot, és listát készít az IP-címekről, feltüntetve az alapértelmezett hálózati kapcsolat állapotát.

A Tűzfal összetevő a hálózati szabályok alapján szűri a teljes hálózati tevékenységet. A hálózati szabályok beállításával az internethozzáférés blokkolásától kezdve a korlátlan hozzáférésig megadhatja a számítógép védelmének kívánt szintjét.

A Tűzfal be- és kikapcsolása

Alapértelmezés szerint a Tűzfal be van kapcsolva és optimális módban működik. Szükség esetén kikapcsolhatja a Tűzfalat.

Az összetevő kétféle módon engedélyezhető és tiltható le:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

A Tűzfal be- és kikapcsolása a Védelem és felügyelet lapon a fő alkalmazásablakban:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Védelem** részre.
   Megnyílik a **Védelem** rész.
4. Kattintson a jobb egérgombbal a **Tűzfal** sorra a Tűzfal műveletei helyi menüjének megnyitásához.
5. Végezze el az alábbiak egyikét:
   - A Tűzfal bekapcsolásához a helyi menüben válassza az **Indítás** elemet.
     Az összetevő állapotikonja , mely a **Tűzfal** sorában a bal oldalon látható, átvált ikonra.
   - A Tűzfal kikapcsolásához válassza ki a helyi menüben a **Leállítás** lehetőséget.
     Az összetevő állapotikonja , mely a **Tűzfal** sorában a bal oldalon látható, átvált ikonra.

A Tűzfal be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Ha be szeretné kapcsolni a Tűzfalat, jelölje be a **Tűzfal bekapcsolása** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Tűzfalat, jelölje be a **Tűzfal kikapcsolása** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A hálózati szabályok

A *hálózati szabályok* olyan engedélyezett vagy blokkolt műveletek, amelyeket a Tűzfal hálózati kapcsolódási kísérlet észlelésekor hajt végre.

A Tűzfal két szinten nyújt védelmet a különböző típusú hálózati támadások ellen: a hálózat és a program szintjén. A hálózati szintű védelem hálózati csomagszabályok alkalmazásával történik. A programszintű védelmet olyan szabályok alkalmazása biztosítja, amelyek a telepített alkalmazásoknak engedélyezik a hálózati erőforrások elérését.

A Tűzfal két védelmi szintje alapján az alábbiakat lehet létrehozni:

- *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 Tűzfal alapértelmezés szerint megad bizonyos hálózati csomagszabályokat.
- *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. Ezek a szabályok alkalmasak a hálózati tevékenység szűrésének finomhangolására, például adott típusú hálózati kapcsolat bizonyos alkalmazások számára blokkolt, mások számára pedig engedélyezett.

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 egyes hálózati csomagszabályok és alkalmazásszabályok végrehajtási sorrendje megadható.

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, a gyermekfolyamatok 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.

A hálózati kapcsolat állapota

A Tűzfal felügyeli a felhasználó számítógépén az összes hálózati kapcsolatot, és minden észlelt hálózati kapcsolathoz automatikusan hozzárendel egy-egy állapotot.

A hálózati kapcsolat az alábbi állapottípusok egyikével rendelkezhet:

- **Nyilvános hálózat**. Javasoljuk, hogy olyan hálózatoknál válassza ezt az állapotot, amelyeket nem véd víruskereső alkalmazás, tűzfal vagy szűrő (például internetkávézó szűrői). 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**. Ezt az állapotot azok a hálózatok kapják, amelyeknek a felhasználói megbízhatóak, és így hozzáférhetnek a számítógépen található fájlokhoz és nyomtatókhoz (ilyen például a LAN vagy az otthoni hálózat).

- **Megbízható hálózat**. Ez az állapot az olyan, biztonságos hálózatokhoz tartozik, amelyen a számítógép nincs kitéve az adatokhoz való illetéktelen hozzáférésre irányuló támadásoknak. A Tűzfal az ilyen állapotú hálózaton belül minden hálózati tevékenységet engedélyez.

A hálózati kapcsolat állapotának módosítása

A hálózati kapcsolat státuszának módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.
3. Kattintson a **Elérhető hálózatok** gombra.

   Megnyílik a **Tűzfal** ablak.
4. Válassza ki azt a hálózati kapcsolatot, amelynek módosítani szeretné az állapotát.
5. A helyi menüben válassza ki a hálózati kapcsolat állapotát:

   - **Nyilvános hálózat**.
   - **Helyi hálózat**.
   - **Megbízható hálózat**.

6. A **Tűzfal** ablakban kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

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 és szerkesztése

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

Hálózati csomagszabály létrehozása és szerkesztése:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.

2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Tűzfal** lehetőséget.

3. Kattintson a **Hálózati csomagszabályok** gombra.

4. Megnyílik a **Tűzfal** ablak a **Hálózati csomagszabályok** lapon.

   Ezen a lapon a Tűzfal által beállított alapértelmezett hálózati csomagszabályok listája látható.

5. Végezze el az alábbiak egyikét:

   - Új hálózati csomagszabályt a **Hozzáadás** gombra kattintva hozhat létre.
   - Ha hálózati csomagszabályt szeretne szerkeszteni, válassza ki a listáról, és kattintson a **Szerkesztés** gombra.

   Megnyílik a **Hálózati szabály** ablak.

6. Válassza ki a **Művelet** legördülő listán a Tűzfal által az adott típusú hálózati tevékenység észlelésekor végrehajtandó műveletet:

   - **Engedélyezés**
   - **Blokkolás**
   - **Alkalmazásszabályokkal**.

7. A **Név** mezőbe írja be a hálózati szolgáltatás nevét az alábbi módok egyikével:

   - Kattintson a ikonra a **Név** mező jobb oldalán, és válassza ki a legördülő listán a hálózati szolgáltatás nevét.

     A legördülő lista elemei között a leggyakrabban használt hálózati kapcsolatokat meghatározó hálózati szolgáltatások szerepelnek.

   - Írja be kézileg a hálózati szolgáltatás nevét a **Név** mezőbe.

8. Adja meg az adatátviteli protokollt:

   a. Jelölje be a **Protokoll** jelölőnégyzetet.

   b. A legördülő listán válassza ki azt a protokolltípust, amelynél a Tűzfal a hálózati tevékenységeket figyelemmel kíséri.

      A Tűzfal a TCP, UDP, ICMP, ICMPv6, IGMP és GRE protokollokat használó hálózati kapcsolatokat figyeli.

   Ha a **Név** legördülő listáról választ hálózati szolgáltatást, a **Protokoll** jelölőnégyzet automatikusan bejelölődik, és a mellette lévő legördülő listában a kiválasztott hálózati szolgáltatásnak megfelelő protokolltípus lesz látható. Alapértelmezés szerint a **Protokoll** jelölőnégyzet nincs bejelölve.

9. Az **Irány** legördülő listán adja meg a figyelt hálózati tevékenység irányát.

   A Tűzfal a következő irányokkal rendelkező hálózati kapcsolatokat figyeli:

   - **Bejövő (csomag)**.
   - **Bejövő**.
   - **Bejövő / kimenő**
   - **Kimenő (csomag)**.

- **Kimenő**.

10. Ha az ICMP vagy ICMPv6 protokollt választotta, megadhatja az ICMP csomag típusát és a kódját:

    a. Jelölje be az **ICMP típus** jelölőnégyzetet, majd válassza ki az ICMP csomagtípust a legördülő listán.

    b. Jelölje be az **ICMP kód** jelölőnégyzetet, majd válassza ki az ICMP csomagkódot a legördülő listán.

11. 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:

    a. Írja be a távoli számítógép portjait a **Távoli portok** mezőbe.

    b. Írja be a helyi számítógép portjait a **Helyi portok** mezőbe.

12. A **Hálózati csatolók** táblázatban adja meg azoknak a hálózati csatolóknak a beállításait, amelyekről hálózati csomagokat lehet küldeni, illetve amelyek hálózati csomagokat tudnak fogadni. Ehhez használja a **Hozzáadás**, **Szerkesztés** és **Törlés** gombokat.

13. Ha a hálózati csomagok felügyeletét élettartamuk (TTL) alapján korlátozni szeretné, jelölje be a **TTL** jelölőnégyzetet, a mellette lévő mezőben pedig adja meg a bejövő és / vagy kimenő hálózati csomagok élettartamának értéktartományát.

    Azon hálózati csomagok továbbítását hálózati szabály vezérli, amelyek élettartama nem lépi túl a megadott értéket.

    Ha ezt nem szeretné, törölje a **TTL** jelölőnégyzetet.

14. Adja meg azon távoli számítógépek hálózati címeit, amelyek hálózati csomagokat küldhetnek és / vagy fogadhatnak. Ehhez válassza ki az alábbi értékek közül valamelyiket a **Távoli címek** legördülő listán:

    - **Bármely cím**. A hálózati szabály bármilyen IP-címmel rendelkező távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyel.

    - **Alhálózati címek**. A hálózati szabály a kiválasztott hálózattípushoz kapcsolódó IP-címmel rendelkező távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyeli: **Megbízható hálózatok**, **Helyi hálózatok**, illetve **Nyilvános hálózatok**.

    - **Címek a listából**. A hálózati szabály a lenti listán a **Hozzáadás**, **Szerkesztés** és **Törlés** gombokkal megadható IP-címekkel rendelkező távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyeli.

15. Adja meg azon számítógépek hálózati címeit, amelyeken a Kaspersky Endpoint Security telepítve van, és amelyek hálózati csomagokat fogadhatnak és / vagy küldhetnek. Ehhez válassza ki az alábbi értékek közül valamelyiket a **Helyi címek** legördülő listán:

    - **Bármely cím**. A hálózati szabály bármilyen IP-címmel rendelkező olyan távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyel, amelyeken telepítve van a Kaspersky Endpoint Security.

    - **Címek a listából**. A hálózati szabály a lenti listán a **Hozzáadás**, **Szerkesztés** és **Törlés** gombokkal megadható IP-címekkel rendelkező olyan távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyeli, amelyeken telepítve van a Kaspersky Endpoint Security.

    Néha a helyi címet a hálózati csomagokkal dolgozó alkalmazásoknál nem lehet beszerezni. Ilyenkor a rendszer figyelmen kívül hagyja a **Helyi címek** beállítás értékét.

16. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.

17. A **Hálózati szabály** ablakban kattintson az **OK** gombra.

    Ha új hálózati szabályt hoz létre, az megjelenik a **Hálózati csomagszabályok** lapon a **Tűzfal** ablakban. Alapértelmezés szerint az új hálózati szabály a hálózati szabályok listájának végére kerül.

18. A **Tűzfal** ablakban kattintson az **OK** gombra.

19. A módosítások mentéséhez kattintson a **Mentés** gombra.

Hálózati csomagszabály be- és kikapcsolása

Hálózati csomagszabály be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.

3. Kattintson a **Hálózati csomagszabályok** gombra.

   Megnyílik a **Tűzfal** ablak a **Hálózati csomagszabályok** lapon.

4. A listán válassza ki a szükséges hálózati csomagszabályt.

5. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni a szabályt, jelölje be a hálózati csomagszabály melletti jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a szabályt, törölje a hálózati csomagszabály melletti jelölőnégyzetet.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Tűzfal műveletének módosítása hálózati csomagszabálynál

A Tűzfal hálózati csomagszabályra alkalmazott műveletének módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.

3. Kattintson a **Hálózati csomagszabályok** gombra.

   Megnyílik a **Tűzfal** ablak a **Hálózati csomagszabályok** lapon.

4. Válassza ki a listán azt a hálózati csomagszabályt, amelynek módosítani szeretné a műveletét.

5. Kattintson a **Engedély** oszlopban a jobb egérgombbal a helyi menü megjelenítéséhez, majd válassza ki a kiosztani kívánt műveletet:

- **Engedélyezés**
- **Blokkolás**
- **Az alkalmazásszabály szerint**
- **Események naplózása**

6. A **Tűzfal** ablakban kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Hálózati csomagszabály prioritásának módosítása

Egy hálózati csomagszabály prioritását a hálózati csomagszabályok listáján elfoglalt helye határozza meg. A lista legfelső hálózati csomagszabálya a legmagasabb prioritású.

Minden kézileg létrehozott hálózati csomagszabály a lista végére kerül, és a legalacsonyabb lesz a prioritása.

A Tűzfal a szabályokat abban a sorrendben hajtja végre, ahogy fentről lefelé a hálózati csomagszabályok listáján elhelyezkednek. Az adott hálózati kapcsolatra vonatkozó egyes feldolgozott hálózati csomagszabályoknak megfelelően a Tűzfal vagy engedélyezi, vagy blokkolja a hálózati hozzáférést a hálózati kapcsolat beállításaiban megadott címhez és porthoz.

Hálózati csomagszabály prioritásának módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.
3. Kattintson a **Hálózati csomagszabályok** gombra.

   Megnyílik a **Tűzfal** ablak a **Hálózati csomagszabályok** lapon.
4. Válassza ki a listán azt a hálózati csomagszabályt, amelynek módosítani szeretné a prioritását.
5. A hálózati csomagszabályt a listán a **Mozgatás felfelé** és **Mozgatás lefelé** gombokkal helyezheti a kívánt helyre.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

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 Tűzfal összetevő alapértelmezés szerint az alkalmazáscsoportok hálózati szabályait akkor alkalmazza, ha a csoporton belüli összes alkalmazás hálózati tevékenységét szűri, hasonlóan az Alkalmazásjogosultság-felügyelő összetevőhöz. 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.

Az alkalmazások hálózati szabályainak kezelése során a következő műveleteket végezheti el:

- Új hálózati szabály létrehozása.

  Létrehozhat új hálózati szabályt, mellyel a Tűzfal a kiválasztott alkalmazáscsoportba tartozó alkalmazás(ok) hálózati tevékenységét szabályozza.

- Hálózati szabály be- és kikapcsolása.

  Minden hálózati szabály *Engedélyezve* állapottal kerül a hálózati szabályok listájára. Ha egy hálózati szabály be van kapcsolva, a Tűzfal alkalmazza a szabályt.

  A kézileg létrehozott hálózati szabályokat ki is kapcsolhatja. Ha egy hálózati szabály ki van kapcsolva, a Tűzfal átmenetileg nem alkalmazza a szabályt.

- Hálózati szabály beállításainak módosítása.

  Az új hálózati szabály előállítását követően mindig visszatérhet a beállításaihoz és igény szerinti módosíthatja őket.

- A Tűzfal műveletének módosítása hálózati szabálynál.

  A hálózati szabályok listáján szerkesztheti azt a műveletet, amelyet a Tűzfal egy adott hálózati szabálynál az alkalmazás vagy alkalmazáscsoport hálózati tevékenységének észlelésekor alkalmaz.

- Hálózati szabály prioritásának módosítása.

  Az egyéni hálózati szabály prioritását növelheti vagy csökkentheti.

- Hálózati szabály törlése.

  Az egyéni hálózati szabály törlésével a Tűzfal a továbbiakban nem alkalmazza a szabályokat hálózati tevékenység észlelése esetén a kiválasztott alkalmazásra, illetve alkalmazáscsoportra, és a szabály többé nem jelenik meg az alkalmazás hálózati szabályainak listáján.

Alkalmazás hálózati szabályának létrehozása és szerkesztése

Hálózati szabály létrehozásához vagy szerkesztéséhez egy alkalmazás vagy alkalmazáscsoport számára:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Alapvető fenyegetések elleni védelem** részében válassza ki a **Tűzfal** lehetőséget.

3. Kattintson az **Alkalmazásszabályok** gombra.

   Megnyílik a **Tűzfal** ablak az **Alkalmazás hálózati szabályai** lapon.

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 ki igény szerint az **Alkalmazásjogok** vagy a **Alkalmazáscsoport-jogok** lehetőséget.

   Ezzel megnyílik az **Alkalmazásjogok** vagy az **Alkalmazáscsoport-jogok** ablak.

6. Válassza ki a **Hálózati szabályok** lapot az **Alkalmazásjogok** vagy **Alkalmazáscsoport-jogok** ablakon.

7. Végezze el az alábbiak egyikét:

   - Új hálózati szabály létrehozásához kattintson a **Hozzáadás** gombra.
   - Ha hálózati szabályt szeretne szerkeszteni, válassza ki a listáról, és kattintson a **Szerkesztés** gombra.

   Megnyílik a **Hálózati szabály** ablak.

8. Válassza ki a **Művelet** legördülő listán a Tűzfal által az adott típusú hálózati tevékenység észlelésekor végrehajtandó műveletet:

   - **Engedélyezés**
   - **Blokkolás**

9. A **Név** mezőbe írja be a hálózati szolgáltatás nevét az alábbi módok egyikével:

   - Kattintson a ikonra a **Név** mező jobb oldalán, és válassza ki a legördülő listán a hálózati szolgáltatás nevét.

     A legördülő lista elemei között a leggyakrabban használt hálózati kapcsolatokat meghatározó hálózati szolgáltatások szerepelnek.

   - Írja be kézileg a hálózati szolgáltatás nevét a **Név** mezőbe.

10. Adja meg az adatátviteli protokollt:

    a. Jelölje be a **Protokoll** jelölőnégyzetet.

    b. A legördülő listán válassza ki azt a protokolltípust, amelynél a hálózati tevékenységeket figyelemmel szeretné kísérni.

       A Tűzfal a TCP, UDP, ICMP, ICMPv6, IGMP és GRE protokollokat használó hálózati kapcsolatokat figyeli. Ha a **Név** legördülő listáról választ hálózati szolgáltatást, a **Protokoll** jelölőnégyzet automatikusan bejelölődik, és a mellette lévő legördülő listában a kiválasztott hálózati szolgáltatásnak megfelelő protokolltípus lesz látható. Alapértelmezés szerint a **Protokoll** jelölőnégyzet nincs bejelölve.

11. Az **Irány** legördülő listán adja meg a figyelt hálózati tevékenység irányát.

    A Tűzfal a következő irányokkal rendelkező hálózati kapcsolatokat figyeli:

    - **Bejövő**.
    - **Bejövő / kimenő**.
    - **Kimenő**.

12. Ha az ICMP vagy ICMPv6 protokollt választotta, megadhatja az ICMP csomag típusát és a kódját:

    a. Jelölje be az **ICMP típus** jelölőnégyzetet, majd válassza ki az ICMP csomagtípust a legördülő listán.

    b. Jelölje be az **ICMP kód** jelölőnégyzetet, majd válassza ki az ICMP csomagkódot a legördülő listán.

13. 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:

    a. Írja be a távoli számítógép portjait a **Távoli portok** mezőbe.

    b. Írja be a helyi számítógép portjait a **Helyi portok** mezőbe.

14. Adja meg azon távoli számítógépek hálózati címeit, amelyek hálózati csomagokat küldhetnek és / vagy fogadhatnak. Ehhez válassza ki az alábbi értékek közül valamelyiket a **Távoli címek** legördülő listán:

    - **Bármely cím**. A hálózati szabály bármilyen IP-címmel rendelkező távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyel.
    - **Alhálózati címek**. A hálózati szabály a kiválasztott hálózattípushoz kapcsolódó IP-címmel rendelkező távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyeli: **Megbízható hálózatok**, **Helyi hálózatok**, illetve **Nyilvános hálózatok**.
    - **Címek a listából**. A hálózati szabály a lenti listán a **Hozzáadás**, **Szerkesztés** és **Törlés** gombokkal megadható IP-címekkel rendelkező távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyeli.

15. Adja meg azon számítógépek hálózati címeit, amelyeken a Kaspersky Endpoint Security telepítve van, és amelyek hálózati csomagokat fogadhatnak és / vagy küldhetnek. Ehhez válassza ki az alábbi értékek közül valamelyiket a **Helyi címek** legördülő listán:

    - **Bármely cím**. A hálózati szabály bármilyen IP-címmel rendelkező olyan távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyel, amelyeken telepítve van a Kaspersky Endpoint Security.
    - **Címek a listából**. A hálózati szabály a lenti listán a **Hozzáadás**, **Szerkesztés** és **Törlés** gombokkal megadható IP-címekkel rendelkező olyan távoli számítógépek által küldött és / vagy fogadott hálózati csomagokat felügyeli, amelyeken telepítve van a Kaspersky Endpoint Security.

    Néha a helyi címet a hálózati csomagokkal dolgozó alkalmazásoknál nem lehet beszerezni. Ilyenkor a rendszer figyelmen kívül hagyja a **Helyi címek** beállítás értékét.

16. Ha azt szeretné, hogy a hálózati szabály műveletei megjelenjenek a jelentésben, jelölje be az **Események naplózása** jelölőnégyzetet.

17. A **Hálózati szabály** ablakban kattintson az **OK** gombra.

    Ha új hálózati szabályt hozott létre, az megjelenik a **Hálózati szabályok** lapon.

18. Kattintson az **OK** gombra az **Alkalmazáscsoport-jogoki** ablakban, ha a szabályt alkalmazáscsoportnak szánja, illetve az **Alkalmazásjogok** ablakra, ha a szabályt egy alkalmazásnak szánja.

19. A **Tűzfal** ablakban kattintson az **OK** gombra.

20. A módosítások mentéséhez kattintson a **Mentés** gombra.

Alkalmazás hálózati szabályának be- és kikapcsolása

Alkalmazás hálózati szabályának be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.
3. Kattintson az **Alkalmazás hálózati szabályai** gombra.

   Megnyílik a **Tűzfal** ablak az **Alkalmazásfelügyeleti szabályok** lapon.
4. A listán kiválaszthatja azt az alkalmazást vagy alkalmazások csoportját, amely(ek)nél hálózati szabályt szeretne be- vagy kikapcsolni.
5. Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza ki igény szerint az **Alkalmazásszabályok** vagy a **Csoportszabályok** lehetőséget.

   Ezzel megnyílik az **Alkalmazásfelügyeleti szabályok** vagy az **Alkalmazáscsoport-felügyelő szabályok** ablak.
6. A megnyíló ablakban válassza ki a **Hálózati szabályok** lapot.
7. Válassza ki az alkalmazáscsoport hálózati szabályainak listáján a kívánt hálózati szabályt.
8. Végezze el az alábbiak egyikét:
   - Ha be szeretné kapcsolni a szabályt, jelölje be a hálózati szabály melletti jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a szabályt, törölje a hálózati szabály melletti jelölőnégyzetet.

   > Az alkalmazáscsoportoknak a Tűzfal által alapértelmezés szerint létrehozott hálózati szabályai nem kapcsolhatók ki.
9. Kattintson az **OK** gombra az **Alkalmazáscsoport felügyeleti szabályai** ablakban, ha a szabályt alkalmazáscsoportnak szánja, illetve az **Alkalmazásfelügyeleti szabályok** ablakra, ha a szabályt egy alkalmazásnak szánja.
10. A **Tűzfal** ablakban kattintson az **OK** gombra.
11. A módosítások mentéséhez kattintson a **Mentés** gombra.

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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.
3. Kattintson az **Alkalmazás hálózati szabályai** gombra.

   Megnyílik a **Tűzfal** ablak az **Alkalmazásfelügyeleti szabályok** lapon.
4. Ha módosítani szeretné azt a Tűzfal-műveletet, amely alapértelmezés szerint létrehozott összes hálózati szabályra vonatkozik, válasszon ki egy alkalmazást vagy alkalmazáscsoportot a listán. A kézileg létrehozott hálózati szabályok változatlanul maradnak.
5. Kattintson a **Hálózat** oszlopban a helyi menü megjelenítéséhez, majd válassza ki a kiosztani kívánt műveletet:
   - **Öröklés**
   - **Engedélyezés**
   - **Blokkolás**
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Alkalmazás vagy alkalmazások csoportja egyetlen hálózati szabályához tartozó Tűzfal-reakció módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.
3. Kattintson az **Alkalmazás hálózati szabályai** gombra.

   Megnyílik a **Tűzfal** ablak az **Alkalmazásfelügyeleti szabályok** lapon.
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 ki igény szerint az **Alkalmazásszabályok** vagy a **Csoportszabályok** lehetőséget.

   Ezzel megnyílik az **Alkalmazásfelügyeleti szabályok** vagy az **Alkalmazáscsoport-felügyelő szabályok** ablak.
6. A megnyíló ablakban 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:
   - **Engedélyezés**
   - **Blokkolás**
   - **Események naplózása**

9. Kattintson az **OK** gombra az **Alkalmazáscsoport felügyeleti szabályai** ablakban, ha a szabályt alkalmazáscsoportnak szánja, illetve az **Alkalmazásfelügyeleti szabályok** ablakra, ha a szabályt egy alkalmazásnak szánja.

10. A **Tűzfal** ablakban kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Mentés** gombra.

Alkalmazás hálózati szabálya prioritásának módosítása

Egy hálózati szabály prioritását a hálózati szabályok listáján elfoglalt helye határozza meg. A Tűzfal a szabályokat abban a sorrendben hajtja végre, ahogy fentről lefelé a hálózati szabályok listáján elhelyezkednek. Az adott hálózati kapcsolatra vonatkozó egyes feldolgozott hálózati szabályoknak megfelelően a Tűzfal vagy engedélyezi, vagy blokkolja a hálózati hozzáférést a hálózati kapcsolat beállításaiban jelzett címhez és porthoz.

A kézileg létrehozott hálózati szabályok prioritása magasabb, mint az alapértelmezett hálózati szabályokéi.

Az alkalmazáscsoportok alapértelmezés szerint létrehozott hálózati szabályainak prioritását nem lehet megváltoztatni.

Hálózati szabály prioritásának módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Tűzfal** alrészt.

   Az ablak jobb oldali részén megjelennek a Tűzfal összetevő beállításai.

3. Kattintson az **Alkalmazás hálózati szabályai** gombra.

   Megnyílik a **Tűzfal** ablak az **Alkalmazásfelügyeleti szabályok** lapon.

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 ki igény szerint az **Alkalmazásszabályok** vagy a **Csoportszabályok** lehetőséget.

   Ezzel megnyílik az **Alkalmazásfelügyeleti szabályok** vagy az **Alkalmazáscsoport-felügyelő szabályok** ablak.

6. A megnyíló ablakban válassza ki a **Hálózati szabályok** lapot.

7. Válassza ki azt a hálózati szabályt, amelynek módosítani szeretné a prioritását.

8. A hálózati szabályt a listán a **Mozgatás felfelé** és **Mozgatás lefelé** gombokkal helyezheti a kívánt helyre.

9. Kattintson az **OK** gombra az **Alkalmazáscsoport felügyeleti szabályai** ablakban, ha a szabályt alkalmazáscsoportnak szánja, illetve az **Alkalmazásfelügyeleti szabályok** ablakra, ha a szabályt egy alkalmazásnak szánja.

10. A **Tűzfal** ablakban kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Mentés** gombra.

Hálózatfigyelő

Ez a rész tájékoztatást nyújt a Hálózatfigyelővel kapcsolatban, és ismerteti a Hálózatfigyelő elindításának menetét.

A Hálózatfigyelő

A *Hálózatfigyelő* egy olyan eszköz, amellyel valós időben tekinthetők meg a felhasználó számítógépének hálózati tevékenységével kapcsolatos információk.

A Hálózatfigyelő elindítása

A Hálózatfigyelő elindítása:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Védelem** részre.

   Megnyílik a **Védelem** rész.
4. Kattintson a jobb gombbal a **Tűzfal** sorra a Tűzfal műveletei helyi menüjének megnyitásához.
5. A helyi menüben válassza a **Hálózatfigyelő** elemet.

   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.
   - A **Nyitott portok** lapon látható a számítógép összes nyitott portja.
   - 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 Behatolásmegelőzési rendszer összetevő blokkolta, miután onnan érkező hálózati támadási próbálkozásokat észlelt.

Behatolásmegelőzési rendszer

Ez a rész tájékoztatást nyújt a Behatolásmegelőzési rendszerrel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Behatolásmegelőzési rendszer

A Behatolásmegelőzési rendszer a hálózati támadásokra jellemző bejövő hálózati forgalmat vizsgálja. Hálózati támadásra irányuló próbálkozás észlelésekor a Kaspersky Endpoint Security blokkolja a hálózati tevékenységet, így az nem tudja megtámadni a számítógépet. A képernyőn ekkor megjelenik egy figyelmeztetés a megkísérelt hálózati támadásról a támadó számítógép adataival együtt.

A támadó számítógépről érkező hálózati forgalom egy órán át blokkolva van. A támadó számítógép blokkolására használt beállítások szerkeszthetők.

A Kaspersky Endpoint Security adatbázisai tartalmazzák a már ismert hálózati támadások típusait és az ellenük való védekezés módszereit. A Behatolásmegelőzési rendszer összetevő által észlelhető hálózati támadások listája az alkalmazás adatbázisainak és alkalmazásmoduljainak frissítésekor frissül.

A Behatolásmegelőzési rendszer engedélyezése és letiltása

Alapértelmezés szerint a Behatolásmegelőzési rendszer be van kapcsolva és optimális módban működik. A Behatolásmegelőzési rendszer szükség esetén kikapcsolható.

Az összetevő kétféle módon engedélyezhető és tiltható le:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

A Behatolásmegelőzési rendszer be- és kikapcsolásához végezze el a következőt a Védelem és felügyelet lapon a fő alkalmazásablakban:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Védelem** részre.

   Megnyílik a **Védelem** rész.
4. Kattintson a jobb egérgombbal a **Behatolásmegelőzési rendszer** sorra a Behatolásmegelőzési rendszer műveletei helyi menüjének megnyitásához.
5. Végezze el az alábbiak egyikét:

   - A Behatolásmegelőzési rendszer bekapcsolásához válassza ki a helyi menüben az **Indítás** lehetőséget.

     Az összetevő állapotikonja , mely a **Behatolásmegelőzési rendszer** sorában a bal oldalon látható, átvált ikonra.
   - A Behatolásmegelőzési rendszer kikapcsolásához válassza ki a helyi menüben a **Leállítás** lehetőséget.

Az összetevő állapotikonja , mely a **Behatolásmegelőzési rendszer** sorában a bal oldalon látható, átvált ikonra.

A Behatolásmegelőzési rendszer be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Behatolásmegelőzési rendszer** alrészt.

   A Behatolásmegelőzési rendszer beállításai az ablak jobb oldalán jelennek meg.
3. Végezze el az alábbiakat:

   - Ha be szeretné kapcsolni a Behatolásmegelőzési rendszert, jelölje be a **Behatolásmegelőzési rendszer engedélyezése** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Behatolásmegelőzési rendszert, törölje a **Behatolásmegelőzési rendszer engedélyezése** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Behatolásmegelőzési rendszer beállításai

A Behatolásmegelőzési rendszer beállításainak megadása érdekében a következő műveleteket végezheti el:

- A támadó számítógép blokkolására használt beállítások megadása.
- A blokkolásból kizárt címek listájának előállítása.

A támadó számítógép blokkolására használt beállítások szerkesztése.

A támadó számítógép blokkolására használt beállítások szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Behatolásmegelőzési rendszer** alrészt.

   A Behatolásmegelőzési rendszer beállításai az ablak jobb oldalán jelennek meg.
3. Jelölje be **A támadó számítógép hozzáadása a blokkolt számítógépek listájához ennyi ideig** jelölőnégyzetet.

   Ha ez a jelölőnégyzet be van jelölve, akkor a Behatolásmegelőzési rendszer hálózati támadásra tett próbálkozás észlelésekor megadott ideig blokkolja a támadó számítógépről érkező hálózati forgalmat. Ezzel automatikusan védi a számítógépet az ugyanerről a címről érkező lehetséges további hálózati támadásoktól.

   Ha ez a jelölőnégyzet nincs bejelölve, akkor a Behatolásmegelőzési rendszer hálózati támadásra tett próbálkozás észlelésekor nem kapcsolja be az automatikus védelmet az ugyanazon címről érkező esetleges további hálózati támadások ellen.
4. A támadó számítógép blokkolásának időtartamát **A támadó számítógép hozzáadása a blokkolt számítógépek listájához ennyi ideig** jelölőnégyzet mellett lehet módosítani.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

A blokkolásból kizárt címek beállítása

A blokkolásból kizárt címek beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **Behatolásmegelőzési rendszer** alrészt.

   A Behatolásmegelőzési rendszer beállításai az ablak jobb oldalán jelennek meg.
3. Kattintson a **Kizárások** gombra.

   Megnyílik a **Kizárások** ablak.
4. Végezze el az alábbiak egyikét:

   - Ha új IP-címet szeretne megadni, kattintson a **Hozzáadás** gombra.
   - Ha korábban megadott IP-címet szeretne szerkeszteni, válassza ki a listáról, és kattintson a **Szerkesztés** gombra.

   Megnyílik az **IP-cím** ablak.
5. Adja meg annak a számítógépnek az IP-címét, amelyről a hálózati támadásokat nem szabad blokkolni.
6. Az **IP-cím** ablakban kattintson az **OK** gombra.
7. A **Kizárások** ablakban kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

A BadUSB védelem

Ez a rész tájékoztatást nyújt a BadUSB védelem összetevőről.

A BadUSB védelem

Egyes vírusok az USB eszközök firmware-ét módosítva becsapják az operációs rendszert, így az az USB eszközt billentyűzetként észleli.

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 alkalmazás billentyűzetként azonosít, akkor felkéri a felhasználót, hogy írjon be ezen a billentyűzeten vagy a képernyőn megjelenő billentyűzeten (ha van) egy általa előállított számkódot. Ezt az eljárást nevezik billentyűzethitelesítésnek. Az alkalmazás a hitelesített billentyűzet használatát engedélyezi, a nem hitelesítettét pedig blokkolja.

A BadUSB védelem összetevő a telepítést követően azonnal futni kezd a háttérben. Ha az alkalmazásra nem vonatkozik egy Kaspersky Security Center rendszabály sem, akkor a BadUSB védelem be- és kikapcsolható a számítógép védelmének és felügyeletének ideiglenes szüneteltetésével és újraindításával.

A BadUSB védelem összetevő telepítése

Ha a Kaspersky Endpoint Security telepítése során az alapszintű vagy szokásos telepítést választotta, akkor a BadUSB védelem összetevő nem áll rendelkezésre. Telepítéséhez módosítani kell az alkalmazásösszetevők készletét.

A BadUSB védelem összetevő telepítése:

1. Válassza ki a **Start** menüben az **Alkalmazások→ Kaspersky Endpoint Security 10 for Windows → Módosítás, Javítás vagy Eltávolítás** lehetőséget.

   Elindul a Telepítővarázsló.

2. Az Alkalmazástelepítő varázsló **Alkalmazás módosítása, javítása vagy eltávolítása** ablakában kattintson a **Módosítás** gombra.

   Ezzel megnyílik az Alkalmazástelepítő varázsló **Egyéni telepítés** ablaka.

3. A **BadUSB védelem** összetevő neve melletti ikon helyi menüjében válassza ki a **Funkció telepítése a merevlemezre** lehetőséget.

4. Kattintson a **Tovább** gombra.

5. Kövesse a Telepítővarázsló utasításait.

BadUSB támadás megelőzésének be- és kikapcsolása

A BadUSB támadás megelőzésének be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **BadUSB védelem** alrészt.

   A BadUSB támadás megelőzése beállításai az ablak jobb oldalán jelennek meg.
3. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni a BadUSB támadás megelőzését, jelölje be a **BadUSB védelem engedélyezése** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a BadUSB támadás megelőzését, törölje a **BadUSB védelem engedélyezése** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Képernyőn megjelenő billentyűzet hitelesítéshez történő használatának engedélyezése és tiltása

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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Vírusvédelem** részében válassza ki a **BadUSB védelem** alrészt.

   Az összetevőbeállítások az ablak jobb oldalán jelennek meg.
3. Végezze el az alábbiak egyikét:

   - Jelölje be a **Virtuális billentyűzet használatának tiltása az engedélyezéshez** jelölőnégyzetet, ha blokkolni szeretné a képernyőn megjelenő billentyűzet engedélyezésre történő használatát.
   - Törölje a **Virtuális billentyűzet használatának tiltása az engedélyezéshez** jelölőnégyzetet, ha engedélyezni szeretné a képernyőn megjelenő billentyűzet engedélyezésre történő használatát.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Billentyűzethitelesítés

Az operációs rendszer által billentyűzetként felismert, a BadUSB védelem összetevő telepítése előtt a számítógéphez csatlakoztatott USB eszközök az összetevő telepítését követően hitelesítettnek minősülnek.

Az alkalmazás csak akkor követeli meg az operációs rendszer által billentyűzetként azonosított csatlakoztatott USB eszköz hitelesítését, ha az USB billentyűzet hitelesítési kérése be van kapcsolva. A felhasználó a hitelesítés megtörténtéig nem használhat hitelesítetlen billentyűzetet.

Ha az USB billentyűzet hitelesítési kérése ki van kapcsolva, a felhasználó az összes csatlakoztatott billentyűzetet használhatja. Az USB billentyűzet hitelesítési kérésének bekapcsolása után az alkalmazás azonnal megjelenít egy, az egyes csatlakoztatott és hitelesítetlen billentyűzetek hitelesítésére irányuló kérést.

Billentyűzet hitelesítése:

1. Az USB billentyűzet hitelesítésének bekapcsolt állapotában csatlakoztassa a billentyűzetet egy USB porthoz.

   Megnyílik a **<Billentyűzet neve> billentyűzethitelesítés** ablak, melyben a csatlakoztatott billentyűzet adatai és a hitelesítésre szolgáló számkód látható.

2. Írja be a csatlakoztatott billentyűzeten vagy a képernyőn megjelenő billentyűzeten (ha van) a hitelesítési ablakban látható véletlenszerűen előállított számkódot.

3. Kattintson az **OK** gombra.

   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 hitelesítést 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. A számkód beírását háromszor lehet megpróbálni. Ha a számkód beírása egymás után háromszor hibás vagy a felhasználó bezárja a **<Billentyűzet neve> billentyűzethitelesítés** ablakot, az alkalmazás blokkolja a billentyűzethez való hozzáférést. A billentyűzet ismételt csatlakoztatásakor és az operációs rendszer újraindításakor az alkalmazás ismét felkéri a felhasználót, hogy végezze el a billentyűzet hitelesítését.

Alkalmazásindítás-felügyelő

Ez a rész tájékoztatást nyújt az Alkalmazásindítás-felügyelővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

Az Alkalmazásindítás-felügyelő

Az Alkalmazásindítás-felügyelő összetevő figyeli a felhasználók alkalmazások indítására tett próbálkozásait, és az alkalmazások indítását *Alkalmazásindítás-felügyelő szabályok* révén szabályozza.

Az olyan alkalmazások indítását, amelyek beállításai egyik Alkalmazásindítás-felügyelő szabálynak sem felelnek meg, az összetevő kiválasztott üzemmódja szabályozza. Alapértelmezés szerint a *Feketelista* mód van kiválasztva. Ez a mód az összes felhasználó számára engedélyezi bármely alkalmazás elindítását.

A felhasználók alkalmazások elindítására tett minden próbálkozása naplózásra kerül jelentésekben.

Az Alkalmazásfelügyelő engedélyezése és letiltása

Noha az Alkalmazásfelügyelő alapértelmezés szerint ki van kapcsolva, szükség esetén be lehet kapcsolni.

Az Alkalmazásfelügyelő be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Biztonsági felügyelet** részben válassza ki az **Alkalmazásfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.
3. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni az Alkalmazásfelügyelőt, jelölje be az **Alkalmazásfelügyelő bekapcsolása** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni az Alkalmazásfelügyelőt, törölje az **Alkalmazásfelügyelő bekapcsolása** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az Alkalmazásindítás-felügyelő funkciónak korlátozásai

Az Alkalmazásindítás-felügyelő összetevő működése az alábbi esetekben korlátozott:

- Az alkalmazás verziófrissítésekor az Alkalmazásindítás-felügyelő összetevő beállításainak importálása nem támogatott.

  Az Alkalmazásindítás-felügyelő működésének visszaállításához ismét meg kell adnia az összetevő beállításait.

- Ha nincs kapcsolat a KSN kiszolgálókkal, a Kaspersky Endpoint Security az alkalmazások és moduljaik reputációjára vonatkozó információkat csak a helyi adatbázisokból szerzi be. Ha a helyi adatbázisokban egy adott alkalmazásra vonatkozóan nincsenek információk, akkor az alkalmazás egyik megbízhatósági csoportba való besorolására sem kerül sor.

  Az alkalmazások KSN kiszolgálókkal való kapcsolat esetén való besorolása eltérhet a kapcsolat hiányában végzett besorolásuktól.

- A Kaspersky Security Center adatbázisában 150 000 feldolgozott fájlra vonatkozó adat tárolható. E bejegyzésszám elértével az új fájlok feldolgozására nem kerül sor. A leltározási műveletek folytatásához törölnie kell a korábban a Kaspersky Security Center adatbázisban leltárba vett fájlokat azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van.

- Az összetevő csak akkor felügyeli a szkriptek indítását, ha a szkript a parancssoron keresztül kerül az értelmezőhöz.

  Ha az értelmező indítását az Alkalmazásindítás-felügyelő szabályok lehetővé teszik, az összetevő nem blokkolja az adott értelmezőből indított szkripteket.

- 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:

  - { cCmdLineParser::itCmd, _T("%ComSpec%") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };

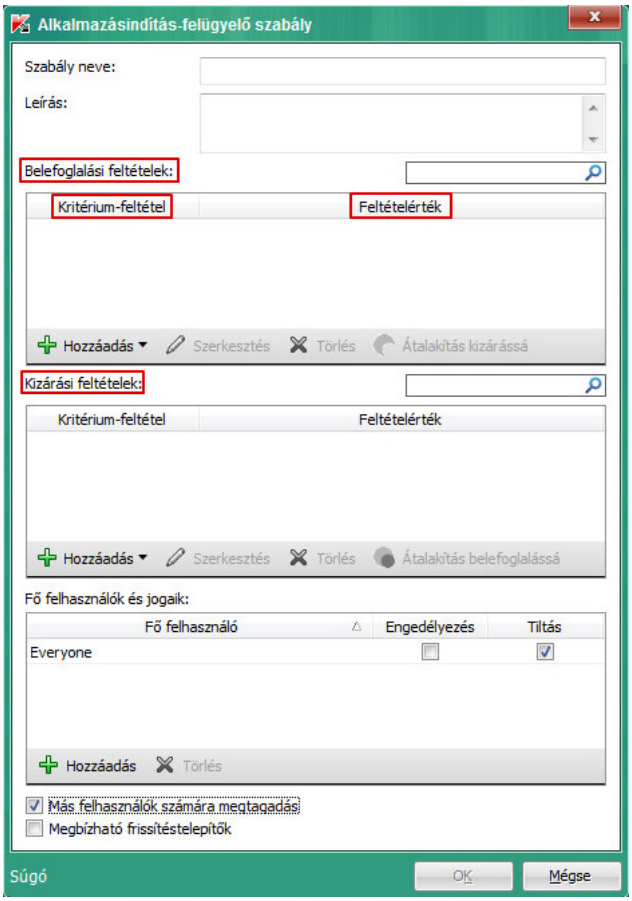
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Az Alkalmazásfelügyeleti szabályok

A Kaspersky Endpoint Security az alkalmazások felhasználók által történő elindítását szabályok révén felügyeli. Az Alkalmazásfelügyeleti szabály megadja a kiváltó feltételeket, valamint a szabály kiváltása esetén az Alkalmazásfelügyelő összetevő által elvégzett műveletet (az alkalmazás felhasználók által történő elindításának engedélyezését, illetve blokkolását).

A szabálykiváltó feltételek

A szabályt kiváltó feltételnél a következő összefüggés áll fenn: „feltétel típusa – feltétel kritériuma – feltétel értéke” (lásd az alábbi ábrát). A szabályt kiváltó feltételek alapján a Kaspersky Endpoint Security egy szabályt alkalmaz (vagy nem alkalmaz) egy alkalmazásra.



Alkalmazásfelügyeleti szabály. A szabálykiváltó feltételek paraméterei

A szabályok szerepeltetési és kizárásai feltételeket használnak:

- *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 végrehajtható fájlját tartalmazó mappának vagy az alkalmazás végrehajtható fájljának elérési útvonala.
- Metaadatok: alkalmazás végrehajtható fájljának neve, alkalmazás végrehajtható fájljának verziója, alkalmazás neve, alkalmazás verziója, alkalmazás forgalmazója.
- Alkalmazás végrehajtható fájljának hash kódja.
- Tanúsítvány: kiállító, alany, ujjlenyomat.
- Az alkalmazás szerepeltetése KL kategóriában.
- Az alkalmazás cserélhető meghajtón lévő végrehajtható 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.

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:

- **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 jelzi, hogy a Kaspersky Endpoint Security engedélyezi az olyan alkalmazások elindítását, melyekre vonatkoznak a szabályok, de az indítások információit jelentésben rögzíti.

Az Alkalmazásindítás-felügyelő szabályok kezelése

Az Alkalmazásindítás-felügyelő szabályoknál a következő műveleteket végezheti el:

- Új szabály hozzáadása
- Szabályt kiváltó feltételek létrehozása és módosítása
- Szabály állapotának szerkesztése

  Az Alkalmazásindítás-felügyelő szabályok lehetnek bekapcsolva (a szabállyal szemben lévő jelölőnégyzet be van jelölve) vagy kikapcsolva (a szabállyal szemben lévő jelölőnégyzet nincs bejelölve). Az Alkalmazásindítás-felügyelő szabályok létrehozásukat követően alapértelmezés szerint be vannak kapcsolva.
- Szabály törlése

Alkalmazásindítás-felügyelő szabály megadása és szerkesztése

Alkalmazásindítás-felügyelő szabály megadása és szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.
3. Az összetevő beállításainak szerkeszthetővé tételéhez válassza ki az **Alkalmazásindítás-felügyelő bekapcsolása** lehetőséget.
4. Végezze el az alábbiak egyikét:

   - Szabályt a **Hozzáadás** gombra kattintva adhat meg.
   - Ha meglévő szabályt szeretne szerkeszteni, válassza ki a listáról, és kattintson a **Szerkesztés** gombra.

   Megnyílik az **Alkalmazásindítás-felügyelő szabály** ablak.
5. Adja meg vagy szerkessze a szabály beállításait:

   a. A **Szabály neve** mezőben adja meg vagy szerkessze a szabály nevét.

   b. A **Belefoglalási feltételek** táblázatban a szabályt kiváltó belefoglalási feltételek listáját létrehozhatja és szerkesztheti a **Hozzáadás**, **Szerkesztés**, **Törlés** és **Átalakítás kizárássá** gombokkal.

   c. A **Kizárási feltételek** táblázatban a szabályt kiváltó kizárási feltételek listáját létrehozhatja és szerkesztheti a **Hozzáadás**, **Szerkesztés**, **Törlés** és **Átalakítás belefoglalássá** gombokkal.

   d. Szükség esetén módosítsa a szabálykiváltó feltétel típusát:

   - Ha a feltétel típusát belefoglalási feltételről kizárási feltételre szeretné változtatni, válassza ki az adott feltételt a **Belefoglalási feltételek** táblázatban, majd kattintson az **Átalakítás kizárássá** gombra.
   - Ha a feltétel típusát kizárási feltételről belefoglalási feltételre szeretné változtatni, válassza ki az adott feltételt a **Kizárási feltételek** táblázatban, majd kattintson az **Átalakítás belefoglalássá** gombra.

   e. 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 **Fő felhasználók és jogaik** táblázatban a **Hozzáadás** gombra.

   Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanelt a Microsoft Windowsban. Ebben az ablakban felhasználókat és / vagy felhasználói csoportokat választhat ki.

   Alapértelmezés szerint a felhasználók listájára a **Mindenki** érték kerül. A szabály az összes felhasználóra vonatkozik.

   > Ha a táblázatban nincs megadva felhasználó, a szabályt nem lehet menteni.

   f. Jelölje be az **Fő felhasználók és jogaik** táblázatban a felhasználók és / vagy felhasználói csoportok nevével szemben lévő **Engedélyezés**, illetve **Blokkolás** jelölőnégyzeteket az alkalmazások indításához fűződő jogok megadásához.

   Az alapértelmezés szerint bejelölt jelölőnégyzet az Alkalmazásindítás-felügyelő üzemmódjától függ.

   g. Jelölje be a **Más felhasználók számára megtagadás** jelölőnégyzetet, ha azt szeretné, hogy a szabályt kiváltó feltételeknek megfelelő alkalmazások indítása minden olyan felhasználó számára blokkolva legyen, aki nem szerepel az **Fő felhasználó** oszlopban, és nem is tartozik az **Fő felhasználó** oszlopban megadott felhasználói csoportok valamelyikébe.

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 **Fő felhasználók és jogaik** táblázatban, és nem is tartoznak az **Fő felhasználók és jogaik** táblázatban megadott felhasználói csoportok valamelyikébe.

h. Ha azt szeretné, hogy a Kaspersky Endpoint Security a szabályt kiváltó feltételeknek megfelelő alkalmazásokat olyan megbízható frissítőknek tekintse, amelyek más alkalmazásokat elindíthatnak, és amelyekhez nincsenek megadva Alkalmazásindítás-felügyelő szabályok, jelölje be a **Megbízható frissítéstelepítők** jelölőnégyzetet.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Alkalmazásfelügyeleti szabályt kiváltó feltétel hozzáadása

Alkalmazásfelügyeleti szabályt kiváltó új feltétel hozzáadása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.

2. Az ablak bal oldalán, a **Biztonsági felügyelet** részben válassza ki az **Alkalmazásfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásfelügyelő összetevő beállításai.

3. Az összetevő beállításainak szerkeszthetővé tételéhez jelölje be az **Alkalmazásfelügyelő** jelölőnégyzetet.

4. Végezze el az alábbiak egyikét:

   - Ha egy új szabályt szeretne létrehozni, és kiváltó feltételt szeretne hozzáadni, kattintson a **Hozzáadás** gombra.
   - Ha meglévő szabályhoz szeretne kiváltó feltételt hozzáadni, válassza ki a listáról, és kattintson a **Szerkesztés** gombra.

   Megnyílik az **Alkalmazásfelügyeleti szabály** ablak.

5. A **Belefoglalási feltételek** vagy **Kizárási feltételek** táblázatban kattintson a **Hozzáadás** hivatkozásra.

A **Hozzáadás** gomb legördülő listájával különféle kiváltó feltételeket adhat hozzá a szabályhoz (lásd a lenti utasításokat).

Szabálykiváltó feltétel hozzáadása a megadott mappában lévő fájlok tulajdonságai alapján:

1. Válassza ki a **Hozzáadás** gomb legördülő listáján a **Feltételek a megadott mappában található fájlok tulajdonságai alapján** lehetőséget.

   Megnyílik a szokásos **Mappa választása** ablak a Microsoft Windowsban.

2. Válassza ki a **Mappa választása** ablakban azoknak az alkalmazásoknak a végrehajtható fájljait tartalmazó mappát, amelyeknek a tulajdonságaira szeretné alapozni egy vagy több szabálykiváltó feltételt.

3. Kattintson az **OK** gombra.

Megnyílik a **Feltétel hozzáadása** ablak.

4. Válassza ki a **Kritérium megjelenítése** legördülő listán azt a kritériumot, amelynek alapján egy vagy több szabálykiváltó feltételt szeretne létrehozni: **Fájl ellenőrzőösszeg-kódja**, **Tanúsítvány**, **KL kategória**, **Metaadatok** vagy **Mappa elérési útja**.

   A Kaspersky Endpoint Security nem támogatja az MD5 hash kódot, és MD5 hash alapján nem felügyeli az alkalmazások indítását. Szabálykiváltó feltételként SHA256 hash szolgál.

5. Ha a **Metaadatok** lehetőséget választotta a **Kritérium megjelenítése** legördülő listán, jelölje be a jelölőnégyzeteket a végrehajtható fájlok azon tulajdonságaival szemben, amelyeket a szabálykiváltó feltételben használni szeretne: **Fájlnév**, **Fájlverzió**, **Alkalmazásnév**, **Alkalmazás verziója** és **Forgalmazó**.

   Ha a megadott tulajdonságok közül egy sincs kiválasztva, a szabályt nem lehet menteni.

6. Ha a **Tanúsítvány** lehetőséget választotta a **Kritérium megjelenítése** legördülő listán, jelölje be a jelölőnégyzeteket azokkal a beállításokkal szemben, amelyeket a szabálykiváltó feltételben használni szeretne: **Kiállító**, **Adatalany** és **Ujjlenyomat**.

   Ha a megadott beállítások közül egy sincs kiválasztva, a szabályt nem lehet menteni.

   Szabálykiváltó feltételként nem javasolt csak a **Kiállító** és az **Adatalany** kritériumokat alkalmazni. E kritériumok használata megbízhatatlan.

7. Jelölje be a jelölőnégyzeteket az alkalmazás azon végrehajtható fájljainak neve mellett, amelyeknek a tulajdonságait bele szeretné venni a szabályt kiváltó feltételekbe.

8. Kattintson a **Tovább** gombra.

   Megjelenik a kialakított szabálykiváltó feltételek listája.

9. Jelölje be a kialakított szabálykiváltó feltételek listáján a jelölőnégyzeteket azokkal a szabálykiváltó feltételekkel szemben, amelyeket az Alkalmazásfelügyeleti szabályhoz hozzá szeretne adni.

10. Kattintson a **Megszakítás** gombra.

Szabálykiváltó feltétel hozzáadása a számítógépen elindított alkalmazások tulajdonságai alapján:

1. Válassza ki a **Hozzáadás** gomb legördülő listáján a **Feltételek az elindított alkalmazások tulajdonságai alapján** lehetőséget.

2. Válassza ki a **Feltétel hozzáadása** ablakban a **Kritérium megjelenítése** legördülő listán azt a kritériumot, amelynek alapján egy vagy több szabálykiváltó feltételt szeretne létrehozni: **Fájl ellenőrzőösszeg-kódja**, **Tanúsítvány**, **KL kategória**, **Metaadatok** vagy **Mappa elérési útja**.

   A Kaspersky Endpoint Security nem támogatja az MD5 hash kódot, és MD5 hash alapján nem felügyeli az alkalmazások indítását. Szabálykiváltó feltételként SHA256 hash szolgál.

3. Ha a **Metaadatok** lehetőséget választotta a **Kritérium megjelenítése** legördülő listán, jelölje be a jelölőnégyzeteket a végrehajtható fájlok azon tulajdonságaival szemben, amelyeket a szabálykiváltó feltételben használni szeretne: **Fájlnév**, **Fájlverzió**, **Alkalmazásnév**, **Alkalmazás verziója** és **Forgalmazó**.

   Ha a megadott tulajdonságok közül egy sincs kiválasztva, a szabályt nem lehet menteni.

4. Ha a **Tanúsítvány** lehetőséget választotta a **Kritérium megjelenítése** legördülő listán, jelölje be a jelölőnégyzeteket azokkal a beállításokkal szemben, amelyeket a szabálykiváltó feltételben használni szeretne: **Kiállító**, **Adatalany** és **Ujjlenyomat**.

   Ha a megadott beállítások közül egy sincs kiválasztva, a szabályt nem lehet menteni.

   Szabálykiváltó feltételként nem javasolt csak a **Kiállító** és az **Adatalany** kritériumokat alkalmazni. E kritériumok használata megbízhatatlan.

5. Jelölje be a jelölőnégyzeteket az alkalmazás azon végrehajtható fájljainak neve mellett, amelyeknek a tulajdonságait bele szeretné venni a szabályt kiváltó feltételekbe.

6. Kattintson a **Tovább** gombra.

   Megjelenik a kialakított szabálykiváltó feltételek listája.

7. Jelölje be a kialakított szabálykiváltó feltételek listáján a jelölőnégyzeteket azokkal a szabálykiváltó feltételekkel szemben, amelyeket az Alkalmazásfelügyeleti szabályhoz hozzá szeretne adni.

8. Kattintson a **Megszakítás** gombra.

Szabálykiváltó feltétel hozzáadása KL kategória alapján:

1. Válassza ki a **Hozzáadás** gomb legördülő listáján a **„KL kategória" feltételi** lehetőséget.

   A *KL kategória* olyan alkalmazások listája, amelyeknek közösek a témaattribútumaik. A listát a Kaspersky szakértői tartják karban. Az „Irodai alkalmazások" KL kategória például a Microsoft Office csomag alkalmazásait, az Adobe® Acrobat® alkalmazást és másokat tartalmaz.

2. Az **Feltételek "KL kategória" alapján** ablakban jelölje be a jelölőnégyzeteket azon KL kategóriák mellett, amelyek alapján szabálykiváltó feltételeket szeretne létrehozni.

   Rákattinthat a KL kategória nevétől balra található unfold_key gombra a beágyazott KL kategóriák szelektív megjelöléséhez.

3. Kattintson az **OK** gombra.

Egyéni szabálykiváltó feltétel hozzáadása:

1. Válassza ki a **Hozzáadás** gomb alatti legördülő listán az **Egyedi feltétel** lehetőséget.

2. Kattintson az **Egyedi feltétel** ablakban a **Kijelölés** gombra, és adja meg az alkalmazás végrehajtható fájljának elérési útját.

3. Válassza ki azt a kritériumot, amelynek alapján szabálykiváltó feltételt szeretne létrehozni: **Fájl ellenőrzőösszeg-kódja**, **Tanúsítvány**, **Metaadatok** vagy **Fájl vagy mappa elérési útja**.

   A Kaspersky Endpoint Security nem támogatja az MD5 hash kódot, és MD5 hash alapján nem felügyeli az alkalmazások indítását. Szabálykiváltó feltételként SHA256 hash szolgál.

   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.

4. Adja meg a kiválasztott kritérium beállításait.

5. Kattintson az **OK** gombra.

Szabálykiváltó feltétel hozzáadása alkalmazás végrehajtható fájlját tároló meghajtóra vonatkozó információ alapján:

1. Válassza ki a **Hozzáadás** gomb alatti legördülő listán a **Feltétel fájlmeghajtó alapján** lehetőséget.
2. Válassza ki a **Feltétel fájlmeghajtó alapján** ablakban lévő **Meghajtó** legördülő listán annak a tárolóeszköznek a típusát, amelyen az alkalmazások indítása szabálykiváltó feltételként szolgál.
3. Kattintson az **OK** gombra.

Alkalmazásindítás-felügyelő szabály állapotának módosítása

Alkalmazásindítás-felügyelő szabály állapotának módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.
3. Az összetevő beállításainak szerkeszthetővé tételéhez válassza ki az **Alkalmazásindítás-felügyelő bekapcsolása** lehetőséget.
4. Válassza ki azt a szabályt, amelynek szerkeszteni kívánja az állapotát.
5. Az **Státusz** oszlopban végezze el az alábbiakat:
   - Ha egy szabály használatát engedélyezni szeretné, jelölje be a vele szemben lévő jelölőnégyzetet.
   - Ha egy szabály használatát le szeretné tiltani, törölje a vele szemben lévő jelölőnégyzetet.
6. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az Alkalmazásindítás-felügyelő szabályok tesztelése

Annak biztosítása érdekében, hogy az Alkalmazásindítás-felügyelő szabályok ne blokkoljanak a munkához szükséges alkalmazásokat, javasoljuk, hogy az újonnan létrehozott szabályokat állítsa tesztmódba, és elemezze működésüket.

Az Alkalmazásindítás-felügyelő szabályok működésének elemzéséhez át kell tekinteni a Kaspersky Security Center részére jelentett Alkalmazásindítás-felügyelő eseményeket. Ha a számítógép felhasználójának munkájához szükséges összes alkalmazás indulása engedélyezett, akkor a szabályok létrehozása megfelelő volt. Egyéb esetben javasoljuk, hogy tekintse át a létrehozott szabályok beállításait.

Az Alkalmazásindítás-felügyelő szabályok tesztmódja alapértelmezés szerint ki van kapcsolva.

Az Alkalmazásindítás-felügyelő szabályok tesztelése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alpontot.

Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.

3. Az összetevő beállításainak szerkeszthetővé tételéhez válassza ki az **Alkalmazásindítás-felügyelő bekapcsolása** lehetőséget.

4. Válassza ki az **Alkalmazásindítás-felügyelő működési mód** legördülő listán valamelyiket az alábbi elemek közül:

   - **Feketelista**, ha a blokkoló szabályokban megadott alkalmazások kivételével az összes alkalmazás elindítását engedélyezni szeretné.

   - **Fehérlista**, ha az engedélyező szabályokban megadott alkalmazások kivételével az összes alkalmazás blokkolását engedélyezni szeretné.

5. A **Művelet** legördülő listán válassza ki az **Értesítés** lehetőséget.

6. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Kaspersky Endpoint Security nem blokkolja azokat az alkalmazásokat, amelyeknek indítását Alkalmazásindítás-felügyelő szabályok tiltják, hanem értesítéseket küld indításukról az Adminisztrációs kiszolgáló részére.

Az Alkalmazásindítás-felügyelő üzenetsablonok szerkesztése

Ha egy felhasználó megpróbálja az Alkalmazásindítás-felügyelő 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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.

3. Az összetevő beállításainak szerkeszthetővé tételéhez válassza ki az **Alkalmazásindítás-felügyelő bekapcsolása** lehetőséget.

4. Kattintson a **Sablonok** gombra.

   Megnyílik az **Üzenetsablonok** ablak.

5. Végezze el az alábbiak egyikét:

   - Ha annak az üzenetnek a sablonját szeretné szerkeszteni, amely az alkalmazás indításának blokkolásakor jelenik meg, válassza ki a **Blokkolás** lapot.

   - Ha annak az üzenetnek a sablonját szeretné szerkeszteni, amelyet a rendszergazda kap, válassza ki a **Üzenet a rendszergazdának** lapot.

6. Módosítsa annak az üzenetnek a sablonját, amely az alkalmazás indításának blokkolásakor jelenik meg, illetve amelyet a rendszergazda kap. Ehhez használja az **Alapértelmezett** és **Változó** gombokat.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az Alkalmazásindítás-felügyelő üzemmódjai

Az Alkalmazásindítás-felügyelő összetevő két módban működhet:

- **Feketelista**. Ebben a módban az Alkalmazásindítás-felügyelő az összes felhasználó számára engedélyezi minden alkalmazás elindítását, kivéve azokét, amelyek meg vannak adva az Alkalmazásindítás-felügyelő blokkolási szabályaiban.

  Alapértelmezés szerint ez a mód van engedélyezve az Alkalmazásindítás-felügyelőben.

- **Fehérlista**. Ebben a módban az Alkalmazásindítás-felügyelő az összes felhasználó számára blokkolja minden alkalmazás elindítását, kivéve azokét, amelyek meg vannak adva az Alkalmazásindítás-felügyelő engedélyezési szabályaiban.

  Ha az Alkalmazásindítás-felügyelő 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.

Az egyes módokban két-két művelet található, amelyeket a futó alkalmazásokon el lehet végezni: a Kaspersky Endpoint Security blokkolhatja az alkalmazások indítását, illetve értesítheti a felhasználót az alkalmazás elindulásáról, ha az egyezik az Alkalmazásindítás-felügyelő szabályok feltételeivel.

Az Alkalmazásindítás-felügyelő e módokban való működése egyaránt beállítható a Kaspersky Endpoint Security helyi felületén, illetve a Kaspersky Security Center segítségével.

A Kaspersky Security Center azonban olyan eszközöket is kínál, amelyek a Kaspersky Endpoint Security helyi felületén nem találhatók meg, köztük az alábbi feladatokhoz szükséges eszközöket:

- Alkalmazáskategóriák létrehozása.

  A Kaspersky Security Center Adminisztrációs Konzolban előállított Alkalmazásindítás-felügyelő szabályok egyedi alkalmazáskategóriákon alapulnak, nem pedig szerepeltetési és kizárási feltételeken, mint a Kaspersky Endpoint Security helyi felülete esetén.

- A helyi hálózat számítógépein telepített alkalmazásokra vonatkozó információk gyűjtése.

Ezért javasoljuk az Alkalmazásindítás-felügyelő összetevő működésének beállítását a Kaspersky Security Center segítségével.

Az Alkalmazásindítás-felügyelő módjának kiválasztása

Az Alkalmazásindítás-felügyelő módjának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.

3. Az összetevő beállításainak szerkeszthetővé tételéhez válassza ki az **Alkalmazásindítás-felügyelő bekapcsolása** lehetőséget.

4. Válassza ki az **Alkalmazásindítás-felügyelő működési mód** legördülő listán valamelyiket az alábbi elemek közül:

   - **Feketelista**, ha a blokkoló szabályokban megadott alkalmazások kivételével az összes alkalmazás elindítását engedélyezni szeretné.
   - **Fehérlista**, ha az engedélyező szabályokban megadott alkalmazások kivételével az összes alkalmazás blokkolását engedélyezni szeretné.

     Ha ez a mód van kiválasztva, két Alkalmazásindítás-felügyelő-szabálya automatikusan létrejön: **Golden Image** és **Megbízható frissítéstelepítők**. Ezeket a szabályokat nem lehet törölni. E szabályok beállításai nem szerkeszthetők. A szabályokat a velük szemben lévő jelölőnégyzet bejelölésével és törlésével lehet be-, illetve kikapcsolni. 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. A szabályok használatára való visszatéréshez mindössze ki kell választani a szükséges módot az **Alkalmazásindítás-felügyelő működési mód** legördülő listán.

5. A **Művelet** legördülő listán válassza ki azt a műveletet, amelyet az összetevő akkor végez el, ha egy felhasználó megpróbál egy, az Alkalmazásindítás-felügyelő szabályok által blokkolt alkalmazást elindítani.

6. Jelölje be a **DLL és illesztőprogramok figyelése** 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.

   Ha a jelölőnégyzet be van jelölve, a DLL modulok és illesztőprogramok figyelemmel kísérésére a Kaspersky Endpoint Security indítása előtt sor kerül. A továbbiakban az összes DLL modul és illesztőprogram alkalmazásindulás előtti figyelésének beállításához indítsa újra a számítógépet, miután bejelölte a **DLL és illesztőprogramok figyelése** jelölőnégyzetet. Ha nem tudja újraindítani a számítógépet, akkor a **DLL és illesztőprogramok figyelése** jelölőnégyzet bejelölését követően betöltheti a DLL modulokat és az illesztőprogramokat, miközben a Kaspersky Endpoint Security fut. Ilyenkor a rendszer csak azokat a DLL modulokat és illesztőrpogramokat figyeli, amelyek a Kaspersky Endpoint Security futása közben töltődnek be.

   A DLL modulok és illesztőprogramok figyelése közben nem javasoljuk az olyan Alkalmazásindítás-felügyelő szabályok használatát, amelyek KL kategóriák alapján készültek. Előfordulhat, hogy a KL kategóriák (ideértve az „Operációs rendszer és összetevői” szabályokat is) megállapítása DLL modulok és illesztőprogramok esetén nem működik megfelelően. Az „Operációs rendszer és összetevői” szabály alapértelmezés szerint jön létre, és a DLL modulok és illesztőprogramok indításakor nem kerül sor terjesztésére. A funkció bekapcsolásakor különálló engedélyező szabályokat kell előállítani a DLL modulok és az illesztőprogramok számára. Ha nem léteznek ilyen engedélyező szabályok, a **DLL és illesztőprogramok felügyelete** funkció használatától a rendszer instabillá válhat.

   Javasoljuk, hogy a programbeállítások megadásánál kapcsolja be a jelszavas védelmet, hogy ki lehessen kapcsolni a létfontosságú DLL modulok és illesztőprogramok indítását blokkoló engedélyező szabályokat, miközben a Kaspersky Security Center rendszabály beállításai változatlanok maradnak.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az Alkalmazásindítás-felügyelő szabályok kezelése a Kaspersky Security Center segítségével

Ez a rész ismerteti az Alkalmazásindítás-felügyelő szabályok Kaspersky Security Center segítségével történő beállítását, és javaslatokkal szolgál az Alkalmazásindítás-felügyelő optimális használata tekintetében.

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 **Alkalmazások jegyzéke** mappában és a **Végrehajtható fájlok** mappában találhatók. 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 **Alkalmazások jegyzéke** mappában vagy a **Végrehajtható fájlok** mappában kiválasztott alkalmazás tulajdonságainak ablakát.

*A tulajdonságok ablak megnyitásához az alkalmazások számára az **Alkalmazások jegyzéke** mappában:*

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában a **További** → **Alkalmazáskezelés** → **Alkalmazások jegyzéke** mappát.
3. Válasszon ki egy alkalmazást.
4. Az alkalmazás helyi menüjében válassza ki a **Tulajdonságok** elemet.

   Megnyílik a **Tulajdonságok: <Alkalmazás neve>** ablak.

*A tulajdonságok ablak megnyitásához a végrehajtható fájlok számára a **Végrehajtható fájlok** mappában:*

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Válassza ki az Adminisztrációs Konzol fájában a **További** → **Alkalmazáskezelés** → **Végrehajtható fájlok** mappát.
3. Válasszon ki egy végrehajtható fájlt.
4. A végrehajtható fájl helyi menüjében válassza ki a **Tulajdonságok** elemet.

   Megnyílik a **Tulajdonságok: <Végrehajtható fájl neve>** ablak.

Alkalmazáskategóriák létrehozása

A szabályok létrehozásának nagyobb kényelme érdekében az alkalmazások számára kategóriákat készíthet, melyeket az Alkalmazásindítás-felügyelő szabályok létrehozása során használhat.

Javasoljuk, hogy hozzon létre egy „Munkaalkalmazások" kategóriát, melybe a vállalatnál használt alkalmazások szokásos készletét helyezze. Ha a különböző felhasználói csoportok munkájuk során más-más alkalmazáskészleteket használnak, akkor az egyes csoportok számára külön alkalmazáskategóriákat hozhat létre.

Alkalmazáskategória létrehozása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki az Adminisztrációs Konzol fájában a **További** → **Alkalmazáskezelés** → **Alkalmazáskategóriák** mappát.
3. Kattintson a munkaterületen a **Kategória létrehozása** gombra.

   Elindul a Felhasználói kategóriakészítő varázsló.
4. Kövesse a Felhasználói kategóriakészítő varázsló utasításait.

Alkalmazásindítás-felügyelő szabályok létrehozása a Kaspersky Security Center segítségével

Alkalmazásindítás-felügyelő szabály létrehozása a Kaspersky Security Center segítségével:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
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.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. A **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alrészt.

   Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.

7. Kattintson a **Hozzáadás** gombra.

   Megnyílik az **Alkalmazásindítás-felügyelő szabály** ablak.

8. Válassza ki a **Kategória** legördülő listán azt a létrehozott alkalmazáskategóriát, amelynek alapján szabályt szeretne létrehozni.

9. Adja meg azon felhasználók és / vagy felhasználói csoportok listáját, akiknél be szeretné állítani a kiválasztott kategóriába tartozó alkalmazások indítási jogosultságát. Ehhez kattintson az **Fő felhasználók és jogaik** táblázatban a **Hozzáadás** gombra.

   Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanel a Microsoft Windowsban. Ebben az ablakban felhasználókat és / vagy felhasználói csoportokat választhat ki.

10. Az **Fő felhasználók és jogaik** táblázatban:

    - Ha engedélyezni szeretné, hogy a kiválasztott kategóriába tartozó alkalmazásokat a felhasználók és / vagy felhasználói csoportok elindíthassák, jelölje be az adott felhasználókkal szemben lévő **Engedélyezés** jelölőnégyzeteket.

    - Ha blokkolni szeretné, hogy a kiválasztott kategóriába tartozó alkalmazásokat a felhasználók és / vagy felhasználói csoportok elindíthassák, jelölje be az adott felhasználókkal szemben lévő **Blokkolás** jelölőnégyzeteket.

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 az **Fő felhasználó** oszlopban, és nem is tartozik az **Fő felhasználó** oszlopban megadott felhasználói csoportok valamelyikébe.

12. Ha azt szeretné, hogy a Kaspersky Endpoint Security a szabályban megadott kategóriába tartozó alkalmazásokat olyan megbízható frissítőknek tekintse, amelyek más alkalmazásokat elindíthatnak, és amelyekhez nincsenek megadva Alkalmazásindítás-felügyelő szabályok, jelölje be a **Megbízható frissítéstelepítők** jelölőnégyzetet.

13. Kattintson az **OK** gombra.

14. A rendszabály tulajdonságai ablakának **Alkalmazásindítás-felügyelő** részében kattintson az **Alkalmaz** gombra.

Alkalmazásindítás-felügyelő szabály állapotának módosítása a Kaspersky Security Center segítségével

Alkalmazásindítás-felügyelő szabály állapotának módosítása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

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.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. A **Végpontfelügyelő** részben válassza ki az **Alkalmazásindítás-felügyelő** alrészt.

   Az ablak jobb oldali részén megjelennek az Alkalmazásindítás-felügyelő összetevő beállításai.

7. Válassza ki azt az Alkalmazásindítás-felügyelő szabályt, amelynek módosítani szeretné az állapotát.

8. Az **Státusz** oszlopban végezze el az alábbiak egyikét:

   - Ha egy szabály használatát engedélyezni szeretné, jelölje be a vele szemben lévő jelölőnégyzetet.
   - Ha egy szabály használatát le szeretné tiltani, törölje a vele szemben lévő jelölőnégyzetet.

9. Kattintson az **Alkalmaz** gombra.

Alkalmazásjogosultság-felügyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt az Alkalmazásjogosultság-felügyelővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

Az Alkalmazásjogosultság-felügyelő

Az Alkalmazásjogosultság-felügyelő megelőzi, hogy az alkalmazások az operációs rendszerre esetleg veszélyes műveletbe kezdjenek, így felügyelve a hozzáférést az operációs rendszer erőforrásaihoz és a személyazonosításra alkalmas adatokhoz.

Ez az összetevő *alkalmazásfelügyeleti szabályok* révén szabályozza az alkalmazások tevékenységét, így a védett erőforrásokhoz (fájlokhoz, mappákhoz, beállításkulcsokhoz) való hozzáférését. Az alkalmazásfelügyeleti szabályok olyan korlátozáskészletek, amelyek az operációs rendszeren lévő alkalmazások különböző műveleteire és a számítógép erőforrásaihoz való hozzáférési jogosultságokra vonatkoznak.

Az alkalmazások hálózati tevékenységét a Tűzfal összetevő kíséri figyelemmel.

Egy alkalmazás első elindulásakor az Alkalmazásjogosultság-felügyelő megvizsgálja az alkalmazást, és besorolja egy megbízhatósági csoportba. A megbízhatósági csoport határozza meg azokat az alkalmazásfelügyeleti szabályokat, amelyeket a Kaspersky Endpoint Security az alkalmazás tevékenységének felügyeletére alkalmaz.

Javasoljuk, hogy vegyen részt a Kaspersky Security Network, hogy az Alkalmazásjogosultság-felügyelő még eredményesebben működjön. A Kaspersky Security Network kapott adatok lehetővé teszik az alkalmazásoknak a különböző csoportokba való pontosabb besorolását, valamint az alkalmazásfelügyeleti szabályok optimalizálását.

Az alkalmazás következő indításakor az Alkalmazásjogosultság-felügyelő ellenőrzi integritását. Amennyiben az alkalmazás nem változott meg, az összetevő alkalmazza rá a meglevő alkalmazásfelügyeleti szabályt. Ha az alkalmazás módosult, az Alkalmazásjogosultság-felügyelő újra átvizsgálja, mint az első elindulásnál.

A hang- és videó eszközfelügyelő korlátozásai

A hang-adatfolyam védelme

A hang-adatfolyam védelmére az alábbi különleges szempontok vonatkoznak:

- A funkció működéséhez engedélyezve kell lennie a Behatolásmegelőző rendszer összetevőnek.
- Ha az alkalmazás a Behatolásmegelőző rendszer összetevő indítása előtt elkezdett hang-adatfolyamot fogadni, a Kaspersky Endpoint Security lehetővé teszi, hogy az alkalmazás fogadja a hang-adatfolyamot, és nem jelenít meg értesítést.

- Ha az alkalmazás az hang-adatfolyamot fogadását követően a **Nem megbízható** vagy a **Magas korlátozás** csoportba került, a Kaspersky Endpoint Security lehetővé teszi, hogy az alkalmazás fogadja a hang-adatfolyamot, és nem jelenít meg értesítést.

- Az alkalmazás hangrögzítő eszközhöz való hozzáférési beállításainak módosítását követően (például a Behatolásmegelőző rendszer ablakban a felhasználó blokkolta az adatfolyam fogadását az alkalmazás által) az alkalmazást újra kell indítani, hogy többé ne fogadja a hang-adatfolyamot.

- A hangrögzítő eszközök hang-adatfolyamához való hozzáférésének felügyelete nem függ az alkalmazás webkamerához való hozzáférési 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.

Hang- és videoeszközök működésének különleges szempontjai a Kaspersky Endpoint Security telepítése és frissítése során

Amikor a Kaspersky Endpoint Security telepítése után először hang- vagy videórögzítő, illetve -lejátszó alkalmazásokat futtat, előfordulhat, hogy a hang- vagy videórögzítés, 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.

Az alkalmazások webkamerákhoz való hozzáférése

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 **képalkotó eszközként** jelennek meg a Windows Eszközkezelőben.

Támogatott webkamerák

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.

A Behatolásmegelőző rendszer be- és kikapcsolása

A Behatolásmegelőző rendszer összetevő alapértelmezés szerint be van kapcsolva, és a Kaspersky szakértői által javasolt módban működik. Szükség esetén letilthatja a Behatolásmegelőző rendszer összetevőt.

A Behatolásmegelőző rendszer összetevő be- és kikapcsolása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Fejlett fenyegetések elleni védelem** részében válassza ki a **Behatolásmegelőző rendszer** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Behatolásmegelőző rendszer összetevő beállításai.
3. Az ablak jobb oldali részén tegye az alábbiak egyikét:
   - Jelölje be a **Behatolásmegelőző rendszer** jelölőnégyzetet, ha be szeretné kapcsolni a Behatolásmegelőző rendszer összetevőt.
   - Törölje a **Behatolásmegelőző rendszer** jelölőnégyzetet, ha ki szeretné kapcsolni a Behatolásmegelőző rendszer összetevőt.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az alkalmazások megbízhatósági csoportjainak kezelése

Az egyes alkalmazások első elindulásakor az Alkalmazásjogosultság-felügyelő 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 ezzel egy időben 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 indításakor a Kaspersky Endpoint Security minden alkalommal újabb lekérdezést küld a KSN adatbázis részére, és ha az alkalmazás reputációja megváltozott a KSN adatbázisaiban, 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 indított alkalmazások automatikusan bekerülnek a **Megbízhatósági csoport kiválasztása** ablakban megadott megbízhatósági csoportba.

Az összetevő kizárólag a Kaspersky Endpoint Security előtt indított alkalmazások hálózati tevékenységét kíséri figyelemmel a Tűzfal beállításaiban megadott hálózati szabályok alapján.

Az alkalmazások megbízhatósági csoportokba való beosztási beállításainak megadása

Ha be van kapcsolva a részvétel a Kaspersky Security Network, a Kaspersky Endpoint Security a KSN részére minden alkalommal lekérdezést küld az alkalmazások reputációjára vonatkozóan, amikor sor kerül elindításukra. A KSN-től érkező válasz alapján az alkalmazás az Alkalmazásjogosultság-felügyelő beállításaiban megadottól eltérő megbízhatósági csoportba kerülhet.

Az alkalmazások megbízhatósági csoportokba való elhelyezési beállításainak megadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Ha a megbízható gyártóktól származó és digitális aláírással rendelkező alkalmazásokat automatikusan a Megbízható csoportba szeretné helyezni, jelölje be a **A digitális aláírással rendelkező alkalmazások kezelése megbízhatóként** jelölőnégyzetet.

   A *megbízható gyártók* olyan szoftvergyártók, amelyeket a Kaspersky megbízható csoportba helyezett. A gyártói tanúsítványt manuálisan is hozzáadhatja a megbízható rendszertanúsítvány-tárolóhoz.
4. Válassza ki, hogyan történjen az ismeretlen alkalmazások megbízhatósági csoportokba való beosztása:

   - Ha az ismeretlen alkalmazásokat heurisztikus elemzés segítségével szeretné megbízhatósági csoportokba beosztani, jelölje be a **Heurisztikus elemzés használata csoport meghatározásához** jelölőnégyzetet, és adja meg az elindított alkalmazások vizsgálatára engedélyezett időtartamot a **Maximális idő a csoport meghatározására** mezőben.
   - Ha az összes ismeretlen alkalmazást egy adott megbízhatósági csoportba szeretné helyezni, válassza az **Automatikus áthelyezés a következő csoportba** lehetőséget, és válassza ki a megfelelő megbízhatósági csoportot a legördülő listán.

     Biztonsági okokból a **Megbízható** csoport nem szerepel az **Automatikus áthelyezés a következő csoportba** beállítás értékei között.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

Megbízhatósági csoport módosítása

Egy alkalmazás első elindulásakor a Kaspersky Endpoint Security az alkalmazást automatikusan besorolja egy megbízhatósági csoportba. Szükség esetén az alkalmazást kézileg egy másik csoportba helyezheti.

A Kaspersky szakemberei nem javasolják az alkalmazások áthelyezését az automatikusan kiosztott megbízhatósági csoportból másik megbízhatósági csoportba. Ehelyett módosíthatja az egyes alkalmazások jogait, ha szükséges.

Annak a megbízhatósági csoportnak a megváltoztatása, amelybe az alkalmazást a Kaspersky Endpoint Security első indításakor automatikusan beosztotta:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalának **Fejlett fenyegetések elleni védelem** részében válassza ki a **Behatolásmegelőző rendszer** lehetőséget.

   Az ablak jobb oldali részén megjelennek a Behatolásmegelőző rendszer összetevő beállításai.
3. Kattintson az **Alkalmazások** gombra.

   Ezzel megnyílik az **Alkalmazásjogok** ablak **Behatolásmegelőző rendszer** lapja.
4. Válassza ki az **Alkalmazásjogok** lapon a kért alkalmazást.
5. Végezze el az alábbiak egyikét:

   - Kattintson a jobb egérgombbal az alkalmazás helyi menüjének megjelenítéséhez. Az alkalmazás helyi menüjében válassza ki az **Áthelyezés csoportba** → **<csoport neve>** elemet.
   - A helyi menü megnyitásához kattintson a **Megbízható** / **Alacsony korlátozás** / **Magas korlátozás** / **Nem megbízható** hivatkozásra. A helyi menüben válassza ki a kívánt megbízhatósági csoportot.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Kaspersky Endpoint Security előtt indított alkalmazások megbízhatósági csoportjának kiválasztása

Az összetevő kizárólag a Kaspersky Endpoint Security előtt indított alkalmazások hálózati tevékenységét kíséri figyelemmel. A felügyelet a Tűzfal beállításaiban megadott hálózati szabályoknak megfelelően történik. Annak megadásához, hogy az ilyen alkalmazások hálózati tevékenységei figyelésénél melyik hálózati szabályokat kell alkalmazni, ki kell választani egy megbízhatósági csoportot.

A Kaspersky Endpoint Security előtt indított alkalmazások megbízhatósági csoportjának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Kattintson a **Szerkesztés** gombra.

   Ezzel megnyílik a **Megbízhatósági csoport kiválasztása** ablak.
4. Válassza ki a szükséges megbízhatósági csoportot.
5. Kattintson az **OK** gombra.
6. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az Alkalmazásfelügyelő szabályainak kezelése

Alapértelmezés szerint az adott alkalmazás tevékenységeinek felügyelete azon megbízhatósági csoport számára meghatározott alkalmazásfelügyeleti szabályok alapján történik, amelybe a Kaspersky Endpoint Security az alkalmazást annak első futásakor besorolta. Szükség esetén az alkalmazásfelügyeleti szabályokat a teljes megbízhatósági csoport szintjén, egyes alkalmazásonként, illetve a megbízhatósági csoportban található alkalmazások csoportjára nézve szerkesztheti.

A megbízhatósági csoporton belüli egyes alkalmazásokra vagy alkalmazáscsoportokra meghatározott alkalmazásfelügyeleti szabályoknak magasabb a prioritásuk, mint a megbízhatósági csoport szintjén meghatározott alkalmazásfelügyeleti szabályoknak. Ez annyit jelent, hogy ha a megbízhatósági csoporton belüli egyes alkalmazásokra vagy alkalmazáscsoportokra meghatározott alkalmazásfelügyeleti szabályok beállításai eltérnek a megbízhatósági csoport alkalmazásfelügyeleti szabályainak beállításaitól, akkor az Alkalmazásjogosultság-felügyelő összetevő a megbízhatósági csoporton belüli egyes alkalmazások, illetve alkalmazáscsoportok tevékenységét az adott alkalmazásokra vagy alkalmazáscsoportokra meghatározott alkalmazásfelügyeleti szabályok szerint felügyeli.

A megbízhatósági csoportok és alkalmazáscsoportok alkalmazásfelügyeleti szabályainak módosítása

A különböző megbízhatósági csoportok optimális alkalmazásfelügyeleti szabályai alapértelmezés szerint létrejönnek. Az alkalmazáscsoport felügyeleti szabályainak beállításai öröklik az értékeket a megbízhatósági csoport felügyeleti szabályainak beállításaitól. A megbízhatósági csoport előre beállított felügyeleti szabályai és az alkalmazáscsoport felügyeleti szabályai szerkeszthetők.

A megbízhatósági csoport előre beállított felügyeleti szabályainak és az alkalmazáscsoport felügyeleti szabályainak szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Kattintson az **Alkalmazások** gombra.

   Ezzel megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Alkalmazásfelügyeleti szabályok** lapja.
4. Válassza ki a szükséges megbízhatósági csoportot vagy alkalmazáscsoportot.
5. Válassza ki valamelyik megbízhatósági csoport vagy alkalmazáscsoport helyi menüjében a **Csoportszabályok** elemet.

   Megnyílik az **Alkalmazáscsoport felügyeleti szabályai** ablak.
6. Az **Alkalmazáscsoport felügyeleti szabályai** ablakban tegye az alábbiak egyikét:

   - A megbízhatósági csoport, illetve alkalmazáscsoport operációs rendszer beállításjegyzékének, a felhasználói fájloknak és az alkalmazásbeállításoknak a hozzáférési jogosultságait megszabó felügyeleti szabályok szerkesztéséhez válassza ki a **Fájlok és beállításjegyzék** lapot.
   - A megbízhatósági csoport, illetve alkalmazáscsoport operációs rendszer folyamatainak és objektumainak a hozzáférési jogosultságait megszabó felügyeleti szabályok szerkesztéséhez válassza ki a **Jogok** lapot.

7. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában.

8. A helyi menüből válassza ki a kívánt elemet.

   - **Öröklés**
   - **Engedélyezés**
   - **Blokkolás**
   - **Események naplózása**

   A megbízhatósági csoportok felügyeleti szabályainak szerkesztése esetén az **Öröklés** elem nem áll rendelkezésre.

9. Kattintson az **OK** gombra.

10. Az **Alkalmazások** ablakban kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Mentés** gombra.

Alkalmazásfelügyeleti szabály szerkesztése

Az alkalmazáscsoporthoz vagy megbízhatósági csoporthoz tartozó alkalmazások alkalmazásfelügyeleti szabályainak beállításai alapértelmezés szerint öröklik a megbízhatósági csoport felügyeleti szabályainak beállításait. Az alkalmazásfelügyeleti szabályok beállításait szerkesztheti.

Alkalmazásfelügyeleti szabály módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.

3. Kattintson az **Alkalmazások** gombra.
   Ezzel megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Alkalmazásfelügyeleti szabályok** lapja.

4. Válassza ki a szükséges alkalmazást.

5. Végezze el az alábbiak egyikét:

   - Az alkalmazás helyi menüjében válassza ki az **Alkalmazásszabályok** elemet.
   - Kattintson a **További** gombra az **Alkalmazásfelügyeleti szabályok** lap jobb alsó sarkában.

   Megnyílik az **Alkalmazásfelügyeleti szabályok** ablak.

6. Az **Alkalmazásfelügyeleti szabályok** ablakban tegye az alábbiak egyikét:

- Az alkalmazás operációs rendszer beállításjegyzékének, a felhasználói fájloknak és az alkalmazásbeállításoknak a hozzáférési jogosultságait megszabó felügyeleti szabályok szerkesztéséhez válassza ki a **Fájlok és beállításjegyzék** lapot.

- Az alkalmazás operációs rendszer folyamatainak és objektumainak a hozzáférési jogosultságait megszabó felügyeleti szabályok szerkesztéséhez válassza ki a **Jogok** lapot.

7. A helyi menü megnyitásához kattintson a jobb egérgombbal a kívánt erőforrásnak megfelelő művelet oszlopában.

8. A helyi menüből válassza ki a kívánt elemet.

   - **Öröklés**

   - **Engedélyezés**

   - **Blokkolás**

   - **Események naplózása**

9. Kattintson az **OK** gombra.

10. Az **Alkalmazások** ablakban kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az alkalmazásfelügyeleti szabályok Kaspersky Security Network történő letöltéseinek és frissítéseinek kikapcsolása

Ha a Kaspersky Security Network egy alkalmazásról új információk észlelhetők, akkor a Kaspersky Endpoint Security alapértelmezés szerint a KSN adatbázisból letöltött felügyeleti szabályokat alkalmazza az adott alkalmazásra. Ezután kézileg szerkesztheti az alkalmazáshoz tartozó felügyeleti szabályokat.

Ha egy alkalmazás az első elindításkor a Kaspersky Security Network adatbázisában még nem volt megtalálható, de az adatai később bekerültek, a Kaspersky Endpoint Security alapértelmezés szerint automatikusan frissíti az alkalmazásra vonatkozó felügyeleti szabályokat.

A Kaspersky Security Network alkalmazásfelügyeleti szabályainak letöltése és a korábban ismeretlen alkalmazásra vonatkozó felügyeleti szabályok automatikus frissítése kikapcsolható.

Az alkalmazásfelügyeleti szabályok Kaspersky Security Network történő letöltéseinek és frissítéseinek kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.

3. Törölje a **Felügyeleti szabályok frissítése a korábban ismeretlen alkalmazásokhoz a KSN adatbázisokból** jelölőnégyzetet.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A szülő folyamat korlátozásai öröklésének kikapcsolása

Alkalmazásindítást a felhasználó vagy egy másik futó alkalmazás kezdeményezhet. Ha az alkalmazásindítást egy másik alkalmazás kezdeményezi, indítási sorozat jön létre, amely szülő- és gyerekfolyamatokból áll.

Ha egy alkalmazás védett erőforráshoz próbál hozzáférni, az Alkalmazásjogosultság-felügyelő elemzi az alkalmazás összes szülőfolyamatát, és megállapítja, hogy van-e hozzáférési jogosultságuk a védett erőforráshoz. Ekkor alkalmazásra kerül a legalacsonyabb prioritás szabálya: az alkalmazás hozzáférési jogának a szülőfolyamatok hozzáférési jogával való összehasonlításakor a rendszer a legalacsonyabb prioritást alkalmazza az alkalmazás tevékenységére.

A hozzáférési jogok prioritása az alábbiak szerint alakul:

1. **Engedélyezés** A hozzáférési jog a legmagasabb prioritású.
2. **Blokkolás** A hozzáférési jog a legalacsonyabb prioritású.

Ez a mechanizmus megakadályozza, hogy nem megbízható alkalmazás vagy korlátozott jogokkal rendelkező alkalmazás megbízható alkalmazást használjon, és így adott jogosultságokat igénylő műveleteket végezzen.

Ha egy alkalmazás tevékenysége a szülőfolyamat elégtelen jogai miatt blokkolásra kerül, szerkesztheti ezeket a szabályokat, vagy kikapcsolhatja a szülőfolyamat korlátozásainak öröklését.

A szülőfolyamat korlátozásai öröklésének kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Kattintson az **Alkalmazások** gombra.
   Ezzel megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Alkalmazásfelügyeleti szabályok** lapja.
4. Válassza ki a szükséges alkalmazást.
5. Az alkalmazás helyi menüjében válassza ki az **Alkalmazásszabályok** elemet.
   Megnyílik az **Alkalmazásfelügyeleti szabályok** ablak.
6. Az **Alkalmazásfelügyeleti szabályok** ablakban válassza ki a **Kizárások** lapot.
7. Jelölje be a **Ne örökölje a szülőfolyamat (alkalmazás) korlátozásait** jelölőnégyzetet.
8. Kattintson az **OK** gombra.
9. Az **Alkalmazások** ablakban kattintson az **OK** gombra.
10. A módosítások mentéséhez kattintson a **Mentés** gombra.

Adott alkalmazásműveletek kizárása alkalmazásfelügyeleti szabályokból

Adott alkalmazásműveletek kizárása alkalmazásfelügyeleti szabályokból:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Kattintson az **Alkalmazások** gombra.
   Ezzel megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Alkalmazásfelügyeleti szabályok** lapja.
4. Válassza ki a szükséges alkalmazást.
5. Az alkalmazás helyi menüjében válassza ki az **Alkalmazásszabályok** elemet.
   Megnyílik az **Alkalmazásfelügyeleti szabályok** ablak.
6. Válassza ki a **Kizárások** lapot.
7. Jelölje be azon alkalmazásműveletek mellett a jelölőnégyzeteket, amelyeket nem szükséges figyelemmel kísérni.
8. Kattintson az **OK** gombra.
9. Az **Alkalmazások** ablakban kattintson az **OK** gombra.
10. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az elavult alkalmazásfelügyeleti szabályok eltávolítása

Alapértelmezés szerint a 60 napja nem használt alkalmazásokra vonatkozó felügyeleti szabályok automatikusan törlődnek. A nem használt alkalmazásokra vonatkozó felügyeleti szabályok megőrzésének ideje módosítható, és a szabályok automatikus törlése is kikapcsolható.

Az elavult alkalmazásfelügyeleti szabályok eltávolítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Ha azt szeretné, hogy a Kaspersky Endpoint Security törölje a nem használt alkalmazások felügyeleti szabályait, jelölje be a **Azon alkalmazások szabályainak törlése, amelyek már nennyi ideje inaktívak** jelölőnégyzetet, és adja meg a napok számát.
   - A nem használt alkalmazások felügyeleti szabályai automatikus törlésének kikapcsolásához törölje a **Azon alkalmazások szabályainak törlése, amelyek már nennyi ideje inaktívak** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Operációs rendszer erőforrások és azonosító adatok védelme

A Behatolásmegelőző rendszer összetevő kezeli az alkalmazások jogosultságát az operációs rendszer különböző kategóriákba sorolt erőforrásain és a személyes adatokon végzett műveletekre.

A Kaspersky szakemberei előre kialakított kategóriákba sorolták a védett erőforrásokat. A védett erőforrások előre kialakított kategóriái és az alapértelmezés szerint ezekbe a kategóriákba tartozó erőforrások nem szerkeszthetők és nem törölhetők.

A következő műveleteket végezheti el:

- Védett erőforrások új kategóriájának megadása.
- Új védett erőforrás hozzáadása.
- Egy erőforrás védelmének kikapcsolása.

Védett erőforrások kategóriájának megadása

Védett erőforrások új kategóriájának megadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Kattintson az **Erőforrások** gombra.

   Erre megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Védett erőforrások** lapja.
4. A **Védett erőforrások** lap bal oldali részén válassza ki a védett erőforrások azon részét vagy kategóriáját, amelyhez a védett erőforrások új kategóriáját hozzá szeretné adni.
5. Kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki a **Kategória** lehetőséget.

   Megnyílik a **Védett erőforrások kategóriája** ablak.
6. A megnyíló **Védett erőforrások kategóriája** ablakban adja meg a védett erőforrások új kategóriájának nevét.
7. Kattintson az **OK** gombra.

   Megjelenik egy új elem a védett erőforrások kategóriáinak listáján.
8. Az **Alkalmazásjogosultság-felügyelő** ablakban kattintson az **OK** gombra.
9. A módosítások mentéséhez kattintson a **Mentés** gombra.

Miután megadta a védett erőforrások kategóriáját, szerkesztheti vagy eltávolíthatja, ha a **Védett erőforrások** lap bal felső részén lévő **Szerkesztés** vagy **Eltávolítás** gombra kattint.

Védett erőforrás hozzáadása

Védett erőforrás hozzáadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.
3. Kattintson az **Erőforrások** gombra.

   Erre megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Védett erőforrások** lapja.
4. A **Védett erőforrások** lap bal oldali részén válassza ki a védett erőforrások azon kategóriáját, amelyhez az új védett erőforrást hozzá szeretné adni.
5. Kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki a megadni kívánt erőforrás típusát:

   - **Fájl vagy mappa**.
   - **Beállításkulcs**.

   Megnyílik a **Védett erőforrás** ablak.
6. A **Védett erőforrás** ablakban írja be a védett erőforrás nevét a **Név** mezőbe.
7. Kattintson az **Tallózás...** gombra.
8. Adja meg a megnyíló ablakban a szükséges beállításokat a megadni kívánt védett erőforrás típusától függően. Kattintson az **OK** gombra.
9. A **Védett erőforrás** ablakban kattintson az **OK** gombra.

   Megjelenik egy új elem a kiválasztott kategóriába tartozó védett erőforrások listáján a **Védett erőforrások** lapon.
10. Az **Alkalmazásjogosultság-felügyelő** ablakban kattintson az **OK** gombra.
11. A módosítások mentéséhez kattintson a **Mentés** gombra.

Miután megadta a védett erőforrást, szerkesztheti vagy eltávolíthatja, ha a **Védett erőforrások** lap bal felső részén lévő **Szerkesztés** vagy **Eltávolítás** gombra kattint.

Erőforrás védelmének letiltása

Erőforrás védelmének kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Alkalmazásjogosultság-felügyelő** alpontot.

Az ablak jobb oldali részén megjelennek az Alkalmazásjogosultság-felügyelő összetevő beállításai.

3. Az ablak jobb oldali részén kattintson az **Erőforrások** gombra.

   Erre megnyílik az **Alkalmazásjogosultság-felügyelő** ablak **Védett erőforrások** lapja.

4. Végezze el az alábbiak egyikét:

   - Válassza ki a lap bal oldali részén a védett erőforrások listáján azt az erőforrást, amelynek a védelmét ki szeretné kapcsolni, és törölje a neve melletti jelölőnégyzetet.

   - Kattintson a **Kizárások** lehetőségre, és végezze el az alábbiakat:

     a. A **Kizárások** ablakban kattintson a **Hozzáadás** gombra. Válassza ki a legördülő listán azt az erőforrástípust, amelyet az Alkalmazásjogosultság-felügyelő általi védelemből való kizárások listájára fel szeretne venni: **Fájl vagy mappa**, illetve **Beállításkulcs**.

     Megnyílik a **Védett erőforrás** ablak.

     b. A **Védett erőforrás** ablakban írja be a védett erőforrás nevét a **Név** mezőbe.

     c. Kattintson az **Tallózás...** gombra.

     d. Adja meg a megnyíló ablakban a szükséges beállításokat az Alkalmazásjogosultság-felügyelő általi védelemből való kizárások listájára felvenni kívánt védett erőforrás típusától függően.

     e. Kattintson az **OK** gombra.

     f. A **Védett erőforrás** ablakban kattintson az **OK** gombra.

     Az Alkalmazásjogosultság-felügyelő általi védelemből való kizárások listáján megjelenik egy új elem.

     > Miután az Alkalmazásjogosultság-felügyelő általi védelemből való kizárások listájára felvette az erőforrást, szerkesztheti vagy eltávolíthatja, ha a **Kizárások** ablak felső részén lévő **Szerkesztés** vagy **Eltávolítás** gombra kattint.

     g. A **Kizárások** ablakban kattintson az **OK** gombra.

5. Az **Alkalmazásjogosultság-felügyelő** ablakban kattintson az **OK** gombra.

6. A módosítások mentéséhez kattintson a **Mentés** gombra.

Sebezhetőség-figyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt a Sebezhetőség-figyelővel kapcsolatban, és ismerteti az összetevő be- és kikapcsolásának menetét.

A Sebezhetőség-figyelő

A Sebezhetőség-figyelő összetevő valós időben vizsgálja a felhasználó számítógépén elindított és futó alkalmazásokban a sebezhetőségeket. Ha a Sebezhetőség-figyelő összetevő be van kapcsolva, nem szükséges a Sebezhetőségi vizsgálati feladatot elindítani. Ez a vizsgálat akkor releváns, ha egyáltalán nem vagy csak régen került sor a felhasználó számítógépén lévő alkalmazások Sebezhetőségi vizsgálati feladatára.

A Sebezhetőség-figyelő be- és kikapcsolása

A Sebezhetőség-figyelő összetevő alapértelmezés szerint le van tiltva. A Sebezhetőség-figyelőt engedélyezheti, ha szükséges.

Az összetevő kétféle módon engedélyezhető és tiltható le:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

A Sebezhetőség-figyelő be- és kikapcsolása a Védelem és felügyelet lapon a fő alkalmazásablakban:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Végpontfelügyelő** részre.
   Megnyílik a **Végpontfelügyelő** rész.
4. Kattintson a jobb egérgombbal a helyi menü megjelenítéséhez a Sebezhetőség-figyelő összetevőre vonatkozó adatokat tartalmazó sorban.
   Megnyílik az összetevő műveleteinek kiválasztására szolgáló menü.
5. Végezze el az alábbiak egyikét:
   - A Sebezhetőség-figyelő bekapcsolásához válassza ki az **Indítás** lehetőséget.
     Az összetevő állapotikonja , mely a **Sebezhetőség-figyelő** sorában a bal oldalon látható, átvált ikonra.
   - A Sebezhetőség-figyelő kikapcsolásához válassza ki a **Leállítás** lehetőséget.
     Az összetevő állapotikonja , mely a **Sebezhetőség-figyelő** sorában a bal oldalon látható, átvált ikonra.

A Sebezhetőség-figyelő be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Sebezhetőség-figyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Sebezhetőség-figyelő összetevő beállításai.
3. Az ablak jobb oldali részén tegye az alábbiak egyikét:

   - Ha azt szeretné, hogy a Kaspersky Endpoint Security sebezhetőségi vizsgálatot indítson a felhasználó számítógépén futó és a felhasználó által elindított alkalmazásokon, jelölje be a **Sebezhetőség-figyelő engedélyezése** jelölőnégyzetet.
   - Ha nem szeretné, hogy a Kaspersky Endpoint Security sebezhetőségi vizsgálatot indítson a felhasználó számítógépén futó és a felhasználó által elindított alkalmazásokon, törölje a **Sebezhetőség-figyelő engedélyezése** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Eszközfelügyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt az Eszközfelügyelővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

Az Eszközfelügyelő

Az Eszközfelügyelő a bizalmas adatok biztonságáról úgy gondoskodik, hogy korlátozza a felhasználók hozzáférését a számítógépen telepített vagy ahhoz csatlakoztatott eszközökhöz, ideértve az alábbiakat:

- Adattároló eszközök (merevlemezek, cserélhető meghajtók, szalagos meghajtók és CD-/DVD-meghajtók)
- Adatátviteli eszközök (modemek, külső hálózati kártyák)
- Adatokból papíralapú példányt előállító eszközök (nyomtatók)
- Csatlakozási buszok (vagy egyszerűen „buszok”), amelyek az eszközök számítógépekhez való csatlakoztatására szolgáló felületeket jelentenek (például USB-t, FireWire-t és infravörös portot)

Az Eszközfelügyelő a felhasználók eszközökhöz való hozzáférését *eszközhozzáférési szabályok* (más néven „hozzáférési szabályok”) és *csatlakozóbusz-hozzáférési szabályok* (más néven buszhozzáférési szabályok) révén kezeli.

Az Eszközfelügyelő be- és kikapcsolása

Alapértelmezés szerint az Eszközfelügyelő engedélyezve van. Az Eszközfelügyelőt szükség esetén letilthatja.

Az összetevő kétféle módon engedélyezhető és tiltható le:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

*Az Eszközfelügyelő be- és kikapcsolása a **Védelem és felügyelet** lapon a fő alkalmazásablakban:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Végpontfelügyelő** részre.

   Megnyílik a **Végpontfelügyelő** rész.
4. Kattintson a jobb egérgombbal a helyi menü megnyitásához az Eszközfelügyelő összetevőre vonatkozó adatokat tartalmazó sorban.

   Megnyílik az összetevő műveleteinek kiválasztására szolgáló menü.

5. Végezze el az alábbiak egyikét:

   - Az Eszközfelügyelő bekapcsolásához válassza ki a menüben az **Indítás** lehetőséget.
   - Az Eszközfelügyelő kikapcsolásához válassza ki a menüben a **Leállítás** lehetőséget.

Az Eszközfelügyelő be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.
3. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni az Eszközfelügyelőt, jelölje be az **Eszközfelügyelő bekapcsolása** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni az Eszközfelügyelőt, törölje az **Eszközfelügyelő bekapcsolása** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az eszközök és csatlakozóbuszok hozzáférési szabályai

Az eszközhozzáférési szabály olyan paraméterek kombinációja, amely az Eszközfelügyelő összetevőben az alábbi funkciókat határozza meg:

- Adott időszakban adott eszköztípusokhoz való hozzáférés engedélyezése kiválasztott felhasználók és / vagy felhasználói csoportok számára.

  Kiválaszthat egy felhasználót és / vagy felhasználói csoportot, és eszközhozzáférési ütemezést készíthet számára.
- Memóriaeszközök tartalma olvasási jogának beállítása.
- Memóriaeszközök tartalma szerkesztési jogának beállítása.

Az Eszközfelügyelő összetevő osztályozásában alapértelmezés szerint minden eszköztípushoz létrejönnek hozzáférési szabályok. Ezek a szabályok minden felhasználó részére mindig teljes hozzáférést adnak, ha az adott eszköztípusok csatlakozóbuszaihoz való hozzáférés engedélyezve van.

A csatlakozóbuszok hozzáférési szabályai engedélyezik vagy blokkolják az adott buszhoz való hozzáférést.

Az Eszközfelügyelő összetevő osztályozásában jelen lévő összes csatlakozóbuszhoz alapértelmezés szerint a hozzájuk való hozzáférést engedélyező szabályok jönnek létre.

Az eszközhozzáférési és csatlakozóbuszhoz való hozzáférési szabályokat nem lehet létrehozni és törölni, hanem csak szerkeszteni.

A megbízható eszközök

A *megbízható eszközök* olyan eszközök, amelyekhez mindig teljes körűen hozzáférnek azok a felhasználók, akik a megbízható eszköz beállításaiban meg vannak adva.

A megbízható eszközökkel történő munkavégzés során az alábbi műveletek használhatók:

- Eszköz hozzáadása a megbízható eszközök listájához.
- A megbízható eszközhöz hozzáféréssel rendelkező felhasználó és / vagy felhasználói csoport módosítása.
- Eszköz törlése a megbízható eszközök listájáról.

Ha a megbízható eszközök listájához hozzáadott egy eszközt, és az adott eszköztípushoz a hozzáférést blokkoló vagy korlátozó hozzáférési szabályt hozott létre, a Kaspersky Endpoint Security attól függően dönti el, hogy biztosít-e hozzáférést az eszközhöz, hogy az szerepel-e a megbízható eszközök listáján. A megbízható eszközök listáján való szereplés prioritása magasabb, mint a hozzáférési szabály.

Az eszközök hozzáférésére vonatkozó szokásos döntések

A Kaspersky Endpoint Security döntést hoz az eszközök hozzáférésének engedélyezéséről, miután a felhasználó a számítógéphez csatlakoztatja őket.

Az eszközök hozzáférésére vonatkozó szokásos döntések

Szám	Kezdeti feltételek	Ideiglenes intézkedések, amíg megszületik az eszközhöz való hozzáférésre vonatkozó döntés			Az eszközhöz való hozzáférésre vonatkozó döntés
		Annak ellenőrzése, hogy az eszköz szerepel-e a megbízható eszközök listáján.	Az eszközhöz való hozzáférés tesztelése a hozzáférési szabály alapján	A buszhoz való hozzáférés tesztelése a buszhozzáférési szabály alapján	
1	Az eszköz nem szerepel az Eszközfelügyelő összetevő eszközbesorolásában.	Nem szerepel a megbízható eszközök listáján.	Nincs hozzáférési szabály.	Nem kerül sor vizsgálatra.	Hozzáférés engedélyezve.
2	Az eszköz megbízható.	Szerepel a megbízható eszközök listáján.	Nem kerül sor vizsgálatra.	Nem kerül sor vizsgálatra.	Hozzáférés engedélyezve.
3	Az eszközhöz való hozzáférés engedélyezve.	Nem szerepel a megbízható eszközök listáján.	Hozzáférés engedélyezve.	Nem kerül sor vizsgálatra.	Hozzáférés engedélyezve.
4	Az eszközhöz való hozzáférés a busztól függ.	Nem szerepel a megbízható eszközök listáján.	A hozzáférés a busztól függ.	Hozzáférés engedélyezve.	Hozzáférés engedélyezve.
5	Az eszközhöz való hozzáférés a busztól függ.	Nem szerepel a megbízható eszközök listáján.	A hozzáférés a busztól függ.	Hozzáférés blokkolva.	Hozzáférés blokkolva.
6	Az eszközhöz való	Nem szerepel a	Hozzáférés	Nincs	Hozzáférés

	hozzáférés engedélyezve. Nem található buszhozzáférési szabály.	megbízható eszközök listáján.	engedélyezve.	buszhozzáférési szabály.	engedélyezve.
7	Az eszközhöz való hozzáférés blokkolva.	Nem szerepel a megbízható eszközök listáján.	Hozzáférés blokkolva.	Nem kerül sor vizsgálatra.	Hozzáférés blokkolva.
8	Nem található eszközhozzáférési vagy buszhozzáférési szabály.	Nem szerepel a megbízható eszközök listáján.	Nincs hozzáférési szabály.	Nincs buszhozzáférési szabály.	Hozzáférés engedélyezve.
9	Nincs eszközhozzáférési szabály.	Nem szerepel a megbízható eszközök listáján.	Nincs hozzáférési szabály.	Hozzáférés engedélyezve.	Hozzáférés engedélyezve.
10	Nincs eszközhozzáférési szabály.	Nem szerepel a megbízható eszközök listáján.	Nincs hozzáférési szabály.	Hozzáférés blokkolva.	Hozzáférés blokkolva.

Az eszközhozzáférési szabály az eszköz csatlakozását követően szerkeszthető. Ha az eszköz csatlakoztatva van és a hozzáférési szabály engedélyezi a hozzáférést, később azonban szerkeszti a hozzáférési szabályt és blokkolja a hozzáférést, a Kaspersky Endpoint Security a következő alkalommal blokkolja a hozzáférést, amikor az eszközhöz bármilyen fájlműveleti kérés érkezik (a mappaszerkezet megtekintése, olvasás, írás). A fájlrendszer nélküli eszköz csak a következő csatlakoztatás alkalmával blokkolódik.

Ha az olyan számítógép felhasználójának, amelyen a Kaspersky Endpoint Security telepítve van, hozzáférést kell kérnie egy olyan eszközhöz, amely a felhasználó szerint tévedésből van blokkolva, küldje el a felhasználónak a kéréshozzáférési utasításokat.

Az eszközhozzáférési szabályok szerkesztése

Az eszköztípustól függően különféle hozzáférési beállításokat lehet módosítani, például az eszközhöz hozzáférést kapó felhasználók listáját, a hozzáférési ütemezést és az engedélyezett és blokkolt hozzáférést.

Eszköz hozzáférési szabályának szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.
3. Az ablak jobb oldalán válassza ki az **Eszköztípusok** lapot.

   Az **Eszköztípusok** lapon találhatók az összes olyan eszköz hozzáférési szabályai, amely az Eszközfelügyelő összetevő osztályozásában szerepel.
4. Válassza ki a szerkeszteni kívánt hozzáférési szabályt.
5. Kattintson a **Szerkesztés** gombra. Ez a gomb csak az olyan eszköztípusoknál használható, amelyek rendelkeznek fájlrendszerrel.

   Megnyílik az **Eszköz-hozzáférési szabály konfigurálása** ablak.

Alapértelmezés szerint az eszközök hozzáférési szabályai minden felhasználó részére mindig teljes hozzáférést adnak. A hozzáférési szabály a **Felhasználók és / vagy felhasználócsoportok** listán tartalmazza az **Mind** csoportot. **A kiválasztott felhasználócsoport jogai hozzáférés-ütemezés szerint** táblázatban a hozzáférési szabály az **Alapértelmezett ütemezés** értéket tartalmazza az eszközökhöz való hozzáféréshez az eszközökkel való műveletek minden típusának végrehajtási jogaival.

6. Az eszközhozzáférési szabály beállításainak szerkesztése:

   a. Válasszon ki egy felhasználót és / vagy felhasználói csoportot a **Felhasználók és / vagy felhasználócsoportok** listán.

   A **Felhasználók és / vagy felhasználócsoportok** listát a **Hozzáadás**, **Szerkesztés** és **Eltávolítás** gombokkal szerkesztheti.

   b. **A kiválasztott felhasználócsoport jogai hozzáférés-ütemezés szerint** táblázatban adja meg az eszközhozzáférési ütemezést a kiválasztott felhasználó és / vagy felhasználói csoport esetén. Ehhez jelölje be azon eszközök hozzáférési ütemezéseinek neve mellett a jelölőnégyzeteket, amelyeket a szerkesztendő eszközhozzáférési szabályban használni szeretne.

   Az eszközök hozzáférési ütemezése listájának szerkesztését a **Létrehozás**, **Szerkesztés**, **Másolás** és **Eltávolítás** gombokkal végezheti **A kiválasztott felhasználócsoport jogai hozzáférés-ütemezés szerint** táblázatban.

   c. A szerkesztés alatt álló szabályban használt eszközhozzáférési ütemezéseknél egyenként adja meg az eszközökkel való munkavégzés során engedélyezett műveleteket. Ehhez **A kiválasztott felhasználócsoport jogai hozzáférés-ütemezés szerint** táblázatban jelölje be az érintett műveletek neveit tartalmazó oszlopokban lévő jelölőnégyzeteket.

   d. Kattintson az **OK** gombra.

   Miután egy eszközhozzáférési szabály alapértelmezett beállításait szerkesztette, az eszköztípushoz való hozzáférési beállítás a **Hozzáférés** oszlopban az **Eszköztípusok** lapon *Korlátozás szabályokkal* értékre változik.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Bejegyzések felvétele az eseménynaplóba és kizárása onnan

Eseménynaplózás csak a cserélhető meghajtókon lévő fájlokkal végzett műveleteknél használható.

Az eseménynaplózás be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.

3. Az ablak jobb oldalán válassza ki az **Eszköztípusok** lapot.

   Az **Eszköztípusok** lapon találhatók az összes olyan eszköz hozzáférési szabályai, amely az Eszközfelügyelő összetevő osztályozásában szerepel.

4. Válassza ki a **Cserélhető meghajtók** lehetőséget az eszközök táblázatában.

   A táblázat felső részén használhatóvá válik a **Naplózás** gomb.

5. Kattintson a **Naplózás** gombra.

   Ezzel megnyílik a **Naplózási beállítások** ablak.

6. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni a cserélhető meghajtókon végzett fájltörlési és -írási műveletek naplózását, jelölje be a **Naplózás engedélyezése** jelölőnégyzetet.

     A Kaspersky Endpoint Security minden alkalommal eseményt ment a naplófájlba és üzenetet küld a Kaspersky Security Center Adminisztrációs kiszolgáló részére, amikor a felhasználó a cserélhető meghajtókon lévő fájlokon írási vagy törlési műveleteket végez.

   - Egyéb esetben törölje a **Naplózás engedélyezése** jelölőnégyzetet.

7. Adja meg, mely műveleteket szeretné naplózni. Ehhez végezze el az alábbiak egyikét:

   - Ha azt szeretné, hogy a Kaspersky Endpoint Security az összes eseményt naplózza, jelölje be az **Összes fájlra vonatkozó adat mentése** jelölőnégyzetet.

   - Ha azt szeretné, hogy a Kaspersky Endpoint Security csak az adott formátumú fájlokra vonatkozó információkat naplózza, akkor jelölje be a **Szűrés fájlformátum alapján** részben a kívánt fájlformátumok jelölőnégyzeteit.

8. Adja meg, hogy a Kaspersky Endpoint Security felhasználói műveletei közül melyeket szeretne eseményekként naplózni. Ehhez:

   a. A **Felhasználók** részben kattintson a **Kijelölés** gombra.

      Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanel a Microsoft Windowsban.

   b. Adja meg vagy szerkessze a felhasználókat és / vagy felhasználói csoportokat.

   Ha a **Felhasználók** részben megadott felhasználók cserélhető meghajtókon lévő fájlokba írnak vagy onnan fájlokat törölnek, a Kaspersky Endpoint Security az e műveletekre vonatkozó információkat menti az eseménynaplóba, és üzenetet küld a Kaspersky Security Center Adminisztrációs kiszolgáló részére.

9. A **Naplózási beállítások** ablakban kattintson az **OK** gombra.

10. A módosítások mentéséhez kattintson a **Mentés** gombra.

A cserélhető meghajtókon lévő fájlokhoz kapcsolódó eseményeket a Kaspersky Security Center Adminisztrációs Konzolon az **Adminisztrációs kiszolgáló** 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 beállításaiban.

Wi-Fi-hálózat felvétele a megbízható listára

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

Wi-Fi-hálózat felvétele a megbízható listára:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.

3. Az ablak jobb oldalán válassza ki az **Eszköztípusok** lapot.

   Az **Eszköztípusok** lapon találhatók az összes olyan eszköz hozzáférési szabályai, amely az Eszközfelügyelő összetevő osztályozásában szerepel.

4. Kattintson a jobb egérgombbal a **Hozzáférés** oszlopban a **Wi-Fi** eszközzel szemben a helyi menü megnyitásához.

5. Válassza ki a **Blokkolás kivételekkel** lehetőséget.

6. Az eszközök listáján válassza ki a **Wi-Fi** lehetőséget, majd kattintson a **Szerkesztés** gombra.

   Ezzel megnyílik a **Megbízható Wi-Fi hálózatok** ablak.

7. Kattintson a **Hozzáadás** gombra.

   Ezzel megnyílik a **Megbízható Wi-Fi hálózat** ablak.

8. A **Megbízható Wi-Fi hálózat** ablakban:

   - Adja meg a **Hálózat neve** mezőben a megbízható listára felvenni kívánt Wi-Fi-hálózat nevét.
   - Válassza ki a **Hitelesítés típusa** legördülő listán a megbízható Wi-Fi hálózathoz kapcsolódáskor használt hitelesítés típusát.
   - Válassza ki a **Titkosítás típusa** legördülő listán a megbízható Wi-Fi hálózat forgalmát biztonságossá tevő titkosítás típusát.
   - A **Megjegyzés** mezőben a felvett Wi-Fi-hálózatra vonatkozóan bármilyen információt megadhat.

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

9. A **Megbízható Wi-Fi hálózat** ablakban kattintson az **OK** gombra.

10. A **Megbízható Wi-Fi hálózatok** ablakban kattintson az **OK** gombra.

A csatlakozóbuszok hozzáférési szabályainak szerkesztése

A csatlakozóbuszok hozzáférési szabályainak szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.

3. Válassza ki a **Csatlakozási buszok** lapot.

   A **Csatlakozási buszok** lapon megjelennek az Eszközfelügyelő összetevő által osztályozott összes csatlakozóbusz hozzáférési szabályai.

4. Válassza ki a szerkeszteni kívánt csatlakozóbusz-szabályt.

5. A hozzáférési paraméter értékének módosítása:

   - A csatlakozóbuszhoz való hozzáférés engedélyezéséhez kattintson a jobb gombbal a **Hozzáférés** oszlopra a helyi menü megnyitásához, majd válassza ki az **Engedélyezés** lehetőséget.
   - A csatlakozóbuszhoz való hozzáférés blokkolásához kattintson a jobb gombbal a **Hozzáférés** oszlopra a helyi menü megnyitásához, majd válassza ki az **Blokkolás** lehetőséget.

6. A módosítások mentéséhez kattintson a **Mentés** gombra.

Megbízható eszközökkel végzett műveletek

Ez a rész a megbízható eszközökkel végzett műveletekre vonatkozó információkat tartalmaz.

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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.
3. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.
4. Kattintson a **Kijelölés** gombra.

   Megnyílik a **Megbízható eszközök kiválasztása** ablak.
5. Az eszközök neve melletti jelölőnégyzettel kiválaszthatja a megbízható eszközök listájára felvenni kívánt eszközöket.

   Az **Eszközök** oszlopban lévő lista a **Csatlakoztatott eszközök megjelenítése** legördülő listán kiválasztott értéktől függ.
6. Kattintson a **Kijelölés** gombra.

   Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanelt a Microsoft Windowsban.
7. A Microsoft Windows **Felhasználók vagy csoportok kiválasztása** ablakában adja meg azokat a felhasználókat és / vagy felhasználói csoportokat, amelyeknél a Kaspersky Endpoint Security a kiválasztott eszközt megbízhatóként ismeri fel.

   A Microsoft Windows **Felhasználók és / vagy csoportok kiválasztása** ablakában megadott felhasználók és / vagy felhasználói csoportok nevei az **Engedélyezve a következő felhasználók és / vagy csoportok számára** mezőben jelennek meg.
8. A **Megbízható eszközök kiválasztása** ablakban kattintson az **OK** gombra.

   A **Megbízható eszközök** lapon lévő táblázatban az **Eszközfelügyelő** összetevő beállítási ablakában megjelenik egy sor, amelyben a hozzáadott megbízható eszköz paraméterei láthatók.

9. Ismételje meg a 4–7. Lépéseket a megbízható eszközök listájára felvenni kívánt összes eszközzel a megadott felhasználóknál és / vagy felhasználói csoportoknál.

10. A módosítások mentéséhez kattintson a **Mentés** gombra.

Eszközök felvétele a megbízható listára az eszköztípus vagy -azonosító alapján

Alapértelmezés szerint eszköz megbízható eszközök listájára történő felvételekor minden felhasználó (a Mindenki felhasználói csoport) hozzáférést kap hozzá.

Eszközök felvétele a megbízható listára az eszköztípus vagy -azonosító alapján:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez megbízható eszközök listáját szeretné elkészíteni.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.

   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. A **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alrészt.

7. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.

8. Kattintson a **Hozzáadás** gombra.

   Megnyílik a gomb helyi menüje.

9. A **Hozzáadás** gomb helyi menüjében tegye az alábbiak egyikét:

   - Válassza ki az **Eszközök azonosító alapján** gombot, ha ismert egyedi azonosítójú eszközöket szeretne felvenni a megbízható eszközök listájára.

   - Válassza ki az **Eszközök típus alapján** elemet, ha a megbízható eszközök listájára olyan eszközöket szeretne felvenni, amelyeknek ismeri VID (forgalmazói azonosító), illetve PID (termékazonosító) számát.

10. A megnyíló ablakban válassza ki az **Eszköz típusa** legördülő listán a lenti táblázatban megjeleníteni kívánt eszközök típusát.

11. Kattintson a **Frissítés** gombra.

    A táblázatban megjelenik azon eszközök listája, amelyeknek ismert az eszközazonosítójuk és / vagy -típusuk, és amelyek az **Eszköz típusa** legördülő listán kiválasztott típushoz tartoznak.

12. Az eszközök neve melletti jelölőnégyzettel kiválaszthatja a megbízható eszközök listájára felvenni kívánt eszközöket.

13. Kattintson a **Kijelölés** gombra.

    Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanelt a Microsoft Windowsban.

14. A Microsoft Windows **Felhasználók vagy csoportok kiválasztása** ablakában adja meg azokat a felhasználókat és / vagy felhasználói csoportokat, amelyeknél a Kaspersky Endpoint Security a kiválasztott eszközt megbízhatóként ismeri fel.

    A Microsoft Windows **Felhasználók és / vagy csoportok kiválasztása** ablakában megadott felhasználók és / vagy felhasználói csoportok nevei az **Engedélyezve a következő felhasználók és / vagy csoportok számára** mezőben jelennek meg.

15. Kattintson az **OK** gombra.

    A **Megbízható eszközök** lapon lévő táblázatban sorok jelennek meg, amelyekben a hozzáadott megbízható eszközök paraméterei láthatók.

16. A módosítások mentéséhez kattintson az **OK** vagy az **Alkalmaz** gombra.

Eszközök felvétele a megbízható listára az eszközazonosító maszkja alapján

Alapértelmezés szerint eszköz megbízható eszközök listájára történő felvételekor minden felhasználó (a Mindenki felhasználói csoport) hozzáférést kap hozzá.

Az eszközöket azonosítójuk maszkja alapján kizárólag a Kaspersky Security Center Adminisztrációs Konzolon lehet a megbízható eszközök listájára felvenni.

Eszközök felvétele a megbízható listára azonosítójuk maszkja alapján:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez megbízható eszközök listáját szeretné elkészíteni.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. A **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alrészt.
7. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.
8. Kattintson a **Hozzáadás** gombra.

   Megnyílik a gomb helyi menüje.
9. A **Hozzáadás** gomb helyi menüjében válassza ki az **Eszközök azonosítómaszk alapján** elemet.

   Megnyílik a **Megbízható eszközök hozzáadása azonosítómaszk alapján** ablak.

10. Adja meg a **Megbízható eszközök hozzáadása azonosítómaszk alapján** ablakban az eszközazonosítók maszkját a **Maszk** mezőben.

11. Kattintson a **Kijelölés** gombra.

    Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanelt a Microsoft Windowsban.

12. A Microsoft Windows **Felhasználók vagy csoportok kiválasztása** ablakában adja meg azokat a felhasználókat és / vagy felhasználói csoportokat, amelyeknél a Kaspersky Endpoint Security a megadott maszkkal egyező típusú vagy azonosítójú eszközöket megbízhatóként ismeri fel.

    A Microsoft Windows **Felhasználók és / vagy csoportok kiválasztása** ablakában megadott felhasználók és / vagy felhasználói csoportok nevei az **Engedélyezve a következő felhasználók és / vagy csoportok számára** mezőben jelennek meg.

13. Kattintson az **OK** gombra.

    A **Megbízható eszközök** lapon lévő táblázatban az **Eszközfelügyelő** összetevő beállítási ablakában megjelenik egy sor, ahol az a szabály látható, amely az eszközök megbízható eszközök listájára való felvételét szabályozza az azonosítójuk maszkja alapján.

14. A módosítások mentéséhez kattintson a **Mentés** gombra.

Felhasználók megbízható eszközhöz való hozzáférésének beállítása

Alapértelmezés szerint eszköz megbízható eszközök listájára történő felvételekor minden felhasználó (a Mindenki felhasználói csoport) hozzáférést kap hozzá. Beállíthatja a felhasználók (vagy felhasználói csoportok) megbízható eszközhöz való hozzáférését.

Felhasználók megbízható eszközhöz való hozzáférésének beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.

3. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.

4. Válassza ki a megbízható eszközök listáján azt az eszközt, melynek szerkeszteni szeretné hozzáférési szabályait.

5. Kattintson a **Szerkesztés** gombra.

   Megnyílik az **Megbízható eszközök hozzáférési szabályának konfigurálása** ablak.

6. Kattintson a **Kijelölés** gombra.

   Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanelt a Microsoft Windowsban.

7. A Microsoft Windows **Felhasználók vagy csoportok kiválasztása** ablakában adja meg azokat a felhasználókat és / vagy felhasználói csoportokat, amelyeknél a Kaspersky Endpoint Security a kiválasztott eszközt megbízhatóként ismeri fel.

8. Kattintson az **OK** gombra.

   A Microsoft Windows **Felhasználók és / vagy csoportok kiválasztása** ablakában megadott felhasználók és / vagy felhasználói csoportok nevei az **Engedélyezve a következő felhasználók és / vagy csoportok számára** mezőben jelennek meg a **Megbízható eszközök hozzáférési szabályának konfigurálása** ablakban.

9. Kattintson az **OK** gombra.
10. A módosítások mentéséhez kattintson a **Mentés** gombra.

Eszköz eltávolítása a megbízható eszközök listájáról

Eszköz eltávolítása a megbízható eszközök listájáról:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.
3. Az ablak jobb oldalán válassza ki a **Megbízható eszközök** lapot.
4. Válassza ki a megbízható eszközök listájáról eltávolítani kívánt eszközt.
5. Kattintson az **Eltávolítás** gombra.
6. A módosítások mentéséhez kattintson a **Mentés** gombra.

A megbízható eszközök listájáról eltávolított eszközhöz való hozzáférésről a Kaspersky Endpoint Security az eszközhozzáférési szabályok és a csatlakozóbusz-hozzáférési szabályok alapján dönt.

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 hálózatoki rendszergazdának, 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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki az **Eszközfelügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek az Eszközfelügyelő összetevő beállításai.
3. Az ablak jobb oldali részén kattintson a **Sablonok** gombra.
   Megnyílik az **Üzenetsablonok** ablak.
4. Végezze el az alábbiak egyikét:
   - Az eszközökhöz való hozzáférés blokkolásáról és az eszközök tartalmán végzett műveletek tiltásáról szóló üzenet sablonjának módosításához válassza ki a **Blokkolás** lapot.

- A rendszergazdának küldött üzenet sablonjának módosításához válassza ki a **Üzenet a rendszergazdának** lapot.

5. Szerkessze az üzenetsablont. Használhatja a következő gombokat is: **Változó**, **Alapértelmezett** és **Hivatkozás** (ez a gomb csak a **Blokkolás** lapon található meg).
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Blokkolt eszközhöz való hozzáférés megszerzése

Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

A Kaspersky Endpoint Security eszközhöz ideiglenes hozzáférést nyújtó funkciója csak akkor használható, ha a Kaspersky Endpoint Security a Kaspersky Security Center rendszabály szerint működik, és ez a funkció a rendszabály beállításaiban be van kapcsolva (lásd: *Kaspersky Security Center Rendszergazdai útmutató*).

Hozzáférés kérése blokkolt eszközhöz az Eszközfelügyelő összetevő beállítási ablakában:

1. A fő alkalmazásablakban válassza ki a **Védelem és felügyelet** lapot.
2. Kattintson a **Végpontfelügyelő** részre.

   Megnyílik a **Végpontfelügyelő** rész.
3. Kattintson a jobb egérgombbal a helyi menü megnyitásához az Eszközfelügyelő összetevőre vonatkozó adatokat tartalmazó sorban.

   Megnyílik az összetevő műveleteinek kiválasztására szolgáló menü.
4. Kattintson a **Hozzáférés az eszközhöz** gombra.

   Megnyílik a **Hozzáférés kérése az eszközhöz** ablak.
5. Válassza ki a csatlakoztatott eszközök listáján azt az eszközt, amelyhez hozzáférést szeretne kapni.
6. Kattintson a **Kéréshozzáférési fájl előállítása** gombra.

   Erre megnyílik a **Hozzáférés-kérési fájl létrehozása** ablak.
7. Adja meg a **Hozzáférés időtartama** mezőben azt az időszakot, ameddig hozzáférést szeretne az eszközhöz.
8. Kattintson a **Mentés** gombra.

   Ezzel megnyílik a szokásos **Kéréshozzáférési fájl mentése** ablak a Microsoft Windowsban.
9. A Microsoft Windows **Kéréshozzáférési fájl mentése** ablakában válassza ki azt a mappát, amelybe az eszköz kéréshozzáférési fájlját menteni szeretné, majd kattintson a **Mentés** gombra.
10. Küldje el az eszköz kéréshozzáférési fájlját a helyi hálózati rendszergazdának.
11. A helyi hálózati rendszergazdától megérkezik az eszköz hozzáférési kulcsfájlja.
12. Kattintson az **Hozzáférés kérése az eszközhöz** ablakban a **Hozzáférési kulcs aktiválása** gombra.

Megnyílik a szokásos **Hozzáférési kulcs megnyitása** ablak a Microsoft Windowsban.

13. Válassza ki a Microsoft Windows **Hozzáférési kulcs megnyitása** ablakában az eszköz helyi hálózati rendszergazdától kapott hozzáférési kulcsfájlját, majd kattintson a **Megnyitás** lehetőségre.

    Megnyílik a **Az eszköz hozzáférési kulcsának aktiválása** ablak, és megjeleníti a megadott hozzáférésre vonatkozó adatokat.

14. A **Az eszköz hozzáférési kulcsának aktiválása** ablakban kattintson az **OK** gombra.

Hozzáférés kérése blokkolt eszközhöz az eszköz blokkolásáról tájékoztató üzenetben lévő hivatkozásra kattintva:

1. Kattintson az eszköz vagy csatlakozóbusz blokkolásáról tájékoztató üzenetet tartalmazó ablakban a **Hozzáférés kérése** hivatkozásra.

   Erre megnyílik a **Hozzáférés-kérési fájl létrehozása** ablak.

2. Adja meg a **Hozzáférés időtartama** mezőben azt az időszakot, ameddig hozzáférést szeretne az eszközhöz.

3. Kattintson a **Mentés** gombra.

   Ezzel megnyílik a szokásos **Kéréshozzáférési fájl mentése** ablak a Microsoft Windowsban.

4. A Microsoft Windows **Kéréshozzáférési fájl mentése** ablakában válassza ki azt a mappát, amelybe az eszköz kéréshozzáférési fájlját menteni szeretné, majd kattintson a **Mentés** gombra.

5. Küldje el az eszköz kéréshozzáférési fájlját a helyi hálózati rendszergazdának.

6. A helyi hálózati rendszergazdától megérkezik az eszköz hozzáférési kulcsfájlja.

7. Kattintson az **Hozzáférés kérése az eszközhöz** ablakban a **Hozzáférési kulcs aktiválása** gombra.

   Megnyílik a szokásos **Hozzáférési kulcs megnyitása** ablak a Microsoft Windowsban.

8. Válassza ki a Microsoft Windows **Hozzáférési kulcs megnyitása** ablakában az eszköz helyi hálózati rendszergazdától kapott hozzáférési kulcsfájlját, majd kattintson a **Megnyitás** lehetőségre.

   Megnyílik a **Az eszköz hozzáférési kulcsának aktiválása** ablak, és megjeleníti a megadott hozzáférésre vonatkozó adatokat.

9. A **Az eszköz hozzáférési kulcsának aktiválása** ablakban kattintson az **OK** gombra.

Az eszközhöz való hozzáférés engedélyezésének időtartama eltérhet a kért időtartamtól. Az eszközhöz annyi ideig kap hozzáférést, amennyit a helyi hálózati rendszergazda az eszköz hozzáférési kulcsának előállításakor megszabott.

Blokkolt eszközhöz való hozzáférésre szolgáló kulcs létrehozása a Kaspersky Security Center segítségével

Ha egy felhasználónak ideiglenesen hozzáférést szeretne adni egy blokkolt eszközhöz, az eszközhöz hozzáférési kulcs szükséges. A Kaspersky Security Center segítségével hozhat létre hozzáférési kulcsot.

Hozzáférési kulcs létrehozása blokkolt eszközhöz:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógép tartozik.

3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki az ügyfélszámítógépek listáján azt a számítógépet, amelynek a felhasználója részére ideiglenes hozzáférést szeretne adni egy zárolt eszközhöz.

5. A számítógép helyi menüjében válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** lehetőséget.

   Megnyílik a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablak.

6. Válassza ki az **Eszközfelügyelő** lapot.

7. Az **Eszközfelügyelő** lapon kattintson a **Tallózás** gombra.

   Megnyílik a szokásos **Kéréshozzáférési fájl kiválasztása** ablak a Microsoft Windowsban.

8. Válassza ki a **Kéréshozzáférési fájl kiválasztása** ablakban a felhasználótól kapott kéréshozzáférési fájl elérési útját, majd kattintson a **Megnyitás** lehetőségre.

   Az **Eszközfelügyelő** megjeleníti annak a zárolt eszköznek az adatait, amelyhez a felhasználó hozzáférést kért.

9. Adja meg a **Hozzáférés időtartama** beállítás értékét.

   Ez a beállítás szabja meg, mennyi időre kap hozzáférést a felhasználó a zárolt eszközhöz. Az alapértelmezett érték az, amelyet a felhasználó a hozzáférés-kérési fájl létrehozásakor adott meg.

10. Adja meg az **Aktiválási időtartam** beállítás értékét.

    Ez a beállítás szabja meg, hogy a felhasználó a kapott hozzáférési kulcs segítségével mennyi ideig aktiválhatja a blokkolt eszközhöz való hozzáférést.

11. Kattintson a **Mentés** gombra.

    Ezzel megnyílik a szokásos **Hozzáférési kulcs mentése** ablak a Microsoft Windowsban.

12. Válassza ki azt a célmappát, ahová a blokkolt eszköz hozzáférési kulcsát tartalmazó fájlt menteni szeretné.

13. Kattintson a **Mentés** gombra.

Webfelügyelő

Ez az összetevő akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ez az összetevő nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész tájékoztatást nyújt a Webfelügyelővel kapcsolatban, és ismerteti az összetevő beállításainak megadását.

A Webfelügyelő

A Webfelügyelő lehetővé teszi a helyi hálózati felhasználók műveleteinek felügyeletét a webes erőforrásokhoz való hozzáférésének korlátozása, illetve blokkolása révén.

A webes erőforrás egyedi weboldal vagy több weboldal, illetve webhely vagy több webhely, melyeknek közös funkciójuk van.

A Webfelügyelő az alábbi lehetőségeket kínálja:

- Takarékosság a forgalommal.

  A forgalom felügyelete a multimédiás fájlok letöltéseinek korlátozása vagy blokkolása, illetve a felhasználó munkaköri feladataihoz nem kapcsolódó webes erőforrásokhoz való hozzáférés korlátozása vagy blokkolása révén történik.

- Hozzáférés korlátozása a webes erőforrások tartalmi kategóriái szerint.

  A forgalommal való takarékosság és az alkalmazottak idejének nem megfelelő felhasználásából fakadó potenciális veszteségek csökkentése érdekében korlátozhatja, illetve blokkolhatja a hozzáférést webes erőforrások adott kategóriáihoz (például blokkolhatja az „Internetes kommunikációs média" kategóriába tartozó webes erőforrásokhoz való hozzáférést).

- Webes erőforrások elérésének központosított felügyelete.

  A Kaspersky Security Center használata esetén rendelkezésre állnak a webes erőforrásokhoz való hozzáférés személyes és csoportos beállításai.

A webes erőforrásokhoz való hozzáférésre vonatkozó összes korlátozás és blokkolás webes erőforrások hozzáférési szabályai formájában van megvalósítva.

A Webfelügyelő be- és kikapcsolása

Alapértelmezés szerint a Webfelügyelő engedélyezve van. A Webfelügyelőt szükség esetén letilthatja.

Az összetevő kétféle módon engedélyezhető és tiltható le:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

*A Webfelügyelő be- és kikapcsolása a **Védelem és felügyelet** lapon a fő alkalmazásablakban:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Végpontfelügyelő** részre.

   Megnyílik a **Végpontfelügyelő** rész.
4. Kattintson a jobb egérgombbal a helyi menü megnyitásához a Webfelügyelő összetevőre vonatkozó adatokat tartalmazó sorban.

   Megnyílik az összetevő műveleteinek kiválasztására szolgáló menü.
5. Végezze el az alábbiak egyikét:

   - A Webfelügyelő bekapcsolásához válassza ki a menüben az **Indítás** lehetőséget.
   - A Webfelügyelő kikapcsolásához válassza ki a menüben a **Leállítás** lehetőséget.

A Webfelügyelő be- és kikapcsolása az alkalmazás beállítási ablakából:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Webfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni a Webfelügyelőt, jelölje be a **Webfelügyelő bekapcsolása** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a Webfelügyelőt, törölje a **Webfelügyelő bekapcsolása** jelölőnégyzetet.

   Ha a Webfelügyelő ki van kapcsolva, a Kaspersky Endpoint Security nem felügyeli a webes erőforrásokhoz való hozzáférést.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Webes erőforrás tartalmi kategóriái

A webes erőforrások lent felsorolt tartalmi kategóriáit (a továbbiakban „kategóriák” is) úgy választottuk ki, hogy a webes erőforrások által tárolt adatblokkokat a lehető legteljesebben írják le, figyelembe véve funkcionális és tematikus jellemzőiket. A kategóriák listán belüli sorrendje nem tükrözi azok relatív fontosságát, illetve elterjedtségét az interneten. A kategóriák nevei ideiglenesek, és kizárólag a Kaspersky alkalmazásainak és webhelyeinek céljaira használjuk. A nevek nem feltétlenül tükrözik a törvény által nekik tulajdonított jelentést. Egyazon webes erőforrás egyszerre több kategóriába is tartozhat.

Felnőtteknek szánt tartalom

Ez a kategória az alábbi típusú webes erőforrásokat tartalmazza:

- Emberek vagy humanoid lények nemi szerveit, illetve emberek vagy humanoid lények közösülését vagy önmaguk izgatását ábrázoló fényképet vagy videót tartalmazó webes erőforrások.

- Emberek vagy humanoid lények nemi szerveit, illetve emberek vagy humanoid lények közösülését vagy önmaguk izgatását leíró szöveges anyagokat – köztük irodalmi és művészi igényű anyagokat – tartalmazó webes erőforrások.
- Az emberi kapcsolatok szexuális szempontjának megvitatásának szentelt webes erőforrások.
- Erotikus anyagokat, emberek szexuális viselkedését valósághűen bemutató műveket, illetve nemi izgalom keltésére szánt művészi műveket tartalmazó webes erőforrások.
- Kialakult célközönséggel rendelkező hivatalos médiavállalatok és online közösségek webes erőforrásai, amelyek az emberi kapcsolatok szexuális vonatkozásának szentelt külön részt és / vagy különálló cikkeket tartalmaznak.
- Szexuális perverzióknak szentelt webes erőforrások.
- Szex során használandó és nemi izgalom felkeltésére szolgáló termékeket, valamint szexuális szolgáltatásokat és intim randevúzást – ideértve az interneten erotikus videocsevegésen keresztül nyújtott szolgáltatásokat, a „telefonszexet" és a „sextinget" („virtuális szex") is – hirdető és értékesítő webes erőforrások.
- Webes erőforrások a következő tartalommal:
  - Tudományos és népszerű témájú szexuális felvilágosításról szóló cikkek és blogok.
  - Orvosi enciklopédiák, különösen a szexuális reprodukcióról szóló fejezeteik.
  - Orvosi intézmények forrásai, főleg a nemi szervekről szóló fejezeteik.

Szoftver, hang, videó

Ez a kategória az alábbi, egyenként kiválasztható alkategóriákat tartalmazza:

- **Hang és videó**.

  Ez az alkategória hang- és videoanyagokat – filmeket, sportközvetítések felvételeit, koncertfelvételeket, zeneszámokat, filmrészleteket, videókat, oktatóanyagok hang- és videofelvételeit stb. – terjesztő webes erőforrásokat tartalmaz.

- **Torrentek**.

  Ez az alkategória korlátlan méretű fájlok megosztására szolgáló torrentkövetők webhelyeit tartalmazza.

- **Fájlmegosztás**.

  Ez az alkategória fájlmegosztó webhelyeket tartalmaz a terjesztett fájlok fizikai helyétől függetlenül.

Alkohol, dohány, kábítószerek

Ez az alkategória olyan webes erőforrásokat tartalmaz, amelyeknek a tartalma közvetlenül vagy közvetve alkoholos vagy alkoholtartalmú termékekkel, dohánytermékekkel, illetve narkotikus, pszichotróp és / vagy kábító hatású anyagokkal függ össze.

- Az ilyen anyagokat és fogyasztásuk kellékeit hirdető és értékesítő webes erőforrások.
- A narkotikus, pszichotróp és / vagy kábító hatású anyagok fogyasztására vagy előállítására vonatkozó utasításokat tartalmazó webes erőforrások.

Ebbe a kategóriába beletartoznak a tudományos és orvosi témákkal foglalkozó webes erőforrások is.

Erőszak

Ebbe a kategóriába tartoznak azok a webes erőforrások, amelyek emberek elleni fizikai vagy pszichológiai erőszakot, illetve állatokkal való kegyetlen bánásmódot ábrázoló fényképet, videót vagy szöveges anyagot tartalmaznak.

- Kivégzéseket, kínzást és bántalmazást, valamint az ehhez való eszközöket bemutató, illetve leíró webes erőforrások.

  Átfedésben van a „Fegyverek, robbanóanyagok, pirotechnika" kategóriával.

- Gyilkosságot, verekedést, bántalmazást vagy nemi erőszakot, illetve emberek, állatok vagy képzeletbeli lények bántalmazását vagy megalázását tartalmazó jeleneteket ábrázoló vagy leíró webes erőforrások.
- Életet és / vagy egészséget veszélybe sodró cselekedeteket – így öncsonkítást vagy öngyilkosságot – ösztönző webes erőforrások.
- Az erőszak és / vagy kegyetlenség megengedhetőségét igazoló vagy indokló, illetve emberek vagy állatok ellen erőszakra felbujtó információkat tartalmazó webes erőforrások.
- Háborúk, fegyveres konfliktusok és katonai összecsapások, balesetek, természeti és egyéb katasztrófák, ipari vagy társadalmi válságok, illetve emberi szenvedés áldozatainak és atrocitásainak különösen valósághű ábrázolását vagy leírását tartalmazó webes erőforrások.
- Böngészőben működő számítógépes játékok, melyben erőszakos és kegyetlen jelenetek találhatók, ideértve a „lövöldözős", „harcolós", „öldöklős" stb. játékokat.

  Átfedésben van a „Számítógépes játékok" kategóriával.

Fegyverek, robbanóanyagok, pirotechnika

Ebbe a kategóriába tartoznak a fegyverekről, robbanóanyagokról és pirotechnikai termékekről szóló információkat tartalmazó webes erőforrások:

- Fegyverek, robbanóanyagok, pirotechnikai termékek gyártóinak és áruházainak webhelyei.
- Fegyverek, robbanóanyagok és pirotechnikai termékek készítésének vagy használatának szentelt webes erőforrások.
- Fegyvereknek, robbanóanyagoknak és pirotechnikai termékeknek szentelt elemző, történeti, gyártási és enciklopédikus anyagokat tartalmazó webes erőforrások.

A „fegyverek" kifejezés az olyan készülékekre, termékekre és eszközökre terjed ki, amelyek emberek és állatok életében vagy egészségében történő károkozásra és / vagy berendezések és szerkezetek tönkretételére készültek.

Durva nyelvezet, obszcenitás

Ebbe a kategóriába beletartoznak azok a webes erőforrások, amelyeken obszcén nyelvhasználat észlelhető.

Átfedésben van a „Csak felnőtteknek való tartalom” kategóriával.

Ebbe a kategóriába beletartoznak az olyan webes erőforrások is, amelyek obszcenitást tanulmányozó nyelvészeti és filológiai anyagokat tartalmaznak.

Internetes kommunikáció

Ebbe a kategóriába olyan webes erőforrások tartoznak, amelyek lehetővé teszik, hogy a felhasználók (regisztrációt követően vagy anélkül) személyes üzeneteket küldhessenek az adott webes erőforrások vagy más internetes szolgáltatások felhasználóinak és / vagy (nyilvánosan elérhető, vagy korlátozott) tartalmakat adhassanak hozzá az adott webes erőforrásokhoz bizonyos feltételek alapján. Az alábbi alkategóriák közül választhat egyet:

- **Csevegőszobák és fórumok**.

  Ebbe az alkategóriába tartoznak azok a webes erőforrások, amelyek különféle témák különleges webes alkalmazások segítségével történő nyilvános megvitatására szolgálnak, illetve azok a webes erőforrások, amelyek valós idejű kommunikációt lehetővé tevő azonnali üzenetküldő alkalmazások terjesztésére vagy támogatására szolgálnak.

- **Blogok**.

  Ebbe az alkategóriába tartoznak a blogplatformok, melyek blogok készítésére és fenntartására szolgáló fizetős vagy ingyenes szolgáltatásokat nyújtó webhelyek.

- **Közösségi hálózatok**.

  Ebbe az alkategóriába tartoznak azok a webhelyek, amelyek személyek, szervezetek és kormányzatok közti kapcsolatok létesítésére, megjelenítésére és kezelésére szolgálnak, és a részvétel feltételeként felhasználói fiók regisztrálását kötik ki.

- **Társkereső webhelyek**.

  Ebbe az alkategóriába fizetős vagy ingyenes szolgáltatásokat nyújtó különféle közösségi hálózatokként szolgáló webes erőforrások tartoznak.

  Átfedésben van a „Csak felnőtteknek való tartalom” kategóriákkal.

- **Webalapú e-mail**.

  Ebbe az alkategóriába csak az e-maileket és kapcsolódó adatokat (például személyes névjegyeket) tartalmazó e-mail-szolgáltatás és levelezőoldalak bejelentkezési oldalai tartoznak. Ez a kategória nem tartalmazza az internetszolgáltató egyéb weboldalait, amelyek szintén e-mail-szolgáltatást kínálnak.

Szerencsejáték, lottó, sorshúzás

Ebbe a kategóriába olyan webes erőforrások tartoznak, amelyek pénzben játszott szerencsejátékban való részvételi lehetőséget kínálnak, még akkor is, ha a pénzzel történő részvétel nem kötelező feltétele a webhelyhez való hozzáférésnek. Ebbe a kategóriába az alábbiakat kínáló webes erőforrások tartoznak:

Olyan szerencsejáték, ahol a résztvevőknek pénzzel kell beszállniuk.

Átfedésben van a „Számítógépes játékok” kategóriával.

- Pénzzel történő fogadással járó sorsolások.
- Lottószelvények vagy -számok vásárlásával járó lottók.
- Olyan információk, amelyek kiválthatják a szerencsejátékban, sorsolásban vagy lottóban való részvétel vágyát.

Ebbe a kategóriába olyan játékok tartoznak, amelyek különálló módként ingyenes részvételt kínálnak, valamint azok a webes erőforrások, amelyek a felhasználók számára aktívan hirdetnek ebbe a kategóriába tartozó webes erőforrásokat.

Online üzletek, bankok, fizetési rendszerek

Ebbe a kategóriába azok a webes erőforrások tartoznak, amelyek külön erre való alkalmazások segítségével nem készpénzes pénzösszegekben történő internetes tranzakciókra szolgálnak. Az alábbi alkategóriák közül választhat egyet:

- **Online áruházak**.

  Ebbe az alkategóriába árukat, munkát vagy szolgáltatásokat egyének és / vagy jogi entitások részére értékesítő internetes áruházak és aukciók tartoznak, ideértve az olyan áruházak webhelyeit is, amelyek kizárólag az interneten értékesítenek, valamint a fizikai áruházak internetes profiljait, ahol az interneten is lehet fizetni.

- **Bankok**.

  Ebbe az alkategóriába tartoznak a bankok azon speciális weboldalai, amelyeken az interneten banki műveleteket lehet végezni, ideértve a bankszámlák közti (elektronikus) átutalásokat, a banki letétek és valutaátváltások elvégzését, harmadik felek szolgáltatásainak kifizetését stb.

- **Fizetési rendszerek**.

  Ebbe az alkategóriába elektronikus pénzrendszerek weboldalai tartoznak, melyek hozzáférést kínálnak a felhasználó személyes fiókjához.

- **Kriptopénz és bányászat**.

  Ebbe az alkategóriába tartoznak az olyan weboldalak, amik kriptovalutával történő vásárlással és eladással kapcsolatos szolgáltatásokat kínálnak, valamint a kriptovalutához és bányászathoz tartozó információs szolgáltatásokat nyújtanak.

Műszaki szempontból a fizetés történhet bármilyen típusú bankkártyákkal (műanyag és virtuális, bankkártya és hitelkártya, helyi és nemzetközi) és elektronikus pénzzel. A webes erőforrások attól függetlenül ebbe a kategóriába tartozhatnak, hogy olyan műszaki szempontok adottak-e, mint például az adatátvitel SSL protokoll segítségével, 3D biztonságos hitelesítés alkalmazása stb.

Munkakeresés

Ebbe a kategóriába tartoznak a munkáltatók és álláskeresők összehozására szolgáló webes erőforrások:

- Toborzóügynökségek webhelyei (munkavállalói ügynökségek és / vagy fejvadász ügynökségek).
- Álláslehetőségek és a velük járó előnyök leírását tartalmazó munkáltatói webhelyek.
- Munkáltatók és toborzóügynökségek ajánlatait tartalmazó független portálok.
- Szakmai közösségi hálózatok, amelyek minden más mellett lehetővé teszik olyan szakemberek adatainak közzétételét és megkeresését, akik éppen nem keresnek aktívan állást.

Anonimizálók

Ebbe a kategóriába azok a webes erőforrások tartoznak, amelyek közvetítő szerepet játszanak más webes erőforrások tartalmának letöltésében különleges webes alkalmazások segítségével az alábbi célokból:

- A helyi hálózati rendszergazda által beállított, webcímek vagy IP-címek elérésére vonatkozó korlátozások megkerülése;
- Névtelen hozzáférés webes erőforrásokhoz, köztük olyanokhoz, amelyek kifejezetten elutasítják a bizonyos IP-címekről vagy azok csoportjától (például származási ország alapján csoportosított IP-címekről) érkező HTTP kéréseket.

Ebbe a kategóriába egyaránt beletartoznak azok a webes erőforrások, amelyek kizárólag a fent említett célokra szolgálnak („anonimizálók"), és azok, amelyek műszakilag hasonló funkciót kínálnak.

Számítógépes játékok

Ebbe a kategóriába tartoznak a különböző műfajú számítógépes játékoknak szentelt webes erőforrások:

- Számítógépes játékok fejlesztőinek webhelyei.
- Számítógépes játékok megvitatásának szentelt webes erőforrások.
- Internetes játékokban való részvétel műszaki lehetőségét kínáló webes erőforrások, akár más résztvevőkkel együtt, akár egyénileg, alkalmazások helyi telepítésével vagy anélkül („böngészőben futó játékok").
- Játékszoftverek hirdetésére, terjesztésére és támogatására szolgáló webes erőforrások.

Vallások, vallásos szervezetek

Ebbe a kategóriába tartoznak a vallásos ideológiával és / vagy bármilyen megjelenési formában előforduló kultusszal rendelkező nyilvános mozgalmakkal, szervezetekkel és szövetségekkel kapcsolatos anyagokat tartalmazó webes erőforrások.

- Hivatalos vallási szervezetek webhelyei különböző szinteken a nemzetközi vallásoktól a helyi vallási közösségekig.
- Olyan, be nem jegyzett vallási szervezetek és társaságok webhelyei, amelyek történetileg úgy keletkeztek, hogy egy domináns vallási szervezetből vagy közösségből váltak le.
- A hagyományos vallási mozgalmaktól függetlenül – például egy konkrét vallásalapító kezdeményezésére – keletkezett vallási szervezetek és közösségek webhelyei.

- A különböző hagyományos vallások képviselőit közti együttműködést megcélzó vallások közti szervezetek webhelyei.
- A vallásokat tárgyaló akadémikus, történeti és enciklopédikus anyagokat tartalmazó webes erőforrások.
- A hitélet részét képező vallásgyakorlat részletes bemutatását vagy leírását tartalmazó webes erőforrások, ideértve az Isten, illetve az adott vallás szerint természetfeletti hatalommal rendelkező lények és / vagy tárgyak imádatával járó rítusokat és rituálékat.

Hírmédia

Ebbe a kategóriába tartoznak a tömegsajtó és az internetes kiadványok által előállított nyilvános hírtartalmakat kínáló webes erőforrások, amelyek lehetővé teszik, hogy a felhasználók megadják saját híreiket:

- Hivatalos médiavállalatok webhelyei.
- Információs szolgáltatásokat nyújtó webhelyek, melyek feltüntetik a hivatalos információforrásokat.
- Különféle hivatalos és nemhivatalos forrásokból híreket gyűjtő szolgáltatásokat kínáló webhelyek.
- Olyan webhelyek, ahol a hírtartalmakat maguk a felhasználók állítják elő („közösségi híroldalak").

Reklámcsíkok

Ebbe a kategóriába a reklámcsíkokat tartalmazó webes erőforrások tartoznak. A reklámcsíkokon lévő hirdetési információk elvonhatják a felhasználó figyelmét tevékenységétől, letöltésük pedig növeli a bejövő adatforgalmat.

Regionális jogi korlátozások

Ez a kategória a következő alkategóriákat foglalja magába:

- **Az Oroszországi Föderáció törvényi követelményei miatt blokkolva**.
  Ebbe az alkategóriába tartoznak az orosz törvények által tiltott webes erőforrások.
- **Blokkolva a belga törvények alapján**.
  Ebbe az alkategóriába tartoznak a belga törvények által tiltott webes erőforrások.
- **Blokkolva a japán törvények alapján**.
  Ebbe az alkategóriába tartoznak a Japán törvények által tiltott webes erőforrások.

A webes erőforrások hozzáférési szabályai

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. Bizonyos kategóriákba 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 felhasználói csoportoknak 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:

- A Forgatókönyvek és Stílustáblázatok szabály, melyek minden felhasználónak mindig engedélyezik a hozzáférést az olyan webes erőforrásokhoz, amelyeknek a címei a fájlok nevét css, js vagy vbs kiterjesztéssel tartalmazzák. Például: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- Az „Alapértelmezett szabály", amely minden felhasználónak mindig minden webes erőforráshoz hozzáférést engedélyez.

A webes erőforrások hozzáférési szabályainak műveletei

A webes erőforrások hozzáférési szabályain a következő műveleteket végezheti el:

- Új szabály hozzáadása

- Szabály szerkesztése

- Prioritás hozzárendelése szabályhoz

  A szabály prioritását a rövid leírását tartalmazó sor helye határozza meg a Webfelügyelő összetevő beállítási ablakában lévő, a hozzáférési szabályokat tartalmazó táblázatban. Ez azt jelenti, hogy a hozzáférési szabályok táblázatában magasabb helyen lévő szabály prioritása magasabb, mint az alatta lévő szabályé.

  Ha a felhasználó megpróbál hozzáférni egy olyan webes erőforráshoz, amely több szabály paramétereivel egyezik, a Kaspersky Endpoint Security a legmagasabb prioritású szabály szerinti műveletet végzi el.

- Szabály tesztelése.

  Ellenőrizheti a szabályok konzisztenciáját a Szabályok diagnosztikája funkcióval.

- Szabály engedélyezése és letiltása.

A webes erőforrások hozzáférési szabályai lehetnek engedélyezettek (működési állapot: *Be*) és letiltottak (működési állapot: *Ki*). Alapértelmezés szerint a szabályok létrehozásukat követően engedélyezve vannak (működési állapot: *Be).* A szabályt le is tilthatja.

- Szabály törlése

Webes erőforrások hozzáférési szabályainak megadása és szerkesztése

Webes erőforrások hozzáférési szabályainak megadása és szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Webfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Végezze el az alábbiak egyikét:
   - Szabályt a **Hozzáadás** gombra kattintva adhat meg.
   - Ha egy szabályt szeretne szerkeszteni, válassza ki a táblázatban, és kattintson a **Szerkesztés** gombra.

   Megnyílik a **Szabály a webes erőforrásokhoz való hozzáférésre** ablak.
4. Adja meg vagy szerkessze a szabály beállításait. Ehhez:
   a. A **Név** mezőben adja meg vagy szerkessze a szabály nevét.
   b. Válassza ki a **Tartalomszűrés** legördülő listán a kívánt lehetőséget:
      - **Bármely tartalom**.
      - **Tartalomkategória alapján**.
      - **Adattípus alapján**.
      - **Tartalomkategória és adattípus alapján**.
   c. Ha a **Bármely tartalom** elemtől eltérő lehetőséget választ, megnyílnak a tartalmi kategóriák és / vagy adattípusok kiválasztására szolgáló részek. 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.
   d. Válassza ki az **Alkalmazás a következő címekre** legördülő listán a kívánt lehetőséget:
      - **Minden címre**.
      - **Egyedi címekre**.
   e. Az **Egyedi címekre** lehetőség kiválasztása esetén megnyílik egy rész, ahol létrehozhatja a webes erőforrások listáját. A webes erőforrások címeit a **Hozzáadás**, **Szerkesztés** és **Törlés** gombokkal adhatja meg, illetve szerkesztheti.

f. Jelölje be a **Felhasználók és / vagy csoportok megadása** jelölőnégyzetet.

g. Kattintson a **Kijelölés** gombra.

Megnyílik a szokásos **Felhasználók vagy csoportok kiválasztása** párbeszédpanelt a Microsoft Windowsban.

h. Adja meg vagy szerkessze azoknak a felhasználóknak és / vagy felhasználói csoportoknak a listáját, akiknél a szabálynak megfelelően sor kerül a webes erőforrások hozzáférésének engedélyezésére vagy blokkolására.

i. Válassza ki a **Művelet** legördülő listán a kívánt lehetőséget:

- **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.

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

1. Kattintson a **Szabályütemezés** legördülő listával szemben lévő **Beállítások** gombra.

   Megnyílik a **Szabályütemezés** ablak.

2. Ha a szabály ütemezéséhez olyan időszakot szeretne hozzáadni, amikor a szabály nem érvényes, akkor kattintson a szabály ütemezését megjelenítő táblázatban azokra a cellákra, amelyek megfelelnek a kiválasztani kívánt időpontnak és a hét kívánt napjának.

   A cellák színe ekkor szürkére változik.

3. Ha egy olyan időszakot, amikor a szabály érvényes, egy olyannal szeretne helyettesíteni, amikor a szabály nem érvényes, kattintson a táblázatban azokra a szürke cellákra, amelyek a kívánt időpontnak és a hét kívánt napjának felelnek meg.

   A cellák színe ekkor zöldre változik.

4. Kattintson a **Mentés másként** gombra.

   Megnyílik a **Szabályütemezés neve** ablak.

5. Gépelje be a szabályütemezés nevét, vagy hagyja meg a javasolt alapértelmezett nevet.

6. Kattintson az **OK** gombra.

5. Kattintson a **Szabály a webes erőforrásokhoz való hozzáférésre** ablakban az **OK** gombra.

6. A módosítások mentéséhez kattintson a **Mentés** gombra.

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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Webfelügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Az ablak jobb oldalán válassza ki azt a szabályt, amelynek a prioritását meg szeretné változtatni.
4. A szabályt a listán a **Mozgatás felfelé** és **Mozgatás lefelé** gombokkal helyezheti a kívánt helyre.
5. Ismételje meg a 3–4. lépéseket azokkal a szabályokkal, amelyeknek meg szeretné változtatni a prioritását.
6. A módosítások mentéséhez kattintson a **Mentés** gombra.

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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Webfelügyelő** alpontot.
   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Az ablak jobb oldali részén kattintson a **Diagnosztika** gombra.
   Megnyílik a **Szabálydiagnosztika** ablak.
4. Töltse ki a **Feltételek** rész mezőit:
   a. 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.
   b. Ha azokat a szabályokat szeretné tesztelni, amelyeket a Kaspersky Endpoint Security a webes erőforrásokhoz való hozzáférés vezérlésére használ adott felhasználók és / vagy felhasználói csoportok esetén, adja meg a felhasználók és / vagy felhasználói csoportok listáját.
   c. Ha azokat a szabályokat szeretné tesztelni, amelyeket a Kaspersky Endpoint Security adott tartalmi kategóriákba és / vagy adattípus-kategóriákba tartozó webes erőforrásokhoz való hozzáférés vezérlésére használ, válassza ki a **Tartalomszűrés**legördülő listán a kívánt lehetőséget (**Tartalomkategória alapján**, **Adattípus alapján**, illetve **Tartalomkategória és adattípus alapján**).
   d. 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.
5. Kattintson a **Teszt** 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 **Teszt** 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.

A webes erőforrások hozzáférési szabályainak engedélyezése és letiltása

A webes erőforrások hozzáférési szabályainak engedélyezése és letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Webfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Az ablak jobb oldalán válassza ki azt a szabályt, amelyet be, illetve ki szeretne kapcsolni.
4. Az **Státusz** 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.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

A webes erőforrások hozzáférési szabályainak áttelepítése az alkalmazás korábbi verzióiból

A Service Pack 1 Maintenance Release 1 vagy az alkalmazás korábbi verziója Kaspersky Endpoint Security 10 Service Pack 2 for Windows verzióra frissítésekor a webes erőforrások tartalmi kategóriáin alapuló webes erőforrások hozzáférési szabályainak áttelepítése az alábbiak szerint történik:

- A „Fórumok és csevegések”, a „Webes e-mail” és a „Közösségi hálózatok” tartalmi kategóriái közül egyen vagy többön alapuló hozzáférési szabályok az „Internetes kommunikációs média” webes erőforrás tartalmi kategóriába kerülnek.
- Az „Elektronikus áruházak” és a „Fizetési rendszerek” tartalmi kategóriái közül egyen vagy többön alapuló hozzáférési szabályok az „Elektronikus kereskedelem” 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.

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 kézileg új listát készítenie a webes erőforrások címeiről, amikor hozzáférési szabályt állít be. A webes erőforrások címeit tartalmazó lista exportálási és importálási lehetősége például akkor jöhet jól, ha hasonló paraméterekkel rendelkező hozzáférési szabályokat készít.

Webes erőforrások címlistájának exportálása fájlba:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalán, a **Biztonsági felügyelet** részben válassza ki a **Webfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Válassza ki azt a szabályt, amelynél a webes erőforrások címlistáját fájlba szeretné exportálni.
4. Kattintson a **Szerkesztés** gombra.

   Megnyílik a **Szabály a webes erőforrásokhoz való hozzáférésre** ablak.
5. Ha nem szeretné a teljes címlistát exportálni, hanem csak egy részét, válassza ki a szükséges webes erőforrások címeit.
6. Kattintson a webes erőforrások címlistáját tartalmazó mezőtől jobbra lévő gombra.

   Megnyílik a művelet megerősítését kérő ablak.
7. Végezze el az alábbiak egyikét:

   - Ha a webes erőforrások címlistájáról csak a kijelölt elemeket szeretné exportálni, kattintson a művelet megerősítését kérő ablakban az **Igen** gombra.
   - Ha a webes erőforrások címlistáján lévő összes elemet exportálni szeretné, kattintson a művelet megerősítését kérő ablakban a **Nem** gombra.

     Megnyílik a Microsoft Office-ban szokásos **Mentés másként** ablak.
8. Válassza ki a Microsoft Windows **Mentés másként** ablakában azt a fájlt, amelybe a webes erőforrások címlistáját exportálni szeretné. Kattintson a **Mentés** gombra.

Webes erőforrások címlistájának importálása fájlból szabályba:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldalán, a **Biztonsági felügyelet** részben válassza ki a **Webfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Végezze el az alábbiak egyikét:

   - Ha webes erőforrások új hozzáférési szabályát szeretné létrehozni, kattintson a **Hozzáadás** gombra
   - Válassza ki a webes erőforrások szerkeszteni kívánt hozzáférési szabályát. Ezután kattintson a **Szerkesztés** gombra.

Megnyílik a **Szabály a webes erőforrásokhoz való hozzáférésre** ablak.

4. Végezze el az alábbiak egyikét:

   - Ha webes erőforrások új hozzáférési szabályát hozza létre, válassza ki az **Egyedi címekre** elemet az **Alkalmazás a következő címekre** legördülő listán.

   - Ha webes erőforrások hozzáférési szabályát szerkeszti, lépjen a jelen utasítások 5. lépésére.

5. Kattintson a webes erőforrások címlistáját tartalmazó mezőtől jobbra lévő gombra.

   Ha új szabályt hoz létre, megnyílik a Microsoft Windows szokásos **Fájl megnyitása** ablaka.

   Ha szabályt szerkeszt, megnyílik egy megerősítést kérő ablak.

6. Végezze el az alábbiak egyikét:

   - Ha webes erőforrások új hozzáférési szabályát szerkeszti, lépjen a jelen utasítások 7. lépésére.

   - Ha webes erőforrások hozzáférési szabályát szerkeszti, a művelet megerősítését kérő ablakban végezze el az alábbi műveletek egyikét:

     - Ha a webes erőforrások címlistáján lévő importált elemeket hozzá szeretné adni a meglévőkhöz, kattintson az **Igen** gombra.

     - Ha a webes erőforrások címlistáján a meglévő elemeket törölni szeretné, az importáltakat pedig hozzáadni, kattintson a **Nem** gombra.

   Megnyílik a **Fájl megnyitása** ablak a Microsoft Windowsban.

7. A Microsoft Windows **Fájl megnyitása** ablakában válassza ki az webes erőforrások importálni kívánt címlistáját tartalmazó fájlt.

8. Kattintson a **Megnyitás** gombra.

9. Kattintson a **Szabály a webes erőforrásokhoz való hozzáférésre** ablakban az **OK** gombra.

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.pelda.com/page_0-9abcdef.html.

   Ha `*` karaktert szeretne a címmaszkban szerepeltetni, írja be kétszer a `*` karaktert.

2. A címmaszk elején álló `www.` Karaktersorozatot a rendszer `*.` sorozatként értelmezi.

   Példa: a www.pelda.com címmaszkot a rendszer *.pelda.com címmaszkként kezeli.

3. Ha egy címmaszk nem * karakterrel kezdődik, akkor a címmaszk tartalma megegyezik a *. előtaggal ellátott azonos tartalommal.

4. A címmaszk elején lévő *. karaktersorozatot a rendszer *. karakterekként vagy üres karakterláncként értelmezi.

   Példa: a http://www.*.pelda.com címmaszk lefedi a http://www2.pelda.com címet is.

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.example.com/abc, ahol az a, b és c bármilyen karakter lehet.

6. Ha egy címmaszk / karakterre végződik, akkor a címmaszk tartalma megegyezik a **. utótaggal ellátott azonos tartalommal.

7. A címmaszk végén lévő /* karaktersorozatot a rendszer /* karakterekként vagy üres karakterláncként értelmezi.

8. A webes erőforrások címeinek ellenőrzése címmaszk alapján történik, figyelembe véve a protokollt is (http vagy https):

   - Ha a címmaszkban nem szerepel a hálózati protokoll, akkor bármilyen hálózati protokollt tartalmazó címeket lefedi.

     Példa: a pelda.com címmaszk lefedi a http://pelda.com és a https://pelda.com címeket.

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

     Példa: a http://*.pelda.com címmaszk lefedi 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	*.pelda.com	http://www.123example.com	Nem	Lásd: 1. szabály.
2	*.pelda.com	http://www.123.example.com	Igen	Lásd: 1. 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: 2., 1. szabály.
7	www.pelda.com	https://www.pelda.com	Igen	Lásd: 2., 1. szabály.
8	http://www.*.pelda.com	http://123.pelda.com	Igen	Lásd: 2., 4., 1. szabály.

9	www.pelda.com	http://www.example.com/abc	Igen	Lásd: 2., 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 Webfelügyelő üzenetsablonjainak szerkesztése

A Webfelügyelő szabályainak tulajdonságaiban megadott művelet típusától függően a Kaspersky Endpoint Security az alábbi típusú üzenetek egyikét jeleníti meg, ha a felhasználó internetes erőforrásokhoz próbál hozzáférni (az alkalmazás felváltja azt üzenetet tartalmazó HTML oldallal a HTTP kiszolgáló válaszát):

- Figyelmeztető üzenet. Ez az üzenet figyelmezteti a felhasználót, hogy a webes erőforrást nem ajánlott felkeresni és / vagy ellentétes a vállalati biztonsági szabályzattal. A Kaspersky Endpoint Security akkor jelenít meg figyelmeztető üzenetet, ha a **Figyelmeztetés** lehetőség van kiválasztva a webes erőforrást leíró szabály beállításaiban lévő **Művelet** legördülő listán.

  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 beállításaiban lévő **Művelet** legördülő listán.

  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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Végpontfelügyelő** részben válassza ki a **Webfelügyelő** alpontot.

   Az ablak jobb oldali részén megjelennek a Webfelügyelő összetevő beállításai.
3. Az ablak jobb oldali részén kattintson a **Sablonok** gombra.

   Megnyílik az **Üzenetsablonok** ablak.

4. Végezze el az alábbiak egyikét:

   - Ha annak az üzenetnek a sablonját szeretné szerkeszteni, amely a webes erőforrás felkeresésének mellőzésére figyelmezteti a felhasználót, válassza ki a **Figyelmeztetés** lapot.

   - Ha annak az üzenetnek a sablonját szeretné szerkeszteni, amely a webes erőforráshoz való hozzáférés blokkolásáról tájékoztatja a felhasználót, válassza ki a **Blokkolás** lapot.

   - A rendszergazdának küldött üzenet sablonjának szerkesztéséhez válassza ki a **Üzenet a rendszergazdának** lapot.

5. Szerkessze az üzenetsablont. Használhatja a **Változó** legördülő listát, valamint az **Alapértelmezett** és a **Hivatkozás** (ez a gomb nem használható a **Üzenet a rendszergazdának** lapon) gombokat.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

KATA végponti érzékelő

A KATA végponti érzékelő összetevő beállításaihoz kizárólag a Kaspersky Security Center Adminisztrációs Konzolon lehet hozzáférni. Az összetevő használatához telepíteni kell az adminisztrációs bővítményt.

Ez a rész tájékoztatást nyújt a KATA végponti érzékelővel kapcsolatban, és ismerteti az összetevő be- és kikapcsolásának menetét.

A KATA végponti érzékelő

A *KATA végponti érzékelő* a Kaspersky Anti Targeted Attack Platform egyik összetevője. Ez a megoldás különféle fenyegetések – például célzott támadások – gyors észlelésére szolgál.

Az összetevő telepítése ügyfélszámítógépeken történik. Ezeken a számítógépeken az összetevő folyamatosan figyeli a folyamatokat, az aktív hálózati kapcsolatokat és a módosított fájlokat, és mindezen információkat továbbítja a Kaspersky Anti Targeted Attack Platform részére.

Az összetevő a következő operációs rendszereken működik:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

A Kaspersky Anti Targeted Attack Plaformmal kapcsolatos olyan további információkért, amik nem találhatóak meg a jelen dokumentumban, lásd a Kaspersky Anti Targeted Attack Plaform súgóját.

A KATA végponti érzékelőt tartalmazó számítógépek bejövő kapcsolatait közvetlenül a Kaspersky Anti Targeted Attack Platform kiszolgálótól kell engedélyezni proxykiszolgáló nélkül.

A KATA végponti érzékelő összetevő be- és kikapcsolása

A KATA végponti érzékelő összetevő be- és kikapcsolása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél a rendszabály beállításait szeretne szerkeszteni.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. A **Speciális beállítások** részben válassza ki a **KATA végponti érzékelő** alrészt.

7. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni a KATA végponti érzékelőt, jelölje be a **KATA végponti érzékelő** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni a KATA végponti érzékelőt, törölje a **KATA végponti érzékelő** jelölőnégyzetet.

8. Ha az előző lépésben bejelölte a **KATA végponti érzékelő** jelölőnégyzetet, akkor adja meg a **Kiszolgáló címe** mezőben a Kaspersky Anti Targeted Attack Platform kiszolgáló címét, mely az alábbi részekből áll:

   a. Protokoll neve

   b. A kiszolgáló IP-címe vagy teljesen megadott tartományneve (FQDN)

   c. A kiszolgálón lévő Windows Event Collector elérési útja

9. Kattintson az **OK** gombra.

10. Alkalmazza a rendszabályt.

    A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Adattitkosítás

Ha a Kaspersky Endpoint Security alkalmazást a Microsoft Windows for Workstations operációs rendszert futtató számítógépre telepíti, az adattitkosítási funkció teljes mértékben rendelkezésre áll. Ha a Kaspersky Endpoint Security alkalmazás Microsoft Windows for File Servers operációs rendszert futtató számítógépen van telepítve, csak a BitLocker meghajtótitkosítási technológiával történő merevlemeztitkosítás áll rendelkezésre.

Ez a rész a merevlemezek, a cserélhető meghajtók, valamint a számítógép helyi meghajtóin lévő fájlok és mappák titkosítását tárgyalja, és ismerteti, hogyan lehet a számítógép helyi meghajtóin lévő fájlok titkosítását és visszafejtését beállítani és elvégezni a Kaspersky Endpoint Security és a Kaspersky Endpoint Security adminisztrációs bővítmény segítségével.

Ha nincs hozzáférés a titkosított adatokhoz, akkor tekintse meg a titkosított adatokkal való munkavégzésre vonatkozó különleges utasításokat (Munkavégzés titkosított fájlokkal korlátozott fájltitkosítási funkció esetén, Munkavégzés titkosított eszközökkel, ha nincs hozzájuk hozzáférés).

Titkosítási beállítások megjelenítésének engedélyezése a Kaspersky Security Center rendszabályban

Titkosítási beállítások megjelenítésének engedélyezése a Kaspersky Security Center rendszabályban:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki az Adminisztrációs Konzol fájában lévő **Adminisztrációs kiszolgáló – <Számítógép neve>** csomópont helyi menüjében a **Megtekintés → Felület beállításai** elemet.

   Megnyílik a **Felület beállításai** ablak.
3. A **Felület beállításai** ablakban jelölje be a **Titkosítás és adatvédelem megjelenítése** jelölőnégyzetet.
4. Kattintson az **OK** gombra.

Az 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.

Ha a licenc lejárt, az alkalmazás nem titkosít új adatokat, a régebben titkosított adatok pedig titkosítva, használható állapotban maradnak. Ekkor az új adatok titkosításához a programot olyan új licenccel kell aktiválni, amely lehetővé teszi a titkosítás használatát.

Ha a licenc lejárt, a Végfelhasználói licencszerződést megszegte, illetve a kulcs, a Kaspersky Endpoint Security vagy a titkosítási összetevők törlésre kerültek, akkor a korábban titkosított fájlok titkosított állapota nem garantálható. Ennek az 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:

- **Fájlok titkosítása 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. A Kaspersky Security Center rendszabályának alkalmazását követően a Kaspersky Endpoint Security az alábbi fájlokat titkosítja és fejti vissza:
  - A listákra titkosítás és visszafejtés céljából egyedileg felvett fájlok.
  - A listákra titkosítás és visszafejtés céljából felvett mappákban tárolt fájlok.
  - külön alkalmazások által előállított fájlok.

  A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

- **Cserélhető meghajtók titkosítása**. Megadhat alapértelmezett titkosítási szabályt, melynek alapján az alkalmazás ugyanazt a műveletet végzi el minden cserélhető meghajtóval, illetve megadhat külön-külön titkosítási szabályokat az egyes cserélhető meghajtókhoz.

  Az alapértelmezett titkosítási szabály prioritása alacsonyabb, mint az egyes cserélhető meghajtókhoz készített titkosítási szabályoké. A megadott eszköztípusú cserélhető meghajtókhoz készített titkosítási szabályok prioritása alacsonyabb, mint a megadott eszközazonosítójú cserélhető meghajtókhoz készítetteké.

  Cserélhető meghajtón lévő fájlok titkosítási szabályának kiválasztásához a Kaspersky Endpoint Security ellenőrzi, hogy az eszköztípus vagy -azonosító ismert-e. Az alkalmazás ekkor elvégzi az alábbi műveletek közül valamelyiket:
  - Ha csak az eszköztípus ismert, az alkalmazás az adott eszköztípusú cserélhető meghajtókhoz készített titkosítási szabályt alkalmazza (ha van).
  - Ha csak az eszközazonosító ismert, az alkalmazás az adott eszközazonosítójú cserélhető meghajtókhoz készített titkosítási szabályt alkalmazza (ha van).
  - Ha az eszköztípus és -azonosító egyaránt ismert, az alkalmazás az adott eszközazonosítójú cserélhető meghajtókhoz készített titkosítási szabályt alkalmazza (ha van). Ha nincs ilyen szabály, de az adott eszköztípusú cserélhető meghajtókhoz készített titkosítási szabály van, az alkalmazás ezt a szabályt alkalmazza. Ha sem az adott eszközazonosítóhoz, sem az adott eszköztípushoz nincs megadva titkosítási szabály, az alkalmazás az alapértelmezett titkosítási szabályt alkalmazza.
  - Ha sem az eszköztípus, sem az eszközazonosító nem ismert, az alkalmazás az alapértelmezett titkosítási szabályt alkalmazza.

  Az alkalmazás segítségével a cserélhető meghajtókat előkészítheti a rajtuk tárolt adatok hordozható módban történő használatára. A hordozható mód engedélyezését követően a titkosítási funkcióval nem rendelkező számítógépekhez csatlakoztatott cserélhető meghajtókon lévő titkosított fájlokhoz is hozzáférhet.

  Az alkalmazás a Kaspersky Security Center rendszabály alkalmazásakor a titkosítási szabályban megadott műveletet végzi el.

- **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 archívumok 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.

- **Merevlemezek titkosítása**. 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 merevlemez-titkosítási szabályt, és listát készíthet a titkosításból kizárni kívánt merevlemezekről. A Kaspersky Endpoint Security a Kaspersky Security Center rendszabály alkalmazását követően elvégzi a merevlemezek szektoronkénti titkosítását. Az alkalmazás a merevlemezek összes logikai partícióját egyidejűleg titkosítja. A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

  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, illetve a helyi hálózati rendszergazda által a Hitelesítési ügynök-fiók kezelési feladatai segítségével létrehozott Hitelesítési ügynök-fiók felhasználónevét és jelszavát. Ezek a fiókok azon Microsoft Windows fiókokon alapulnak, amelyekkel a felhasználó az operációs rendszerbe bejelentkezik. Kezelheti a Hitelesítési ügynök-fiókokat, és használhat Single Sign-On (SSO) technológiát, melynek révén automatikusan bejelentkezhet az operációs rendszerbe a Hitelesítési ügynök-fiók 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. Működéséről további információ a *Kaspersky Security Center Rendszergazdai útmutatóban* található.

  > Az alkalmazás verziójának Kaspersky Endpoint Security 10 Service Pack 2 for Windows verzióra frissítésekor a Hitelesítési ügynök-fiókok listája nem kerül mentésre.

  A titkosított merevlemezekhez való hozzáférés csak olyan számítógépekről lehetséges, amelyeken a Kaspersky Endpoint Security merevlemez-titkosítási funkcióval van telepítve. Ez az óvintézkedés minimálisra csökkenti a titkosított merevlemezeken lévő adatok kiszivárgásának kockázatát, ha a vállalat helyi hálózatán kívül próbálnak hozzájuk férni.

A merevlemezeket és cserélhető meghajtókat titkosíthatja a **Csak a használt lemezterület titkosítása** funkció segítségével. E funkció csak új, korábban nem használt eszközök esetén javasolt. Ha már használatban lévő eszközön alkalmaz titkosítást, akkor javasolt az egész eszközt titkosítani. Ez gondoskodik az összes adat védelméről – azokról is, amelyeket már letörölt, de még visszakereshető információkat tartalmaznak.

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. Ily módon az új eszközökön új fájlok írásával párhuzamosan egy idő elteltével minden szektor titkosítva lesz, ha a számítógépen be van kapcsolva a szokásos titkosítás a **Csak a használt lemezterület titkosítása** funkcióval.

A fájlok visszafejtéséhez szükséges adatokat a számítógépet a titkosítás folyamán felügyelő Kaspersky Security Center Adminisztrációs kiszolgáló biztosítja. Ha a titkosított fájlokat tartalmazó számítógépet valamilyen okból más Adminisztrációs kiszolgáló felügyelte, és a titkosított fájlhoz egyszer sem fértek hozzá, akkor az alábbi módok egyikének segítségével lehet hozzáférést szerezni:

- titkosított objektumokhoz való hozzáférés kérése a helyi hálózati rendszergazdától;
- titkosított eszközökön lévő adatok helyreállítása a Visszaállító segédprogrammal;
- A számítógépet a titkosítás folyamán felügyelő Kaspersky Security Center Adminisztrációs kiszolgáló beállításainak visszaállítása biztonsági másolatból, és e beállítások alkalmazása a titkosított objektumokat tartalmazó számítógépet jelenleg felügyelő Adminisztrációs kiszolgálón.

Az alkalmazás titkosítás közben szervizfájlokat hoz létre. A merevlemez nem töredezett szabad területének nagyjából két-három százaléka 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.

A Kaspersky Endpoint Security és a Kaspersky Anti-Virus for UEFI titkosítási funkciói közti kompatibilitás nem támogatott. Az olyan számítógépek merevlemezeinek titkosítása, amelyen telepítve van a Kaspersky Anti-Virus for UEFI, működésképtelenné teszi a Kaspersky Anti-Virus for UEFI alkalmazást.

A titkosítási funkció korlátozásai

Az új partíciók létrehozása a titkosított merevlemezeken, valamint a meglévő partíciók formázása a titkosított merevlemezeken adatveszteséghez vezethet.

A merevlemezek Kaspersky lemeztitkosítási technológiával történő titkosítása a hardver- és szoftverkövetelményeknek meg nem felelő merevlemezeknél nem használható.

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.
- Az Intel® Rapid Start technológia és a hibernáló partíciót tartalmazó meghajtók még akkor is, ha az Intel® Rapid Start technológia ki van kapcsolva.
- Négynél több kiterjesztett partíciót tartalmazó MBR formátumú meghajtók.

- Nem a rendszert tartalmazó meghajtón található lapozófájl.
- Több rendszerrel indítható, egyszerre több telepített operációs rendszert tartalmazó rendszer.
- Dinamikus partíciók (csak az elsődleges partíciók támogatottak).
- 2%-nál kevesebb szabad, nem töredezett lemezterülettel rendelkező meghajtók.
- 512 vagy 4096 bájttól eltérő, 512 bájtot emuláló szektorméretű meghajtók.
- Hibrid meghajtók.

A titkosítási algoritmus módosítása

A Kaspersky Endpoint Security által az adattitkosításhoz használt titkosítási algoritmus a terjesztőkészletben található titkosítási könyvtáraktól függ.

A titkosítási algoritmus módosítása:

1. A titkosítási algoritmus megváltoztatásának megkezdése előtt fejtse vissza a Kaspersky Endpoint Security által titkosított objektumokat.

   A titkosítási algoritmus 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 bitszámú titkosítási könyvtárakat tartalmazó terjesztőkészletből.

A Single Sign-On (SSO) technológia engedélyezése

A Single Sign-On (SSO) technológia nem kompatibilis a fiókok bejelentkezési adatait szolgáltató harmadik felekkel.

A Single Sign-On (SSO) technológia engedélyezése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné kapcsolni a Single Sign-On (SSO) technológiát.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.

- Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Általános titkosítási beállítások** alrészt.
7. A **Általános titkosítási beállítások** alrészben kattintson a **Beállítás** gombra a **Jelszóbeállítások** részben.

   Ezzel megnyílik a **Hitelesítési ügynök** lap a **Titkosítási jelszó beállításai** ablakban.
8. Jelölje be a **Egyszeri bejelentkezés (SSO) technológia használata** jelölőnégyzetet.
9. Kattintson az **OK** gombra.
10. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.
11. Alkalmazza a rendszabályt.

    A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

A fájltitkosításra vonatkozó különleges szempontok

A fájltitkosítási funkció használata során vegye figyelembe az alábbiakat:

- A cserélhető meghajtók titkosításának előre megadott beállításait tartalmazó Kaspersky Security Center-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 állapotú fájlokat nem titkosítja és nem fejti vissza.
- A Kaspersky Endpoint Security csak az operációs rendszer helyi felhasználói profiljai esetén titkosítja és fejti vissza az előre megadott mappákban lévő fájlokat. A Kaspersky Endpoint Security a barangoló felhasználói profilok, a kötelező felhasználói profilok, az ideiglenes felhasználói profilok előre megadott mappáiban és az átirányított mappákban lévő fájlokat nem titkosítja és nem fejti vissza. A Kaspersky által titkosításra javasolt szokásos mappák listájához az alábbi mappák tartoznak:
  - Saját dokumentumok
  - Kedvencek
  - Cookie-k
  - Asztal
  - Ideiglenes Internet Explorer-fájlok
  - Ideiglenes fájlok
  - Outlook-fájlok
- 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%, %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 fájlok titkosítási feladata során nem kerül sor titkosításukra.

- 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

Fájlok titkosítása a számítógép helyi meghajtóin

A számítógép helyi meghajtóin lévő fájlok titkosítása akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. A számítógép helyi meghajtóin lévő fájlok titkosítása nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész a számítógép helyi meghajtóin lévő fájlok titkosítását tárgyalja, és ismerteti, hogyan lehet a számítógép helyi meghajtóin lévő fájlok titkosítását beállítani és elvégezni a Kaspersky Endpoint Security és a Kaspersky Endpoint Security Console Plug-in segítségével.

Fájlok titkosítása a számítógép helyi meghajtóin

A Kaspersky Endpoint Security nem támogatja azon fájlok titkosítását, amik tartalma a OneDrive cloud tárhelyen található, és blokkolja, hogy a titkosított fájlok OneDrive cloud tárhelyre történő másolását, ha ezek a fájlok nincsenek hozzáadva a visszafejtés szabályhoz.

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.

Fájlok titkosítása helyi meghajtókon:

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.
5. Kattintson duplán a házirend-tulajdonságok ablak megnyitásához.
6. Az **Adattitkosítás** részben válassza ki a **Fájl szintű titkosítás** lehetőséget.
7. Az ablak bal oldalán válassza ki a **Titkosítás** fület.
8. A **Titkosítási mód** legördülő listán válassza ki az **Alapértelmezett szabályok** elemet.
9. Kattintson a **Titkosítás** lapon a **Hozzáadás** gombra, a legördülő listán pedig válassza ki valamelyiket az alábbi elemek közül:
   a. Válassza ki az **Előre megadott mappák** elemet a Kaspersky szakértői által javasolt helyi felhasználói profilok mappáiban lévő fájlok titkosítási szabályhoz való hozzáadásához.
      Megnyílik az **Előre megadott mappák kiválasztása** ablak.
   b. Válassza ki az **Egyéni mappa** elemet kézileg beírt mappa elérési útvonalának titkosítási szabályhoz való hozzáadásához.
      Megnyílik az **Egyéni mappa hozzáadása** ablak.
   c. Válassza ki a **Fájlok kiterjesztés alapján** elemet fájlkiterjesztések titkosítási szabályhoz való hozzáadásához. A Kaspersky Endpoint Security csak a megadott kiterjesztésű új és módosult fájlokat titkosítja a számítógépen lévő összes helyi meghajtón.
      Megnyílik a **Fájlkiterjesztések listájának hozzáadása / szerkesztése** ablak.
   d. Válassza ki a **Fájlok kiterjesztéscsoportok alapján** elemet fájlkiterjesztések csoportjainak titkosítási szabályhoz való hozzáadásához. A Kaspersky Endpoint Security a kiterjesztéscsoportok listáján szereplő kiterjesztéssel rendelkező fájlokat titkosítja a számítógépen lévő összes helyi meghajtón.
      Megnyílik a **Fájlkiterjesztések csoportjainak kiválasztása** ablak.
10. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.
11. Alkalmazza a rendszabályt.
    A Kaspersky Security Center irányelv alkalmazásának részleteiért lásd a Kaspersky Security Center Súgót.

A rendszabály alkalmazását követően a Kaspersky Endpoint Security azonnal titkosítja a titkosítási szabályban szereplő, a visszafejtési szabályban pedig nem szereplő fájlokat.

> 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 Kaspersky Endpoint Security akkor titkosítja a titkosítatlan fájlokat, ha tulajdonságaik (fájl elérési útvonala/neve/kiterjesztése) a módosítást követően továbbra is megfelelnek a titkosítási szabály feltételeinek.

A Kaspersky Endpoint Security a megnyitott fájlok titkosítását bezárásukig elhalasztja.

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.

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.

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 Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a titkosított fájlokhoz való hozzáférési szabályokat alkalmazások számára.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Fájlok és mappák titkosítása** alrészt.
7. A **Titkosítási mód** legördülő listán válassza ki az **Alapértelmezett szabályok** elemet.

   A hozzáférési szabályok alkalmazására kizárólag **Alapértelmezett szabályok** módban kerül sor. Ha a hozzáférési szabályok **Alapértelmezett szabályok** módban történő alkalmazását követően átvált **Maradjon változatlan** módba, a Kaspersky Endpoint Security minden hozzáférési szabályt figyelmen kívül hagy. Minden alkalmazás minden titkosított fájlhoz hozzáfér.

8. Az ablak jobb oldalán válassza ki az **Alkalmazások szabályai** lapot.
9. 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.

   Megnyílik az **Alkalmazások hozzáadása a Kaspersky Security Center listából** ablak.

   Végezze el az alábbiakat:

   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. Jelölje be az **Alkalmazások** oszlopban azokkal az alkalmazásokkal szemben lévő jelölőnégyzeteket, amelyekhez titkosított fájlokra vonatkozó hozzáférési szabályt szeretne kialakítani.

   d. Válassza ki az **Szabály az alkalmazás(ok)hoz** legördülő listán azt a szabályt, amely az alkalmazások titkosított fájlokhoz való hozzáférését megszabja.

e. 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.

f. Kattintson az **OK** gombra.

Az alkalmazások titkosított fájlokhoz való hozzáférési szabályainak adatai az **Alkalmazások szabályai** lapon lévő táblázatban jelennek meg.

10. Ha kézileg szeretne alkalmazásokat választani, kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki az **Egyéni alkalmazások** elemet.

    Megnyílik az **Alkalmazások végrehajtható-fájl neveinek hozzáadása / szerkesztése** ablak.

    Végezze el az alábbiakat:

    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 az **Szabály az alkalmazás(ok)hoz** legördülő listán azt a szabályt, amely az alkalmazások titkosított fájlokhoz való hozzáférését megszabja.

    d. Kattintson az **OK** gombra.

    Az alkalmazások titkosított fájlokhoz való hozzáférési szabályainak adatai az **Alkalmazások szabályai** lapon lévő táblázatban jelennek meg.

11. A módosítások mentéséhez kattintson az **OK** gombra.

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 Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani az adott alkalmazások által létrehozott fájlok titkosítását.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Fájlok és mappák titkosítása** alrészt.

7. A **Titkosítási mód** legördülő listán válassza ki az **Alapértelmezett szabályok** elemet.

   A titkosítási szabályok alkalmazására kizárólag **Alapértelmezett szabályok** módban kerül sor. Ha a titkosítási szabályok **Alapértelmezett szabályok** 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.

8. Az ablak jobb oldalán válassza ki az **Alkalmazások szabályai** lapot.

9. 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.

   Megnyílik az **Alkalmazások hozzáadása a Kaspersky Security Center listából** ablak.

   Végezze el az alábbiakat:

   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. Jelölje be az **Alkalmazások** oszlopban azokkal az alkalmazásokkal szemben lévő jelölőnégyzeteket, amelyek által létrehozott fájlokat titkosítani szeretné.

   d. Az **Szabály az alkalmazás(ok)hoz** 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.

   f. Kattintson az **OK** gombra.

   A kiválasztott alkalmazások által létrehozott és módosított fájlok titkosítási szabályára vonatkozó információk megjelennek az **Alkalmazások szabályai** lapon lévő táblázatban.

10. Ha kézileg szeretne alkalmazásokat választani, kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki az **Egyéni alkalmazások** elemet.

    Megnyílik az **Alkalmazások végrehajtható-fájl neveinek hozzáadása / szerkesztése** ablak.

    Végezze el az alábbiakat:

    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. Az **Szabály az alkalmazás(ok)hoz** legördülő listán válassza ki az **Összes létrehozott fájl titkosítása** elemet.

d. Kattintson az **OK** gombra.

A kiválasztott alkalmazások által létrehozott és módosított fájlok titkosítási szabályára vonatkozó információk megjelennek az **Alkalmazások szabályai** lapon lévő táblázatban.

11. A módosítások mentéséhez kattintson az **OK** gombra.

Visszafejtési szabály előállítása

Visszafejtési szabály előállítása:

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.
5. Kattintson duplán a házirend-tulajdonságok ablak megnyitásához.
6. Az **Adattitkosítás** részben válassza ki a **Fájl szintű titkosítás** lehetőséget.
7. Az ablak bal oldalán válassza ki a **Visszafejtés** fület.
8. A **Titkosítási mód** legördülő listán válassza ki az **Alapértelmezett szabályok** elemet.
9. 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 Lab szakértői által javasolt helyi felhasználói profilok mappáiban lévő fájlok visszafejtési szabályhoz való hozzáadásához.

   Megnyílik az **Előre megadott mappák kiválasztása** ablak.

   b. Válassza ki az **Egyéni mappa** elemet kézileg beírt mappa elérési útvonalának visszafejtési szabályhoz való hozzáadásához.

   Megnyílik az **Egyéni mappa hozzáadása** ablak.

   c. Válassza ki a **Fájlok kiterjesztés alapján** elemet fájlkiterjesztések visszafejtési szabályhoz való hozzáadásához. A Kaspersky Endpoint Security nem titkosítja a megadott kiterjesztésű fájlokat a számítógépen lévő összes helyi meghajtón.

   Megnyílik a **Fájlkiterjesztések listájának hozzáadása / szerkesztése** ablak.

   d. Válassza ki a **Fájlok kiterjesztéscsoportok alapján** elemet fájlkiterjesztések csoportjainak visszafejtési szabályhoz való hozzáadásához. A Kaspersky Endpoint Security a kiterjesztéscsoportok listáján szereplő kiterjesztéssel rendelkező fájlokat nem titkosítja a számítógépeken lévő összes helyi meghajtón.

   Megnyílik a **Fájlkiterjesztések csoportjainak kiválasztása** ablak.

10. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.

11. Alkalmazza a rendszabályt.

    A Kaspersky Security Center irányelv alkalmazásának részleteiért lásd a Kaspersky Security Center Súgót.

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 Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a helyi meghajtókon lévő fájlok visszafejtését.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Fájlok és mappák titkosítása** alrészt.
7. Az ablak bal oldalán válassza ki a **Titkosítás** fület.
8. 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 egyszerre több elemet is törölhet. Ehhez válassza ki a kívánt fájlokat úgy, hogy a **CTRL** billentyűt lenyomva tartja, miközben a bal egérgombbal rájuk kattint, 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.
9. Fájlvisszafejtési lista kialakítása.
10. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.
11. Alkalmazza a rendszabályt.

A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

A rendszabály alkalmazását követően a Kaspersky Endpoint Security azonnal visszafejti a visszafejtési szabályba felvett titkosított fájlokat.

A Kaspersky Endpoint Security akkor fejti vissza a titkosított fájlokat, ha paramétereik (fájl elérési útvonala/neve/kiterjesztése) megváltoznak, és így egyeznek a visszafejtési listára felvett objektumok paramétereivel.

A Kaspersky Endpoint Security a megnyitott fájlok visszafejtését bezárásukig elhalasztja.

Titkosított csomagok létrehozása

A Kaspersky Endpoint Security nem végez fájltömörítést a titkosított csomagok létrehozása során.

Titkosított csomag létrehozása:

1. A Kaspersky Endpoint Security telepített példányát és bekapcsolt titkosítási funkciót tartalmazó számítógépen bármely fájlkezelővel kiválaszthatja a titkosított csomaghoz hozzáadni kívánt fájlokat és / vagy mappákat. Az egér jobb gombjával kattintva nyissa meg a helyi menüt.

2. Válassza ki a helyi menüben a **Hozzáadás titkosított csomaghoz** lehetőséget.

   Megnyílik a Microsoft Windows szokásos **Elérési út választása a titkosított csomag mentéséhez** párbeszédpanel.

3. A Microsoft Windows szokásos **Elérési út választása a titkosított csomag mentéséhez** párbeszédpanelén válassza ki a titkosított csomag mentési célmappáját a cserélhető meghajtón. Kattintson a **Mentés** gombra.

   Megnyílik a **Hozzáadás titkosított csomaghoz** ablak.

4. Gépelje be és erősítse meg a jelszót a **Hozzáadás titkosított csomaghoz** ablakban.

5. Kattintson a **Létrehozás** gombra.

   Elindul a titkosított csomag létrehozásának folyamata. A folyamat befejeztét követően a cserélhető meghajtó kiválasztott célmappájában egy önkicsomagoló jelszóval védett titkosított csomag lesz található.

Ha megszakítja a titkosított csomag létrehozását, a Kaspersky Endpoint Security az alábbi műveleteket végzi el:

1. Megszakítja a fájlok csomagba másolásának folyamatát, és minden folyamatban lévő csomagtitkosítási műveletet befejez, ha van ilyen.

2. Eltávolítja a csomag létrehozása és titkosítása során létrejött összes ideiglenes fájlt és magát a titkosított csomag fájlját.

3. Értesíti a felhasználót, hogy a titkosított csomag létrehozási folyamata kényszerítetten megszakadt.

Titkosított csomagok kibontása

Titkosított csomag kicsomagolása:

1. Válasszon ki bármely fájlkezelőben egy titkosított csomagot. Kattintson a Kicsomagoló varázsló elindításához.

   Megnyílik az **Jelszó megadása** ablak.

2. Adja meg a titkosított csomagot védő jelszót.

3. A **Jelszó megadása** ablakban kattintson az **OK** gombra.

   Ha a jelszó megadása sikerült, megnyílik a Microsoft Windows szokásos **Tallózás** párbeszédpanelje.

4. A Microsoft Windows szokásos **Tallózás** párbeszédpaneljén válassza ki a titkosított csomag kicsomagolásának célmappáját, majd kattintson az **OK** gombra.

   Elkezdődik a titkosított csomag célmappába történő kicsomagolási folyamata.

Ha a titkosított csomag korábban már kicsomagolásra került a megadott célmappában, a mappában lévő fájlokat a titkosított csomagban lévő fájlok felülírják.

Ha megszakítja a titkosított csomag kicsomagolását, a Kaspersky Endpoint Security az alábbi műveleteket végzi el:

1. Leállítja a csomag visszafejtési folyamatát, és megszakítja a fájlok titkosított csomagból történő kimásolásának minden műveletét, ha vannak ilyenek.

2. Törli a titkosított csomag visszafejtése és kibontása során létrehozott összes ideiglenes fájlt, valamint a titkosított csomagból már a célmappába másolt összes fájlt.

3. Értesíti a felhasználót, hogy a titkosított csomag kicsomagolási folyamata kényszerítetten megszakadt.

Cserélhető meghajtók titkosítása

A cserélhető meghajtók titkosítása akkor használható, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. A cserélhető meghajtók titkosítása nem használható, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

Ez a rész a cserélhető meghajtók titkosítását tárgyalja, és ismerteti, hogyan lehet a cserélhető meghajtók titkosítását beállítani és elvégezni a Kaspersky Endpoint Security és a Kaspersky Endpoint Security adminisztrációs bővítmény segítségével.

Cserélhető meghajtók titkosításának megkezdése

Cserélhető meghajtók titkosítása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a cserélhető meghajtók titkosítását.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.

- Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Cserélhető meghajtók titkosítása** alrészt.

7. Válassza ki a **Titkosítási mód** legördülő listán azt az alapértelmezett műveletet, amelyet a Kaspersky Endpoint Security az összes olyan cserélhető meghajtókon tárolt fájlokon elvégez, amelyet a kiválasztott adminisztrációs csoportba tartozó számítógépeekhez csatlakoztatnak.

   - **Teljes cserélhető meghajtó titkosítása**. E lehetőség kiválasztása esetén a Kaspersky Security Center rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtók tartalmát szektoronként titkosítja. Ennek következtében az alkalmazás nem csupán a cserélhető meghajtókon tárolt fájlokat, hanem a cserélhető meghajtók fájlrendszereit is titkosítja, ideértve a fájlneveket és mappaszerkezeteket is. A Kaspersky Endpoint Security a már titkosított cserélhető meghajtókat nem titkosítja ismét.

     Ezt a titkosítási forgatókönyvet a Kaspersky Endpoint Security merevlemez-titkosítási funkciói teszik lehetővé.

   - **Összes fájl titkosítása**. E lehetőség kiválasztása esetén a Kaspersky Security Center 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 a már titkosított fájlokat. Az alkalmazás nem titkosítja a cserélhető meghajtók fájlrendszereit, így a titkosított fájlok neveit és a mappaszerkezeteket.

   - **Csak az új fájlok titkosítása**. E lehetőség kiválasztása esetén a Kaspersky Security Center 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.

   - **Teljes cserélhető meghajtó visszafejtése**. E lehetőség kiválasztása esetén a Kaspersky Security Center rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtókon lévő összes titkosított fájlt visszafejti a cserélhető meghajtók fájlrendszereivel együtt, ha azok titkosítására korábban sor került.

     Ezt a titkosítási forgatókönyvet a Kaspersky Endpoint Security fájltitkosítási és merevlemez-titkosítási funkciói teszik lehetővé.

   - **Maradjon változatlan**. E lehetőség kiválasztása esetén a Kaspersky Security Center rendszabály cserélhető meghajtókhoz megadott titkosítási beállításokkal történő alkalmazásakor a Kaspersky Endpoint Security a cserélhető meghajtókon nem titkosítja és nem fejti vissza a fájlokat.

8. Hozzon létre titkosítási szabályokat azon cserélhető meghajtókon lévő fájlokhoz, amelyek tartalmát titkosítani szeretné.

9. Alkalmazza a rendszabályt.

A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Ha a rendszabály alkalmazását követően a felhasználó cserélhető meghajtót csatlakoztat vagy már csatlakoztatva van ilyen, a Kaspersky Endpoint Security értesíti a felhasználót, hogy a cserélhető meghajtóra titkosítási szabály vonatkozik, mely szerint a cserélhető meghajtón tárolt titkosított fájlok titkosításra kerülnek.

Ha a *Maradjon változatlan* szabály van megadva a cserélhető meghajtó adatainak titkosításához, az alkalmazás nem jelenít meg értesítést a felhasználó részére.

Az alkalmazás figyelmezteti a felhasználót, hogy a titkosítás folyamata eltarthat egy ideig.

Az alkalmazás a titkosítási művelet megerősítését kéri a felhasználótól, és az alábbi műveleteket végzi el:

- Titkosítja az adatokat a rendszabály beállításai szerint, ha a felhasználó beleegyezik a titkosításba.
- Az adatokat titkosítás nélkül hagyja, ha a felhasználó nem fogadja el a titkosítást, és a cserélhető meghajtó fájljaihoz való hozzáférést csak olvashatóra korlátozza.
- Az adatokat titkosítás nélkül hagyja, ha a felhasználó figyelmen kívül hagyja a titkosításra vonatkozó kérdést, a cserélhető meghajtó fájljainak hozzáférését csak olvashatóra korlátozza, és ismét felkéri a felhasználót az adattitkosítás megerősítésére, amikor legközelebb sor kerül a Kaspersky Security Center rendszabály alkalmazására, illetve cserélhető meghajtó csatlakoztatására.

A cserélhető meghajtók adattitkosításának előre megadott beállításait tartalmazó Kaspersky Security Center-rendszabály a kezelt számítógépek egy adott csoportja számára van kialakítva. Emiatt az adattitkosítás eredménye cserélhető meghajtókon attól a számítógéptől függ, amelyhez a cserélhető meghajtót csatlakoztatja.

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.

Ha sikertelen egy cserélhető meghajtó titkosítása, tekintse meg az **Adattitkosítás** jelentést a Kaspersky Endpoint Security felületen. A fájlok elérését blokkolhatja egy másik alkalmazás. Ebben az esetben próbálja meg kihúzni a cserélhető meghajtót a számítógépből, majd dugja be újra.

Titkosítási szabály megadása cserélhető meghajtóknál

Titkosítási szabály megadása cserélhető meghajtóknál:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél cserélhető meghajtókra vonatkozó titkosítási szabályt szeretne megadni.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Cserélhető meghajtók titkosítása** alrészt.

7. Kattintson a bal egérgombbal 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.

     Megnyílik az **Eszközök hozzáadása a megbízható eszközök listából** ablak.

   - Ha olyan cserélhető meghajtóknál szeretne titkosítási szabályokat megadni, amelyek szerepelnek a Kaspersky Security Center listáján, válassza ki a **A Kaspersky Security Center eszközlistájából** lehetőséget.

     Megnyílik az **Eszközök hozzáadása a Kaspersky Security Center listából** ablak.

8. Ha az előző lépésben a **A Kaspersky Security Center eszközlistájából** lehetőséget választotta, adja meg az eszközök táblázatban való megjelenítéséhez a szűrőket. Ehhez:

   a. Adja meg a következő paraméterek értékeit: **Azon eszközök megjelenítése a táblázatban, melyekhez a következő meg van adva**, **Eszköztípus**, **Név**, **Számítógép** és **Kaspersky lemeztitkosítás**.

   b. Kattintson a **Frissítés** gombra.

9. Az **Eszköz típusa** oszlopban jelölje be a jelölőnégyzeteket azon cserélhető meghajtók nevei mellett, amelyeknél titkosítási szabályokat szeretne létrehozni.

10. Válassza ki a **Titkosítási mód a kiválasztott eszközökhöz** legördülő listán azt a műveletet, amelyet a Kaspersky Endpoint Security a kiválasztott cserélhető meghajtókon tárolt fájlokon végez.

11. 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.

12. 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 **Teljes cserélhető meghajtó titkosítása** módú rendszabály alkalmazását követően a fájlok által el nem foglalt szektorok továbbra sem lesznek titkosítva.

13. 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, válassza a **Frissítés** lehetőséget.

14. Kattintson az **OK** gombra.

A létrehozott titkosítási szabályok sorai az **Egyéni szabályok** táblázatban jelennek meg.

15. A módosítások mentéséhez kattintson az **OK** gombra.

A cserélhető meghajtók hozzáadott titkosítási szabályait a rendszer azokra a cserélhető meghajtókra alkalmazza, amelyeket a Kaspersky Security Center módosított rendszabálya által felügyelt bármely számítógéphez csatlakoztatnak.

Titkosítási szabály szerkesztése cserélhető meghajtóknál

Titkosítási szabály szerkesztése cserélhető meghajtónál:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél cserélhető meghajtókra vonatkozó titkosítási szabályt szeretne szerkeszteni.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Cserélhető meghajtók titkosítása** alrészt.
7. Válassza ki azon cserélhető meghajtók listáján, amelyekhez titkosítási szabályok vannak beállítva, a kívánt cserélhető meghajtóhoz tartozó bejegyzést.
8. Kattintson a **Szabály beállítása** gombra a kiválasztott cserélhető meghajtó titkosítási szabályának szerkesztéséhez.

   Megnyílik a **Szabály beállítása** gomb helyi menüje.
9. Válassza ki a **Szabály beállítása** gomb helyi menüjében azt a műveletet, amelyet a Kaspersky Endpoint Security a kiválasztott cserélhető meghajtón tárolt fájlokon végez.
10. A módosítások mentéséhez kattintson az **OK** gombra.

A cserélhető meghajtók módosított titkosítási szabályait a rendszer azokra a cserélhető meghajtókra alkalmazza, amelyeket a Kaspersky Security Center módosított rendszabálya által felügyelt bármely számítógéphez csatlakoztatnak.

Hordozható mód engedélyezése a cserélhető meghajtókon lévő titkosított fájlok eléréséhez

Hordozható mód engedélyezése a cserélhető meghajtókon lévő titkosított fájlok eléréséhez:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél engedélyezni szeretné a hordozható módot a cserélhető meghajtókon lévő titkosított fájlok eléréséhez.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Cserélhető meghajtók titkosítása** alrészt.

7. Jelölje be a **Hordozható mód** jelölőnégyzetet.

   A hordozható mód az összes fájl vagy csak az új fájlok titkosításához használható.

8. Kattintson az **OK** gombra.

9. Alkalmazza a rendszabályt.

   A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

10. Csatlakoztassa a cserélhető meghajtót egy olyan eszközhöz, amelyen a Kaspersky Security Center rendszabály alkalmazásra került.

11. Erősítse meg a cserélhető meghajtó titkosítási műveletét.

    Ekkor megnyílik egy ablak, ahol jelszót állíthat elő a Hordozható fájlkezelő számára.

12. Adjon meg a jelszóerősségi követelményekneki megfelelő jelszót, és erősítse meg.

13. Kattintson az **OK** gombra.

    A Kaspersky Endpoint Security a Kaspersky Security Center rendszabályban meghatározott titkosítási szabályoknak megfelelően titkosítja a cserélhető meghajtón lévő fájlokat. A titkosított fájlokkal való munkavégzéshez használt Hordozható fájlkezelő is a cserélhető meghajtóra kerül.

A hordozható mód engedélyezését követően a titkosítási funkcióval nem rendelkező számítógépekhez csatlakoztatott cserélhető meghajtókon lévő titkosított fájlokhoz is hozzáférhet.

Cserélhető meghajtók visszafejtése

Cserélhető meghajtók visszafejtése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a cserélhető meghajtók visszafejtését.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Cserélhető meghajtók titkosítása** alrészt.

7. Ha a cserélhető meghajtókon lévő összes titkosított fájlt vissza szeretné fejteni, válassza a **Titkosítási mód** legördülő listán a **Teljes cserélhető meghajtó visszafejtése** lehetőséget.

8. Ha egyes cserélhető meghajtókon lévő adatokat szeretne visszafejteni, szerkessze azon cserélhető meghajtók titkosítási szabályait, amelynek az adatait vissza szeretné fejteni. Ehhez:

   a. Válassza ki azon cserélhető meghajtók listáján, amelyekhez titkosítási szabályok vannak beállítva, a kívánt cserélhető meghajtóhoz tartozó bejegyzést.

   b. Kattintson a **Szabály beállítása** gombra a kiválasztott cserélhető meghajtó titkosítási szabályának szerkesztéséhez.

      Megnyílik a **Szabály beállítása** gomb helyi menüje.

   c. Válassza ki az **Összes fájl visszafejtése** elemet a **Szabály beállítása** gomb helyi menüjében.

9. A módosítások mentéséhez kattintson az **OK** gombra.

10. Alkalmazza a rendszabályt.

A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Ha a rendszabály alkalmazását követően a felhasználó cserélhető meghajtót csatlakoztat vagy már csatlakoztatva van ilyen, a Kaspersky Endpoint Security értesíti a felhasználót, hogy a cserélhető meghajtóra titkosítási szabály vonatkozik, mely szerint a rajta tárolt titkosított fájlok, valamint fájlrendszere (ha titkosítva van) visszafejtésre kerül. Az alkalmazás figyelmezteti a felhasználót, hogy a visszafejtés folyamata eltarthat egy ideig.

A cserélhető meghajtók adattitkosításának előre megadott beállításait tartalmazó Kaspersky Security Center-rendszabály a kezelt számítógépek egy adott csoportja számára van kialakítva. Emiatt az adatvisszafejtés eredménye cserélhető meghajtókon attól a számítógéptől függ, amelyhez a cserélhető meghajtót csatlakoztatja.

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.

Ha sikertelen egy cserélhető meghajtó visszafejtése, tekintse meg az **Adattitkosítás** jelentést a Kaspersky Endpoint Security felületen. A fájlok elérését blokkolhatja egy másik alkalmazás. Ebben az esetben próbálja meg kihúzni a cserélhető meghajtót a számítógépből, majd dugja be újra.

Merevlemezek titkosítása

Ha a Kaspersky Endpoint Security Microsoft Windows for Workstations rendszert futtató számítógépen van telepítve, akkor titkosításhoz felhasználhatja a BitLocker meghajtótitkosítási és a Kaspersky lemeztitkosítási technológiát. Ha a Kaspersky Endpoint Security alkalmazás Microsoft Windows for File Servers operációs rendszert futtató számítógépen van telepítve, csak a BitLocker meghajtótitkosítási technológia áll rendelkezésre.

Ez a rész a merevlemezek titkosítását tárgyalja, és ismerteti, hogyan lehet a merevlemezek titkosítását beállítani és elvégezni a Kaspersky Endpoint Security és a Kaspersky Endpoint Security Console Plug-in segítségével.

A merevlemezek titkosítása

A merevlemez titkosításának 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 és 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 merevlemez titkosítása 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 merevlemezek titkosítását. 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 merevlemez titkosítása 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 merevlemez titkosításának megkezdését követően a Kaspersky Endpoint Security a merevlemezekre írt összes adatot titkosítja.

Ha a merevlemez titkosítása 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 titkosítását.

Ha az operációs rendszer a merevlemezek titkosítása 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 titkosítását.

Ha az operációs rendszer a merevlemez titkosítása közben alvó módba lép, a Kaspersky Endpoint Security a Hitelesítési ügynök betöltése nélkül folytatja a merevlemez titkosítását, amikor az operációs rendszer kilép alvó módból.

A Hitelesítési ügynök segítségével kétféleképpen lehet a felhasználói hitelesítést elvégezni:

- Adja meg a hálózati rendszergazda által a Kaspersky Security Center eszközeivel létrehozott Hitelesítési ügynök-fiók felhasználónevét és jelszavát.
- Adja meg a token vagy a számítógéphez csatlakoztatott okoskártya jelszavát.

A Hitelesítési ügynök alábbi nyelvek billentyűzetkiosztásait támogatja:

- Angol (Egyesült Királyság)
- Angol (Egyesült Államok)
- Arab (Algéria, Marokkó, Tunézia; AZERTY kiosztás)
- Spanyol (Latin-Amerika)
- olasz
- Német (Németország és Ausztria)
- Német (Svájc)
- Portugál (Brazília, ABNT2 kiosztás)
- Orosz (105 gombos IBM/Windows billentyűzetek QWERTY kiosztással)
- Török (QWERTY kiosztás)
- Francia (Franciaország)
- Francia (Svájc)
- Francia (Belgium, AZERTY kiosztás)
- Japán (106 gombos billentyűzetek QWERTY kiosztással)

A Hitelesítési ügynökben akkor használható egy adott billentyűzetkiosztás, ha az meg van adva az operációs rendszer nyelvi és regionális beállításaiban, és a Microsoft Windows üdvözlő képernyőjén is használható.

Ha a Hitelesítési ügynök-fiók neve olyan szimbólumokat tartalmaz, amelyeket a Hitelesítési ügynökben rendelkezésre álló billentyűzetkiosztások segítségével nem lehet beírni, a titkosított merevlemezekhez csak azt követően lehet hozzáférni, hogy visszaállításra kerültek a Visszaállító segédprogrammal, illetve visszaállításra került a Hitelesítési ügynök-fiók felhasználóneve és jelszava.

A Kaspersky Endpoint Security a következő tokeneket, okoskártya-olvasókat és okoskártyákat támogatja:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)
- SafeNet eToken 4100 72K Java (Smart Card)

- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Merevlemezek titkosítása a Kaspersky lemeztitkosítási technológia segítségével

A számítógép merevlemezeinek titkosítása előtt javasolt ellenőrizni, hogy a számítógép nincs-e megfertőzve. Ehhez indítsa el a Teljes vizsgálat vagy a Kritikus területek vizsgálata feladatot. Rootkittel fertőzött számítógép merevlemezének titkosítása következtében a számítógép működésképtelenné válhat.

Merevlemezek titkosítása a Kaspersky lemeztitkosítási technológia segítségével:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a merevlemezek titkosítását.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Merevlemezek titkosítása** alrészt.
7. A **Titkosítási technológia** legördülő listán válassza ki az **Kaspersky lemeztitkosítás** lehetőséget.

A Kaspersky lemeztitkosítási technológia nem használható, ha a számítógépen BitLocker segítségével titkosított merevlemezek találhatók.

8. A **Titkosítási mód** legördülő listán válassza ki az **Összes merevlemez titkosítása** elemet.

Ha a titkosításból ki szeretne zárni néhány merevlemezt, készítsen listát ezekről a merevlemezekről.

9. 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 használt lemezterület titkosítása** jelölőnégyzetet.

  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 a teljes merevlemezt titkosítani szeretné, törölje a **Csak a használt lemezterület titkosítása** jelölőnégyzetet.

  Ez a funkció csak titkosítatlan eszközökre vonatkozik. Ha egy eszköz titkosítására korábban már sor került a **Csak a használt lemezterület titkosítása** funkcióval, akkor **Összes merevlemez titkosítása** módú rendszabály alkalmazását követően a fájlok által el nem foglalt szektorok továbbra sem lesznek titkosítva.

10. A módosítások mentéséhez kattintson az **OK** gombra.

11. Alkalmazza a rendszabályt.

    A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Merevlemezek titkosítása a BitLocker meghajtótitkosítási technológia segítségével

A számítógép merevlemezeinek titkosítása előtt javasolt ellenőrizni, hogy a számítógép nincs-e megfertőzve. Ehhez indítsa el a Teljes vizsgálat vagy a Kritikus területek vizsgálata feladatot. Rootkittel fertőzött számítógép merevlemezének titkosítása következtében a számítógép működésképtelenné válhat.

A kiszolgálói operációs rendszert futtató számítógépeken a BitLocker meghajtótitkosítási technológia használatához szükséges lehet a **BitLocker meghajtótitkosítás** összetevő telepítése a Szerepek és összetevők hozzáadása varázsló segítségével.

Merevlemezek titkosítása a BitLocker meghajtótitkosítási technológia segítségével:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a merevlemezek titkosítását.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Merevlemezek titkosítása** alrészt.

7. A **Titkosítási technológia** legördülő listán válassza ki az **BitLocker meghajtótitkosítás** lehetőséget.

8. A **Titkosítási mód** legördülő listán válassza ki az **Összes merevlemez titkosítása** elemet.

9. Ha rendszerindítási környezetben érintőképernyős billentyűzet segítségével szeretne adatokat beírni, jelölje be a **Táblagépeken rendszerindítás előtti billentyűzetbevitelt igénylő hitelesítés alkalmazása** jelölőnégyzetet.

   Javasoljuk, hogy ezt a beállítást csak olyan eszközöknél használja rendszerindítás előtti környezetben, amelyek alternatív adatbeviteli eszközöket – például UISB billentyűzetet – is tartalmaznak.

10. Válassza ki az alábbi titkosítási típusok egyikét:

    - Ha hardveres titkosítást szeretne használni, jelölje be a **Hardveres titkosítás használata** jelölőnégyzetet.
    - Ha szoftveres titkosítást szeretne használni, törölje a **Hardveres titkosítás használata** jelölőnégyzetet.

11. 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 használt lemezterület titkosítása** jelölőnégyzetet.
    - Ha a teljes merevlemezt titkosítani szeretné, törölje a **Csak a használt lemezterület titkosítása** jelölőnégyzetet.

      Ez a funkció csak titkosítatlan eszközökre vonatkozik. Ha egy eszköz titkosítására korábban már sor került a **Csak a használt lemezterület titkosítása** funkcióval, akkor **Összes merevlemez titkosítása** módú rendszabály alkalmazását követően a fájlok által el nem foglalt szektorok továbbra sem lesznek titkosítva.

12. Válassza ki a BitLocker segítségével titkosított merevlemezek hozzáférési módszerét.

    - Ha Trusted Platform Module (TPM) segítségével szeretne titkosítási kulcsokat tárolni, válassza a **Trusted Platform Module (TPM) használata** lehetőséget.
    - Ha a merevlemezek titkosítását nem Trusted Platform Module (TPM) segítségével végzi, válassza a **Jelszó használata** lehetőséget, és adja meg a **Jelszó minimális hossza** mezőben, hogy a jelszónak legalább hány karaktert kell tartalmaznia.

A Trusted Platform Module (TPM) rendelkezésre állása Windows 7 és Windows 2008 R2 operációs rendszereken és korábbi verziókon kötelező.

13. Ha az előző lépésben a **Trusted Platform Module (TPM) használata** lehetőséget választotta:

    - Ha be szeretné állítani, hogy a felhasználónak PIN-kódot kelljen megadnia, amikor titkosítási kulcshoz próbál hozzáférni, jelölje be a **PIN-kód használata** jelölőnégyzetet, és adja meg a **PIN-kód minimális hossza** mezőben, hogy a PIN-kódnak legalább hány számjegyet kell tartalmaznia.

    - Ha a számítógépen Trusted Platform Module nélkül, jelszóval szeretne titkosított merevlemezekhez hozzáférni, jelölje be a **Jelszó használata, ha a Trusted Platform Module (TPM) nem használható** jelölőnégyzetet, és adja meg a **Jelszó minimális hossza** mezőben, hogy a jelszónak legalább hány karaktert kell tartalmaznia.

      Ilyenkor a titkosítási kulcsokhoz való hozzáférésre a megadott jelszóval kerül sor, ugyanúgy, mint ha a **Jelszó használata** jelölőnégyzet van bejelölve.

      Ha a **Jelszó használata, ha a Trusted Platform Module (TPM) nem használható** jelölőnégyzet nincs bejelölve, és a Trusted Platform Module nem áll rendelkezésre, akkor a merevlemez titkosítása nem indul el.

14. A módosítások mentéséhez kattintson az **OK** gombra.

15. Alkalmazza a rendszabályt.

    A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Miután alkalmazta a rendszabályt azon az ügyfélszámítógépen, amelyen a Kaspersky Endpoint Security telepítve van, az alábbi lekérdezésekre kerül sor:

- Ha a titkosítási rendszabály rendszermerevlemezre vonatkozik, akkor megjelenik a PIN-kód ablaka, ha a Trusted Platform Module használatban van, egyébként pedig megjelenik a jelszót kérő ablak az előtöltés hitelesítéséhez.

- Ha a számítógép operációs rendszerén be van kapcsolva a Federal Information Processing szabványú kompatibilitási mód, akkor Windows 8 és újabb verzió esetén az operációs rendszer megjelenít egy USB eszközcsatlakoztatási kérési ablakot a visszaállítási kulcs fájljának mentéséhez.

Ha nincs hozzáférés a titkosítási kulcsokhoz, a felhasználó kérheti, hogy a helyi hálózati rendszergazda adjon neki visszaállítási kulcsot (amennyiben azt korábban nem mentette az USB eszközre, vagy elvesztette).

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 Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél a titkosításból kizárt merevlemezek listáját szeretné elkészíteni.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Merevlemezek titkosítása** alrészt.
7. A **Titkosítási technológia** legördülő listán válassza ki az **Kaspersky lemeztitkosítás** lehetőséget.

   A titkosításból kizárt merevlemezeknek megfelelő bejegyzések megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban. Ez a táblázat üres, ha korábban nem készített listát a titkosításból kizárt merevlemezekről.
8. Merevlemezek felvétele a titkosításból kizárt merevlemezek listájára:
   a. Kattintson a **Hozzáadás** gombra.

      Megnyílik az **Eszközök hozzáadása a Kaspersky Security Center listából** ablak.
   b. Adja meg az **Eszközök hozzáadása a Kaspersky Security Center listából** ablakban a következő paraméterek értékeit: **Név**, **Számítógép**, **Lemeztípus** és **Kaspersky lemeztitkosítás**.
   c. Kattintson a **Frissítés** gombra.
   d. Jelölje be a **Név** oszlopban azon merevlemezeknek megfelelő táblázatsorokban a jelölőnégyzeteket, amelyeket fel szeretne venni a titkosításból kizárt merevlemezek listájára.
   e. Kattintson az **OK** gombra.

   A kiválasztott merevlemezek megjelennek **Ne titkosítsa a következő merevlemezeket** táblázatban.
9. Ha a kizárások listájáról merevlemezeket szeretne eltávolítani, válasszon ki egy vagy több sort **Ne titkosítsa a következő merevlemezeket** táblázatban, és kattintson a **Törlés** gombra.

   Több sort úgy választhat ki a táblázatban, ha kijelölésük közben lenyomva tartja a **Ctrl** billentyűt.
10. A módosítások mentéséhez kattintson az **OK** gombra.

Merevlemez visszafejtése

A merevlemezeket akkor is vissza lehet fejteni, ha nincs adattitkosítást lehetővé tevő aktív licenc.

A merevlemezek visszafejtése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a merevlemezek visszafejtését.

3. A munkaterületen válassza ki a **Rendszabályok** lapot.

4. Válassza ki a szükséges rendszabályt.

5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:

   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

6. Az **Adattitkosítás** részben válassza ki a **Merevlemezek titkosítása** alrészt.

7. Válassza ki a **Titkosítási technológia** legördülő listán a merevlemezek titkosításához használt technológiát.

8. Végezze el az alábbiak egyikét:

   - Válassza ki a **Titkosítási mód** legördülő listán az **Összes merevlemez visszafejtése** lehetőséget, ha az összes titkosított merevlemezt vissza szeretné fejteni.
   - Adja hozzá a visszafejteni kívánt titkosított merevlemezeket **Ne titkosítsa a következő merevlemezeket** táblázathoz.

     Ez a lehetőség csak a Kaspersky lemeztitkosítási technológia esetén használható.

9. A módosítások mentéséhez kattintson az **OK** gombra.

10. Alkalmazza a rendszabályt.

    A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Ha a Kaspersky lemeztitkosítási technológia segítségével titkosított merevlemez visszafejtése közben a felhasználó leállítja vagy újraindítja a számítógépet, a Hitelesítési ügynök betöltődik az operációs rendszer legközelebbi indulása előtt. A Kaspersky Endpoint Security a Hitelesítési ügynökben történő sikeres hitelesítést és az operációs rendszer elindulását követően folytatja a merevlemez visszafejtését.

Ha az operációs rendszer a Kaspersky lemeztitkosítási technológia segítségével titkosított merevlemezek visszafejtése közben hibernált módba vált, a Hitelesítési ügynök betöltődik, amikor az operációs rendszer kilép a hibernált módból. A Kaspersky Endpoint Security a Hitelesítési ügynökben történő sikeres hitelesítést és az operációs rendszer elindulását követően folytatja a merevlemez visszafejtését. A merevlemez visszafejtését követően a hibernált mód az operációs rendszer első újraindításáig nem áll rendelkezésre.

Ha az operációs rendszer a merevlemez visszafejtése közben alvó módba lép, a Kaspersky Endpoint Security a Hitelesítési ügynök betöltése nélkül folytatja a merevlemez visszafejtését, amikor az operációs rendszer kilép alvó módból.

A Hitelesítési ügynök kezelése

Titkosított rendszermerevlemezek esetén a Hitelesítési ügynök az operációs rendszer elindulása előtt betöltődik. A Hitelesítési ügynök segítségével hitelesítést végezhet, így hozzáférést szerezhet a titkosított rendszermerevlemezekhez, és betöltheti az operációs rendszert.

A hitelesítési eljárás sikeres befejeztével betöltődik az operációs rendszer. A hitelesítési folyamatra az operációs rendszer újraindulásakor minden alkalommal sor kerül.

Egyes esetekben előfordulhat, hogy a felhasználó nem tudja elvégezni a hitelesítést. A hitelesítés például akkor nem lehetséges, ha a felhasználó elfelejtette a Hitelesítési ügynök-fiókhoz, illetve a tokenhez vagy okoskártyához tartozó hitelesítő adatokat, vagy elvesztette a tokent, illetve okoskártyát.

Ha a felhasználó elfelejtette Hitelesítési ügynök-fiókja hitelesítő adatait, illetve a token vagy okoskártya jelszavát, akkor a vállalati hálózati rendszergazdához kell fordulni visszaállításuk érdekében.

Ha egy felhasználó elvesztett egy tokent vagy okoskártyát, a rendszergazdának kötelező hozzáadnia a token vagy okoskártya elektronikus tanúsítványának fájlját a Hitelesítési ügynök-fiók létrehozására szolgáló parancshoz. Ezután a felhasználónak el kell végeznie a titkosított eszközökön lévő adatok visszaállítási folyamatát.

Token és okoskártya használata a Hitelesítési ügynökkel

A titkosított merevlemezekhez való hozzáféréshez token vagy okoskártya is használható. Ehhez a token vagy okoskártya elektronikus tanúsítványának fájlját meg kell adni a Hitelesítési ügynök-fiók létrehozására szolgáló parancsban.

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.

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.

  Ha a token vagy okoskártya elektronikus tanúsítványa nem felel meg ennek a követelménynek, az adminisztrációs bővítmény nem tölti be a tanúsítvány fájlját a Hitelesítési ügynök-fiók létrehozására szolgáló parancsba, és hibaüzenetet jelenít meg.

- A tanúsítvány célját meghatározó `KeyUsage` paraméterben `keyEncipherment` vagy `dataEncipherment` értéknek kell lennie.

  Ha a token vagy okoskártya elektronikus tanúsítványa nem felel meg ennek a követelménynek, az adminisztrációs bővítmény betölti a tanúsítvány fájlját a Hitelesítési ügynök-fiók létrehozására szolgáló parancsba, és figyelmeztető üzenetet jelenít meg.

- A tanúsítvány legalább 1024 bit hosszúságú RSA kulcsot tartalmaz.

  Ha a token vagy okoskártya elektronikus tanúsítványa nem felel meg ennek a követelménynek, az adminisztrációs bővítmény nem tölti be a tanúsítvány fájlját a Hitelesítési ügynök-fiók létrehozására szolgáló parancsba, és hibaüzenetet jelenít meg.

Hitelesítési ügynök súgóüzeneteinek szerkesztése

A Hitelesítési ügynök súgóüzeneteinek szerkesztése előtt tekintse át a rendszerindítás előtti környezetben támogatott karakterek listáját.

A Hitelesítési ügynök súgóüzeneteinek szerkesztése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél a Hitelesítési ügynök súgóüzeneteit szeretne szerkeszteni.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Általános titkosítási beállítások** alrészt.
7. A megnyíló **Sablonok** részben kattintson a **Súgó** gombra.
   Ezzel megnyílik a **Hitelesítési ügynök súgóüzenetei** ablak.
8. Végezze el az alábbiakat:
   - 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.
9. Szerkessze a súgóüzeneteket.
   Ha vissza szeretné állítani az eredeti szöveget, kattintson az **Alapértelmezett** gombra.
10. Kattintson az **OK** gombra.
11. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.

A Hitelesítési ügynök súgóüzenetiben lévő karakterek korlátozott támogatása

Rendszerindítás előtti környezetben az alábbi Unicode karakterek támogatottak:

- Alapszintű latin ábécé (0000–007F)

- Kiegészítő Latin-1 karakterek(0080–00FF)
- Kiterjesztett Latin-A (0100–017F)
- Kiterjesztett Latin-B (0180–024F)
- Nem kombinált kiterjesztett azonosító karakterek (02B0–02FF)
- Kombinált ékezetek (0300–036F)
- Görög és kopt ábécé (0370–03FF)
- Cirill (0400–04FF)
- Héber (0590–05FF)
- Arab írás (0600–06FF)
- Kiegészítő kiterjesztett latin (1E00–1EFF)
- Írásjelek (2000–206F)
- Pénznemek jelei (20A0–20CF)
- Betűszerű szimbólumok (2100–214F)
- Geometriai ábrák (25A0–25FF)
- Arab B írás bemutató formái (FE70–FEFF)

A listán nem szereplő karakterek a rendszerindítás előtti környezetben nem támogatottak. Ilyen karaktereket nem javasolt a Hitelesítési ügynök súgóüzeneteiben használni.

A Hitelesítési ügynök 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.

- **Bőbeszédű 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.

- **Bőbeszédű 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 kézileg elküldheti a Hitelesítési ügynök nyomkövetési fájlját a Kaspersky részére.

A Hitelesítési ügynök fiókok kezelése

A Kaspersky Security Center alábbi eszközeivel lehet a Hitelesítési ügynök-fiókokat kezelni:

- Csoportos feladat Hitelesítési ügynök-fiókok kezeléséhez. Ezzel a feladattal kezelheti a Hitelesítési ügynök-fiókokat ügyfélszámítógépek csoportjánál.
- **Titkosítás (fiókkezelés)** helyi feladat. Ezzel a feladattal kezelheti a Hitelesítési ügynök-fiókokat egyéni ügyfélszámítógépeknél.

A Hitelesítési ügynök-fiókok kezelési feladata beállításainak megadása:

1. Hitelesítési ügynök-fiók kezelési feladatának létrehozása (Helyi feladat létrehozása, Csoportos feladat létrehozása).
2. Nyissa meg a **Beállítások** részt a **Tulajdonságok: <a Hitelesítési ügynök-fiók kezelési feladatának neve>** ablakban.
3. Parancsok megadása Hitelesítési ügynök-fiók létrehozásához.
4. Parancsok megadása Hitelesítési ügynök-fiók szerkesztéséhez.

5. Parancsok megadása Hitelesítési ügynök felhasználói fiók törléséhez.

6. Szükség esetén a Hitelesítési ügynök-fiók kezeléséhez megadott parancsok szerkesztése. Ehhez válasszon ki egy parancsot a **Parancsok a Hitelesítési ügynök fiókok kezeléséhez** táblázatban, és kattintson a **Szerkesztés** gombra.

7. Szükség esetén a Hitelesítési ügynök-fiók kezeléséhez megadott parancsok törlése. Ehhez válasszon ki egy vagy több parancsot a **Parancsok a Hitelesítési ügynök fiókok kezeléséhez** táblázatban, és kattintson az **Eltávolítás** gombra.

   Több sort úgy választhat ki a táblázatban, ha kijelölésük közben lenyomva tartja a **Ctrl** billentyűt.

8. A módosítások mentéséhez kattintson az **OK** gombra a feladat tulajdonságainak ablakában.

9. A feladat futtatása.

Sor kerül a feladathoz hozzáadott, Hitelesítési ügynök-fiókok kezelésére szolgáló parancsok végrehajtására.

Parancs megadása Hitelesítési ügynök-fiók létrehozásához

Parancs megadása Hitelesítési ügynök-fiók létrehozásához:

1. Nyissa meg a **Beállítások** részt a **Tulajdonságok: <a Hitelesítési ügynök-fiók kezelési feladatának neve>** ablakban.

2. Kattintson a **Hozzáadás** gombra, a legördülő listán pedig válassza ki a **Fiók hozzáadása parancs** lehetőséget.

   Megnyílik az **Felhasználói fiók hozzáadása** ablak.

3. Adja meg a **Felhasználói fiók hozzáadása** mezőben a **Windows fiók** ablakban annak a Microsoft Windows fiók nevét, melynek alapján a Hitelesítési ügynök-fiók létrejön.

   Ehhez gépelje be kézileg a fiók nevét, vagy kattintson a **Kijelölés** gombra.

4. Ha kézileg írta be valamelyik Microsoft Windows fiókot, kattintson az **Engedélyezés** gombra a fiók biztonsági azonosítójának (SID) megállapításához.

   Ha úgy dönt, hogy nem adja meg a biztonsági azonosítót (SID) az **Engedélyezés** gombra kattintva, akkor megállapítására a feladat számítógépen való elvégzésekor kerül sor.

   A Hitelesítési ügynök-fiók létrehozási parancsának megadása során a Microsoft Windows fiók SID értékének megállapítása révén kényelmesen ellenőrizheti, hogy a kézileg megadott Microsoft Windows fióknév helyes-e. Ha a megadott Microsoft Windows felhasználói fiók nem létezik, nem megbízható tartományhoz tartozik, illetve nem azon a számítógépen található, amelynél a **Titkosítás (fiókkezelés)** helyi feladat módosítása történik, a Hitelesítési ügynök-fiók kezelési feladata hibával véget ér.

5. Jelölje be a **Az aktuális felhasználói fiók módosítása** jelölőnégyzetet, ha azt szeretné, hogy a Hitelesítési ügynök számára korábban létrehozott azonos nevű 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 használható, ha a Hitelesítési ügynök-fiók létrehozási parancsát **Titkosítás (fiókkezelés)** helyi feladat tulajdonságaiban adja meg.

6. Gépelje be a **Felhasználónév** mezőbe a Hitelesítési ügynök-fiók nevét, melyet a hitelesítés során a titkosított merevlemezekhez való hozzáféréshez meg kell adni.

7. 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.

8. Ha az előző lépésben bejelölte a **Jelszóalapú hitelesítés engedélyezése** jelölőnégyzetet:

   a. Gépelje be a **Jelszó** mezőbe a Hitelesítési ügynök-fiók jelszavát, melyet a hitelesítés során a titkosított merevlemezekhez való hozzáféréshez meg kell adni.

   b. Erősítse meg a **Jelszó megerősítése** mezőben a Hitelesítési ügynök-fiók előző lépésben megadott jelszavát.

   c. Végezze el az alábbiak egyikét:

      - Válassza ki a **Jelszó módosítása az első hitelesítéskor** lehetőséget, ha azt szeretné, hogy az alkalmazás a parancsban megadott fiókban az első alkalommal hitelesítést végző felhasználót felkérje a jelszó módosítására.

      - Ha ezt nem szeretné, válassza a **Nincs szükség jelszómódosításra** lehetőséget.

9. Jelölje be a **Tanúsítványalapú hitelesítés engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a titkosított merevlemezekhez való hozzáférés céljából történő hitelesítés során felkérje a felhasználót, hogy csatlakoztasson a számítógéphez tokent vagy okoskártyát.

10. Ha az előző lépésben bejelölte a **Tanúsítványalapú hitelesítés engedélyezése** jelölőnégyzetet, kattintson a **Tallózás** gombra, és válassza ki a token vagy okoskártya elektronikus tanúsítványának fájlját a **Tanúsítványfájl kiválasztása** ablakban.

11. Szükség esetén adja meg a **Parancs leírása** mezőben a Hitelesítési ügynök-fiók azon adatait, amelyek a parancs kezeléséhez szükségesek.

12. Végezze el az alábbiak egyikét:

    - Jelölje be a **Hitelesítés engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a parancsban megadott fiókban dolgozó felhasználó számára engedélyezze a Hitelesítési ügynök hitelesítési párbeszédpanelének elérését.

    - Jelölje be a **Hitelesítés blokkolása** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a parancsban megadott fiókban dolgozó felhasználónál blokkolja a Hitelesítési ügynök hitelesítési párbeszédpanelének elérését.

13. A **Felhasználói fiók hozzáadása** ablakban kattintson az **OK** gombra.

Hitelesítési ügynök-fiókot szerkesztő parancs megadása

Parancs megadása Hitelesítési ügynök-fiók szerkesztéséhez:

1. Nyissa meg a **Beállítások** részben a **Tulajdonságok: <a Hitelesítési ügynök-fiók kezelési feladata>** ablakban lévő **Hozzáadás** gomb helyi menüjét, és válassza ki a **Fiókszerkesztési parancs** elemet.

   Megnyílik az **Felhasználói fiók szerkesztése** ablak.

2. Adja meg a **Felhasználói fiók szerkesztése** mezőben a **Windows fiók** ablakban annak a Microsoft Windows fiók nevét, melynek alapján a szerkeszteni kívánt Hitelesítési ügynök-fiók létrejött. Ehhez gépelje be kézileg a fiók nevét, vagy kattintson a **Kijelölés** gombra.

3. Ha kézileg írta be valamelyik Microsoft Windows felhasználói fiókot, kattintson az **Engedélyezés** gombra a fiók biztonsági azonosítójának (SID) megállapításához.

   Ha úgy dönt, hogy nem adja meg a biztonsági azonosítót (SID) az **Engedélyezés** gombra kattintva, akkor megállapítására a feladat számítógépen való elvégzésekor kerül sor.

   A Hitelesítési ügynök-fiók szerkesztési parancsának megadása során a Microsoft Windows felhasználói fiók SID értékének megállapítása révén kényelmesen ellenőrizheti, hogy a kézileg megadott Microsoft Windows fióknév helyes-e. Ha a megadott Microsoft Windows fiók nem létezik vagy nem megbízható tartományhoz tartozik, a Hitelesítési ügynök-fiók kezelési feladata hibával véget ér.

4. Jelölje be a **Felhasználónév módosítása** jelölőnégyzetet, és adja meg a Hitelesítési ügynök-fiók új nevét, ha azt szeretné, hogy a Kaspersky Endpoint Security a lenti mezőbe begépelt névre módosítsa a felhasználónevet minden olyan Hitelesítési ügynök-fióknál, amely a **Windows fiók** mezőben feltüntetett nevű Microsoft Windows fiók segítségével jött létre.

5. Jelölje be a **Jelszóalapú hitelesítés beállításainak módosítása** jelölőnégyzetet, ha a jelszóalapú hitelesítési beállításokat szerkeszthetővé szeretné tenni.

6. 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.

7. Ha az előző lépésben bejelölte a **Jelszóalapú hitelesítés engedélyezése** jelölőnégyzetet:

   a. A **Jelszó** mezőben adja meg a Hitelesítési ügynök-fiók új jelszavát.

   b. Erősítse meg a **Jelszó megerősítése** mezőben az előző lépésben megadott jelszót.

8. 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.

9. Adja meg a jelszómódosítási beállítás Hitelesítési ügynökben történő hitelesítés esetén felvett értékét.

10. Jelölje be a **Tanúsítványalapú hitelesítés beállításainak módosítása** jelölőnégyzetet, ha a token vagy okoskártya elektronikus tanúsítványa alapján történő hitelesítési beállításokat szerkeszthetővé szeretné tenni.

11. 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.

12. Ha az előző lépésben bejelölte a **Tanúsítványalapú hitelesítés engedélyezése** jelölőnégyzetet, kattintson a **Tallózás** gombra, és válassza ki a token vagy okoskártya elektronikus tanúsítványának fájlját a **Tanúsítványfájl kiválasztása** ablakban.

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. A **Felhasználói fiók szerkesztése** ablakban kattintson az **OK** gombra.

Parancs megadása Hitelesítési ügynök-fiók törléséhez

Parancs megadása Hitelesítési ügynök-fiók törléséhez:

1. Nyissa meg a **Beállítások** részben a **Tulajdonságok: <a Hitelesítési ügynök-fiók kezelési feladata>** ablakban lévő **Hozzáadás** gomb helyi menüjét, és válassza ki a **Fiók törlése parancs** elemet.

   Megnyílik a **Felhasználói fiók törlése** ablak.

2. Adja meg a **Felhasználói fiók törlése** mezőben a **Windows fiók** ablakban annak a Microsoft Windows fiók nevét, melynek alapján a törölni kívánt Hitelesítési ügynök-fiók létrejött. Ehhez gépelje be kézileg a fiók nevét, vagy kattintson a **Kijelölés** gombra.

3. Ha kézileg írta be valamelyik Microsoft Windows felhasználói fiókot, kattintson az **Engedélyezés** gombra a fiók biztonsági azonosítójának (SID) megállapításához.

   Ha úgy dönt, hogy nem adja meg a biztonsági azonosítót (SID) az **Engedélyezés** gombra kattintva, akkor megállapítására a feladat számítógépen való elvégzésekor kerül sor.

   A Hitelesítési ügynök-fiók törlési parancsának megadása során a Microsoft Windows felhasználói fiók SID értékének megállapítása révén kényelmesen ellenőrizheti, hogy a kézileg megadott Microsoft Windows fióknév helyes-e. Ha a megadott Microsoft Windows fiók nem létezik vagy nem megbízható tartományhoz tartozik, a Hitelesítési ügynök-fiók kezelési feladata hibával véget ér.

4. A **Felhasználói fiók törlése** ablakban kattintson az **OK** gombra.

A Hitelesítési ügynök-fiók hitelesítő adatainak visszaállítása

Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

A Hitelesítési ügynök-fiók felhasználónevének és jelszavának visszaállítása:

1. A Hitelesítési ügynök a titkosított merevlemezeket tartalmazó számítógépen az operációs rendszer betöltődése előtt töltődik be. Kattintson a Hitelesítési ügynök felületén az **Elfelejtettem a jelszót** gombra a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítási folyamatának megkezdéséhez.

2. A Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítási kérési egységeinek beszerzéséhez kövesse a Hitelesítési ügynök utasításait.

3. Diktálja be a kérési blokkok tartalmát a számítógép nevével együtt a vállalati helyi hálózati rendszergazdának.

4. Adja meg a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítási kérésére kapott válasz részeit, amelyeket a helyi hálózati rendszergazda állított elő és adott át Önnek.

5. Adja meg a Hitelesítési ügynök-fiók új jelszavát, majd erősítse meg.

   A Hitelesítési ügynök-fiókhoz tartozó felhasználónév a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítási kérésére kapott válasz részeinek segítségével van megadva.

Miután megadta és megerősítette a Hitelesítési ügynök-fiókhoz tartozó új jelszót, a jelszót a rendszer menti, Ön pedig hozzáférhet a titkosított merevlemezekhez.

Reagálás a Hitelesítési ügynök-fiók hitelesítési adatainak visszaállítására irányuló felhasználói kérésekre

A Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítási kérésére kapott válasz felhasználói részeinek elkészítése és elküldése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amely a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítását kérő felhasználó számítógépét tartalmazza.

3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki az **Eszközök** lapon a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítását kérő felhasználó számítógépét, majd a jobb egérgombbal nyissa meg a helyi menüt.

5. A helyi menüjében válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** lehetőséget.

   Megnyílik a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablak.

6. Válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablakban a **Hitelesítési ügynök** lapot.

7. Válassza ki a **Használatban lévő titkosító algoritmus** részben a titkosítási algoritmus típusát.

8. Válassza ki a **Fiók** legördülő listán azon felhasználó számára létrehozott Hitelesítési ügynök-fiók nevét, aki a Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítását kéri.

9. Válassza ki a **Merevlemez** legördülő listán azt a titkosított merevlemezt, amelyhez vissza szeretné állítani a hozzáférést.

10. Adja meg a **Felhasználói kérés** részben a felhasználó által bediktált kérésblokkokat.

    A Hitelesítési ügynök-fiókhoz tartozó felhasználónév és jelszó visszaállítási kérésére kapott válasz részeinek tartalma a **Hozzáférési kulcs** mezőben jelenik meg.

11. Diktálja be a válasz blokkjainak tartalmát a felhasználónak.

Az adattitkosítási részletek megtekintése

Ez a rész ismerteti, hogyan lehet megtekinteni az adattitkosítás részleteit.

A titkosítási állapot

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:

- *Rendszabály nincs definiálva*. A számítógépen nincs Kaspersky Security Center rendszabály definiálva.
- *Titkosítás/visszafejtés folyamatban*. 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 és / vagy -visszafejtés a Kaspersky Security Center számítógépre alkalmazott rendszabályában megadott titkosítási beállításoknak megfelelően elkészült.
- *Felhasználó által megszakítva*. A felhasználó nem erősítette meg a fájltitkosítási műveletet a cserélhető meghajtón.
- *Nem támogatott*. A számítógépen nem áll rendelkezésre adattitkosítási funkció.

A titkosítási állapot megtekintése

A számítógép adatai titkosítási állapotának megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott számítógép tartozik.
3. Válassza ki a munkaterületen az **Eszközök** lapot.

   A munkaterület **Eszközök** lapján a kiválasztott adminisztrációs csoportba tartozó számítógépek tulajdonságai láthatók.
4. A munkaterület **Eszközök** lapján csúsztassa a görgetősávot a jobb szélső állásba.

   A **Titkosítás állapota** oszlopban a kiválasztott adminisztrációs csoportba tartozó számítógépek adatainak titkosítási állapota látható. Az állapot a számítógép helyi meghajtóin lévő fájlok titkosítására, a számítógép merevlemezeinek titkosítására, valamint a számítógéphez csatlakoztatott cserélhető meghajtók titkosítására vonatkozó információkból áll össze.

A titkosítási statisztika megtekintése a Kaspersky Security Center részletes ablaktábláiban

A titkosítási állapot megtekintése a Kaspersky Security Center részletes ablaktábláiban:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki a konzolfában az **Adminisztrációs kiszolgáló – <Számítógép neve>** csomópontot.
3. Az Adminisztrációs Konzol fájától jobbra lévő munkaterületen válassza ki a **Statisztika** lapot.
4. Hozzon létre új oldalt, melyen az adattitkosítási statisztikát tartalmazó részletes ablaktáblák találhatók. Ehhez:
   a. A **Statisztika** lapon kattintson a **Megtekintés testreszabása** gombra.
      Megnyílik a **Tulajdonságok: Statisztika** ablak.
   b. A **Tulajdonságok: Statisztika** ablakban kattintson a **Hozzáadás** gombra.
      Megnyílik a **Tulajdonságok: Új oldal** ablak.
   c. Gépelje be az **Általános** részben a **Tulajdonságok: Új oldal** ablakban az oldal nevét.
   d. A **Részletes ablaktáblák** ablakban kattintson a **Hozzáadás** gombra.
      Megnyílik az **Új részletes ablaktábla** ablak.
   e. Válassza ki az **Új részletes panel** ablakban a **Védelem állapota** csoportban az **Eszköz titkosítása** elemet.
   f. Kattintson az **OK** gombra.
      Megnyílik a **Tulajdonságok: Titkosítás vezérlése** ablak.
   g. Szükség esetén szerkessze a részletes ablaktábla beállításait. Ehhez használja a **Megtekintés** és **Eszközök** részeket a **Tulajdonságok: Eszköz titkosítása** ablakban.
   h. Kattintson az **OK** gombra.
   i. Ismételje meg az utasítások d–h. Lépéseit a **Cserélhető meghajtók titkosítása** elem kiválasztásával a **Védelem állapota** részben az **Új részletes ablaktábla** ablakban.
      A hozzáadott részletes ablaktáblák megjelennek a **Részletes ablaktáblák** listán a **Tulajdonságok: Új oldal** ablakban.
   j. A **Tulajdonságok: Új oldal** ablakban kattintson az **OK** gombra.
      Az előző lépésekben létrehozott részletes ablaktáblákat tartalmazó oldal neve megjelenik az **Oldalak** listán a **Tulajdonságok: Statisztika** ablakban.
   k. A **Tulajdonságok: Statisztika** ablakban kattintson a **Bezárás** gombra.
5. Nyissa meg a **Statisztika** 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 Konzolját.
2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amely azt az ügyfélszámítógépet tartalmazza, amelyen a fájltitkosítási hibák listáját meg

szeretné tekinteni.

3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki az **Eszközök** lapon a számítógép nevét s listán, majd a jobb egérgombbal kattintva nyissa meg a helyi menüt.

5. Végezze el az alábbiak egyikét:

   - A számítógép helyi menüjében válassza ki a **Védelem** elemet.
   - A számítógép helyi menüjében válassza ki a **Tulajdonság** elemet. Válassza ki a **Tulajdonságok:<számítógép neve>** ablakban a **Védelem** részt.

6. Kattintson a **Védelem** részben a **Tulajdonságok: <számítógép neve>** ablakban az **Adattitkosítási hibák listájának megtekintése** hivatkozásra az **Adattitkosítási hibák** 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 **Adattitkosítási hibák** ablakból.

Az adattitkosítási jelentés megtekintése

Az adattitkosítási jelentés megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Az Adminisztrációs Konzol **Adminisztrációs kiszolgáló** csomópontján válassza ki a **Jelentések** lapot.

3. Kattintson a **Jelentéssablon létrehozása** gombra.

   Ekkor elindul a Jelentéssablon-varázsló.

4. Kövesse a Jelentéssablon-varázsló utasításait. Válassza ki a **Jelentéssablon típusának kiválasztása** ablak **Egyéb** részében az alábbi elemek közül valamelyiket:

   - **Kezelt eszköz titkosításának állapotjelentése**.
   - **Tárolt eszköz adattitkosítási jelentése**.
   - **Titkosítási hibák jelentése**.
   - **Titkosított fájlokhoz való blokkolt hozzáférési jelentés**.

   Miután végzett az Új jelentéssablon varázslóval, az új jelentéssablon megjelenik a **Jelentések** lapon lévő táblázatban.

5. Válassza ki az utasítások előző lépéseiben létrehozott jelentéssablont.

Megkezdődik a jelentés előállítási folyamata. A jelentés egy új ablakban jelenik meg.

Korlátozott fájltitkosítási funkciókkal rendelkező titkosított fájlok kezelése

A Kaspersky Security Center rendszabály alkalmazásakor, majd fájlok titkosításakor a Kaspersky Endpoint Security a titkosított fájlok közvetlen eléréséhez szükséges hozzáférési kulcsot kap. A titkosítási kulcs segítségével a fájltitkosítás közben aktív bármely Windows felhasználói fiókban dolgozó felhasználó közvetlenül hozzáférhet a titkosított fájlokhoz. A fájltitkosítás közben inaktív Windows fiókokban dolgozó felhasználóknak a titkosított fájlokhoz való hozzáféréshez kapcsolódniuk kell a Kaspersky Security Centerhez.

Az alábbi körülmények esetén előfordulhat, hogy a titkosított fájlok nem hozzáférhetők:

- A felhasználó számítógépe tárolja a titkosítási kulcsokat, de nincs kapcsolat a Kaspersky Security Centerrel, ami 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 törölve vannak a felhasználó számítógépén. Ilyenkor a felhasználó a helyi és cserélhető lemezeken lévő titkosított fájlokat megnyithatja, de tartalmuk titkosítottan jelenik meg.

  A felhasználó az alábbi körülmények esetén dolgozhat titkosított fájlokkal:

  - Olyan számítógépen létrehozott titkosított csomagokba helyezett fájlok, amelyeken telepítve van a Kaspersky Endpoint Security.
  - Olyan cserélhető meghajtókon tárolt fájlok, amelyeken engedélyezve van a hordozható mód.

Hozzáférés titkosított fájlokhoz Kaspersky Security Center-kapcsolat nélkül

Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

Hozzáférés titkosított fájlokhoz Kaspersky Security Center-kapcsolat nélkül:

1. Próbáljon meg hozzáférni a szükséges titkosított fájlhoz.

   Ha a számítógép helyi meghajtóján tárolt fájlhoz való hozzáférési próbálkozás közben nincs kapcsolat a Kaspersky Security Centerrel, a Kaspersky Endpoint Security elkészít egy fájlt, melyben a számítógép helyi meghajtóján tárolt összes fájlhoz való hozzáférési kérés található. Ha cserélhető meghajtón tárolt fájlhoz próbál hozzáférni, a Kaspersky Endpoint Security elkészít egy fájlt, melyben a cserélhető meghajtón tárolt összes fájlhoz való hozzáférési kérés található. Megnyílik a **Fájlhozzáférés blokkolva** ablak.

2. Küldje el a titkosított fájlokhoz való hozzáférési kérést tartalmazó fájlt a helyi hálózati rendszergazdának. Ehhez végezze el az alábbiak egyikét:

   - Ha a hozzáférést kérő fájlt e-mailben szeretné elküldeni a helyi hálózati rendszergazdának, kattintson a **Küldés e-mailben** gombra.
   - Ha a titkosított fájlokhoz való hozzáférést kérő fájlt menteni szeretné, és a helyi hálózati rendszergazdához más módon juttatja el, kattintson a **Mentés** gombra.

3. Szerezze be a titkosított fájlokhoz való hozzáférési kulcsfájlt, melyet a helyi hálózati rendszergazda készített el és adott át Önnek.

4. A titkosított fájlokhoz való hozzáférési kulcsfájlt az alábbi módokon aktiválhatja:

   - Válassza ki bármely fájlkezelőben a titkosított fájlokhoz való hozzáférési kulcsfájlt. Megnyitásához kattintson rá duplán.

   - Végezze el az alábbiakat:

     a. Nyissa meg a Kaspersky Endpoint Security főablakát.

     b. Kattintson a gombra.

     Ezzel megnyílik az **Események** ablak.

     c. Válassza ki a **Fájlok és eszközök hozzáférésének állapota** lapot.

     A lapon megjelenik a titkosított fájlokhoz való hozzáférésre vonatkozó összes kérés.

     d. Válassza ki azt a kérést, amelyhez a titkosított fájlokhoz való hozzáférési kulcsfájlt megkapta.

     e. A titkosított fájlokhoz való hozzáférési kulcsfájl betöltéséhez kattintson a **Tallózás** lehetőségre.

     Megnyílik a szokásos **Hozzáférési kulcsfájl kiválasztása** párbeszédpanel a Microsoft Windowsban.

     f. Válassza ki a Microsoft Windows szokásos **Hozzáférési kulcsfájl kiválasztása** ablakában a rendszergazda által adott .kesdr kiterjesztésű fájlt, melynek neve egyezik a kéréshozzáférési fájl nevével.

     g. Kattintson a **Megnyitás** gombra.

     h. Az **Események** ablakban kattintson az **OK** gombra.

Ha a számítógép helyi meghajtóján tárolt fájlhoz való hozzáférési próbálkozás közben kéréshozzáférési fájl készül, a Kaspersky Endpoint Security a számítógép helyi meghajtóján tárolt összes fájlhoz megadja a hozzáférést. Ha egy cserélhető meghajtón tárolt fájlhoz való hozzáférési próbálkozás közben kéréshozzáférési fájl készül, a Kaspersky Endpoint Security a cserélhető meghajtón tárolt összes fájlhoz megadja a hozzáférést. A cserélhető meghajtókon tárolt titkosított fájlokhoz való hozzáféréshez a az egyes cserélhető meghajtókhoz külön-külön hozzáférési kulcsfájlt kell kérni.

Felhasználói hozzáférés megadása titkosított fájlokhoz Kaspersky Security Center-kapcsolat nélkül

Felhasználói hozzáférés megadása titkosított fájlokhoz Kaspersky Security Center-kapcsolat nélkül:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét tartalmazza.

3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki az **Eszközök** lapon a titkosított fájlokhoz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal nyissa meg a helyi menüt.

5. A helyi menüjében válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** lehetőséget.

   Megnyílik a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablak.

6. Válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablakban a **Titkosítás** lapot.

7. A **Titkosítás** lapon kattintson a **Tallózás** gombra.

   Megnyílik a szokásos **Kéréshozzáférési fájl kiválasztása** párbeszédpanel a Microsoft Windowsban.

8. Adja meg a **Kéréshozzáférési fájl kiválasztása** ablakban a felhasználótól kapott kérésfájl elérési útját, majd kattintson a **Megnyitás** lehetőségre.

   A Kaspersky Security Center előállítja a titkosított fájlok eléréséhez szükséges kulcsfájlt. A felhasználói kérés részletei a **Titkosítás** lapon látható.

9. Végezze el az alábbiak egyikét:

   - Ha az előállított hozzáférési kulcsfájlt e-mailben szeretné elküldeni a felhasználónak, kattintson a **Küldés e-mailben** gombra.
   - Ha a titkosított fájlok hozzáférési kulcsfájlját menteni szeretné, és a felhasználóhoz más módon juttatja el, kattintson a **Mentés** gombra.

A titkosított fájlokhoz való hozzáférés üzenetsablonjainak szerkesztése

A titkosított fájlokhoz való hozzáférés üzenetsablonjainak szerkesztése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél szerkeszteni szeretné a titkosított fájlokhoz való hozzáférés üzenetsablonjait.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. Az **Adattitkosítás** részben válassza ki a **Általános titkosítási beállítások** alrészt.
7. A megnyíló **Sablonok** részben kattintson a **Sablonok** gombra.

   Megnyílik a **Sablonok** ablak.

8. Végezze el az alábbiakat:
   - Ha a felhasználói üzenetsablont szeretné szerkeszteni, válassza ki a **Felhasználó üzenete** lapot. A **Fájlhozzáférés megtagadva** ablak akkor jelenik meg, ha a felhasználó egy titkosított fájlhoz próbál hozzáférni, miközben a számítógépen nem található a titkosított fájlokhoz való hozzáféréshez szükséges kulcs. Ha a **Küldés e-mailben** gombra kattint a **Fájlhozzáférés megtagadva** ablakban, automatikusan létrejön a felhasználói üzenet. Ezt az üzenetet a vállalati helyi hálózati rendszergazda kapja meg a titkosított fájlokhoz való hozzáférést kérő fájllal együtt.

- Ha a rendszergazdai üzenetsablont szeretné szerkeszteni, válassza ki a **Rendszergazda üzenete** lapot. Ez az üzenet automatikusan létrejön, amikor a **Küldés e-mailben** gombra kattint a **Hozzáférés megadása titkosított fájlokhoz** ablakban, és elküldésre kerül a felhasználó részére, miután a felhasználó hozzáférést kapott a titkosított fájlokhoz.

9. Szerkessze az üzenetsablonokat.

   Az **Alapértelmezett** gombot és a **Változó** legördülő listát használhatja.

10. Kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.

Munkavégzés titkosított eszközökkel, ha nincs hozzájuk hozzáférés

Titkosított eszközökhöz való hozzáférés megszerzése

Az alábbi esetekben fordulhat elő, hogy a felhasználónak titkosított eszközökhöz való hozzáférést kell kérelmeznie:

- A merevlemez titkosítása egy másik számítógépen történt.
- Az eszköz titkosítási kulcsa nem található a számítógépen (például az adott számítógépen titkosított cserélhető meghajtóhoz való első hozzáférési kísérlet esetén), és a számítógép nem kapcsolódik a Kaspersky Security Centerhez.

  Miután a felhasználó a hozzáférési kulcsot alkalmazta a titkosított eszközön, a Kaspersky Endpoint Security menti a titkosítási kulcsot a felhasználó számítógépén, és engedélyezi az eszközhöz való hozzáférést a további hozzáférési próbálkozások során, még akkor is, ha nincs kapcsolat a Kaspersky Security Centerrel.

Az alábbiak szerint lehet hozzáférést szerezni a titkosított eszközökhöz:

1. A felhasználó a Kaspersky Endpoint Security alkalmazás felhasználói felületén kéréshozzáférési fájlt készít, mely kesdc kiterjesztésű, és elküldi a vállalati hálózati rendszergazdának.
2. A rendszergazda a Kaspersky Security Center Adminisztrációs Konzol segítségével hozzáférési kulcsfájlt készít, melynek kiterjesztése kesdr, és elküldi a felhasználónak.
3. A felhasználó alkalmazza a hozzáférési kulcsot.

Titkosított eszközökön lévő adatok visszaállítása

A felhasználó a Titkosított eszköz helyreállító segédprogram (a továbbiakban: visszaállító segédprogram) segítségével dolgozhat titkosított eszközökkel. Ez az alábbi esetekben lehet szükséges:

- A hozzáférési kulcs alkalmazása a hozzáférés megszerzése érdekében nem volt sikeres.
- A titkosított eszközt tartalmazó számítógépen nincsenek telepítve a titkosítási összetevők.

A titkosított eszközökhöz való hozzáférés visszaállító segédprogram segítségével történő visszaállításához szükséges adatok a felhasználó számítógépének memóriájában valamennyi ideig titkosítatlan formában találhatók. Az ilyen adatok illetéktelen elérésének kockázata csökkentése érdekében javasoljuk, hogy a titkosított eszközökhöz való hozzáférést megbízható számítógépeken állítsa vissza.

Az alábbiak szerint lehet visszaállítani a titkosított eszközökön lévő adatokat:

1. A felhasználó a visszaállító segédprogrammal kéréshozzáférési fájlt készít, mely fdertc kiterjesztésű, és elküldi a vállalati hálózati rendszergazdának.
2. A rendszergazda a Kaspersky Security Center Adminisztrációs Konzol segítségével hozzáférési kulcsfájlt készít, melynek kiterjesztése fdertr, és elküldi a felhasználónak.
3. A felhasználó alkalmazza a hozzáférési kulcsot.

Titkosított rendszermerevlemezeken lévő adatok visszaállításához a felhasználó a Visszaállító segédprogramban megadhatja a Hitelesítési ügynök-fiók hitelesítési adatait is. Ha a Hitelesítési ügynök-fiók metaadatai megsérültek, a felhasználónak kéréshozzáférési 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, amelyen a műveletet elvégzi. Ez megakadályozza a meghajtó ismételt titkosítását.

Hozzáférés szerzése titkosított eszközökhöz alkalmazás felhasználói felületén keresztül

Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

Hozzáférés szerzése titkosított eszközökhöz alkalmazás felhasználói felületén keresztül:

1. Próbáljon meg hozzáférni a szükséges titkosított eszközhöz.

   Megnyílik a **Az adatok hozzáférése blokkolva van** ablak.

2. Küldje el a vállalati hálózati rendszergazda részére a titkosított eszköz kesdc kiterjesztésű kéréshozzáférési fájlját. Ehhez végezze el az alábbiak egyikét:

   - Ha a titkosított eszköz kéréshozzáférési fájlját e-mailben szeretné elküldeni a vállalati hálózati rendszergazdának, kattintson a **Küldés e-mailben** gombra.
   - Ha a titkosított eszközhöz való kéréshozzáférési fájlt menteni szeretné, és a vállalati hálózati rendszergazdához más módon juttatja el, kattintson a **Mentés** gombra.

Ha anélkül zárta be az **Az adatok hozzáférése blokkolva van** ablakot, hogy a kéréshozzáférési fájlt mentette volna vagy elküldte volna a vállalati hálózati rendszergazdának, akkor ezt később bármikor megteheti az **Események** ablak **Fájlok és eszközök hozzáférésének állapota** lapon. Az ablak megnyitásához kattintson a gombra a fő alkalmazásablakban.

3. Szerezze be és mentse a titkosított eszközhöz való hozzáférési kulcsfájlt, melyet a vállalati hálózati rendszergazda készített el és adott át Önnek.

4. Az alábbi módszerek egyikével alkalmazhatja a titkosított eszközhöz való hozzáférési kulcsot:

   - Keresse meg bármely fájlkezelőben a titkosított eszköz hozzáférési kulcsfájlját, és nyissa meg dupla kattintással.

   - Végezze el az alábbiakat:

     a. Nyissa meg a Kaspersky Endpoint Security főablakát.

     b. Kattintson a gombra az **Események** ablak megnyitásához.

     c. Válassza ki a **Fájlok és eszközök hozzáférésének állapota** lapot.

        A lapon megjelenik a titkosított fájlokhoz és eszközökhöz való hozzáférésre vonatkozó összes kérés.

     d. Válassza ki azt a kérést, amelyhez a titkosított eszközhöz való hozzáférési kulcsfájlt megkapta.

     e. A titkosított eszközhöz való megkapott hozzáférési kulcsfájl betöltéséhez kattintson a **Tallózás** lehetőségre.

        Megnyílik a szokásos **Hozzáférési kulcsfájl kiválasztása** párbeszédpanel a Microsoft Windowsban.

     f. Válassza ki a Microsoft Windows szokásos **Hozzáférési kulcsfájl kiválasztása** ablakában a rendszergazda által adott kesdr kiterjesztésű fájlt, melynek neve egyezik a titkosított eszköz kéréshozzáférési fájljának nevével.

     g. Kattintson a **Megnyitás** gombra.

     h. A **Fájlok és eszközök hozzáférésének állapota** ablakban kattintson az **OK** gombra.

Ennek hatására a Kaspersky Endpoint Security megadja a hozzáférést a titkosított eszközhöz.

Felhasználói hozzáférés megadása titkosított eszközökhöz

Felhasználói hozzáférés megadása titkosított eszközökhöz:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.

2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez a titkosított eszközhöz hozzáférést kérő felhasználó számítógépét tartalmazza.

3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki az **Eszközök** lapon a titkosított eszközhöz hozzáférést kérő felhasználó számítógépét, majd a jobb egérgombbal nyissa meg a helyi menüt.

5. A helyi menüjében válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** lehetőséget.

   Megnyílik a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablak.

6. Válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablakban a **Titkosítás** lapot.

7. A **Titkosítás** lapon kattintson a **Tallózás** gombra.

   Megnyílik a szokásos **Kéréshozzáférési fájl kiválasztása** párbeszédpanel a Microsoft Windowsban.

8. Adja meg a **Kéréshozzáférési fájl kiválasztása** ablakban a felhasználótól kapott kesdc kiterjesztésű kérésfájl elérési útját.

9. Kattintson a **Megnyitás** gombra.

   A Kaspersky Security Center előállítja a titkosított eszköz eléréséhez szükséges kesdr kiterjesztésű hozzáférési kulcsfájlt. A felhasználói kérés részletei a **Titkosítás** lapon látható.

10. Végezze el az alábbiak egyikét:

    - Ha az előállított hozzáférési kulcsfájlt e-mailben szeretné elküldeni a felhasználónak, kattintson a **Küldés e-mailben** gombra.
    - Ha a titkosított eszköz hozzáférési kulcsfájlját menteni szeretné, és a felhasználóhoz más módon juttatja el, kattintson a **Mentés** gombra.

BitLockerrel titkosított merevlemezekhez való visszaállítási kulcs átadása felhasználó részére

BitLockerrel titkosított rendszermerevlemezhez való visszaállítási kulcs küldése felhasználó részére:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez a titkosított meghajtóhoz hozzáférést kérő felhasználó számítógépét tartalmazza.
3. Válassza ki a munkaterületen az **Eszközök** lapot.
4. Válassza ki az **Eszközök** lapon a titkosított meghajtóhoz hozzáférést kérő felhasználó számítógépét.
5. Nyissa meg a jobb egérgombbal a helyi menüt, és válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** lehetőséget.

   Megnyílik a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablak.

6. Válassza ki a **Hozzáférés engedélyezése az eszközökhöz és adatokhoz offline módban** ablakban a **Hozzáférés BitLocker-védelemmel rendelkező rendszermeghajtóhoz** lapot.
7. Kérje be a felhasználótól a BitLocker jelszóbeviteli ablakban jelzett visszaállítási kulcsazonosítót, és vesse össze a **Visszaállítási kulcs azonosítója** mezőben lévő azonosítóval.

   Ha az azonosítók nem egyeznek, a kulcs nem használható a megadott rendszermeghajtóhoz való hozzáférés visszaállítására. Győződjön meg arról, hogy a kiválasztott számítógép neve egyezik a felhasználó számítógépének nevével.

8. Küldje el a felhasználónak a **Visszaállítási kulcs** mezőben jelzett kulcsot.

BitLockerrel titkosított nem a rendszert tartalmazó merevlemezhez való visszaállítási kulcs küldése felhasználó részére:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki az Adminisztrációs Konzol fájában a **További** → **Titkosítás és adatvédelem** → **Titkosított eszközök** mappát.

   A munkaterületen megjelenik a titkosított eszközök listája.
3. Válassza ki a munkaterületen azt a titkosított eszközt, amelyhez vissza szeretné állítani a hozzáférést.
4. Kattintson a jobb egérgombbal a helyi menü megjelenítéséhez, és válassza ki a **Hozzáférési kulcs beszerzése a megadott titkosított eszközhöz** lehetőséget.

   Ezzel megnyílik a **Hozzáférés visszaállítása BitLockerrel titkosított meghajtóhoz** ablak.
5. Kérje be a felhasználótól a BitLocker jelszóbeviteli ablakban jelzett visszaállítási kulcsazonosítót, és vesse össze a **Visszaállítási kulcs azonosítója** 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.
6. Küldje el a felhasználónak a **Visszaállítási kulcs** mezőben jelzett kulcsot.

A Visszaállító segédprogram végrehajtható fájljának létrehozása

Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

A Visszaállító segédprogram végrehajtható fájljának létrehozása:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a gombra a főablak bal alsó sarkában a **Támogatás** ablak megnyitásához.
3. A **Támogatás** ablakban kattintson a **Titkosított eszköz visszaállítása** gombra.

   Elindul a Titkosított eszköz helyreállító segédprogramja.
4. Kattintson a Visszaállító segédprogram ablakában az **Önálló Helyreállító segédprogram létrehozása** gombra.

   Megnyílik az **Önálló Helyreállító segédprogram létrehozása** ablak.
5. Gépelje be kézileg a **Mentés ide** ablakba a Visszaállító segédprogram végrehajtható fájlja mentési mappájának elérési útját, vagy kattintson a **Tallózás** gombra.
6. Kattintson az **OK** gombra az **Önálló Helyreállító segédprogram létrehozása** ablakban.

   Sor kerül a Visszaállító segédprogram végrehajtható fájljának (fdert.exe) mentésére a kiválasztott mappában.

Titkosított eszközökön lévő adatok helyreállítása a Visszaállító segédprogrammal

Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

Titkosított eszközhöz való hozzáférés helyreállítása a Visszaállító segédprogrammal:

1. Futtassa a Visszaállító segédprogram az alábbi módok egyikén:

   - Kattintson a gombra a Kaspersky Endpoint Security fő ablakában a **Támogatás** ablak megnyitásához, majd kattintson a **Titkosított eszköz visszaállítása** gombra.

   - Futtassa a Visszaállító segédprogram fdert.exe végrehajtható fájlját. Ezt a fájlt a Kaspersky Endpoint Security állítja elő.

2. Válassza ki a Visszaállító segédprogram ablakében az **Eszköz kiválasztása** legördülő listán 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. 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 gyűjtésének folyamatát.

5. A diagnosztika eredményeitől függően kattintson a **Feloldás** vagy a **Visszafejtés** gombra.

   Megnyílik az **Eszközfeloldási beállítások** vagy az **Eszközvisszafejtés beállításai** ablak.

6. Ha az adatokat Hitelesítési ügynök-fiókkal szeretné visszaállítani:

   a. Válassza ki a **Hitelesítési ügynök fiókbeállításainak használata** lehetőséget.

   b. Adja meg a **Név** és **Jelszó** mezőkben a Hitelesítési ügynök-fiók hitelesítési adatait.

   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.

7. Ha hozzáférési kulccsal szeretné az adatokat visszaállítani:

   a. Válassza ki az **Eszköz-hozzáférési kulcs manuális megadása** lehetőséget.

   b. Kattintson a **Hozzáférési kulcs fogadása** gombra.

   c. Megnyílik az **Eszköz-hozzáférési kulcs fogadása** ablak.

   d. Kattintson a **Mentés** gombra, és válassza ki azt a mappát, amelybe az fdertc kiterjesztésű kéréshozzáférési fájlt menteni szeretné.

   e. Küldje el a kéréshozzáférési 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.

f. Szerezze be és mentse a hozzáférési kulcsfájlt, melyet a vállalati hálózati rendszergazda készített el és adott át Önnek.

g. Kattintson a **Betöltés** gombra, és a megnyíló ablakban válassza ki az fdertr kiterjesztésű hozzáférési kulcsfájlt.

8. Ha eszközt fejt vissza, akkor a többi visszafejtési beállítást is meg kell adnia az **Eszközvisszafejtés beállításai** ablakban. Ehhez:

   - Adja meg a visszafejteni kívánt területet:
     - Ha a teljes eszközt vissza szeretné fejteni, válassza a **Teljes eszköz visszafejtése** lehetőséget.
     - Ha az eszközön lévő adatok egy részét szeretné visszafejteni, válassza az **Egyedi eszközterületek visszafejtése** lehetőséget, és adja meg a visszafejteni kívánt terület határait a **Indítás** és **Befejezés** mezőkben.
   - Válassza ki a visszafejtett adatok írásának helyét:
     - Ha az eredeti eszközön lévő adatokat felül szeretné írni a visszafejtett adatokkal, törölje az **Adatok mentése fájlba a visszafejtés után** jelölőnégyzetet.
     - Ha a visszafejtett adatokat az eredeti titkosított adatoktól elkülönítve szeretné menteni, jelölje be az **Adatok mentése fájlba a visszafejtés után** jelölőnégyzetet, és adja meg az adatok mentésének elérési útját a **Tallózás** gombra kattintva.

9. Kattintson az **OK** gombra.

Megkezdődik az eszköz feloldási/visszafejtési folyamata.

Válaszadás a titkosított eszközökön lévő adatok visszaállítására irányuló felhasználói kérésre

Kulcsfájl előállítása titkosított eszköz eléréséhez, majd átadása felhasználó számára:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki az Adminisztrációs Konzol fájában a **További → Titkosítás és adatvédelem → Titkosított eszközök** mappát.
3. Válassza ki a munkaterületen azt a titkosított eszközt, amelyhez hozzáférési kulcsfájlt szeretne előállítani, az eszköz helyi menüjében pedig válassza ki a **Hozzáférési kulcs beszerzése a megadott titkosított eszközhöz** lehetőséget.

Ha nem biztos benne, hogy a kéréshozzáférési fájl melyik számítógéphez készült, válassza ki az Adminisztrációs Konzol fájában a **További → Titkosítás és adatvédelem** mappát, és a munkaterületen kattintson az **Eszköz titkosítási kulcsának beszerzése** hivatkozásra.

Megnyílik a **Hozzáférés engedélyezése az eszközhöz** ablak.

4. Válassza ki a használatban lévő titkosítási algoritmust. Ehhez válasszon egyet az alábbi lehetőségek közül:

   - **AES256**, ha a Kaspersky Endpoint Security telepítése az eszköz titkosítását végző számítógépen lévő aes256 mappában található terjesztőcsomagból történt;
   - **AES56**, ha a Kaspersky Endpoint Security telepítése az eszköz titkosítását végző számítógépen lévő aes56 mappában található terjesztőcsomagból történt;

5. Kattintson az **Tallózás...** gombra.

   Megnyílik a szokásos **Kéréshozzáférési fájl kiválasztása** párbeszédpanel a Microsoft Windowsban.

6. Adja meg a **Kéréshozzáférési fájl kiválasztása** ablakban a felhasználótól kapott fdertc kiterjesztésű kérésfájl elérési útját.

7. Kattintson a **Megnyitás** gombra.

   A Kaspersky Security Center előállítja a titkosított eszköz eléréséhez szükséges fdertr kiterjesztésű hozzáférési kulcsfájlt.

8. Végezze el az alábbiak egyikét:

   - Ha az előállított hozzáférési kulcsfájlt e-mailben szeretné elküldeni a felhasználónak, kattintson a **Küldés e-mailben** gombra.
   - Ha a titkosított eszköz hozzáférési kulcsfájlját menteni szeretné, és a felhasználóhoz más módon juttatja el, kattintson a **Mentés** gombra.

Titkosított adatokhoz való hozzáférés visszaállítása az operációs rendszer hibáját követően

Operációs rendszerhiba után csak fájlszintű titkosítás (FLE) esetén állíthatja vissza az adatokat. Nem állíthatja vissza az adatok elérését, ha teljes lemeztitkosítást (FDE) használ.

Titkosított adatokhoz való hozzáférés visszaállításához az operációs rendszer hibáját követően:

1. Telepítse újra az operációs rendszert a merevlemez formázása nélkül.
2. Telepítse a Kaspersky Endpoint Security alkalmazást.
3. Kapcsolat létrehozása a számítógép és a számítógép által vezérelt Kaspersky Security Center Adminisztrációs 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.

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 végrehajtható fájljának létrehozása.

2. A Windows rendszerindítás előtti környezet egyéni lemezképének létrehozása. A Windows rendszerindítás előtti környezet egyéni lemezképének létrehozása közben a Visszaállító segédprogram végrehajtható fájljának hozzáadása a lemezképhez.

3. A Windows rendszerindítás előtti környezet egyéni lemezképének mentése rendszerindításra alkalmas adathordozóra, például CD-re vagy cserélhető meghajtóra.

   A Windows rendszerindítás előtti környezet egyéni lemezképének létrehozására vonatkozó utasítások a Microsoft súgófájlokban találhatók (például a Microsoft TechNet erőforrásban).

Hálózati védelem

Ez a rész tájékoztatást nyújt a hálózati forgalom figyelésével kapcsolatban, és ismerteti a figyelemmel kísért hálózati portok beállításainak megadását.

A Hálózati védelem

A Kaspersky Endpoint Security működése során az olyan védelmi összetevők, mint a Levél víruskereső, a Webes víruskereső és az IM víruskereső figyelik számítógépen a bizonyos protokollokkal továbbított és a megadott nyitott TCP és UDP portokon átmenő adatforgalmat. A Levél víruskereső például az SMTP-kapcsolaton küldött adatokat, míg a Webes víruskereső a HTTP-, és FTP-kapcsolatok adatátvitelét ellenőrzi.

A Kaspersky Endpoint Security az operációs rendszer TCP és UDP portjait több csoportra osztja aszerint, hogy mekkora a valószínűsége a feltörésüknek. Egyes hálózati portok olyan szolgáltatásokra vannak fenntartva, amelyek sebezhetőek lehetnek. Javasoljuk, hogy ezeket a portokat alaposabban figyelje, mivel ezeken nagyobb a támadások valószínűsége. 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 Levél víruskereső, a Webes víruskereső és az IM víruskereső összetevők a hálózati forgalom figyelése közben különösen odafigyelnek.

A hálózati forgalomfigyelés beállításainak megadása

A hálózati forgalom figyelési beállításainak megadása érdekében a következő műveleteket végezheti el:

- Minden hálózati port figyelésének bekapcsolása.
- A figyelt hálózati portok listájának létrehozása.
- Azon alkalmazások listájának létrehozása, amelyeknél minden hálózati portot figyelni szeretne.

Minden hálózati port figyelésének bekapcsolása

Minden hálózati port figyelésének bekapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Vírusvédelem** részt.
   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Figyelt portok** részben válassza ki az **Minden hálózati port figyelése** elemet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A figyelt hálózati portok listájának létrehozása

A figyelt hálózati portok listájának létrehozása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Figyelt portok** részben válassza ki a **Csak a kijelölt portok figyelése** elemet.
4. 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.
5. A hálózati portok listáján hajtsa végre a következő lépéseket:

   - Jelölje be a jelölőnégyzeteket azokkal a hálózati portokkal szemben, amelyeket fel szeretne venni a figyelemmel kísért hálózati portok listájára.

     Alapértelmezés szerint a jelölőnégyzetek be vannak jelölve az összes olyan hálózati porttal szemben, amelyek fel vannak sorolva a **Hálózati portok** ablakban.
   - Törölje a jelölőnégyzeteket azokkal a hálózati portokkal szemben, amelyeket ki szeretne zárni a figyelemmel kísért hálózati portok listájáról.
6. Ha a lista nem tartalmaz egy hálózati portot, az alábbi módon veheti fel rá:

   a. Kattintson a hálózati portok listája alatti **Hozzáadás** hivatkozásra a **Hálózati port** ablak megnyitásához.

   b. A **Port** mezőben adja meg a hálózati port számát.

   c. Adja meg a hálózati port nevét a **Leírás** mezőben.

   d. Kattintson az **OK** gombra.

   A **Hálózati port** ablak bezár. Az újonnan hozzáadott hálózati port a hálózati portok listájának végére kerül.
7. A **Hálózati portok** ablakban kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

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 jelölje be az **Minden hálózati port figyelése** jelölőnégyzetet a **Figyelt portok** részben, vagy állítsa be az összes port figyelemmel kísérését az olyan alkalmazásoknál, amelyek FTP kapcsolatot létesítenek.

Azon alkalmazások listájának létrehozása, amelyeknél minden hálózati portot figyelni szeretne

Létrehozhatja azon alkalmazások táblázatát, amelyeknél a Kaspersky Endpoint Security az összes hálózati portot figyeli.

Javasoljuk, hogy az FTP protokollon keresztül adatokat fogadó, illetve küldő alkalmazásokat vegye fel azon alkalmazások listájára, amelyeknél a Kaspersky Endpoint Security az összes hálózati portot figyelemmel kíséri.

Azon alkalmazások listájának létrehozása, amelyeknél minden hálózati portot figyelni szeretne:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Figyelt portok** részben válassza ki a **Csak a kijelölt portok figyelése** elemet.
4. Kattintson a **Beállítások** gombra.

   Megnyílik a **Hálózati portok** ablak.
5. Jelölje be **A megadott alkalmazások figyelése minden porton** jelölőnégyzetet.
6. **A megadott alkalmazások figyelése minden porton** jelölőnégyzet alatti alkalmazáslistán végezze el a következőt:

   - Jelölje be a jelölőnégyzeteket azon alkalmazások nevei mellett, amelyeknél az összes hálózati portot figyelni szeretné.

     Alapértelmezés szerint a jelölőnégyzetek be vannak jelölve az összes olyan alkalmazás mellett, amelyek fel vannak sorolva a **Hálózati portok** ablakban.

   - Törölje a jelölőnégyzeteket azon alkalmazások nevei mellett, amelyeknél nem szeretné az összes hálózati portot figyelni.
7. Ha az alkalmazáslista nem tartalmaz egy alkalmazást, az alábbi módon veheti fel rá:

   a. Kattintson a **Hozzáadás** hivatkozásra az alkalmazáslista alatt, és nyissa meg a helyi menüt.

   b. Válassza ki a helyi menüben, hogyan szeretné felvenni az alkalmazást az alkalmazáslistára:

      - Válassza az **Alkalmazások** parancsot, ha a számítógépre telepített alkalmazások listájáról szeretne alkalmazást választani. Megnyílik az **Alkalmazás kiválasztása** ablak, ahol megadhatja az alkalmazás nevét.

      - Az alkalmazás végrehajtható fájljának megadásához válassza a**Tallózás** parancsot. Megnyílik a Microsoft Windows szokásos **Megnyitás** ablaka, ahol megadhatja az alkalmazás végrehajtható fájljának nevét.

     Az alkalmazás kiválasztását követően megnyílik az **Alkalmazás** ablak.

   c. A **Név** mezőben írja be a kiválasztott alkalmazás nevét.

   d. Kattintson az **OK** gombra.

     Az **Alkalmazás** ablak bezár. A hozzáadott alkalmazás megjelenik alkalmazások listájának végén.
8. A **Hálózati portok** ablakban kattintson az **OK** gombra.
9. A módosítások mentéséhez kattintson a **Mentés** gombra.

Adatbázisok és alkalmazás-szoftvermodulok frissítése

Ez a rész tájékoztatást nyújt adatbázis- és alkalmazásmodul-frissítésekkel (más néven „frissítésekkel") kapcsolatban, és ismerteti a frissítési beállítások megadásának menetét.

Az adatbázisok és alkalmazásmodulok frissítéseiről

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 proxykiszolgálóval csatlakozik az internethez, meg kell adnia a kapcsolat 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 súgófájljok is frissülhetnek.

Ha az adatbázisok elavultak, a frissítőcsomag nagy méretű lehet, és további internetforgalmat (több tucat MB) generálhat.

A Kaspersky Endpoint Security adatbázisainak aktuális állapotára vonatkozó információk a **Frissítés** részben láthatók a **Feladatok** ablakban.

A frissítés eredményeit és a frissítési feladat végrehajtása során történt eseményeket a Kaspersky Endpoint Security egy jelentésben naplózza.

A frissítésforrások

A *frissítésforrás* a Kaspersky Endpoint Security adatbázisainak és alkalmazásmoduljainak frissítéseit tartalmazó erőforrás.

A frissítési források közé a Kaspersky Security Center kiszolgálója, a Kaspersky frissítési kiszolgálói, valamint hálózati vagy helyi mappák tartoznak.

A frissítési beállítások megadása

A frissítési beállítások megadása érdekében a következő műveleteket végezheti el:

- Új frissítésforrások hozzáadása.

  A frissítésforrások alapértelmezett listáján a Kaspersky Security Center és a Kaspersky frissítéskiszolgálói szerepelnek. A listára további frissítésforrásokat is felvehet. Frissítésforrásként megadhat HTTP-/FTP-kiszolgálókat és megosztott meghajtókat.

  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.

  > Ha a helyi hálózaton kívüli erőforrást ad meg frissítési forrásként, a frissítés elvégzéséhez internetkapcsolatra van szükség.

- Válassza ki a Kaspersky frissítéskiszolgáló régióját.

  Ha frissítésforrásként a Kaspersky frissítéskiszolgálóit használja, a frissítőcsomag letöltéséhez kiválaszthatja a használni kívánt kiszolgáló helyét. A Kaspersky frissítéskiszolgálói számos országban megtalálhatók. A legközelebbi Kaspersky frissítéskiszolgáló használata lehetővé teszi a frissítőcsomagok letöltési időtartamának csökkentését.

  Alapértelmezés szerint az alkalmazás az érvényes régióra vonatkozó információkat az operációs rendszer beállításjegyzékéből szerzi.

- A Kaspersky Endpoint Security megosztott mappából történő frissítésének beállítása.

  Az internetes forgalommal való takarékoskodás érdekében beállíthatja, hogy a Kaspersky Endpoint Security frissítéseit a helyi hálózaton lévő számítógépek egy megosztott mappából kapják meg. Ehhez a helyi hálózaton lévő egyik számítógép fogadja a naprakész frissítési csomagot a Kaspersky Security Center kiszolgálójától vagy a Kaspersky frissítéskiszolgálóitól, majd a lekért frissítési csomagot egy megosztott mappába másolja. Ezt követően a helyi hálózaton lévő többi számítógép a frissítési csomagot a megosztott mappából megkaphatja.

- Frissítési feladat futásmódjának kiválasztása.

  Ha a frissítési feladat futtatása valamilyen okból (például a számítógép abban az időpontban nem volt bekapcsolva) nem volt lehetséges, beállíthatja a kimaradt feladatot úgy is, hogy automatikusan elinduljon, amint lehet.

A frissítési feladat alkalmazásindítást követő elindulását el is halaszthatja, ha a frissítési feladat **Ütemezés szerint** futásmódját választja ki, és a Kaspersky Endpoint Security kezdési időpontja egyezik a frissítési feladat indítási ütemezésével. Az frissítési feladatok futtatására csak akkor kerülhet sor, ha letelik a megadott időtartam a Kaspersky Endpoint Security elindulása után.

- A frissítési feladatok futásának beállítása másik felhasználói fiók jogosultságaival.

Frissítésforrás hozzáadása

Frissítésforrás hozzáadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.
   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.
3. A **Futásmód és frissítésforrás** részben kattintson a **Frissítésforrás** gombra.
   Ezzel megnyílik a **Forrás** lap a **Frissítés** ablakban.
4. A **Forrás** lapon kattintson a **Hozzáadás** gombra.
   Megnyílik a **Frissítésforrás kiválasztása** ablak.
5. A **Frissítésforrás kiválasztása** ablakban válassza ki a frissítési csomagot tartalmazó mappát, vagy adja meg teljes elérési útját a **Forrás** mezőben.
6. Kattintson az **OK** gombra.
7. A **Frissítés** ablakban kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

A frissítéskiszolgáló régiójának kiválasztása

A frissítéskiszolgáló régiójának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.
   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.
3. A **Futásmód és frissítésforrás** részben kattintson a **Frissítésforrás** gombra.
   Ezzel megnyílik a **Forrás** lap a **Frissítés** ablakban.
4. A **Forrás** lap **Területi beállítások** részében válassza ki a **Kiválasztás listából** lehetőséget.
5. Válassza ki az aktuális helyszínhez legközelebb elhelyezkedő országot a legördülő listáról.
6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Megosztott mappából való frissítések beállítása

A Kaspersky Endpoint Security megosztott mappából történő frissítéseinek beállítása az alábbi lépésekből áll:

1. A frissítési csomag másolásának engedélyezése a helyi hálózaton lévő egyik számítógép valamelyik megosztott mappájába.
2. A Kaspersky Endpoint Security megosztott mappából történő frissítéseinek beállítása a helyi hálózaton lévő többi számítógéphez.

A frissítési csomag megosztott mappába történő másolásának engedélyezése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.

   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.
3. A **További** részben jelölje be a **Frissítések másolása mappába** jelölőnégyzetet.
4. Adja meg annak a megosztott mappának az elérési útját, amelybe a frissítési csomagot helyezi. Ezt az alábbi módszerek valamelyikével teheti meg:
   - Adja meg a megosztott mappa elérési útját a **Frissítések másolása mappába** jelölőnégyzet alatti mezőben.
   - Kattintson az **Tallózás...** gombra. Ezután a megnyíló **Mappa választása** ablakban válassza ki a kívánt mappát, majd kattintson az **OK** gombra.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Kaspersky Endpoint Security megosztott mappából történő frissítésének beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.

   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.
3. A **Futásmód és frissítésforrás** részben kattintson a **Frissítésforrás** gombra.

   Ezzel megnyílik a **Forrás** lap a **Frissítés** ablakban.
4. A **Forrás** lapon kattintson a **Hozzáadás** gombra.

   Megnyílik a **Frissítésforrás kiválasztása** ablak.
5. A **Frissítésforrás kiválasztása** ablakban válassza ki a frissítési csomagot tartalmazó megosztott mappát, vagy adja meg teljes elérési útját a **Forrás** mezőben.
6. Kattintson az **OK** gombra.
7. Törölje a **Forrás** lapon a jelölőnégyzeteket azon frissítésforrások neve mellett, amelyeket nem adott meg megosztott mappaként.

8. Kattintson az **OK** gombra.

9. A módosítások mentéséhez kattintson a **Mentés** gombra.

Frissítési feladat futásmódjának kiválasztása

Frissítési feladat futásmódjának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.

   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.

3. Kattintson a **Futásmód** gombra.

   Ezzel megnyílik a **Futásmód** lap a **Frissítés** ablakban.

4. Válassza ki a **Futásmód** részben a frissítési feladatot indítási lehetőségei közül valamelyiket:

   - 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 **Kézileg** lehetőséget.

   - Ha be szeretné állítani a frissítési feladat indítási ütemezését, válassza ki az **Ütemezés szerint** lehetőséget.

5. Végezze el az alábbiak egyikét:

   - Ha az **Automatikus** vagy **Kézileg** lehetőséget választotta, lépjen a jelen utasítások 6. lépésére.

   - Ha az **Ütemezés szerint** lehetőséget választotta, adja meg a frissítési feladat futási ütemezésének beállításait. Ehhez:

     a. A **Gyakoriság** legördülő listán adja meg a frissítési feladat indítását. Válasszon a következő lehetőségek közül: **Perc**, **Óra**, **Nap**, **Hetente**, **Megadott időpontban**, **Havonta**, illetve **Az alkalmazás elindulása után**.

     b. A **Gyakoriság** legördülő listán kiválasztott elemtől függően adja meg a frissítési feladat kezdési idejét meghatározó beállítások értékeit.

     c. Adja meg a **Futtatás elhalasztása az alkalmazások indítása után** mezőben azt az időközt, amellyel a frissítési feladat elkezdését elhalasztja a Kaspersky Endpoint Security indítása után.

     > Ha az **Az alkalmazás elindulása után** elemet választotta ki a **Gyakoriság** legördülő listán, akkor a **Futtatás elhalasztása az alkalmazások indítása után** mező nem használható.

     d. Ha azt szeretné, hogy a Kaspersky Endpoint Security a kihagyott frissítési feladatokat a lehető leghamarabb megkezdje, jelölje be a **Kihagyott feladatok futtatása** jelölőnégyzetet.

Ha a **Perc**, az **Óra** vagy az **Az alkalmazás elindulása után** elem van kiválasztva a **Gyakoriság** legördülő listán, a **Kihagyott feladatok futtatása** jelölőnégyzet nem használható.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

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 vagy engedélyezett proxykiszolgáló-felhasználó jogosultságainak hiányában nem férhet hozzá (például frissítési csomagot tartalmazó megosztott mappából). A Kaspersky Endpoint Security beállításaiban megadhat egy olyan felhasználót, aki rendelkezik ezekkel a jogosultságokkal, és a Kaspersky Endpoint Security frissítési feladatát elindíthatja ennek a felhasználói fióknak a nevében.

Frissítési feladat elindítása egy másik felhasználó fiókjában:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.

   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.

3. A **Futásmód és frissítésforrás** részben kattintson a **Futásmód** gombra.

   Ezzel megnyílik a **Futásmód** lap a **Frissítés** ablakban.

4. A **Futásmód** lapon lévő **Felhasználó** részben jelölje be a **Feladat futtatása másként** jelölőnégyzetet.

5. A **Név** mezőbe írja be annak a felhasználói fióknak a nevét, amelynek a jogosultságai a frissítési forráshoz való hozzáféréshez szükségesek.

6. A **Jelszó** mezőbe írja be annak a felhasználói fióknak a jelszavát, amelynek a jogosultságai a frissítési forráshoz való hozzáféréshez szükségesek.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az alkalmazásmodulok frissítéseinek beállítása

Az alkalmazásmodulok frissítéseinek beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.

   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.

3. A **További** részben végezze el az alábbiak egyikét:

   - Jelölje be az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás a frissítési csomagokba az alkalmazásmodulok frissítéseit is elhelyezze.
   - Ha ezt nem szeretné, törölje az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzetet.

4. Ha az előző lépésben bejelölte az **Alkalmazásmodulok frissítéseinek letöltése** jelölőnégyzetet, adja meg azokat a feltételeket, amelyek mellett az alkalmazás telepíti alkalmazásmodulok frissítéseit:

   - Válassza a **Kritikus és jóváhagyott frissítések telepítése** lehetőséget helyileg az alkalmazás felületén, illetve a Kaspersky Security Center segítségével, ha azt szeretné, hogy alkalmazás az alkalmazásmodulok kritikus frissítéseit automatikusan telepítse, az egyéb frissítéseket pedig telepítésük jóváhagyását követően.
   - Válassza a **Csak jóváhagyott frissítések telepítése** lehetőséget helyileg az alkalmazás felületén, illetve a Kaspersky Security Center segítségével, ha azt szeretné, hogy alkalmazás a frissítéseket telepítésük jóváhagyását követően telepítse.

5. A módosítások mentéséhez kattintson a **Mentés** gombra.

A frissítési feladatok elindítása és leállítása

A kiválasztott frissítési feladat futásmódjától függetlenül a Kaspersky Endpoint Security frissítési feladatai bármikor elindíthatók és leállíthatók.

A frissítési csomagoknak a Kaspersky kiszolgálóiról való letöltéséhez internetkapcsolat szükséges.

Frissítési feladat elindítása és leállítása:

1. Kattintson a fő alkalmazásablak alsó részén található **Feladatok** gombra.

   Megnyílik a **Feladatok** ablak.

2. Kattintson a frissítési feladat nevét tartalmazó részre.

   Kibomlik a kiválasztott rész.

3. Végezze el az alábbiak egyikét:

   - Ha szeretné elindítani a frissítési feladatot, válassza a menü **Indítás** lehetőségét.

     A frissítési feladat neve alatt látható haladási állapota *Fut* értékre vált.

   - Ha szeretné leállítani a frissítési feladatot, válassza a menü **Leállítás** lehetőségét.

     A frissítési feladat neve alatt látható haladási állapota *Leállt* értékre vált.

Frissítési feladat elindítása és leállítása az egyszerűsített alkalmazásfelület megjelenése közben:

1. Kattintson a jobb egérgombbal a tálca értesítési területén található alkalmazásikon helyi menüjének megjelenítéséhez.

2. A helyi menüben a **Feladatok** legördülő listán végezze el az alábbi műveletek közül valamelyiket:

   - az elindításhoz válasszon ki egy nem futó frissítési feladatot

- a leállításhoz válasszon ki egy futó frissítési feladatot
- a folytatáshoz vagy újraindításhoz válasszon ki egy szünetelő frissítési feladatot

Legutolsó 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 másolatot 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 az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Feladatok** részre.
   Megnyílik a **Feladatok** rész.
4. Kattintson a jobb egérgombbal a **Frissítés** feladat helyi menüjének megnyitásához.
5. Válassza ki a **Frissítés visszagörgetése** lehetőséget.

Proxykiszolgáló beállításainak megadása

Proxykiszolgáló beállításainak megadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Frissítés** lehetőséget.
   Az ablak jobb oldali részén az alkalmazásfrissítési beállítások láthatók.
3. Kattintson a **Proxykiszolgáló** részben a **Beállítások** gombra.
   Megnyílik a **Proxykiszolgáló beállításai** ablak.
4. A **Proxykiszolgáló beállításai** ablakban jelölje be a **Proxykiszolgáló használata** jelölőnégyzetet.
5. Adja meg a proxykiszolgáló beállításait.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A proxykiszolgáló beállításait megadhatja az alkalmazás főablakában is a **Beállítások** lap **Speciális beállítások** részében.

Számítógép vizsgálata

A víruskeresés a számítógép biztonsága szempontjából létfontosságú. A rendszeresen elvégzett vírusvizsgálatok kizárják az olyan rosszindulatú programok terjedésének lehetőségét, amelyeket a biztonsági összetevők nem észleltek az alacsony biztonsági szint miatt, vagy egyéb okokból.

Ez a rész ismerteti a vizsgálati feladatok, biztonsági szintek, vizsgálati módszerek és technológiák konkrétumait és beállításait, és utasításokat közöl azon fájlok kezelésére vonatkozóan, amelyeket a Kaspersky Endpoint Security a vírusvizsgálat során nem dolgozott fel.

A vizsgálati feladatok

A vírusok és egyéb rosszindulatú programok megkeresése, illetve az alkalmazásmodulok integritásának ellenőrzése érdekében a Kaspersky Endpoint Security az alábbi feladatokat tartalmazza:

- **Teljes vizsgálat**. Az egész számítógép alapos vizsgálata. Alapértelmezés szerint a Kaspersky Endpoint Security az alábbi objektumokat vizsgálja:
  - Kernelmemória
  - Az operációs rendszer indulásakor betöltött objektumok
  - Rendszerindító szektorok
  - Az operációs rendszer biztonsági másolata
  - Minden merevlemez és cserélhető meghajtó
- **Kritikus területek vizsgálata**. A Kaspersky Endpoint Security alapértelmezés szerint a rendszermag memóriáját, a futó folyamatokat és a lemez rendszerindító szektorait vizsgálja.
- **Egyéni vizsgálat**. A Kaspersky Endpoint Security a felhasználó által kiválasztott objektumokat vizsgálja. Az alábbi listáról bármely objektumot megvizsgálhatja:
  - Kernelmemória
  - Az operációs rendszer indulásakor betöltött objektumok
  - Az operációs rendszer biztonsági másolata
  - Outlook postafiók
  - Minden merevlemez, cserélhető és hálózati meghajtó
  - Bármely kiválasztott fájl
- **Integritás ellenőrzés**. A Kaspersky Endpoint Security ellenőrzi, hogy az alkalmazásmodulok nem sérültek vagy módosultak-e.

A Teljes vizsgálat és a Kritikus területek vizsgálata feladatok némileg eltérnek a többitől. Ezen feladatok esetében nem ajánlott a vizsgálat hatókörének szerkesztése.

A vizsgálat feladatok elindítását követően a haladásjelző a futó vizsgálati feladat neve melletti mezőben jelenik meg a **Feladatok** részben a Kaspersky Endpoint Security fő ablakának **Védelem és felügyelet** lapján.

A vizsgálat eredményeit és a vizsgálati feladat elvégzése során történt eseményeket a Kaspersky Endpoint Security egy jelentésben naplózza.

A vizsgálati feladatok elindítása és leállítása

A kiválasztott vizsgálati feladat futásmódjától függetlenül a vizsgálati feladatok bármikor elindíthatók és leállíthatók.

Vizsgálati feladat elindítása és leállítása:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Feladatok** részre.

   Megnyílik a **Feladatok** rész.
4. Kattintson a jobb egérgombbal a vizsgálati feladat sorában lévő helyi menü megnyitásához.

   Megnyílik a vizsgálati feladat műveleteit tartalmazó menü.
5. Végezze el az alábbiak egyikét:

   - Ha szeretné elindítani a vizsgálati feladatot, válassza a menü **Vizsgálat indítása** lehetőségét.

     A vizsgálati feladat nevét tartalmazó gombtól jobbra látható haladási állapota *Fut* értékre vált.
   - Ha szeretné leállítani a vizsgálati feladatot, válassza a menü **Vizsgálat leállítása** lehetőségét.

     A vizsgálati feladat nevét tartalmazó gombtól jobbra látható haladási állapota *Leállít* értékre vált.

A vizsgálati feladatok beállításainak megadása

A vizsgálati feladatok beállításainak megadásához az alábbiakat végezheti el:

- A biztonsági szint módosítása.

  Kiválaszthatja az előre beállított biztonsági szintek egyikét, de kézileg is megadhatja a beállításokat. Ha módosítja a biztonsági szint beállításait, mindig visszatérhet az ajánlott biztonsági szintbeállításokhoz.
- A Kaspersky Endpoint Security által fertőzött fájl észlelésekor elvégzett művelet módosítása.
- A vizsgálat hatókörének szerkesztése.

  A vizsgálat hatókörét kiterjesztheti vagy szűkítheti a vizsgálandó objektumok hozzáadásával és eltávolításával, vagy a vizsgálandó fájlok típusának módosítása révén.
- Vizsgálat optimalizálás.

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).

Bekapcsolhatja az iChecker és az iSwift technológiák használatát is. Ezek a technológiák oly módon optimalizálják a fájlok vizsgálatának sebességét, hogy kizárják a legutóbbi vizsgálat óta nem módosult fájlokat.

- Az összetett fájlok vizsgálatának beállítása.
- A vizsgálatmódok beállítása.

  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. A heurisztikus elemzés során a Kaspersky Endpoint Security elemzi az objektumok tevékenységét az operációs rendszerben. A heurisztikus elemzés képes az olyan rosszindulatú objektumokat észlelni, amelyeknek még nem szerepel bejegyzése a Kaspersky Endpoint Security adatbázisában.

- Vizsgálati feladat futásmódjának kiválasztása.

  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.

  A vizsgálati feladat alkalmazásindítást követő elindulását el is halaszthatja, ha a vizsgálati feladat **Ütemezés szerint** frissítési feladat futásmódot választja ki, és a Kaspersky Endpoint Security kezdési időpontja egyezik a vizsgálati feladat indítási ütemezésével. A vizsgálati feladatok futtatására csak akkor kerülhet sor, ha letelik a megadott időtartam a Kaspersky Endpoint Security elindulása után.

- A vizsgálati feladatok futásának beállítása másik felhasználói fiók nevében.
- A cserélhető meghajtók csatlakoztatásakor történő vizsgálat beállításainak megadása.

A biztonsági szint módosítása

A vizsgálati feladatok elvégzéséhez a Kaspersky Endpoint Security különböző beállítás-kombinációkat használ. Ezeket az alkalmazásban mentett beállítás-kombinációkat *biztonsági szinteknek* nevezzük. Három előre beállított biztonsági szint létezik: **Magas**, **Ajánlott** és **Alacsony**. Az **Ajánlott** biztonsági szint beállításai tekinthetők optimálisnak. A Kaspersky szakértői ezeket ajánlják.

Biztonsági szint módosítása:

1. Kattintson a fő alkalmazásablakban a **Beállítások** gombra.
2. Az ablak bal oldali részén, a **Feladatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt.

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.
3. A **Biztonsági szint** részben végezze el az alábbiak egyikét:

   - Ha valamelyik előtelepített biztonsági szintet (**Magas**, **Ajánlott** vagy **Alacsony**) szeretné alkalmazni, válassza ki a csúszkával.

- Ha egyéni biztonsági szintet szeretne beállítani, kattintson a **Beállítások** gombra, majd a vizsgálati feladat nevét viselő megjelenő ablakban adja meg a beállításokat.

  Egyéni biztonsági szint beállítását követően a biztonsági szint neve a **Biztonsági szint** részben **Egyéni** értékre vált.

- Ha a biztonsági szintet **Ajánlott** értékre szeretné módosítani, kattintson az **Alapértelmezett** gombra.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A fertőzött fájlokon végrehajtandó művelet módosítása

A fertőzött fájlokon végrehajtandó művelet módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt.

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. Válassza ki a kívánt lehetőséget a **Művelet fenyegetés észlelésekor** részben:

   - **Művelet automatikus kiválasztása**.

   - **Művelet végrehajtása**.

4. Ha az előző lépésben a **Művelet végrehajtása** lehetőséget választotta, akkor jelölje be az alábbi jelölőnégyzeteket:

   - Jelölje be a **Vírusmentesítés** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security vírusmentesítse azokat az objektumokat, amelyekben fenyegetéseket észlel.

     A Kaspersky Endpoint Security a **Eltávolítás** műveletet a lehetőség kiválasztása esetén is elvégzi azokon a fájlokon, amelyek a Windows Store alkalmazás részei.

   - Jelölje be a **Törlés** jelölőnégyzetet, ha azt szeretné, hogy a Kaspersky Endpoint Security törölje az objektumokat, amelyekben fenyegetéseket észlel.

   - Jelölje be a **Vírusmentesítés** és a **Törlés** jelölőnégyzetet egyaránt, ha azt szeretné, hogy a Kaspersky Endpoint Security megpróbálja vírusmentesíteni azokat az objektumokat, amelyekben fenyegetéseket észlel, és amelyeknél nem jár sikerrel, azokat törölje.

   - Törölje a **Vírusmentesítés** és a **Törlés** jelölőnégyzetet egyaránt, ha azt szeretné, hogy a Kaspersky Endpoint Security ne tegyen semmit azoknál az objektumoknál, amelyekben fenyegetéseket észlel, hanem mindössze a felhasználót értesítse az objektumok vizsgálatának eredményeiről.

5. A módosítások mentéséhez kattintson a **Mentés** gombra.

A vizsgálandó objektumok listájának elkészítése

A vizsgálni kívánt objektumok listáját az alábbi két módszer valamelyikével készítheti el:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

> Ez a módszer csak a **Teljes vizsgálat** és a **Kritikus területek vizsgálata** feladatoknál használható. Az **Egyéni vizsgálat** feladat során vizsgálandó objektumok listáját kizárólag a **Védelem és felügyelet** lapon lehet elkészíteni.

A vizsgálni kívánt objektumok listájának elkészítése a Védelem és felügyelet lapon a fő alkalmazásablakban:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Feladatok** részre.

   Megnyílik a **Feladatok** rész.
4. A feladat nevét tartalmazó sor helyi menüjének megnyitásához kattintson a jobb egérgombbal, és válassza ki a **Vizsgálat hatóköre** lehetőséget.

   Megnyílik a **Vizsgálat hatóköre** ablak.
5. Ha egy új objektumot szeretne hozzáadni a vizsgálat hatóköréhez:
   a. Kattintson a **Hozzáadás** gombra.

      Megnyílik a **Vizsgálat hatókörének kiválasztása** ablak.
   b. Válassza ki az objektumot, majd kattintson a **Hozzáadás** lehetőségre.

      A **Vizsgálat hatókörének kiválasztása** ablakban kiválasztott összes objektum megjelenik a **Vizsgálat hatóköre** listán.
   c. Kattintson az **OK** gombra.
6. Ha egy, a vizsgálat hatókörébe tartozó objektum elérési útját módosítani szeretné:
   a. Válassza ki a vizsgálat hatókörébe tartozó objektumot.
   b. Kattintson a **Szerkesztés** gombra.

      Megnyílik a **Vizsgálat hatókörének kiválasztása** ablak.
   c. Adja meg a vizsgálat hatókörébe tartozó objektum új elérési útját.
   d. Kattintson az **OK** gombra.
7. Ha egy objektumot el szeretne távolítani a vizsgálat hatóköréből:
   a. Válassza ki a vizsgálat hatóköréből eltávolítani kívánt objektumot.

      Több objektumot úgy választhat ki, ha kijelölésük közben lenyomva tartja a **Ctrl** billentyűt.
   b. Kattintson az **Eltávolítás** gombra.

      A törlés megerősítésére szolgáló ablak megnyílik.

c. Az eltávolítást megerősítő ablakban kattintson az **Igen** gombra.

Az alapértelmezett vizsgálati hatókörbe tartozó objektumokat nem lehet eltávolítani, illetve szerkeszteni.

8. Törölje az objektum neve melletti négyzet bejelölését a **Vizsgálat hatóköre** listán, ha ki szeretné zárni az objektumot a vizsgálat hatóköréből.

   Az objektum ekkor a vizsgálat hatókörébe tartozó objektumok listáján marad, de a vizsgálati feladat futásakor nem kerül sor vizsgálatára.

9. Kattintson az **OK** gombra.

10. A módosítások mentéséhez kattintson a **Mentés** gombra.

A vizsgálni kívánt objektumok listájának elkészítése az alkalmazás beállításainak ablakában:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat** vagy a **Kritikus területek vizsgálata**) nevét tartalmazó alrészt.

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. Kattintson a **Vizsgálat hatóköre** gombra.

   Megnyílik a **Vizsgálat hatóköre** ablak.

4. Készítse el a vizsgálni kívánt objektumok listáját az előző utasítások 5–10. lépései szerint.

A vizsgálandó fájlok típusának kiválasztása

A vizsgálni kívánt fájltípusokat az alábbi két módon választhatja ki:

- A **Védelem és felügyelet** lapon a fő alkalmazásablakban.
- Az alkalmazás beállításai ablakból

Ez a módszer csak a **Teljes vizsgálat** és a **Kritikus területek vizsgálata** feladatoknál használható. Az **Egyéni vizsgálat** feladat során vizsgálandó fájltípusokat kizárólag a **Védelem és felügyelet** lapon lehet kiválasztani.

A vizsgálni kívánt fájltípusok kiválasztása a Védelem és felügyelet lapon a fő alkalmazásablakban:

1. Nyissa meg az alkalmazás főablakát.

2. Válassza ki a **Védelem és felügyelet** lapot.

3. Kattintson a **Feladatok** részre.

   Megnyílik a **Feladatok** rész.

4. A feladat nevét tartalmazó sor helyi menüjének megnyitásához kattintson a jobb egérgombbal, és válassza ki a **Beállítások** lehetőséget.

   Megnyílik a kiválasztott vizsgálati feladat nevét tartalmazó ablak.

5. Válassza ki a kiválasztott feladat nevét tartalmazó ablakban a **Hatókör** lapot.

6. A **Fájltípusok** részben adja meg azokat a fájltípusokat, amelyeket a vizsgálati feladat futásakor vizsgálni szeretne:

   - Ha minden fájlt vizsgálni kíván, válassza a **Minden fájl** lehetőséget.
   - Ha a fertőzés által leginkább veszélyeztetett formátumú fájlokat szeretné vizsgálni, válassza a **Formátum alapján vizsgált fájlok** lehetőséget.
   - Ha a fertőzés által általában veszélyeztetett kiterjesztésű fájlokat szeretné vizsgálni, válassza a **Kiterjesztés alapján vizsgált fájlok** lehetőséget.

   A vizsgálandó fájltípusok kiválasztásakor vegye figyelembe az alábbiakat:

   - A rosszindulatú kódok behatolási és későbbi aktiválódási valószínűsége bizonyos fájlformátumok (például .TXT) esetén meglehetősen alacsony. Más formátumok (például .exe, .dll és .doc) ugyanakkor végrehajtható kódot tartalmaz(hat)nak. A rosszindulatú kódok behatolásának és aktiválódásának kockázata az ilyen fájloknál magas.
   - Egy behatoló vírust vagy egyéb rosszindulatú programot küldhet a számítógépre olyan végrehajtható fájlban, amelyet .txt kiterjesztésűre nevezett át. Ha a fájlok kiterjesztés alapján történő vizsgálatát választja, az alkalmazás kihagyja az ilyen fájlt a vizsgálatból. Ha a formátum alapján történő vizsgálat van kiválasztva, a Fájl víruskereső kiterjesztéstől függetlenül elemzi a fájl fejlécét. Ha az elemzés felfedi, hogy a fájl EXE formátumú, akkor az alkalmazás megvizsgálja a fájlt.

7. Kattintson a vizsgálati feladat nevét tartalmazó ablakban az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

A vizsgálni kívánt fájltípusok kiválasztása az alkalmazás beállításainak ablakában:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat** vagy a **Kritikus területek vizsgálata**) nevét tartalmazó alrészt.

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a kiválasztott vizsgálati feladat nevét tartalmazó ablak.

4. Válassza ki a kiválasztott feladat nevét tartalmazó ablakban a **Hatókör** lapot.

5. Végezze el az előző utasítások 5–7. lépését.

A fájlvizsgálat optimalizálása

A fájlvizsgálat optimalizálása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt.

Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a kiválasztott vizsgálati feladat nevét tartalmazó ablak.

4. A megnyíló ablakban válassza a **Hatókör** lapot.

5. A **Vizsgálat optimalizálás** részben végezze el az alábbi műveleteket:

   - Jelölje be a **Csak az új és módosult fájlok vizsgálata** jelölőnégyzetet.
   - Jelölje be a **Azon fájlok kihagyása, melyek vizsgálata tovább tart mint** jelölőnégyzetet, és adja meg a fájlok egyenkénti vizsgálatának időtartamát (másodpercben).

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

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.

Az összetett fájlok vizsgálatának beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt.

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a kiválasztott vizsgálati feladat nevét tartalmazó ablak.

4. A megnyíló ablakban válassza a **Hatókör** lapot.

5. Adja meg az **Összetett fájlok vizsgálata** részben a vizsgálni kívánt összetett fájlok típusát: archívumok, telepítőcsomagok, Office formátumú fájlok, e-mail formátumú fájlok, illetve jelszóval védett archívumok.

6. Ha a **Csak az új és módosult fájlok vizsgálata** jelölőnégyzet nincs bejelölve a **Vizsgálat optimalizálás** részben, akkor kattintson az összetett fájltípus neve melletti **összes/új** hivatkozásra, ha meg szeretné adni az egyes összetett fájltípusoknál, hogy az összes vagy csak az új ilyen típusú fájlt vizsgálni szeretné-e.

   A hivatkozás értéke megváltozik, ha a felhasználó rákattint.

   Ha a **Csak az új és módosult fájlok vizsgálata** jelölőnégyzet be van jelölve, akkor csak az új fájlok vizsgálatára kerül sor.

7. Kattintson a **További** gombra.

   Megnyílik az **Összetett fájlok** ablak.

8. A **Méretkorlát** részben végezze el az alábbiak egyikét:

   - Ha nem szeretné kicsomagolni a nagy méretű összetett fájlokat, jelölje be az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet, és adja meg a szükséges értéket a **Maximális fájlméret** mezőben.
   - Ha mérettől függetlenül ki szeretné csomagolni a nagy méretű összetett fájlokat, törölje az **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzetet.

   A Kaspersky Endpoint Security az archívumokból kibontott nagy méretű fájlokat attól függetlenül vizsgálja, hogy a **Ne csomagoljon ki nagy összetett fájlokat** jelölőnégyzet be van-e jelölve.

9. Kattintson az **OK** gombra.
10. Kattintson a vizsgálati feladat nevét tartalmazó ablakban az **OK** gombra.
11. A módosítások mentéséhez kattintson a **Mentés** gombra.

A vizsgálatmódok használata

A vizsgálatmódok használata:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt.

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.
3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a kiválasztott vizsgálati feladat nevét tartalmazó ablak.
4. A megnyíló ablakban válassza a **További** lapot.
5. Ha azt szeretné, hogy az alkalmazás a vizsgálati feladat futtatásakor heurisztikus elemzést alkalmazzon, akkor a **Vizsgálatmódok** részben jelölje be a Heurisztikus elemzés jelölőnégyzetet. Ezután állítsa be a heurisztikus elemzés szintjét a csúszkával: **Egyszerű vizsgálat**, **Közepes vizsgálat** vagy **Alapos vizsgálat**.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A vizsgálati technológiák használata

A vizsgálati technológiák használata:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt vizsgálati feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt.

Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. A **Biztonsági szint** részben kattintson a **Beállítások** gombra.

   Megnyílik a kiválasztott vizsgálati feladat nevét tartalmazó ablak.

4. A megnyíló ablakban válassza a **További** lapot.

5. A **Vizsgálati technológiák** részben jelölje be a jelölőnégyzeteket azon technológiák neve mellett, amelyeket a vizsgálat során használni szeretne.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Vizsgálati feladat futásmódjának kiválasztása

Vizsgálati feladat futásmódjának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt**.**

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.

3. Kattintson a **Futásmód** gombra.

   Ezzel megnyílik egy ablak a kiválasztott feladat tulajdonságaival a **Futásmód** lapon.

4. Válassza ki a **Futásmód** részben a feladat futásmódját: **Kézileg** vagy **Ütemezés szerint**.

5. Ha az **Ütemezés szerint** lehetőséget választja, adja meg az ütemezés beállításait. Ehhez:

   a. Válassza ki a **Gyakoriság** legördülő listán a feladat futási gyakoriságát (**Perc**, **Óra**, **Nap**, **Hetente**, **Megadott időpontban**, **Havonta**, illetve **Az alkalmazás elindulása után**, **Minden frissítés után**).

   b. Adja meg a kiválasztott gyakoriság függvényében a feladatfutás ütemezését meghatározó speciális beállításokat.

   c. Ha azt szeretné, hogy a Kaspersky Endpoint Security a kihagyott feladatokat a lehető leghamarabb megkezdje, jelölje be a **Kihagyott feladatok futtatása** jelölőnégyzetet.

   > Ha a **Perc**, az **Óra**, az **Az alkalmazás elindulása után** vagy a **Minden frissítés után** elem van kiválasztva a **Gyakoriság** legördülő listán, a **Kihagyott feladatok futtatása** jelölőnégyzet nem használható.

   a. Ha azt szeretné, hogy a Kaspersky Endpoint Security függesszen fel egy feladatot, ha a számítógép erőforrásai korlátozottan állnak rendelkezésre, jelölje be a **Csak akkor fusson, ha a számítógép üresjáratban van** jelölőnégyzetet.

   Ez az ütemezési lehetőség segít a számítógép erőforrásainak megőrzésében.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Vizsgálati feladat elindítása másik felhasználói fiók nevében

Alapértelmezés szerint a vizsgálati feladatok azon fiók jogosultságaival fut, amelybe a felhasználó az operációs rendszeren bejelentkezett. Ugyanakkor előfordulhat, hogy egy vizsgálati feladatot egy másik felhasználói fiókból kell elindítani. A vizsgálati feladat beállításaiban megadhat egy olyan felhasználót, akinek megfelelőek a jogosultságai, és így a vizsgálati feladatot futtathatja az adott felhasználó fiókja nevében.

Vizsgálati feladat elindításának beállítása másik felhasználó fiókjában:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, az **Ütemezett vizsgálatok** részben válassza ki a kívánt feladat (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**) nevét tartalmazó alrészt**.**

   Az ablak jobb oldali részén megjelennek a kiválasztott vizsgálati feladat beállításai.
3. Kattintson a **Futásmód** gombra.

   Ezzel megnyílik egy ablak a kiválasztott feladat tulajdonságaival a **Futásmód** lapon.
4. A **Futásmód** lapon lévő **Felhasználó** részben jelölje be a **Feladat futtatása másként** jelölőnégyzetet.
5. A **Név** mezőbe írja be annak a felhasználói fióknak a nevét, amelynek a jogosultságai a vizsgálati feladat elindításához szükségesek.
6. A **Jelszó** mezőbe írja be annak a felhasználói fióknak a jelszavát, amelynek a jogosultságai a vizsgálati feladat elindításához szükségesek.
7. Kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Cserélhető meghajtók vizsgálata a számítógéphez történő csatlakoztatásukkor

Egyes rosszindulatú programok az operációs rendszer sebezhetőségeit kihasználva megsokszorozzák magukat a helyi hálózatokon és a cserélhető meghajtókon. A Kaspersky Endpoint Security lehetővé teszi a cserélhető meghajtókon a vírusok és egyéb rosszindulatú programok jelenlétének ellenőrzését a meghajtók számítógéphez való csatlakoztatásakor.

A cserélhető meghajtók csatlakoztatásakor történő vizsgálati beállításainak megadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki az **Ütemezett vizsgálatok** részt.

   A feladatbeállítások az ablak jobb oldalán jelennek meg.
3. A **Cserélhető meghajtók vizsgálata csatlakoztatáskor** részben válassza ki a kívánt műveletet a **Művelet a cserélhető meghajtó kapcsolaton** legördülő listán:

- **Ne vizsgálja**
- **Részletes vizsgálat**

  Ebben a módban a Kaspersky Endpoint Security a cserélhető meghajtókon lévő összes fájlt megvizsgálja, köztük az összetett objektumokban találhatóakat is.
- **Gyors vizsgálat**

  Ebben a módban a Kaspersky Endpoint Security csak a potenciálisan megfertőzhető fájlokat vizsgálja, és nem csomagolja ki az összetett objektumokat.

4. Ha azt szeretné, hogy a Kaspersky Endpoint Security csak azokat a cserélhető meghajtókat vizsgálja meg, amelyek mérete nem haladja meg a megadott értéket, jelölje be a **Cserélhető meghajtó maximális mérete** jelölőnégyzetet, és adja meg a mellette lévő mezőben az értéket megabájtban.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

A feldolgozatlan fájlok kezelése

Ez a rész utasításokat tartalmaz az olyan fertőzött és valószínűleg fertőzött fájlok kezelésére vonatkozóan, amelyeket a Kaspersky Endpoint Security nem dolgozott fel, miközben a számítógépen megvizsgálta a vírusok és egyéb fenyegetések jelenlétét.

A feldolgozatlan fájlok

Kaspersky Endpoint Security naplózza az olyan fájlokra vonatkozó adatokat, amelyeket valamilyen okból fel nem dolgozott fel. Ezek az adatok a feldolgozatlan fájlok listájára események formájában kerülnek fel.

A fertőzött fájlok akkor tekinthetők *feldolgozottnak*, ha a Kaspersky Endpoint Security a megadott alkalmazásbeállításoknak megfelelően az alábbi műveletek egyikét elvégzi rajtuk, miközben a számítógépen vírusok és egyéb fenyegetések jelenlétét vizsgálja:

- Vírusmentesítés.
- Eltávolítás.
- Törlés, ha a vírusmentesítés nem sikerül.

A fertőzött fájlok akkor tekinthetők *feldolgozatlannak*, ha a Kaspersky Endpoint Security 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 vizsgálati feladatok **Művelet fenyegetés észlelésekor** részében a **Tájékoztatás** művelet van kiválasztva, és amikor megjelenik a fertőzött fájlról szóló értesítés, a felhasználó a **Átugrás** műveletet választja.

A feldolgozatlan fájlok listáján kézileg elindíthat Egyéni vizsgálat feladatot az adatbázisok és alkalmazásmodulok frissítését követően. A fájl állapota a vizsgálat után változhat. A fájlokon állapotuktól függően elvégezheti a szükséges műveleteket.

Például az alábbi műveleteket végezheti el:

- Törölheti a *Fertőzött* állapotú fájlokat.
- Visszaállíthatja a fontos információkat tartalmazó fertőzött fájlokat, és visszaállíthatja a *Vírusmentesített* és *Nem fertőzött* jelölésű fájlokat.
- Karanténba helyezheti a *Valószínűleg fertőzött* állapotú fájlokat.

A feldolgozatlan fájlok listájának kezelése

A feldolgozatlan fájlok listája táblázat formájában jelenik meg.

A következő műveleteket végezheti el a feldolgozatlan fájlokkal:

- A feldolgozatlan fájlok listájának megtekintése.
- A feldolgozatlan fájlok vizsgálata a Kaspersky Endpoint Security adatbázisainak és moduljainak aktuális verziójával.
- A feldolgozatlan fájlok listáján lévő fájlok visszaállítása eredeti mappájukba vagy tetszés szerinti más mappába (ha az eredeti mappába nem lehet írni).
- Fájlok törlése a feldolgozatlan fájlok listájáról.
- A feldolgozatlan fájlt eredetileg tartalmazó mappa megnyitása.

A táblázatban lévő adatok kezelése során a következő műveleteket is elvégezheti:

- A feldolgozatlan fájl eseményeinek szűrése oszlopérték vagy egyéni szűrési feltételek szerint.
- A feldolgozatlan fájlok eseményei keresési funkciójának használata.
- A feldolgozatlan fájlesemények rendezése.
- A feldolgozatlan fájlok listáján látható oszlopok sorrendjének és készletének módosítása.
- A feldolgozatlan fájlesemények csoportosítása.

Szükség esetén a kijelölt feldolgozatlan fájleseményeket a vágólapra másolhatja.

Feldolgozatlan fájlok Egyéni vizsgálat feladatának megkezdése

A feldolgozatlan fájlok Egyéni vizsgálat feladatát kézileg elindíthatja. A vizsgálatot például akkor indíthatja el, ha a legutóbbi vizsgálat valamilyen okból megszakadt, vagy ha az adatbázisok és alkalmazásmodulok legutóbbi frissítését követően újra meg szeretné vizsgálni a feldolgozatlan fájlokat.

Feldolgozatlan fájlok Egyéni vizsgálat feladatának megkezdése:

1. Nyissa meg az alkalmazás főablakát.

2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Feldolgozatlan fájlok** lapot.
4. Válasszon ki a **Feldolgozatlan fájlok** lapon a vizsgálni kívánt fájlokhoz tartozó egy vagy több eseményt.
   Több eseményt úgy választhat ki, ha kijelölésük közben lenyomva tartja a **Ctrl** billentyűt.
5. Az Egyéni vizsgálat feladatot az alábbi módszerek egyikével indítsa el:
   - Kattintson az **Ismételt vizsgálat** gombra.
   - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza az **Ismételt vizsgálat** lehetőséget.

Fájlok törlése a feldolgozatlan fájlok listájáról

Fájlok törlése a feldolgozatlan fájlok listájáról:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Feldolgozatlan fájlok** lapot.
4. Válasszon ki a **Feldolgozatlan fájlok** lapon fájlokhoz tartozó egy vagy több törölni kívánt eseményt.
   Több eseményt úgy választhat ki, ha kijelölésük közben lenyomva tartja a **Ctrl** billentyűt.
5. A fájlokat az alábbi módok egyikével törölheti:
   - Kattintson az **Eltávolítás** gombra.
   - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Törlés** lehetőséget.

Sebezhetőségi vizsgálat

Ez a rész tájékoztatást nyújt a Sebezhetőségi vizsgálati feladat jellemzőire és beállításaira vonatkozóan, és ismerteti a Kaspersky Endpoint Security által a Sebezhetőségi vizsgálati feladatok futása során észlelt sebezhetőségek listájának kezelését.

A futó alkalmazások sebezhetőségeire vonatkozó adatok megtekintése

A futó alkalmazások sebezhetőségeire vonatkozó adatok akkor állnak rendelkezésre, ha a Kaspersky Endpoint Security munkaállomásokra szánt Microsoft Windows rendszert futtató számítógépen van telepítve. Ezek az adatok nem állnak rendelkezésre, ha a Kaspersky Endpoint Security fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépen van telepítve.

A futó alkalmazások sebezhetőségeire vonatkozó adatok megtekintése:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Nyissa meg a **Végpontfelügyelő** részt.
4. Kattintson az **Alkalmazástevékenység-figyelő** gombra.

   Megnyílik az **Alkalmazásjogosultság-felügyelő** ablak az **Alkalmazástevékenység-figyelő** lapon. Az **Alkalmazástevékenység-figyelő** táblázatban megtekintheti az operációs rendszeren futó alkalmazások tevékenységének összegzését. A futó alkalmazások sebezhetőségének Sebezhetőség-figyelő összetevő által megállapított súlyossága a **Sebezhetőség súlyossága** oszlopban látható.

A Sebezhetőségi vizsgálat feladat

Az operációs rendszer sebezhetőségét okozhatják például programozási és tervezési hibák, gyenge jelszavak vagy rosszindulatú programok tevékenysége. A sebezhetőségi vizsgálat során az alkalmazás elemzi az operációs rendszert, és rendellenességeket és a Microsoft és más forgalmazók alkalmazásaiban sérült beállításokat keres.

A sebezhetőségi vizsgálat az operációs rendszer biztonságának diagnosztikai elemzését végzi el, és észleli azokat a szoftverfunkciókat, amelyeket a támadók rosszindulatú objektumok terjesztésére és személyes adatok megszerzésére használhatnak fel.

A Sebezhetőségi vizsgálat feladat elindítását követően a haladásjelző a **Sebezhetőségi vizsgálat** feladat neve melletti mezőben jelenik meg a **Feladatok** részben a Kaspersky Endpoint Security fő ablakának **Védelem és felügyelet** lapján.

A Sebezhetőségi vizsgálat feladatok eredményeit a rendszer jelentésekben naplózza.

Sebezhetőségi vizsgálat feladat indítása és leállítása

A Sebezhetőségi vizsgálatok feladat kiválasztott futásmódjuktól függetlenül bármikor elindíthatók és leállíthatók.

Sebezhetőségi vizsgálat feladat indítása és leállítása:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Kattintson a **Feladatok** részre.

   Megnyílik a **Feladatok** rész.
4. Kattintson a jobb egérgombbal a Sebezhetőségi vizsgálati feladat sorában lévő helyi menü megnyitásához.

   Megnyílik a Sebezhetőségi vizsgálati feladat műveleteit tartalmazó menü.
5. Végezze el az alábbiak egyikét:

   - Ha szeretné elindítani a Sebezhetőségi vizsgálati feladatot, válassza a menü **Vizsgálat indítása** lehetőségét.

     A Sebezhetőségi vizsgálati feladat nevét tartalmazó gombtól jobbra látható haladási állapota *Fut* értékre vált.

   - Ha szeretné leállítani a Sebezhetőségi vizsgálati feladatot, válassza a menü **Vizsgálat leállítása** lehetőségét.

     A Sebezhetőségi vizsgálati feladat nevét tartalmazó gombtól jobbra látható haladási állapota *Leállt* értékre vált.

A Sebezhetőségi vizsgálat beállításainak megadása

A Sebezhetőségi vizsgálat beállításainak megadásához az alábbiakat végezheti el:

- Sebezhetőségi vizsgálat hatókörének létrehozása.

  A védelem hatókörét kiterjesztheti vagy szűkítheti azon alkalmazások hozzáadásával és eltávolításával, amelyekben a sebezhetőségek vizsgálatára sor kerül.

- Sebezhetőségi vizsgálati feladat futásmódjának kiválasztása.

  Ha a feladat futtatása valamilyen okból (például a számítógép abban az időpontban nem volt bekapcsolva) nem volt lehetséges, beállíthatja a kimaradt feladatot úgy is, hogy automatikusan elinduljon, amint lehet.

- A feladatok futásának beállítása másik felhasználói fiók jogosultságaival.

  Alapértelmezés szerint a vizsgálati feladatok azon fiók jogosultságaival fut, amelybe a felhasználó az operációs rendszeren bejelentkezett. Ugyanakkor előfordulhat, hogy egy vizsgálati feladatot egy másik felhasználói fiókból kell elindítani. A feladat beállításaiban megadhat egy olyan felhasználót, akinek megfelelőek a jogosultságai, és így a feladatot futtathatja az adott felhasználó fiókja nevében.

Sebezhetőségi vizsgálat hatókörének létrehozása

A sebezhetőségi vizsgálat hatóköre egy szoftverforgalmazó vagy a szoftver telepítési mappájának elérési útja (például az összes olyan Microsoft-alkalmazás, amely a Program Files mappában található).

Sebezhetőségi vizsgálat hatókörének létrehozása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Sebezhetőségi vizsgálat** lehetőséget.

   Az ablak jobb oldali részén a Sebezhetőségi vizsgálat feladat beállításai láthatók.

3. A **Vizsgálat hatóköre** részben:

   a. Ha azt szeretné, hogy a Kaspersky Endpoint Security a számítógépen telepített Microsoft-alkalmazások sebezhetőségeit vizsgálja, jelölje be a **Microsoft** jelölőnégyzetet.

   b. Ha azt szeretné, hogy a Kaspersky Endpoint Security a számítógépen telepített összes, a Microsoft-alkalmazásoktól eltérő alkalmazások sebezhetőségeit vizsgálja, jelölje be az **Más forgalmazók** jelölőnégyzetet.

   c. A **További sebezhetőségi vizsgálat területe** részben kattintson a **Beállítások** gombra.

      Megnyílik a **Sebezhetőségi vizsgálat hatóköre** ablak.

   d. Hozza létre a sebezhetőségi vizsgálat hatókörét a **Hozzáadás** és az **Eltávolítás** gombokkal.

   e. A **Sebezhetőségi vizsgálat hatóköre** ablakban kattintson az **OK** gombra.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Sebezhetőségi vizsgálati feladat futásmódjának kiválasztása

Sebezhetőségi vizsgálati feladat futásmódjának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Sebezhetőségi vizsgálat** lehetőséget.

   Az ablak jobb oldali részén a Sebezhetőségi vizsgálat feladat beállításai láthatók.

3. Kattintson a **Futásmód** gombra.

   Ezzel megnyílik a **Futásmód** lap a **Sebezhetőségi vizsgálat** ablakban.

4. Válasszon ki a **Futásmód** részben a Sebezhetőségi vizsgálati feladat futásmódra vonatkozó lehetőségei közül egyet vagy többet:

   - Ha kézileg szeretné a Sebezhetőségi vizsgálati feladatot indítani, válassza ki a **Kézileg** lehetőséget.
   - Ha be szeretné állítani a Sebezhetőségi vizsgálati feladat indítási ütemezését, válassza ki az **Ütemezés szerint** lehetőséget.

5. Végezze el az alábbiak egyikét:

   - Ha a **Kézileg** lehetőséget választotta, lépjen a jelen utasítások 6. lépésére.
   - Ha az **Ütemezés szerint** lehetőséget választotta, adja meg a Sebezhetőségi vizsgálati feladat indítási beállításait. Ehhez:

      a. A **Gyakoriság** legördülő listán adja meg a Sebezhetőségi vizsgálati feladat indításának időpontját. Válasszon a következő lehetőségek közül: **Nap**, **Hetente**, **Megadott időpontban**, **Havonta**, **Az alkalmazás elindulása után**, illetve **Minden frissítés után**.

b. A **Gyakoriság** legördülő listán kiválasztott elemtől függően adja meg a Sebezhetőségi vizsgálati feladat kezdési idejét meghatározó beállítások értékeit.

c. Ha azt szeretné, hogy a Kaspersky Endpoint Security a kihagyott Sebezhetőségi vizsgálati feladatokat a lehető leghamarabb megkezdje, jelölje be a **Kihagyott feladatok futtatása** jelölőnégyzetet.

> Ha az **Az alkalmazás elindulása után** vagy a **Minden frissítés után** elem van kiválasztva a **Gyakoriság** legördülő listán, a **Kihagyott feladatok futtatása** jelölőnégyzet nem használható.

6. Kattintson az **OK** gombra.

7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Sebezhetőségi vizsgálati feladat elindítása másik felhasználói fiók jogosultságaival

Alapértelmezés szerint a Sebezhetőségi vizsgálati feladatok azon fiók jogosultságaival futnak, amelybe a felhasználó az operációs rendszeren bejelentkezett. Ugyanakkor előfordulhat, hogy a Sebezhetőségi vizsgálati feladatot egy másik felhasználói fiókból kell elindítani. A Sebezhetőségi vizsgálati feladat beállításaiban megadhat egy olyan felhasználót, akinek megfelelőek a jogosultságai, és így a Sebezhetőségi vizsgálati feladatot elindíthatja az adott felhasználó fiókja nevében.

A Sebezhetőségi vizsgálati feladat elindításának beállítása másik felhasználó fiókjában:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki a **Sebezhetőségi vizsgálat** lehetőséget.

   Az ablak jobb oldali részén a Sebezhetőségi vizsgálat feladat beállításai láthatók.

3. Kattintson a **Futásmód** gombra.

   Ezzel megnyílik a **Futásmód** lap a **Sebezhetőségi vizsgálat** ablakban.

4. A **Futásmód** lapon lévő **Felhasználó** részben jelölje be a **Feladat futtatása másként** jelölőnégyzetet.

5. A **Név** mezőbe írja be annak a felhasználói fióknak a nevét, amelynek a jogosultságai a Sebezhetőségi vizsgálati feladat elindításához szükségesek.

6. A **Jelszó** mezőbe írja be annak a felhasználói fióknak a jelszavát, amelynek a jogosultságai a Sebezhetőségi vizsgálati feladat elindításához szükségesek.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

A sebezhetőségek listájának kezelése

A sebezhetőségek listájának kezelésekor a következő műveleteket hajthatja végre:

- Sebezhetőségek listájának megtekintése.
- A Sebezhetőségi vizsgálat feladat ismételt elindítása az adatbázisok és az alkalmazásmodulok frissítése után.
- A sebezhetőség részletes információinak és a kijavításra vonatkozó ajánlások megtekintése egy külön részben.
- A kijelölt bejegyzések elrejtése a sebezhetőségek listáján.
- A sebezhetőségek listájának szűrése fontossági szint szerint.
- A sebezhetőségek listájának szűrése *Javítva* és *Rejtett* állapotértékek szerint.

A táblázatban lévő adatok kezelése során a következő műveleteket is elvégezheti:

- A sebezhetőségek listájának szűrése oszlopértékek vagy egyéni szűrési feltételek szerint.
- A sebezhetőségek keresési funkciójának használata.
- A sebezhetőségek listáján lévő bejegyzések rendezése.
- A sebezhetőségek listáján látható oszlopok sorrendjének és elrendezésének módosítása.
- A sebezhetőségek listáján lévő bejegyzések csoportosítása.

A sebezhetőségek listája

A Kaspersky Endpoint Security a Sebezhetőségi vizsgálat feladatok eredményeit a sebezhetőségek listáján naplózza.

Miután áttekintette a konkrét sebezhetőségeket és elvégezte a kijavításuk érdekében javasolt műveleteket, a Kaspersky Endpoint Security a sebezhetőségek állapotát *Javítva* értékre állítja.

Ha a sebezhetőségi listán nem szeretné adott sebezhetőségek bejegyzéseit megjeleníteni, dönthet úgy, hogy elrejti őket. A Kaspersky Endpoint Security az ilyen sebezhetőségeket *Rejtett* állapotúra állítja.

A sebezhetőségek listája táblázat formájában jelenik meg. A táblázat minden sora a következő információkat tartalmazza:

- A sebezhetőség súlyossági szintjét jelző ikon. A sebezhetőségek alábbi súlyossági szintjei léteznek:
  - Ikon . **Kritikus**. Ez a súlyossági szint a nagyon veszélyes sebezhetőségekre vonatkozik, melyeket haladéktalanul ki kell javítani. A betolakodók aktívan kihasználják az ilyen szintű sebezhetőségeket, hogy a számítógép operációs rendszerét megfertőzzék, illetve a felhasználó személyes adataihoz hozzáférjenek. A Kaspersky azt javasolja, hogy a Kritikus súlyossági szintű sebezhetőségek kijavítása érdekében azonnal tegyen meg minden lépést.
  - Ikon . **Fontos**. Ez a súlyossági szint a fontos sebezhetőségekre vonatkozik, melyeket hamar ki kell javítani. A betolakodók aktívan kihasználhatják az ilyen szintű sebezhetőségeket. A betolakodók pillanatnyilag nem használják ki aktívan a Fontos súlyossági szintű sebezhetőségeket. A Kaspersky azt javasolja, hogy a Fontos súlyossági szintű sebezhetőségek kijavítása érdekében azonnal tegyen meg minden lépést.
  - Ikon . **Figyelmeztetés**. Ez a súlyossági szint az olyan sebezhetőségekre vonatkozik, amelyek kijavítása elhalasztható. Az ilyen sebezhetőségek a későbbiekben fenyegetést jelenthetnek a számítógép biztonságára nézve.

- Sebezhetőség azonosítója.
- Annak az alkalmazásnak a neve, amelyben sebezhetőség észlelhető.
- A sebezhetőség rövid leírása.
- A szoftver kiadójának adatai, ahogy a digitális aláírás jelzi.
- A sebezhetőség kijavításuk érdekében tett intézkedések eredménye.

A Sebezhetőségi vizsgálat feladat ismételt indítása

A korábban észlelt sebezhetőségekre vonatkozó információk frissítése érdekében újraindíthatja a Sebezhetőségi vizsgálat feladatot. A vizsgálati feladat újraindítása akkor lehet szükséges, ha a sebezhetőségi vizsgálat valamilyen okból megszakadt, illetve ha meg szeretné vizsgálni a számítógépen a sebezhetőséget az adatbázisok és alkalmazásmodulok legutóbbi frissítését követően.

A Sebezhetőségi vizsgálat feladat ismételt indítása:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Sebezhetőségek** fület.

   A **Sebezhetőségek** lap azon sebezhetőségek listáját tartalmazza, amelyeket a Kaspersky Endpoint Security a Sebezhetőségi vizsgálat feladat során az alkalmazásokban és az operációs rendszerben észlelt.
4. Kattintson a **Tárhelyek** ablak jobb alsó sarkában az **Ismételt vizsgálat** hivatkozásra.

   A Kaspersky Endpoint Security frissíti a sebezhetőségek listáján lévő sebezhetőségekre vonatkozó részletes információkat.

A javasolt hibajavítás telepítésével kijavított sebezhetőség állapota újabb sebezhetőségi vizsgálatot követően nem változik.

A sebezhetőség javítása

A sebezhetőségeket az operációs rendszer frissítésének telepítésével, az alkalmazás konfigurációjának módosításával, illetve az alkalmazás hibajavításának telepítésével javíthatja ki.

Az észlelt sebezhetőségek vonatkozhatnak a telepített alkalmazások másolataira az eredeti alkalmazások helyett. Hibajavítással csak akkor lehet sebezhetőséget kijavítani, ha az érintett alkalmazás telepítve van.

A sebezhetőség javítása:

1. Nyissa meg az alkalmazás főablakát.

2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.

3. A **Tárhelyek** ablakban válassza ki a **Sebezhetőségek** fület.

   A **Sebezhetőségek** lap azon sebezhetőségek listáját tartalmazza, amelyeket a Kaspersky Endpoint Security a Sebezhetőségi vizsgálat feladat során az alkalmazásokban és az operációs rendszerben észlelt.

4. Válassza ki a sebezhetőségek listáján az adott sebezhetőségnek megfelelő bejegyzést.

   A sebezhetőségre vonatkozó információkat és a kijavításra vonatkozó javaslatokat tartalmazó rész.

   Az egyes kiválasztott sebezhetőségeknél az alábbi információk találhatók meg:

   - Annak az alkalmazásnak a neve, amelyben sebezhetőség észlelhető.
   - Az az alkalmazásverzió, amelyben sebezhetőség észlelhető.
   - Sebezhetőség súlyossági szintje.
   - Sebezhetőség azonosítója.
   - A legutóbbi sebezhetőség észlelésének dátuma és időpontja.
   - A sebezhetőség kijavítására vonatkozó javaslatok (például az operációs rendszer frissítését vagy egy alkalmazás hibajavítását tartalmazó webhelyre mutató hivatkozás).
   - Hivatkozás a sebezhetőség leírását tartalmazó webhelyre.

5. A sebezhetőség részletes leírásának megtekintéséhez a **További információ** hivatkozásra kattintva megnyithat egy weboldalt, melyen a kijelölt sebezhetőséghez kapcsolódó fenyegetés leírása olvasható. A www.secunia.com webhelyen az alkalmazás jelenlegi verziójának szükséges frissítései letölthetők és telepíthetők.

6. Válasszon ki egyet a következő sebezhetőség-javítási módok közül:

   - Ha az alkalmazáshoz rendelkezésre áll egy vagy több hibajavítás, telepítse a szükséges hibajavítást a neve mellett látható utasításokat követve.
   - Ha rendelkezésre áll az operációs rendszer frissítése, telepítse a szükséges frissítést a neve mellett látható utasításokat követve.

   A sebezhetőség kijavítására a hibajavítás, illetve frissítés telepítését követően kerül sor. A Kaspersky Endpoint Security a sebezhetőség számára olyan állapotot oszt ki, amely jelzi, hogy ki van javítva. A kijavított sebezhetőség bejegyzése a sebezhetőségek listáján szürkén jelenik meg.

7. Ha az ablak alsó részében nem található információ a sebezhetőség kijavítására nézve, akkor a Kaspersky Endpoint Security adatbázisainak és moduljainak frissítését követően ismét elindíthatja a Sebezhetőségi vizsgálat feladatot. Mivel a Kaspersky Endpoint Security a rendszer vizsgálata során a sebezhetőségeket a sebezhetőségek adatbázisa alapján keresi, az alkalmazás frissítése után előfordulhat, hogy kijavított sebezhetőség bejegyzése bukkan fel.

A sebezhetőségek listáján lévő bejegyzések elrejtése

A kijelölt sebezhetőségi bejegyzéseket el lehet rejteni. A Kaspersky Endpoint Security a sebezhetőségek listáján kijelölt, rejtettként jelzett bejegyzésekhez *Rejtett* állapotot rendel hozzá. Ekkor a sebezhetőségek listáját szűrheti a *Rejtett* állapotérték szerint.

A sebezhetőségek listáján lévő bejegyzések elrejtése:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Sebezhetőségek** fület.

   A **Sebezhetőségek** lap azon sebezhetőségek listáját tartalmazza, amelyeket a Kaspersky Endpoint Security a Sebezhetőségi vizsgálat feladat során az alkalmazásokban és az operációs rendszerben észlelt.
4. Válassza ki a sebezhetőségek listáján az elrejteni kívánt sebezhetőségről szóló bejegyzést.

   A sebezhetőségre vonatkozó információkat és a kijavításra vonatkozó javaslatokat tartalmazó rész.
5. Kattintson az **Elrejt** gombra.

   A Kaspersky Endpoint Security a kiválasztott sebezhetőséghez hozzárendeli a *Rejtett* állapotot. A *Rejtett* állapotú sebezhetőségekről szóló bejegyzések a sebezhetőségek listájának végére kerülnek, és szürke színben jelennek meg.
6. Ha a sebezhetőségek listáján egy sebezhetőség bejegyzését el szeretné rejteni, jelölje be a lista tetején lévő **Rejtett** jelölőnégyzetet.

A sebezhetőségek listájának szűrése súlyossági szint szerint

A sebezhetőségek listájának szűrése súlyossági szint szerint:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Sebezhetőségek** fület.

   A **Sebezhetőségek** lap azon sebezhetőségek listáját tartalmazza, amelyeket a Kaspersky Endpoint Security a Sebezhetőségi vizsgálat feladat során az alkalmazásokban és az operációs rendszerben észlelt. A sebezhetőség súlyossági szintjét jelző három ikon (figyelmeztetés, fontos, kritikus) látható a sebezhetőségek listáján a **Súlyosság megjelenítése** sorban. Az ikonokra kattintva súlyossági szint szerint szűrheti a sebezhetőségi listát.
4. Kattintson a sebezhetőségek súlyossági szintjének egy, kettő vagy három ikonjára. A kiválasztott súlyossági szinteknek megfelelő sebezhetőségek megjelennek a listán. Ha meg szeretné szüntetni a listán egy adott súlyossági szintnek megfelelő sebezhetőségek megjelenítését, kattintson ismét az adott súlyossági szint ikonjára. Ha egyetlen súlyossági szint sincs kiválasztva, a sebezhetőségek listája üres.

A sebezhetőségi bejegyzések megadott szűrési feltételei a **Tárhelyek** ablak bezárása után mentésre kerülnek.

A sebezhetőségek listájának szűrése Javítva és Rejtett állapotértékek szerint

A sebezhetőségek listájának szűrése Javítva és Rejtett állapotértékek szerint:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.

3. A **Tárhelyek** ablakban válassza ki a **Sebezhetőségek** fület.

   A **Sebezhetőségek** lap azon sebezhetőségek listáját tartalmazza, amelyeket a Kaspersky Endpoint Security a Sebezhetőségi vizsgálat feladat során az alkalmazásokban és az operációs rendszerben észlelt.

4. A sebezhetőségek állapotát jelző jelölőnégyzetek a **Sebezhetőségek megjelenítése** beállítás mellett láthatók. A sebezhetőségek listájának *Javítva* állapot szerinti szűréséhez végezze el az alábbiak közül valamelyiket:

   - Ha a sebezhetőségek listáján a kijavított sebezhetőségeket meg szeretné jeleníteni, jelölje be a **Javítva** jelölőnégyzetet. A kijavított sebezhetőségek bejegyzései a sebezhetőségek listáján szürkén jelennek meg.

   - Ha a sebezhetőségek listáján a kijavított sebezhetőségeket el szeretné rejteni, törölje a **Javítva** jelölőnégyzetet.

5. A sebezhetőségek listájának *Rejtett* állapot szerinti szűréséhez végezze el az alábbiak közül valamelyiket:

   - Ha a sebezhetőségek listáján a rejtett sebezhetőségeket meg szeretné jeleníteni, jelölje be a **Rejtett** jelölőnégyzetet. A rejtett sebezhetőségek bejegyzései a sebezhetőségek listáján szürkén jelennek meg.

   - Ha a sebezhetőségek listáján a rejtett sebezhetőségeket el szeretné rejteni, törölje a **Rejtett** jelölőnégyzetet.

A sebezhetőségi bejegyzések megadott szűrési feltételei a **Tárhelyek** ablak bezárása után nem kerülnek mentésre.

Az alkalmazásmodulok integritásának ellenőrzése

Ez a rész tájékoztatást nyújt az integritási ellenőrzési feladat jellemzőivel és beállításaival kapcsolatban.

Az Integritás ellenőrzése feladat

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.

Az integritási ellenőrzési feladat elindítását követően a haladásjelző a feladat neve melletti mezőben jelenik meg a **Feladatok** részben a Kaspersky Endpoint Security fő ablakának **Védelem és felügyelet** lapján.

Az integritási ellenőrzési feladatok eredményeit a rendszer jelentésekben naplózza.

Az integritási ellenőrzési feladatok elindítása és leállítása

A kiválasztott futásmódjától függetlenül az integritási ellenőrzési feladatok bármikor elindíthatók és leállíthatók.

Az integritási ellenőrzési feladatok elindítása és leállítása:

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Védelem és felügyelet** lapot.
3. Nyissa meg a **Feladatok** részt.
4. Kattintson a jobb egérgombbal az integritási ellenőrizési feladat sorában lévő helyi menü megnyitásához.
5. Végezze el az alábbiak egyikét:
   - Ha szeretné elindítani az integritási ellenőrzési feladatot, válassza a menü **Vizsgálat indítása** lehetőségét.
     A feladat nevét tartalmazó gombtól jobbra látható haladási állapota *Fut* értékre vált.
   - Ha szeretné leállítani az integritási ellenőrzési feladatot, válassza a menü **Vizsgálat leállítása** lehetőségét.
     A feladat nevét tartalmazó gombtól jobbra látható haladási állapota *Leállít* értékre vált.

Integritási ellenőrzési feladat futásmódjának kiválasztása

Integritási ellenőrzési feladat futásmódjának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Ütemezett vizsgálatok** részében válassza ki az **Integritás ellenőrzés** lehetőséget.
   Az ablak jobb oldali részén az integritási ellenőrzési feladat beállításai láthatók.

3. A **Futásmód** részben válasszon egyet a következő lehetőségek közül:

   - Ha kézileg szeretné az integritási ellenőrzési feladatot indítani, válassza ki a **Kézileg** lehetőséget.
   - Ha be szeretné állítani az integritási ellenőrzési feladat indítási ütemezését, válassza ki az **Ütemezés szerint** lehetőséget.

4. Ha az előző lépésben az **Ütemezés szerint** lehetőséget választotta, adja meg a feladat futási ütemezésének beállításait. Ehhez:

   a. A **Gyakoriság** legördülő listán adja meg az integritási ellenőrzési feladat indításának időpontját. Válasszon a következő lehetőségek közül: **Perc**, **Óra**, **Nap**, **Hetente**, **Megadott időpontban**, **Havonta**, illetve **Az alkalmazás elindulása után**.

   b. A **Gyakoriság** legördülő listán kiválasztott elemtől függően adja meg a feladat kezdési idejét meghatározó beállítások értékeit.

   c. Ha azt szeretné, hogy a Kaspersky Endpoint Security a kihagyott integritási ellenőrzési feladatokat a lehető leghamarabb megkezdje, jelölje be a **Kihagyott feladatok futtatása** jelölőnégyzetet.

      Ha az **Az alkalmazás elindulása után**, a **Perc** vagy az **Óra** elem van kiválasztva a **Gyakoriság** legördülő listán, a **Kihagyott feladatok futtatása** jelölőnégyzet nem használható.

   d. Ha azt szeretné, hogy a Kaspersky Endpoint Security függesszen fel egy feladatot, ha a számítógép erőforrásai korlátozottan állnak rendelkezésre, jelölje be a **Csak akkor fusson, ha a számítógép üresjáratban van** jelölőnégyzetet.

      Ez az ütemezési lehetőség segít a számítógép erőforrásainak megőrzésében.

5. Kattintson az **OK** gombra.

6. A módosítások mentéséhez kattintson a **Mentés** gombra.

A jelentések kezelése

Ez a rész ismerteti a jelentések beállításainak megadását és a jelentések kezelését.

Tudnivalók a jelentésekről

Az egyes Kaspersky Endpoint Security összetevők működésére, az adattitkosítási eseményekre, az egyes vizsgálati feladatok, frissítési feladatok, integritási ellenőrzési feladatok teljesítményére, valamint az alkalmazás általános működésére vonatkozó információk jelentésekbe kerülnek.

A jelentések a 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 jelentések adatai táblázat formájában jelennek meg, melyek események listáját tartalmazzák. A táblázatban minden sor egy-egy különálló esemény adatait tartalmazza. Az események attribútumai a táblázatoszlopokban helyezkednek el. Egyes oszlopok összetettek, melyekben további attribútumokat tartalmazó beágyazott oszlopok találhatók. A további attribútumok megtekintéséhez a grafikon neve melletti ⊞ gombot meg kell nyomni. A különféle összetevők működése közben naplózott eseményekhez, illetve a különféle összetevők teljesítménye más-más attribútumkészlettel rendelkezik.

A következő jelentések állnak rendelkezésre:

- **Rendszer-felülvizsgálat** 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.
- Kaspersky Endpoint Security összetevő működéséről vagy feladat végrehajtásáról szóló jelentés.
- **Titkosítási** jelentés. Információkat tartalmaz az adattitkosítás és -visszafejtés során előforduló eseményekről.

A jelentések az alábbi fontossági szinteket alkalmazzák:

- **Információs üzenetek**. Ikon . A szokásos esetben fontos információkat nem tartalmazó formális események.
- **Figyelmeztetések**. Ikon . Olyan fontos eseményekről szóló értesítések, amelyekre figyelni kell, mert fontos helyzeteket jeleznek a Kaspersky Internet Security program működésében.
- **Kritikus események**. Ikon . Kritikus jelentőségű események, amelyek a Kaspersky Endpoint Security működésével kapcsolatos problémákra vagy a felhasználó számítógépe védelmének sebezhetőségére utalnak.

A jelentések kényelmes feldolgozása érdekében az adatok képernyőn való megjelenése az alábbi módokon módosítható:

- Az események listájának szűrése különböző feltételek szerint.

- Adott esemény megtalálása a keresési funkcióval.
- A kiválasztott esemény megtekintése egy külön részben.
- Az események listájának rendezése jelentésoszlopok szerint.
- Az eseményszűrő által csoportosított események megjelenítése és elrejtése.
- A jelentésben látható oszlopok sorrendjének és elrendezésének módosítása.

Az előállított jelentést szükség esetén szövegfájlba mentheti.

A jelentésből törölhetők továbbá a csoportokba helyezett Kaspersky Endpoint Security összetevőkre és feladatokra vonatkozó információk. A Kaspersky Endpoint Security a kijelölt jelentések összes bejegyzését törli a legkorábbitól kezdve az aktuális időpontig.

Ha a Kaspersky Endpoint Security a Kaspersky Security Center irányítása alatt fut, előfordulhat, hogy az eseményekről szóló információkat megkapja a Kaspersky Security Center Adminisztrációs kiszolgáló. A Kaspersky Security Center jelentések kezeléséről szóló további részletekért lásd a Kaspersky Security Center súgórendszerét.

A jelentések beállításainak megadása

A jelentésbeállításokat a következő módok valamelyikével adhatja meg:

- 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. Megszüntetheti a tárolás időtartamának korlátozását vagy módosíthatja a jelentések tárolásának maximális idejét.

- 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 jelentésfájl méretkorlátozása megszüntethető, illetve módosítható.

A jelentés maximális tárolási időtartamának beállítása

A jelentések maximális tárolási időtartamának módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.
3. Az ablak jobb oldalán a **Jelentésparaméterek** részben végezze el az alábbiak egyikét:
   - A jelentések tárolási időtartamának korlátozásához jelölje be a **Jelentések tárolási ideje max.** jelölőnégyzetet. Adja meg a **Jelentések tárolási ideje max.** jelölőnégyzetben a jelentések maximális tárolási időtartamát.

     A jelentések maximális tárolási időtartama alapértelmezett esetben 30 nap.

- A jelentések tárolási időtartamára vonatkozó korlátozásához törléséhez törölje a **Jelentések tárolási ideje max.** jelölőnégyzetet.

A jelentések tárolásának időtartamára vonatkozó korlátozás alapértelmezés szerint be van kapcsolva.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A jelentésfájlok maximális méretének beállítása

A jelentés maximális fájlméretének beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.
3. Az ablak jobb oldalán a **Jelentésparaméterek** részben végezze el az alábbiak egyikét:
   - A jelentések fájlméretének korlátozásához jelölje be a **Maximális fájlméret** jelölőnégyzetet. Adja meg a **Maximális fájlméret** jelölőnégyzetben a jelentések maximális fájlméretét.

     Alapértelmezés szerint a jelentések fájlmérete 1024 MB-ra korlátozódik.
   - A jelentések fájlméretére vonatkozó korlátozás törléséhez törölje a **Maximális fájlméret** jelölőnégyzetet.

   Alapértelmezés szerint a jelentések fájlméretére vonatkozó korlátozás be van kapcsolva.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Jelentések megtekintése

Jelentések megtekintése:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Jelentések** hivatkozásra a fő alkalmazásablak felső részén a **Jelentések** ablak megnyitásához.
3. Az Minden védelmi összetevő jelentés elkészítéséhez válassza ki a **Jelentések** ablak bal oldali részén az összetevők és feladatok listáján az **Minden védelmi összetevő** elemet.

   Az Minden védelmi összetevő jelentés az ablak jobb oldali részén jelenik meg, amely a Kaspersky Endpoint Security összes védelmi összetevőjének működése során történő események listáját tartalmazza.
4. Egy adott összetevő vagy feladat működéséről szóló jelentés előállításához válassza ki a **Jelentések** ablak bal oldali részén az összetevők és feladatok listáján az adott összetevőt vagy feladatot.

   A jelentés az ablak jobb oldali részén jelenik meg, amely a Kaspersky Endpoint Security kiválasztott védelmi összetevőjének működése során történő események listáját tartalmazza.

Alapértelmezés szerint a jelentés eseményei az **Esemény dátuma** oszlopban lévő értékek növekvő sorrendjében vannak rendezve.

Eseményadatok megtekintése a jelentésekben

A jelentés egyes eseményeinek részletes összegzése is megtekinthető.

A jelentés egyes eseményei részletes összegzésének megtekintése:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Jelentések** hivatkozásra a fő alkalmazásablak felső részén a **Jelentések** ablak megnyitásához.
3. Válassza ki az adott összetevőről vagy feladatról szóló jelentést az ablak bal oldali részén.

   A jelentések hatókörébe tartozó események az ablak jobb oldali részén lévő táblázatban jelennek meg. A jelentésen belül adott események megtalálásához használja a szűrés, keresés és rendezés funkciókat.
4. Válassza ki a jelentésben a kívánt eseményt.

Az alsó részén megjelenik egy rész, melyben az esemény összegzése látható.

Jelentés mentése fájlba

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. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Jelentések** hivatkozásra a fő alkalmazásablak felső részén a **Jelentések** ablak megnyitásához.
3. Végezze el az alábbiak egyikét:

   - Az „Minden védelmi összetevő” jelentés elkészítéséhez válassza ki az **Minden védelmi összetevő** elemet az összetevők és feladatok listáján.

     Az „Minden védelmi összetevő” jelentés az ablak jobb oldali részén jelenik meg, amely az összes védelmi összetevő működése során történő események listáját tartalmazza.

   - Egy adott összetevő vagy feladat működéséről szóló jelentés előállításához válassza ki az összetevők és feladatok listáján az adott összetevőt vagy feladatot.

     A jelentés az ablak jobb oldali részén jelenik meg, amely a kiválasztott védelmi összetevő működése során történő események listáját tartalmazza.
4. Szükség esetén az adatok jelentésekben való megjelenését az alábbiakkal módosíthatja:

   - Események szűrése
   - Események közötti keresés

- Oszlopok átrendezése
- Események rendezése

5. Kattintson a **Jelentés mentése** gombra az ablak jobb felső részén.
   Megnyílik egy helyi menü.
6. Válassza ki a helyi menüben a jelentésfájl mentésének kódolását: **Mentés ANSI kódolással** vagy **Mentés Unicode kódolással**.
   Megnyílik a Microsoft Office-ban szokásos **Mentés másként** ablak.
7. Adja meg a **Mentés másként** ablakban a jelentésfájl célmappáját.
8. Gépelje be a **Fájlnév** mezőbe a jelentésfájl nevét.
9. Válassza ki a **Fájltípus** mezőben a jelentésfájl szükséges formátumát: TXT vagy CSV.
10. Kattintson a **Mentés** gombra.

Jelentések törlése

Információk törlése jelentésekből:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.
3. Az ablak jobb oldalán a **Jelentésparaméterek** részben kattintson a **Jelentések törlése** gombra.
   Megnyílik a **Jelentések törlése** ablak.
4. Jelölje be a jelölőnégyzeteket azokkal a jelentésekkel szemben, amelyekből információkat szeretne törölni:
   - **Összes jelentés**.
   - **Általános védelmi jelentés**. Információkat tartalmaz az alábbi Kaspersky Endpoint Security összetevők működéséről:
     - Fájl víruskereső
     - Levél víruskereső.
     - Webes víruskereső.
     - IM víruskereső.
     - Rendszerfigyelő.
     - Tűzfal.
     - Behatolásmegelőzési rendszer.
     - BadUSB védelem.

- **Vizsgálati feladat jelentés**. Információkat tartalmaz az elvégzett vizsgálati feladatokról:
  - Teljes vizsgálat
  - Kritikus területek vizsgálata
  - Egyéni vizsgálat
  - Integritás ellenőrzése.
- **Frissítési feladat jelentése**. Információkat tartalmaz az elvégzett frissítési feladatokról:
- **Tűzfaljelentés** A Tűzfal működéséről tartalmaz információkat.
- **Felügyeleti összetevők jelentése**. Információkat tartalmaz az alábbi Kaspersky Endpoint Security összetevők működéséről:
  - Alkalmazásindítás-felügyelő.
  - Alkalmazásjogosultság-felügyelő.
  - Sebezhetőség-figyelő.
  - Eszközfelügyelő.
  - Webfelügyelő.
- **Adattitkosítási jelentés**.

5. Kattintson az **OK** gombra.

Értesítési szolgáltatás

Ez a rész tájékoztatást nyújt az értesítési szolgáltatásról, amely a felhasználót a Kaspersky Endpoint Security működése során bekövetkező eseményekre figyelmezteti, és utasításokat tartalmaz az értesítések paramétereinek beállítására vonatkozóan.

A Kaspersky Endpoint Security értesítései

A Kaspersky Endpoint Security működése során különböző események léphetnek fel. Az ilyen eseményekről szóló értesítések lehetnek tisztán tájékoztató jellegűek, vagy tartalmazhatnak létfontosságú információkat. Az értesítések tájékoztatást nyújthatnak például adatbázisok és alkalmazásmodulok sikeres frissítéséről, vagy a javítást igénylő összetevőhibákról.

A Kaspersky Endpoint Security támogatja az információk naplózását az eseményekről a Microsoft Windows eseménynaplóban és / vagy a Kaspersky Endpoint Security eseménynaplójában.

A Kaspersky Endpoint Security az alábbi módokon adja át az értesítéseket:

- a Microsoft Windows tálca értesítési területén előbukkanó értesítések formájában;
- e-mailben.

Az események értesítéseinek kézbesítése beállítható. Az események értesítéseinek módját eseménytípusonként lehet beállítani.

Az értesítési szolgáltatás beállítása

Az értesítési szolgáltatás beállítása érdekében a következő műveleteket végezheti el:

- Azon eseménynaplók beállításainak megadása, amelyekben a Kaspersky Endpoint Security az eseményeket rögzíti.
- A képernyőn megjelenő értesítések megjelenítésének beállítása.
- Az e-mailben elküldött értesítések kézbesítésének beállítása.

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 sorbarendezése.
- Az értesítési szolgáltatás eseményeinek listáján látható oszlopok sorrendjének és készletének módosítása.

Az eseménynapló beállításainak megadása

Az eseménynapló beállításainak megadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.

   Az ablak jobb oldali részén megjelennek a jelentések és tárolók beállításai.
3. Az **Értesítések** részben kattintson a **Beállítások** gombra.

   Ezzel megnyílik az **Értesítések** ablak.

   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.
4. Az ablak bal oldalán válassza ki azt az összetevőt vagy feladatot, amelynek az eseménynaplózási beállításait be szeretné állítani.
5. Jelölje be a kívánt eseményekkel szemben lévő jelölőnégyzeteket a **Mentés a helyi naplóba** és a **Mentés a Windows eseménynaplóba** oszlopokban.

   Azok az események, amelyek jelölőnégyzeteit bejelölte a **Mentés a helyi naplóba** oszlopban, megjelennek az **Alkalmazások és szolgáltatások naplói** alatt a **Kaspersky Eseménynapló** részben. Azok az események, amelyek jelölőnégyzeteit bejelölte a **Mentés a Windows eseménynaplóba** oszlopban, megjelennek a **Windows naplók** alatt az **Alkalmazás** részben. Az eseménynaplók megnyitásához kattintson a **Start** → **Vezérlőpult** → **Adminisztráció** → **Eseménymegtekintő** elemre.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

Az értesítések megjelenítésének és kézbesítésének beállítása

Az értesítések megjelenítésének és kézbesítésének beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.

   Az ablak jobb oldali részén megjelennek a jelentések és tárolók beállításai.
3. Az **Értesítések** részben kattintson a **Beállítások** gombra.

   Ezzel megnyílik az **Értesítések** ablak.

   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.
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 kívánt 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 kívánt 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 **E-mail értesítési beállítások** gombra.

Ezzel megnyílik az **E-mail értesítési beállítások** ablak.

8. Jelölje be az **Eseményértesítések küldése** jelölőnégyzetet a Kaspersky Endpoint Security **Értesítés e-mailben** oszlopban kiválasztott eseményeire vonatkozó információk kézbesítésének engedélyezéséhez.

9. Adja meg az e-mail értesítések kézbesítési beállításait.

10. Kattintson az **OK** gombra.

11. Az **E-mail értesítési beállítások** ablakban kattintson az **OK** gombra.

12. A módosítások mentéséhez kattintson a **Mentés** gombra.

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 **Beállítások** gombra.

2. Az ablak bal oldalának **Általános beállítások** részében válassza ki a **Felület** lehetőséget.

   A Kaspersky Endpoint Security felületének beállításai az ablak jobb oldalán jelennek meg.

3. A **Figyelmeztetések** részben jelölje be a jelölőnégyzeteket azokkal az eseménykategóriákkal szemben, amelyekről értesítést szeretne látni a Microsoft Windows értesítési területén.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Ha a kiválasztott kategóriába tartozó események történnek, az értesítési területen lévő alkalmazásikon a figyelmeztetés súlyosságától függően  hiba történt vagy  újra kell indítani a számítógépet ikonra változik.

A Karantén és másolattároló kezelése

Ez a rész ismerteti a Karantén és másolattároló beállításának és kezelésének menetét.

A Karantén és másolattároló

A *Karantén* a valószínűleg fertőzött fájlok listája. A *valószínűleg fertőzött fájlok* olyan fájlok, amelyek vírusokat és egyéb fenyegetéseket, illetve ezek variációit tartalmazhatják.

Amikor a Kaspersky Endpoint Security egy valószínűleg fertőzött fájlt karanténba helyez, akkor a fájlt nem másolja, hanem áthelyezi: az alkalmazás törli a merevlemezről vagy az e-mail üzenetből, és egy különleges adattárhelyre menti. A fájlok a Karanténban speciális formátumban kerülnek mentésre, ezért nem jelentenek fenyegetést.

A Kaspersky Endpoint Security a valószínűleg fertőzött fájlokat vírusvizsgálattal, valamint a Fájl víruskereső, a Levél víruskereső és a Rendszerfigyelő összetevők működése révén képes észlelni és karanténba helyezni.

A Kaspersky Endpoint Security az alábbi esetekben helyezi karanténba a fájlokat:

- A fájl kódja egy ismert, de részlegesen módosult rosszindulatú programra hasonlít, vagy a rosszindulatú programokéhoz hasonló szerkezete van, és nem szerepel a Kaspersky Endpoint Security adatbázisában. Ebben az esetben a fájl a Fájl víruskereső vagy a Levél víruskereső futtatása, vagy egy víruskeresés során végrehajtott heurisztikus elemzést követően a Karanténba kerül. A heurisztikus elemzés ritkán okoz téves riasztásokat.

- A fájl által végrehajtott műveletek sorozata veszélyes. Ebben az esetben a fájl a Karanténba kerül, miután a Rendszerfigyelő összetevő elemezte viselkedését.

A *Biztonsági mentés* azon fájlok biztonsági másolatainak listája, amelyek a vírusmentesítés során törlődtek vagy módosultak. A *biztonsági másolat* a fájl másolata, mely az első vírusmentesítési vagy törlési kísérlet során készül. A fájlok biztonsági másolatai különleges formátumban vannak tárolva, és nem jelentenek fenyegetést.

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 vírusmentesített fájlmásolatot az eredeti mappába.

Lehetséges, hogy újabb adatbázis- és alkalmazásmodul-frissítést követően a Kaspersky Endpoint Security képes felismerni és semlegesíteni a fenyegetést. Emiatt javasoljuk, hogy a karanténban lévő fájlokat vizsgálja meg az adatbázisok és alkalmazásmodulok minden frissítését követően.

A Karantén és biztonsági másolat beállításainak megadása

Az adattároló a Karanténból és a másolattárolóból áll. A Karantén és biztonsági másolat beállításait az alábbiak szerint lehet megadni:

- A Karanténban lévő fájlok és a Másolattartóban lévő fájlmásolatok maximális tárolási időtartamának megadása.

  A Karanténban lévő fájlok és a Másolattartóban lévő fájlmásolatok maximális tárolási időtartama alapértelmezett esetben 30 nap. A maximális tárolási időtartam lejárta után a Kaspersky Endpoint Security törli a legrégebbi fájlokat az adattárolóból. Megszüntetheti a tárolás időtartamának korlátozását vagy módosíthatja a fájltárolás maximális idejét.

- Megadhatja a Karantén és másolattartó maximális méretét is.

Alapértelmezés szerint a Karantén és másolattároló maximális mérete 100 MB. A maximális adattárolási méret túllépését elkerülendő a Kaspersky Endpoint Security automatikusan törli a legrégebbi fájlokat a Karanténból és másolattárolóból, ha az adattároló eléri maximális méretét. Megszüntetheti a Karantén és másolattároló méretkorlátját, illetve módosíthatja a maximális méretet.

A Karanténban lévő fájlok és a Másolattartóban lévő fájlmásolatok maximális tárolási időtartamának megadása

A Karanténban lévő fájlok és a Másolattartóban lévő fájlmásolatok maximális tárolási időtartamának megadása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.
3. Végezze el az alábbiak egyikét:
   - A Karantén és másolattároló fájltárolási időtartamának korlátozásához jelölje be az ablak jobb oldali részén a **Karantén és biztonsági másolat beállításai** részben az **Objektumok tárolási ideje max.** jelölőnégyzetet. Adja meg az **Objektumok tárolási ideje max.** jelölőnégyzettől jobbra lévő mezőben a Karantén fájljainak és a Másolattartó fájlmásolatainak maximális tárolási időtartamát. A Karanténban lévő fájlok és a Másolattartóban lévő fájlmásolatok tárolási időtartama alapértelmezett esetben 30 napra korlátozódik.
   - A Karantén és másolattároló fájltárolási időtartamának korlátozásának megszüntetéséhez törölje az ablak jobb oldali részén a **Karantén és biztonsági másolat beállításai** részben az **Objektumok tárolási ideje max.** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Karantén és másolattároló maximális méretének megadása

A Karantén és másolattároló maximális méretének beállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.
3. Végezze el az alábbiak egyikét:
   - Ha korlátozni szeretné a Karantén és másolattároló teljes méretét, jelölje be a **Maximális tárhely méret** jelölőnégyzetet az ablak jobb oldalán lévő **Karantén és biztonsági másolat beállításai** részben, és adja meg a Karantén és másolattároló maximális méretét a **Maximális tárhely méret** jelölőnégyzettől jobbra lévő mezőben.

     A Karantén könyvtárat és a fájlok biztonsági másolatait tartalmazó maximális adattárolási méret alapértelmezés szerint 100 MB.
   - Ha törölni szeretné a Karantén és másolattároló méretének korlátozását, törölje a **Maximális tárhely méret** jelölőnégyzetet az ablak jobb oldalán lévő **Karantén és biztonsági másolat beállításai** részben.

   A Karantén és másolattároló mérete alapértelmezés szerint korlátlan.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Karantén kezelése

A Kaspersky Endpoint Security minden állapotú fájl biztonsági másolatait automatikusan törli a Karanténból a speciális beállításokban megadott tárolási időtartam elteltével.

A következő fájlműveletek állnak rendelkezésre a Karantén kezelése során:

- A Kaspersky Endpoint Security által karanténba helyezett fájlok listájának megtekintése.
- A valószínűleg fertőzött fájlok vizsgálata a Kaspersky Endpoint Security adatbázisainak és moduljainak aktuális verziójával.
- Fájlok visszaállítása a Karanténból eredeti mappájukba.
- Fájlok törlése a Karanténból.
- A fájlokat eredetileg tartalmazó mappák megnyitása.

A karanténba helyezett fájlok táblázatos formában jelennek meg.

A táblázatban lévő adatok kezelése során a következő műveleteket is elvégezheti:

- A karanténba helyezett fájlok szűrése oszlopérték vagy egyéni szűrési feltételek szerint.
- A karanténba helyezett fájlok keresési funkciójának használata.
- Karanténbe helyezett fájlok rendezése.
- A karaneténba helyezett fájlok táblázatában látható oszlopok sorrendjének és készletének módosítása.

A kijelölt Karanténeseményeket a vágólapra másolhatja. Több karanténba helyezett fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.

Karanténba helyezett fájlok frissítés utáni vizsgálatának be- és kikapcsolása

Ha a Kaspersky Endpoint Security egy fájl vizsgálata közben a fertőzés jeleit észleli, de nem tudja megállapítani, hogy konkrétan melyik rosszindulatú program fertőzte meg, akkor az adott fájlt a Karanténba helyezi. Lehetséges, hogy újabb adatbázis- és alkalmazásmodul-frissítést követően a Kaspersky Endpoint Security képes felismerni és semlegesíteni a fenyegetéseket. Engedélyezheti a Karanténba helyezett fájlok automatikus vizsgálatát adatbázisok és alkalmazásmodulok minden frissítése után.

Javasoljuk, hogy rendszeresen vizsgálja meg a Karanténban lévő fájlokat. A vizsgálat hatására a fájlok állapota módosulhat. Lehetséges, hogy ekkor egyes fájlokat vírusmentesíteni lehet, és vissza lehet állítani eredeti helyére, és így tovább használhatók.

A karanténba helyezett fájlok frissítések utáni vizsgálatának engedélyezése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolás** lehetőséget.

   Az ablak jobb oldali részén megjelennek a jelentések és tárolók kezelési beállításai.
3. A **Karantén és biztonsági másolat beállításai** részben tegye az alábbiak egyikét:

   - Ha engedélyezni szeretné a karanténban lévő fájlok vizsgálatát a Kaspersky Endpoint Security minden frissítése után, jelölje be a **Frissítés után a karantén ismételt vizsgálata** jelölőnégyzetet.
   - Ha le szeretné tiltani a karanténban lévő fájlok vizsgálatát a Kaspersky Endpoint Security minden frissítése után, törölje a **Frissítés után a karantén ismételt vizsgálata** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Karanténban lévő fájlok Egyéni vizsgálat feladatának megkezdése

Előfordulhat, hogy az adatbázis- és alkalmazásmodul-frissítéseket követően a Kaspersky Endpoint Security képes felismerni és semlegesíteni a karanténban lévő fájlokban található fenyegetéseket. Ha az alkalmazásban nincs beállítva, hogy az adatbázisok és alkalmazásmodulok frissítése után mindig automatikusan vizsgálja meg a karanténban lévő fájlokat, akkor kézileg elindíthatja a karanténban lévő fájlok Egyéni vizsgálat feladatát.

Karanténban lévő fájlok Egyéni vizsgálat feladatának megkezdése:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.

   Megnyílik a **Karantén** lap a **Tárhelyek** ablakban.
3. A **Karantén** lapon jelöljön ki egy vagy több vizsgálni kívánt, valószínűleg fertőzött fájlt.

   Több karanténba helyezett fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.
4. Az Egyéni vizsgálat feladatot az alábbi módszerek egyikével indítsa el:

   - Kattintson az **Ismételt vizsgálat** gombra.
   - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza az **Ismételt vizsgálat** lehetőséget.

A vizsgálat elkészültével megjelenik egy értesítés a megvizsgált fájlok és az észlelt fenyegetések számáról.

Fájlok visszaállítása a Karanténból

Fájlok visszaállítása a Karanténból:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.

   Megnyílik a **Karantén** lap a **Tárhelyek** ablakban.

3. Ha az összes karanténba helyezett fájlt vissza szeretné állítani, válassza ki bármelyik fájl helyi menüjében az **Összes visszaállítása** lehetőséget.

   A Kaspersky Endpoint Security az összes fájlt visszaállítja a Karanténból eredeti mappájába.

4. Egy vagy több karanténba helyezett fájl visszaállítása:

   a. A **Karantén** lapon jelöljön ki egy vagy több, a Karanténból visszaállítani kívánt fájlt.

      Több karanténba helyezett fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.

   b. A fájlokat az alábbi módok egyikével állíthatja vissza:

      - Kattintson a **Visszaállítás** gombra.
      - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Visszaállítás** lehetőséget.

   A Kaspersky Endpoint Security visszaállítja a kiválasztott fájlokat a Karanténból eredeti mappájukba.

Fájlok törlése a Karanténból

Fájlok törlése a Karanténból:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.

   Megnyílik a **Karantén** lap a **Tárhelyek** ablakban.

3. Ha az összes fájlt törölni szeretné a Karanténból, válassza ki bármelyik fájl helyi menüjében az **Összes törlése** lehetőséget.

   A Kaspersky Endpoint Security az összes fájlt törli a Karanténból.

4. Egy vagy több karanténba helyezett fájl törlése:

   a. A **Karantén** lapon lévő táblázatban jelöljön ki egy vagy több, valószínűleg fertőzött fájlt, amelyet törölni szeretne a Karanténból.

      Több karanténba helyezett fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.

   b. A fájlokat az alábbi módok egyikével törölheti:

      - Kattintson az **Eltávolítás** gombra.
      - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Törlés** lehetőséget.

A Kaspersky Endpoint Security a kiválasztott fájlokat törli a Karanténból.

A Másolattartó kezelése

Ha a fájlban rosszindulatú kód észlelhető, a Kaspersky Endpoint Security blokkolja a fájlt, elhelyezi másolatát a Másolattartóba, és megkísérli a vírusmentesítést. Ha a fájl vírusmentesítése sikerül, akkor biztonsági másolatának állapota *Vírusmentesített* értékűre változik. A fájl az eredeti mappában elérhetővé válik. Ha egy fájlt nem lehet vírusmentesíteni, a Kaspersky Endpoint Security törli eredeti mappájából. A fájl a biztonsági másolatból visszaállítható az eredeti mappába.

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 súgófájljaiban*).

A Kaspersky Endpoint Security minden állapotú fájl biztonsági másolatait automatikusan törli a Biztonsági mentésből a speciális beállításokban megadott tárolási időtartam elteltével.

A fájlok biztonsági másolata kézileg is törölhető a Másolattartóból.

A fájlok biztonsági másolatai táblázatos formában jelennek meg.

A Másolattartó kezelése közben az alábbi műveleteket lehet elvégezni a fájlok biztonsági másolataival:

- A fájlok biztonsági másolatai listájának megtekintése.
- Fájlok visszaállítása biztonsági másolataikból eredeti mappájukba.
- Fájlok biztonsági másolatainak törlése a Másolattartóból.

A táblázatban lévő adatok kezelése során a következő műveleteket is elvégezheti:

- A biztonsági másolatok szűrése oszlopérték vagy egyéni szűrési feltételek szerint.
- A biztonsági másolatok keresési funkciójának használata.
- Biztonsági másolatok rendezése.
- A biztonsági másolatok táblázatában látható oszlopok sorrendjének és készletének módosítása.

A Biztonsági mentés kijelölt eseményeit a vágólapra másolhatja. Több Másolattartóban lévő fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.

Fájlok visszaállítása a Másolattartóból

Fájlok visszaállítása a Másolattartóból:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Másolat** lapot.

4. Ha az összes fájlt vissza szeretné állítani a Másolattartóból, válassza ki bármelyik fájl helyi menüjében az **Összes visszaállítása** lehetőséget.

   A Kaspersky Endpoint Security az összes fájlt visszaállítja a biztonsági másolatból eredeti mappájába.

5. Egy vagy több fájl visszaállítása a Másolattartóból:

   a. Válasszon ki a **Másolat** lapon lévő táblázatban egy vagy több Másolattartóban lévő fájlt.

   Több karanténba helyezett fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.

   b. A fájlokat az alábbi módok egyikével állíthatja vissza:

   - Kattintson a **Visszaállítás** gombra.
   - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Visszaállítás** lehetőséget.

A Kaspersky Endpoint Security a kiválasztott fájlokat visszaállítja a biztonsági másolatból eredeti mappájukba.

Fájlok biztonsági másolatainak törlése a Másolattartóból

Fájlok biztonsági másolatainak törlése a Másolattartóból:

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Karantén** hivatkozásra a fő alkalmazásablak felső részén a **Tárhelyek** ablak megnyitásához.
3. A **Tárhelyek** ablakban válassza ki a **Másolat** lapot.
4. Ha a Másolattartóból az összes fájlt törölni szeretné, végezze el az alábbi műveletek egyikét:

   - Válassza ki bármelyik fájl helyi menüjében az **Összes törlése** lehetőséget.
   - Kattintson a **Tároló ürítése** gombra.

   A Kaspersky Endpoint Security az összes fájl biztonsági másolatát törli a Másolattartóból.

5. Ha egy vagy több fájlt szeretne törölni a Másolattartóból:

   a. Válasszon ki a **Másolat** lapon lévő táblázatban egy vagy több Másolattartóban lévő fájlt.

   Több Másolattartóban lévő fájl kiválasztásához kattintson az egér jobb gombjával a helyi menü megnyitásához bármelyik fájlra, és válassza az **Összes kijelölése** elemet. A vizsgálatból kihagyni kívánt fájlok kijelölését úgy törölheti, ha úgy kattint rájuk, hogy közben lenyomva tartja a **Ctrl** billentyűt.

   b. A fájlokat az alábbi módok egyikével törölheti:

   - Kattintson az **Eltávolítás** gombra.
   - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Törlés** lehetőséget.

A Kaspersky Endpoint Security a kiválasztott fájlok biztonsági másolatait törli a Másolattartóból.

Az alkalmazás speciális beállításai

Ez a rész ismerteti a Kaspersky Endpoint Security speciális beállításait és megadásuk módját.

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 terjesztőkészlettel 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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. A **Beállítások kezelése** részben kattintson a **Mentés** gombra.

   Ezzel megnyílik a szokásos **Válasszon egy konfigurációs fájlt** ablak a Microsoft Windowsban.
4. Adja meg a konfigurációs fájl mentésének elérési útját, és adja meg a nevét.

   > Ahhoz, hogy a konfigurációs fájlt a Kaspersky Endpoint Security helyi, illetve távoli telepítéséhez használhassa, az install.cfg nevet kell adnia.

5. Kattintson a **Mentés** gombra.

A Kaspersky Endpoint Security beállításainak importálása konfigurációs fájlból:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. A **Beállítások kezelése** részben kattintson a **Betöltés** gombra.

   Ezzel megnyílik a szokásos **Válasszon egy konfigurációs fájlt** ablak a Microsoft Windowsban.
4. Adja meg a konfigurációs fájl elérési útját.
5. Kattintson a **Megnyitás** gombra.

A Kaspersky Endpoint Security összes beállítási értéke a kiválasztott konfigurációs fájl alapján kerül beállításra.

Megbízható zóna

Ez a rész tájékoztatást nyújt a megbízható zónával kapcsolatban, és utasításokat tartalmaz a vizsgálatból való kizárás beállítására és a megbízható alkalmazások listájának elkészítésére vonatkozóan.

A megbízható zóna

A *megbízható zóna* olyan, a rendszergazda által beállított objektumok és alkalmazások listája, melyeket a Kaspersky Endpoint Security aktív módban nem figyel. Más szóval ez a vizsgálatból való kizárások készlete.

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 következő objektumokat zárhatja ki a vizsgálatból:

- Bizonyos fájlformátumok
- Maszkkal kiválasztott fájlok
- Kiválasztott fájlok
- Mappák
- Alkalmazásfolyamatok

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. Noha az ilyen alkalmazásoknak nincs rosszindulatú funkciójuk, használhatók rosszindulatú programok kiegészítő összetevőjeként. Az ilyen alkalmazásokhoz tartoznak például a távoli felügyeleti programok, az IRC-ügyfelek, az FTP-kiszolgálók, különböző segédprogramok, amelyek folyamatokat állítanak le vagy rejtenek el, billentyűzetfigyelők, jelszófeltörők és automata tárcsázók. Az ilyen alkalmazások nem tartoznak a vírusok kategóriájába. A jogszerű szoftverek részleteiért, amelyekkel a bűnözők károsíthatják a számítógépet vagy a személyes adatokat, kérjük, keresse fel a Kaspersky Virus Encyclopedia-t itt www.securelist.com/threats/riskware.

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 Virus 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 Virus Encyclopedia által megadott névvel vagy névmaszkkal.

Ha a számítógépen adatokat gyűjtő, majd feldolgozás céljából elküldő alkalmazás van telepítve, a Kaspersky Endpoint Security rosszindulatú programként osztályozhatja. Ennek elkerülése érdekében kizárhatja az alkalmazást a vizsgálatból, ha a Kaspersky Endpoint Security alkalmazást a jelen dokumentumban ismertetettek szerint állítja be.

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 programfolyamat által mentett objektumokat, és felügyeli az összes alkalmazás tevékenységét és az általuk generált hálózati forgalmat. A Kaspersky Endpoint Security a megbízható alkalmazások listáján szereplő alkalmazásokat kizárja a vizsgálatból.

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 billentyűzeten begépelt szöveg rögzítése például az automatikus billentyűzetkiosztás-átváltók esetén rutinszerű eljárás (ilyen például a Punto Switcher). Az ilyen alkalmazások jellemzőinek figyelembe vételéhez és tevékenységük figyelésből való kizárásához célszerű őket a megbízható alkalmazások listájára felvenni.

A megbízható alkalmazások 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.

Kizárás a vizsgálatból létrehozása

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.

Kizárás a vizsgálatból létrehozása:

1. Nyissa meg az alkalmazásbeállítások ablakot.
2. Az ablak bal oldalának **Általános beállítások** részében válassza ki a **Kizárások** lehetőséget.

   A kizárások beállításai az ablak jobb oldalán jelennek meg.
3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Megbízható zóna** ablak a **Kizárások a vizsgálatból** lapon.
4. Kattintson a **Hozzáadás** gombra.

   Megnyílik a **Kizárás a vizsgálatból** ablak. Ebben az ablakban vizsgálatból való kizárást hozhat létre a **Tulajdonságok** rész egy vagy mindkét kritériumával.
5. Fájl vagy mappa vizsgálatból való kizárása:

   a. A **Tulajdonságok** részben jelölje be a **Fájl vagy mappa** jelölőnégyzetet.

   b. Kattintson a **válasszon fájlt vagy mappát** hivatkozásra a **Vizsgálatból való kizárás leírása** 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.

   Egy fájl vagy mappa névmaszkjában használhat csillag karaktert (*), hogy helyettesítsen egy karaktert a fájl nevében.

   Például, használhat maszkokat a következő elérési útvonalak hozzáadásához:

   - Elérési útvonalak 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.

d. A **Fájl vagy mappa neve** ablakban kattintson az **OK** gombra.

A hozzáadott fájlra vagy mappára mutató hivatkozás megjelenik a **Vizsgálatból való kizárás leírása** részben a **Kizárás a vizsgálatból** ablakban.

6. Adott nevű objektumok kizárása a vizsgálatból:

a. A **Tulajdonságok** részben jelölje be az **Objektum neve** jelölőnégyzetet.

b. Kattintson az **objektum nevének megadása** hivatkozásra a **Vizsgálatból való kizárás leírása** részben az **Objektum neve** ablak megnyitásához.

c. Adja meg az objektum nevét vagy névmaszkját a Kaspersky Virus Encyclopedia osztályozása szerint:

d. Az **Objektum neve** ablakban kattintson az **OK** gombra.

A hozzáadott objektumnévre mutató hivatkozás megjelenik a **Vizsgálati kizárás leírása** részben a **Kizárás a vizsgálatból** ablakban.

7. Szükség esetén adjon meg rövid megjegyzést a **Megjegyzés** mezőben a vizsgálatból való létrehozott kizárással kapcsolatban.

8. Adja meg, mely Kaspersky Endpoint Security összetevők használják a vizsgálatból való kizárást:

a. Kattintson a **bármelyik** hivatkozásra a **Vizsgálatból való kizárás leírása** részben az **összetevők kiválasztása** hivatkozás aktiválásához.

b. Az **összetevők kiválasztása** hivatkozásra kattintva megnyílik a **Védelem összetevői** ablak.

c. Jelölje be a jelölőnégyzeteket azokkal az összetevőkkel szemben, amelyekben alkalmazni szeretné a vizsgálatból való kizárást.

d. A **Védelem összetevői** ablakban kattintson az **OK** gombra.

Ha a vizsgálatból való kizárás beállításaiban meg vannak adva összetevők, akkor a kizárás csak akkor jut érvényre, ha a Kaspersky Endpoint Security megadott összetevői végeznek vizsgálatot.

Ha a vizsgálatból való kizárás beállításaiban nincsenek megadva összetevők, akkor a kizárás a Kaspersky Endpoint Security összes összetevője által végzett vizsgálat során érvényre jut.

9. A **Kizárás a vizsgálatból** ablakban kattintson az **OK** gombra.

   A megadott vizsgálatból való kizárás megjelenik a táblázatban a **Kizárások a vizsgálatból** lapon a **Megbízható zóna** ablakban. A vizsgálatból való kizárás megadott beállításai megjelennek a **Vizsgálatból való kizárás leírása** részben.

10. A **Megbízható zóna** ablakban kattintson az **OK** gombra.

11. A módosítások mentéséhez kattintson a **Mentés** gombra.

Kizárás a vizsgálatból módosítása

Kizárás a vizsgálatból módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.

3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Megbízható zóna** ablak a **Kizárások a vizsgálatból** lapon.

4. Válassza ki a listán a módosítani kívánt vizsgálatból való kizárást.

5. Módosítsa a vizsgálatból való kizárás beállításait az alábbi módszerek egyikével:

   - Kattintson a **Szerkesztés** gombra.

     Megnyílik a **Kizárások a vizsgálatból** ablak.

   - Nyissa meg a szükséges hivatkozás szerkesztésére szolgáló ablakot a **Vizsgálati kizárás leírása** mezőben lévő hivatkozásra kattintva.

6. Ha az előző lépésben a **Szerkesztés** gombra kattintott, kattintson az **OK** gombra a **Kizárás a vizsgálatból** ablakban.

   A vizsgálatból való kizárás módosított beállításai megjelennek a **Vizsgálati kizárás leírása** részben.

7. A **Megbízható zóna** ablakban kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

Kizárás a vizsgálatból törlése

Kizárás a vizsgálatból törlése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.

3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.

Megnyílik a **Megbízható zóna** ablak a **Kizárások a vizsgálatból** lapon.

4. Válassza ki a vizsgálatból való kizárások listáján a kívánt vizsgálatból való kizárást.
5. Kattintson az **Eltávolítás** gombra.
   A törölt vizsgálatból való kizárás eltűnik a listáról.
6. A **Megbízható zóna** ablakban kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A vizsgálatból való kizárás be- és kikapcsolása

A vizsgálatból való kizárás be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.
   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.
   Megnyílik a **Megbízható zóna** ablak a **Kizárások a vizsgálatból** lapon.
4. Válassza ki a vizsgálatból való kizárások listáján a kívánt kizárást.
5. Végezze el az alábbiak egyikét:
   - A vizsgálatból való kizárás bekapcsolásához jelölje be a neve melletti jelölőnégyzetet.
   - A vizsgálatból való kizárás kikapcsolásához törölje a neve melletti jelölőnégyzetet.
6. Kattintson az **OK** gombra.
7. A módosítások mentéséhez kattintson a **Mentés** gombra.

A megbízható alkalmazások listájának szerkesztése

A megbízható alkalmazások listájának szerkesztése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.
   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.
   Megnyílik a **Megbízható zóna** ablak.
4. A **Megbízható zóna** ablakban válassza ki a **Megbízható alkalmazások** lapot.

5. Alkalmazás hozzáadása a megbízható alkalmazások listájára:

   a. Kattintson a **Hozzáadás** gombra.

   b. A megnyíló helyi menüjében tegye az alábbiak egyikét:

   - Ha az alkalmazást a számítógépen telepített alkalmazások listáján szeretné megkeresni, válassza ki a menü **Alkalmazások** elemét.

     Megnyílik az **Alkalmazás kiválasztása** ablak.

   - Ha az adott alkalmazás végrehajtható fájljának elérési útvonalát meg szeretné adni, válassza ki a **Tallózás** lehetőséget.

     Megnyílik a szokásos **Fájl megnyitása** ablak a Microsoft Windowsban.

   c. Az alkalmazást az alábbi módok egyikével választhatja ki:

   - Ha az előző lépésben az **Alkalmazások** lehetőséget választotta, válassza ki az alkalmazást a számítógépen telepített alkalmazások listáján, majd kattintson az **OK** gombra az **Alkalmazás kiválasztása** ablakban.

   - Ha az előző lépésben a **Tallózás** lehetőséget választotta, adja meg az adott alkalmazás végrehajtható fájljának elérési útját, majd kattintson a **Megnyitás** gombra a Microsoft Windows szokásos **Megnyitás** ablakában.

   Ezekkel a műveletekkel megnyílik az **Alkalmazás vizsgálati kizárásai** ablak.

   a. Jelölje be a kiválasztott alkalmazás megfelelő megbízható zónaszabályaival szemben lévő jelölőnégyzeteket:

   - **Ne vizsgáljon nyitott fájlokat**.
   - **Ne figyelje az alkalmazástevékenységet**.
   - **Ne örökölje a szülőfolyamat (alkalmazás) korlátozásait**.
   - **Ne figyelje a gyerek-alkalmazás tevékenységet**.
   - **Ne blokkolja az alkalmazásfelülettel való interakciót**.
   - **Ne vizsgáljon hálózati forgalmat**.

   b. Az **Alkalmazás vizsgálati kizárásai** ablakban kattintson az **OK** gombra.

   A hozzáadott megbízható alkalmazás megjelenik a megbízható alkalmazások listáján.

6. A megbízható alkalmazások beállításainak szerkesztése:

   a. Válasszon ki egy megbízható alkalmazást a megbízható alkalmazások listáján.

   b. Kattintson a **Szerkesztés** gombra.

   c. Megnyílik az **Alkalmazás vizsgálati kizárásai** ablak.

   d. Jelölje be vagy törölje a kiválasztott alkalmazás megfelelő megbízható zónaszabályaival szemben lévő jelölőnégyzeteket:

Ha az **Alkalmazás vizsgálati kizárásai** ablakban nincsenek kiválasztva megbízható zónaszabályok, a megbízható alkalmazás szerepelni fog a vizsgálatban. Ilyenkor a megbízható alkalmazás nem kerül le a megbízható alkalmazások listájáról, de jelölőnégyzete törlődik.

e. Az **Alkalmazás vizsgálati kizárásai** ablakban kattintson az **OK** gombra.

7. Megbízható alkalmazás eltávolítása a megbízható alkalmazások listájáról:

   a. Válasszon ki egy megbízható alkalmazást a megbízható alkalmazások listáján.

   b. Kattintson az **Eltávolítás** gombra.

8. A **Megbízható zóna** ablakban kattintson az **OK** gombra.

9. A módosítások mentéséhez kattintson a **Mentés** gombra.

Megbízható zónaszabályok engedélyezése és letiltása a megbízható alkalmazások listáján szereplő alkalmazásnál

Megbízható zónaszabályok műveletének engedélyezése és letiltása a megbízható alkalmazások listáján szereplő alkalmazásnál:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.

3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Megbízható zóna** ablak.

4. A **Megbízható zóna** ablakban válassza ki a **Megbízható alkalmazások** lapot.

5. Válassza ki a megbízható alkalmazások listáján a szükséges megbízható alkalmazást.

6. Végezze el az alábbiak egyikét:

   - Ha egy megbízható alkalmazást ki szeretne zárni a Kaspersky Endpoint Security vizsgálatából, jelölje be a neve melletti jelölőnégyzetet.

   - Ha egy megbízható alkalmazást be szeretne venni a Kaspersky Endpoint Security vizsgálatába, törölje a neve melletti jelölőnégyzetet.

7. Kattintson az **OK** gombra.

8. A módosítások mentéséhez kattintson a **Mentés** gombra.

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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Megbízható zóna** ablak.
4. A **Megbízható zóna** ablakban válassza ki a **Megbízható rendszertanúsítvány tárhelye** lapot.
5. Jelölje be a **Megbízható rendszertanúsítvány tárhelyének használata** jelölőnégyzetet.
6. Válassza ki a **Megbízható rendszertanúsítvány tárhelye** legördülő listán, hogy a Kaspersky Endpoint Security melyik rendszertárhelye tekintendő megbízhatónak.
7. A **Megbízható zóna** ablakban kattintson az **OK** gombra.
8. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Kaspersky Endpoint Security önvédelme

Ez a rész ismerteti a Kaspersky Endpoint Security önvédelmi és távoli felügyeleti védelmi mechanizmusait, és azok beállításainak megadását.

A Kaspersky Endpoint Security önvédelme

A Kaspersky Endpoint Security védelmet nyújt a számítógép számára a rosszindulatú programok ellen, ideértve azokat is, amelyek megpróbálják blokkolni a Kaspersky Endpoint Security működését, vagy akár törölni a számítógépről.

A számítógép biztonsági rendszerének stabilitásáról a Kaspersky Endpoint Security önvédelmi és távoli felügyeleti védelmi mechanizmusai gondoskodnak.

Az *Önvédelem* mechanizmus megelőzi a merevlemezen lévő alkalmazásfájlok, a memóriafolyamatok és a beállításjegyzék bejegyzései módosítását és törlését.

A *Távoli felügyeleti védelem* a távoli számítógépekről érkező, alkalmazásszolgáltatások felügyeletével próbálkozó összes kísérletet blokkolja.

A 64 bites operációs rendszert futtató számítógépeken a Kaspersky Endpoint Security önvédelme csak a helyi merevlemezeken található alkalmazásfájlok és a beállításjegyzék-bejegyzések törlésének és módosításának megelőzésére terjed ki.

Az önvédelem be- és kikapcsolása

A Kaspersky Endpoint Security önvédelmi mechanizmusa alapértelmezés szerint be van kapcsolva. Az önvédelmet szükség esetén kikapcsolhatja.

Az önvédelem be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. Végezze el az alábbiak egyikét:

   - Ha be szeretné kapcsolni az Önvédelmi mechanizmust, jelölje be az **Önvédelem engedélyezése** jelölőnégyzetet.
   - Ha ki szeretné kapcsolni az Önvédelmi mechanizmust, törölje az **Önvédelem engedélyezése** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Távoli felügyeleti védelem be- és kikapcsolása

Alapértelmezés szerint a távoli felügyeleti védelmi mechanizmus be van kapcsolva. A távoli felügyeleti védelmi mechanizmust szükség esetén kikapcsolhatja.

A távoli felügyeleti védelmi mechanizmus ki- és bekapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. Végezze el az alábbiak egyikét:

   - Ha a távoli felügyeleti védelmi mechanizmust be szeretné kapcsolni, jelölje be a **A rendszerszolgáltatás külső kezelésének letiltása** jelölőnégyzetet.
   - Ha a távoli felügyeleti védelmi mechanizmust ki szeretné kapcsolni, törölje a **A rendszerszolgáltatás külső kezelésének letiltása** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A távoli adminisztrációs alkalmazások támogatása

Időnként szükség lehet távoli adminisztrációs alkalmazás használatára, miközben be van kapcsolva a külső felügyelet elleni védelem.

A távoli adminisztrációs alkalmazások működésének bekapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a bal oldalon lévő **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. A **Kizárások a vizsgálatból és megbízható alkalmazások** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Megbízható zóna** ablak.
4. A **Megbízható zóna** ablakban válassza ki a **Megbízható alkalmazások** lapot.
5. Kattintson a **Hozzáadás** gombra.
6. A megnyíló helyi menüjében tegye az alábbiak egyikét:

   - Válassza az **Alkalmazások** elemet, ha a számítógépre telepített alkalmazások listájáról szeretne távoli adminisztrációs alkalmazást választani.

     Megnyílik az **Alkalmazás kiválasztása** ablak.

   - Ha a távoli adminisztrációs alkalmazás végrehajtható fájljának elérési útvonalát meg szeretné adni, válassza ki a **Tallózás** lehetőséget.

     Megnyílik a szokásos **Fájl megnyitása** ablak a Microsoft Windowsban.
7. Az alkalmazást az alábbi módok egyikével választhatja ki:

   - Ha az előző lépésben az **Alkalmazások** lehetőséget választotta, válassza ki az alkalmazást a számítógépen telepített alkalmazások listáján, majd kattintson az **OK** gombra az **Alkalmazás kiválasztása** ablakban.

   - Ha az előző lépésben a **Tallózás** lehetőséget választotta, adja meg az adott alkalmazás végrehajtható fájljának elérési útját, majd kattintson a **Megnyitás** gombra a Microsoft Windows szokásos **Megnyitás** ablakában.

   Ezekkel a műveletekkel megnyílik az **Alkalmazás vizsgálati kizárásai** ablak.
8. Jelölje be a **Ne figyelje az alkalmazástevékenységet** jelölőnégyzetet.
9. Az **Alkalmazás vizsgálati kizárásai** ablakban kattintson az **OK** gombra.

   A hozzáadott megbízható alkalmazás megjelenik a megbízható alkalmazások listáján.
10. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Kaspersky Endpoint Security teljesítménye és más alkalmazásokkal való kompatibilitása

Ez a rész tájékoztatást nyújt a Kaspersky Endpoint Security teljesítményéről és más alkalmazásokkal való kompatibilitásáról, és útmutatást kínál az észlelhető objektumok típusainak és a Kaspersky Endpoint Security üzemmódjának kiválasztása tekintetében.

A Kaspersky Endpoint Security teljesítménye és más alkalmazásokkal való kompatibilitása

A Kaspersky Endpoint Security teljesítménye

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 vizsgálati feladat
- Sebezhetőségi 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 kézileg indíthatja el a feladatokat.

A fejlett vírusmentesítő technológia használata

A mai rosszindulatú programok 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 programoktól, amelyek már elindították folyamataikat a RAM-ban, és amelyek megakadályozzák, hogy a Kaspersky Endpoint Security más módszerekkel távolítsa el őket. Ennek eredményeképpen a fenyegetés semlegesítésre kerül. A Fejlett vírusmentesítés közben ajánlott tartózkodni az új folyamatok indításától, illetve az operációs rendszer beállításjegyzékének szerkesztésétől. A fejlett vírusmentesítő technológia az operációs rendszer jelentős erőforrásait vesz igénybe, amitől a többi alkalmazás lelassulhat.

Miután a Fejlett vírusmentesítési folyamat futása munkaállomásokra való Microsoft Windows rendszert futtató számítógépen véget ért, a Kaspersky Endpoint Security engedélyt kér a felhasználótól a számítógép újraindítására. A rendszer újraindítása során a Kaspersky Endpoint Security törli a rosszindulatú programok fájljait, és elindít a számítógépen egy kisebbfajta teljes vizsgálatot.

Az újraindítási kérdés a fájlkiszolgálókra szánt Microsoft Windows rendszert futtató számítógépeken a fájlkiszolgálókra szánt Kaspersky Endpoint Security jellemzői miatt nem lehetséges. 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. A fájlkiszolgálók aktív fertőzéseinek vírusmentesítéséhez kapcsolja be a fájlkiszolgálóknak szánt Aktív vírusmentesítési technológiát, és indítson *Víruskeresés* csoportos feladatot olyankor, amikor a fájlkiszolgáló felhasználóinak megfelel.

Az észlelhető objektumok típusának kiválasztása

Az észlelhető objektumok típusának kiválasztása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.
3. Az **Objektumok** részben kattintson a **Beállítások** gombra.

   Megnyílik az **Objektumok észlelése** ablak.
4. Jelölje be a jelölőnégyzeteket azokkal az objektumtípusokkal szemben, amelyeket észlelni szeretne a Kaspersky Endpoint Security alkalmazással:

   - **Rosszindulatú eszközök**
   - **Reklámprogram**
   - **Automata tárcsázók**

- **Egyéb**
- **Esetleg kárt okozó csomagolt fájlok**
- **Többszörösen csomagolt fájlok**

5. Kattintson az **OK** gombra.

   Bezáródik az **Objektumok észlelése** ablak. A kiválasztott objektumtípusok felsorolása az **Objektumok** rész **A következő objektumtípusok észlelése engedélyezett** listán látható.

6. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Fejlett vírusmentesítési technológia be- és kikapcsolása munkaállomásokon

A Fejlett vírusmentesítési technológia be- és kikapcsolása munkaállomásokon:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Vírusvédelem** részt.

   Az ablak jobb oldali részén jelennek meg a vírusvédelmi beállítások.

3. Az ablak jobb oldali részén tegye az alábbiak egyikét:

   - Jelölje be a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzetet a fejlett vírusmentesítő technológia bekapcsolásához.
   - Törölje a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzetet a fejlett vírusmentesítő technológia kikapcsolásához.

4. A módosítások mentéséhez kattintson a **Mentés** gombra.

Ha a Fejlett vírusmentesítési feladat a Kaspersky Security Centeren keresztül indul el, az operációs rendszer funkcióinak többsége a felhasználó számára nem érhető el. A munkaállomás újraindul, ha a vizsgálati feladat befejeződött.

A Fejlett vírusmentesítési technológia be- és kikapcsolása fájlkiszolgálókon

A fájlkiszolgálókra szánt Fejlett vírusmentesítő technológia bekapcsolásához végezze el az alábbiak egyikét:

- Kapcsolja be a Fejlett vírusmentesítési technológiát az aktív Kaspersky Security Center rendszabály tulajdonságaiban. Ehhez:

  a. Nyissa meg a rendszabály tulajdonságainak ablakában az **Általános védelmi beállítások** részt.

  b. Jelölje be a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzetet.

  c. A módosítások mentéséhez kattintson az **OK** gombra a rendszabály tulajdonságainak ablakában.

- A Kaspersky Security Center Vírusvizsgálati csoportos feladatának tulajdonságaiban jelölje be a **Fejlett vírusmentesítés futtatása azonnal** jelölőnégyzetet.

A fájlkiszolgálókra szánt Fejlett vírusmentesítő technológia kikapcsolásához végezze el az alábbiak egyikét:

- Kapcsolja be a Fejlett vírusmentesítési technológiát a Kaspersky Security Center rendszabály tulajdonságaiban. Ehhez:

  a. Nyissa meg a rendszabály tulajdonságainak ablakában az **Általános védelmi beállítások** részt.

  b. Törölje a **Fejlett vírusmentesítő technológia engedélyezése** jelölőnégyzetet.

  c. A módosítások mentéséhez kattintson az **OK** gombra a rendszabály tulajdonságainak ablakában.

- A Kaspersky Security Center Vírusvizsgálati csoportos feladatának tulajdonságaiban törölje a **Fejlett vírusmentesítés futtatása azonnal** jelölőnégyzetet.

Az energiatakarékos mód be- és kikapcsolása

Az energiatakarékos mód be- és kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. Az **Működési mód** részben kattintson a **Beállítások** gombra.

   Megnyílik az **Működési mód** ablak.
4. Végezze el az **Működési mód** ablakban az alábbi műveleteket.

   - Az energiatakarékos mód bekapcsolásához jelölje be az **Ütemezett vizsgálatok elhalasztása, amíg a számítógép akkumulátorról üzemel** jelölőnégyzetet.

     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
     - Sebezhetőségi vizsgálat feladat
     - Integritás ellenőrzés feladat

   - Ha ki szeretné kapcsolni az energiatakarékos módot, törölje az **Ütemezett vizsgálatok elhalasztása, amíg a számítógép akkumulátorról üzemel** jelölőnégyzetet. Ilyenkor a Kaspersky Endpoint Security az ütemezett vizsgálatokat a számítógép tápforrásától függetlenül elvégzi.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

Erőforrások más alkalmazásoknak történő átadásának engedélyezése és letiltása

Erőforrások más alkalmazásoknak történő átadásának engedélyezése és letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. Az **Működési mód** részben kattintson a **Beállítások** gombra.

   Megnyílik az **Működési mód** ablak.
4. Végezze el az **Működési mód** ablakban az alábbi műveleteket.

   - Ha engedélyezni szeretné azt a módot, amikor az erőforrások átadhatók más alkalmazások részére, jelölje be az **Erőforrások adása más alkalmazásoknak** jelölőnégyzetet.

     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
     - Sebezhetőségi vizsgálat feladat
     - Integritás ellenőrzés feladat
   - Ha le szeretné tiltani azt a módot, amikor az erőforrások átadhatók más alkalmazások részére, törölje az **Erőforrások adása más alkalmazásoknak** jelölőnégyzetet. Ilyenkor a Kaspersky Endpoint Security az ütemezett vizsgálatokat a többi alkalmazás működésétől függetlenül végzi el.

   Az alkalmazás alapértelmezés szerint úgy van beállítva, hogy az erőforrásokat átadja a többi alkalmazásnak.
5. A módosítások mentéséhez kattintson a **Mentés** gombra.

Jelszavas védelem

Ez a rész ismerteti a Kaspersky Endpoint Security elérésének jelszavas korlátozását.

A Kaspersky Endpoint Security elérésének korlátozása

Egy-egy számítógépet több, a számítógéphez különböző méretekben értő felhasználó is használhat. Ha a felhasználók korlátlanul hozzáférhetnek a Kaspersky Endpoint Security alkalmazáshoz és beállításaihoz, csökkenhet a számítógép védelmének általános szintje.

A Kaspersky Endpoint Security alkalmazáshoz való hozzáférést úgy korlátozhatja, hogy felhasználónevet és jelszót állít be, és megadja azokat a műveleteket, amelyeknél az alkalmazás ezeket kéri a felhasználótól:

A Kaspersky Endpoint Security 10 Service Pack 2 for Windows korábbi verziójáról történő frissítéskor megmarad a jelszó (ha be volt állítva). A jelszóvédelem beállításainak első szerkesztése alkalmával használja a KLAdmin alapértelmezett felhasználónevet.

A jelszavas védelem be- és kikapcsolása

Javasoljuk, hogy óvatosan járjon el, ha jelszóval korlátozza az alkalmazáshoz való hozzáférést. Ha elfelejti a jelszót, a jelszóvédelem kikapcsolása ügyében lépjen kapcsolatba a Kaspersky terméktámogatásával.

Jelszóvédelem engedélyezése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Általános beállítások** részében válassza ki a **Felület** lehetőséget.

   A Kaspersky Endpoint Security felületének beállításai az ablak jobb oldalán jelennek meg.
3. A **Jelszóvédelem** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Jelszóvédelem** ablak.
4. Jelölje be a **Jelszóvédelem engedélyezése** jelölőnégyzetet.
5. Adja meg a **Felhasználónév** mezőben azt a felhasználónevet, amelyet a **Jelszóellenőrzés** ablakban meg kell adni, ha a továbbiakban jelszóval védett műveletek végzésére kerül sor.
6. Adja meg az **Új jelszó** mezőben az alkalmazás hozzáférési jelszavát.
7. Erősítse meg a jelszót a **Jelszó megerősítése** mezőben.
8. Ha az alkalmazás összes műveletének hozzáférését korlátozni szeretné, kattintson a **Jelszó hatóköre** részben az **Összes kijelölése** gombra.
9. Ha a felhasználó hozzáférését szelektíven szeretné korlátozni, jelölje be a **Jelszó hatóköre** részben a kívánt műveletek neve melletti jelölőnégyzeteket:
   - **Alkalmazásbeállítások megadása**.
   - **Kilépés az alkalmazásból**.
   - **Védelmi összetevők letiltása**.
   - **Felügyeleti összetevők letiltása**.
   - **Kulcs eltávolítása**.

- **Alkalmazás eltávolítása/módosítása/visszaállítása**.
- **Hozzáférés visszaállítása a titkosított meghajtókon tárolt adatokhoz**.
- **Jelentések megtekintése**.

10. Kattintson az **OK** gombra.

    Az alkalmazás ellenőrzi a megadott jelszót. Ha a jelszavak egyeznek, az alkalmazás alkalmazza a jelszót. Ha a jelszavak nem egyeznek, az alkalmazás felkéri, hogy ismét erősítse meg a jelszót a **Jelszó megerősítése** mezőben.

11. A módosítások mentéséhez kattintson az alkalmazás beállításainak ablakában a **Mentés** gombra.

A jelszóvédelem bekapcsolását követően az alkalmazás minden alkalommal jelszót kér, amikor a jelszó hatókörébe tartozó művelet végzésére kerül sor. Ha nem szeretné, hogy az alkalmazás minden alkalommal bekérje a jelszót, amikor a jelenlegi munkamenet során ismét jelszóval védett műveletet kísérel meg, jelölje be a **Jelszó mentése az aktuális munkamenethez** jelölőnégyzetet a **Jelszóellenőrzés** ablakban.

Ha a **Jelszó mentése az aktuális munkamenethez** jelölőnégyzet nincs bejelölve, az alkalmazás minden alkalommal bekéri a jelszót, amikor jelszóval védett műveletet kísérel meg.

A jelszóvédelem kikapcsolása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Általános beállítások** részében válassza ki a **Felület** lehetőséget.

   A Kaspersky Endpoint Security felületének beállításai az ablak jobb oldalán jelennek meg.
3. A **Jelszóvédelem** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Jelszóvédelem** ablak.
4. Törölje a **Jelszóvédelem engedélyezése** jelölőnégyzetet.

   A jelszóvédelmet csak akkor kapcsolhatja ki, ha KLAdminként van bejelentkezve. A jelszóvédelmet nem lehetséges kikapcsolni, ha más felhasználói fiókot vagy ideiglenes jelszót használ.
5. Kattintson az **OK** gombra.
6. A módosítások mentéséhez kattintson az alkalmazás beállításainak ablakában a **Mentés** gombra.

   Megnyílik a **Jelszóellenőrzés** ablak.
7. Adja meg a felhasználónevét a **Felhasználónév** mezőben.
8. Adja meg a Kaspersky Endpoint Security jelszavát a **Jelszó** mezőben.
9. Kattintson az **OK** gombra.

A Kaspersky Endpoint Security hozzáférési jelszavának módosítása

A Kaspersky Endpoint Security hozzáférési jelszavának módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.
3. A **Jelszavas védelem** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Jelszavas védelem** ablak.
4. Adja meg a felhasználónevét a **Felhasználónév** mezőben.
5. Adja meg az **Új jelszó** mezőben az alkalmazás hozzáférésének új jelszavát.
6. Adja meg a **Jelszó megerősítése** mezőben ismét az új jelszót.
7. Kattintson az **OK** gombra.

   Az alkalmazás ellenőrzi a megadott jelszót. Ha a jelszavak egyeznek, az alkalmazás alkalmazza az új jelszót, és bezárja a **Jelszavas védelem** ablakot. Ha a jelszavak nem egyeznek, az alkalmazás felkéri, hogy ismét erősítse meg a jelszót a **Jelszó megerősítése** mezőben.
8. A módosítások mentéséhez kattintson az alkalmazás beállításainak ablakában a **Mentés** gombra.

Ideiglenes jelszó használata

A Kaspersky Security Center rendszabály által kezelt ügyfélszámítógépekkel végzet munka során előfordulhat, hogy a felhasználóknak a Kaspersky Endpoint Security alkalmazással a rendszabály szintjén jelszóvédett műveleteket kell elvégezniük. A jelszóvédelem bekapcsolt állapotában a jelszó hatókörébe tartozó műveleteket kizárólag a Kaspersky Security Center rendszergazda végezheti el. Ha azonban a Kaspersky Security Centerrel való kapcsolat megszakadt (például ha a felhasználó a vállalati hálózaton kívül tartózkodik), a Kaspersky Security Center helyi felületével való munkavégzés funkciói korlátozottak.

Ha a Kaspersky Security Center rendszergazda a felhasználót szeretné feljogosítani a szükséges műveletek elvégzésére, ám a rendszabály beállításaiban megadott jelszót nem szeretné átadni neki, létrehozhat ideiglenes jelszót. Az ideiglenes jelszó érvényességi időtartama és műveleti hatóköre korlátozott. Miután a felhasználó az alkalmazás helyi felületén megadja az ideiglenes jelszót, rendelkezésére állnak a Kaspersky Security Center rendszergazda által engedélyezett műveletek.

Az ideiglenes jelszó lejártát követően a Kaspersky Endpoint Security a Kaspersky Security Center rendszabály beállításainak megfelelően működik tovább. Ekkor a felhasználó többé nem használhatja a rendszabály szintjén jelszóvédett műveleteket.

Ideiglenes jelszó előállítása a Kaspersky Security Center Adminisztrációs Konzoljával

Ideiglenes jelszó létrehozása és felhasználónak való elküldése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amely az ideiglenes jelszót kérő felhasználó számítógépét tartalmazza.
3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki az ideiglenes jelszót kérő felhasználó számítógépének helyi menüjében a **Tulajdonságok** elemet.

   Megnyílik a **Tulajdonságok:<Számítógép neve>** ablak.

5. Válassza ki a **Tulajdonságok:<Számítógép neve>** ablakban az **Alkalmazások** részt.

6. Válassza ki a Kaspersky Endpoint Security Service Pack 2 for Windows alkalmazást, és nyissa meg az alkalmazás tulajdonságainak ablakát az alábbi módszerek egyikével:

   - Kattintson a **Tulajdonságok** gombra a képernyő alján.
   - Az alkalmazás helyi menüjében válassza ki a **Tulajdonságok** elemet.

   Ezzel megnyílik az **Alkalmazás beállítások "<Alkalmazás neve>"** ablak.

7. Az **Alkalmazás beállítások „<Alkalmazás neve>"** ablakban lévő **Speciális beállítások** részben válassza ki az **Alkalmazás beállítások** alrészt.

8. A **Jelszavas védelem** részben kattintson a **Beállítások** gombra.

   Megnyílik a **Jelszavas védelem** ablak.

9. A **Jelszavas védelem** ablakban lévő **Ideiglenes jelszó** részben kattintson a **Beállítások** gombra.

   > Ez a gomb akkor használható, ha a Kaspersky Security Centernél a számítógépen futó Kaspersky Security Center rendszabályban be van kapcsolva a jelszóvédelem.

   Megnyílik az **Ideiglenes jelszó létrehozása** ablak.

10. Adja meg a **Lejárat dátuma** mezőben azt a dátumot, amelytől kezdve a felhasználó többé nem használhatja az ideiglenes jelszót.

    Ezen a napon az ideiglenes jelszó érvényét veszti. A Kaspersky Endpoint Security helyi felületén műveletek elvégzéséhez való hozzáférés megadásához új ideiglenes jelszót kell létrehozni.

11. Jelölje be az **Ideiglenes jelszó hatóköre** táblázatban a jelölőnégyzeteket azokkal a műveletekkel szemben, amelyeknek a felhasználó rendelkezésére kell állniuk, miközben az ideiglenes jelszó érvényes.

12. Kattintson a **Létrehozás** gombra.

    Ezzel megnyílik a titkosított jelszót tartalmazó **Ideiglenes jelszó** ablak.

13. Másolja ki a jelszót és az alkalmazására vonatkozó utasításokat, majd küldje el a felhasználónak.

Ideiglenes jelszó alkalmazása a Kaspersky Endpoint Security felületén

> Az alábbi utasítások olyan ügyfélszámítógépek felhasználói számára készültek, amelyeken telepítve van a Kaspersky Endpoint Security.

Ideiglenes jelszó alkalmazása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.

2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   Az alkalmazásbeállítások az ablak jobb oldalán jelennek meg.

3. A **Jelszavas védelem** részben kattintson az **Ideiglenes jelszó** gombra.

   Megnyílik az **Ideiglenes jelszó** ablak.

4. Jelölje be az **Ideiglenes jelszó engedélyezése** jelölőnégyzetet.

5. Adja meg a beviteli mezőben a Kaspersky Security Center rendszergazdától kapott jelszót.

6. A módosítások mentéséhez kattintson az **OK** gombra.

Miután alkalmazta az ideiglenes jelszót, rendelkezésére állnak a Kaspersky Security Center rendszergazda által engedélyezett műveletek. Az **Ideiglenes jelszó** ablakban megjelenik az ideiglenes jelszó lejárati dátuma, és az engedélyezett műveletek.

Az alkalmazás távoli adminisztrációja a Kaspersky Security Centeren keresztül

Ez a rész ismerteti a Kaspersky Endpoint Security adminisztrációját a Kaspersky Security Centeren keresztül.

Az alkalmazás kezelése a Kaspersky Security Centeren keresztül

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.

Az alkalmazások Kaspersky Security Centeren keresztül történő kezelésére vonatkozó további, a jelen dokumentumban nem található információ a *Kaspersky Security Center Rendszergazdai útmutatóban* található.

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

Az adminisztrációs bővítmény verziója az ügyfélszámítógépen telepített Kaspersky Endpoint Security 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, hanem ezeket a felhasználó a Kaspersky Endpoint Security helyi felületén adhatja meg.

Az adminisztrációs bővítmény különböző verzióival való munkavégzés különleges szempontjai

Az adminisztrációs bővítménnyel az alábbi elemeket lehet módosítani:

- Rendszabályok
- Rendszabályprofilok
- Csoportos feladatok
- Helyi feladatok
- A Kaspersky Endpoint Security helyi beállításai

A Kaspersky Endpoint Security a Kaspersky Security Centeren keresztül csak akkor kezelhető, ha az adminisztrációs bővítmény verziója megegyezik vagy újabb, mint a Kaspersky Endpoint Security adminisztrációs bővítménnyel való kompatibilitására vonatkozó információkban megadott verzió. Az adminisztrációs bővítmény kötelező legalacsonyabb verzióját a terjesztőkészletben található installer.ini fájl ismerteti.

Az adminisztrációs bővítmény minden összetevő megnyitása esetén ellenőrzi kompatibilitására vonatkozó információit. Ha az adminisztrációs bővítmény verziója megegyezik vagy nagyobb, 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.

Korábban megadott beállítások módosítása az adminisztrációs bővítmény későbbi verziójával

Az adminisztrációs bővítmény későbbi verziójával minden korábban megadott beállítást lehet módosítani, és meg lehet adni azokat az új beállításokat is,a melyek az adminisztrációs bővítmény korábban használt verziójában nem voltak jelen.

Az új beállításoknál az adminisztrációs bővítmény későbbi verziója az alapértelmezett értékeket osztja ki a rendszabályok, rendszabályprofilok és feladatok első mentésekor.

Miután rendszabály, rendszabályprofil vagy csoportos feladat beállításait az adminisztrációs bővítmény későbbi verziójával módosította, az összetevőket az adminisztrációs bővítmény korábbi verzióival többé nem lehet kezelni. A Kaspersky Endpoint Security helyi beállításai és a helyi feladatok beállításai a korábbi verziójú adminisztrációs bővítményben továbbra is használhatók.

A Kaspersky Endpoint Security elindítása és leállítása ügyfélszámítógépen

Az alkalmazás elindítása és leállítása ügyfélszámítógépen:

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 ügyfélszámítógép tartozik.
3. Válassza ki a munkaterületen az **Eszközök** 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.

   Megnyílik az ügyfélszámítógép tulajdonságainak ablaka.
6. Válassza ki az ügyfélszámítógép tulajdonságainak ablakában az **Alkalmazások** részt.

   Megjelenik az ügyfélszámítógépen telepített Kaspersky alkalmazások 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, vagy végezze el az alábbiakat:

     a. Válassza ki a **Tulajdonságok** lehetőséget a Kaspersky Endpoint Security helyi menüjében, vagy kattintson a **Tulajdonságok** gombra, mely a Kaspersky alkalmazások listája alatt található.

     Megnyílik a **Kaspersky Endpoint Security for Windows beállításai** ablak.

     b. Kattintson az **Általános** részben lévő **Indítás** gombra az ablak jobb oldali részében.

   - Az alkalmazás leállításához kattintson a gombra a Kaspersky alkalmazások listájának jobb oldalán, vagy végezze el az alábbiakat:

     a. Válassza ki a **Tulajdonságok** lehetőséget a Kaspersky Endpoint Security helyi menüjében, vagy kattintson a **Tulajdonságok** gombra, mely a Kaspersky alkalmazások listája alatt található.

Megnyílik a **Kaspersky Endpoint Security for Windows beállításai** ablak.

b. Kattintson az **Általános** részben lévő **Leállítás** gombra az ablak jobb oldali részében.

A Kaspersky Endpoint Security beállításainak megadása

A Kaspersky Endpoint Security beállításainak megadása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Nyissa meg az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógép tartozik.
3. Válassza ki a munkaterületen az **Eszközök** lapot.
4. Válassza ki azt a számítógépet, amelyen meg szeretné adni a Kaspersky Endpoint Security beállításait.
5. Az ügyfélszámítógép helyi menüjében válassza ki a **Tulajdonságok** elemet.

   Megnyílik az ügyfélszámítógép tulajdonságainak ablaka.
6. Válassza ki az ügyfélszámítógép tulajdonságainak ablakában az **Alkalmazások** részt.

   Megjelenik az ügyfélszámítógépen telepített Kaspersky alkalmazások listája az ügyfélszámítógép tulajdonságainak ablakában a jobb oldalon.
7. Válassza ki a Kaspersky Endpoint Security 10 for Windows alkalmazást.
8. Végezze el az alábbiak egyikét:

   - Válassza ki a **Tulajdonságok** elemet a Kaspersky Endpoint Security 10 for Windows helyi menüjéből.
   - Kattintson a Kaspersky alkalmazások listája alatti **Tulajdonságok** gombra.

   Megnyílik a **Kaspersky Endpoint Security 10 for Windows alkalmazás beállításai** ablak.
9. Adja meg a **Speciális beállítások** részben a Kaspersky Endpoint Security beállításait, valamint a jelentések és tárolók beállításait.

   A **Kaspersky Endpoint Security 10 for Windows alkalmazás beállításai** ablak többi része ugyanaz, mint a Kaspersky Security Center szokásos alkalmazás részeiben. E részek ismertetése a *Kaspersky Security Center Rendszergazdai útmutatóban* található.

   > Ha egy alkalmazásra olyan rendszabály érvényes, amely tiltja adott beállítások megváltoztatását, akkor ezek nem szerkeszthetők az alkalmazás beállításainak **Speciális beállítások** részben történő megadása során.
10. A módosítások mentéséhez kattintson a **Kaspersky Endpoint Security 10 for Windows alkalmazás beállításai** ablakban az **OK** gombra.

A feladatok kezelése

Ez a rész ismerteti a feladatok kezelésének menetét a Kaspersky Endpoint Security alkalmazásban. A Kaspersky Security Center feladatkezelésének részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

A Kaspersky Endpoint Security feladatai

A Kaspersky Security Center feladatok révén felügyeli a Kaspersky alkalmazások tevékenységét az ügyfélszámítógépeken. A feladatok valósítják meg az elsődleges adminisztrációs funkciókat, így a kulcstelepítést, a számítógép vizsgálatát, valamint adatbázisok és alkalmazásmodulok frissítését.

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.
- Adminisztrációs csoporthoz nem tartozó számítógépek készletéhez beállított feladatok.

  Az adminisztrációs csoporthoz nem tartozó számítógépek készletéhez beállított feladatok kizárólag a feladat beállításaiban megadott ügyfélszámítógépekre érvényesek. Ha új ügyfélszámítógépeket ad azon számítógépek készletéhez, amelyekhez a feladat be van állítva, a feladat az új számítógépekre nem vonatkozik. Ha a feladatot ezeknél a számítógépeknél is alkalmazni szeretné, hozzon létre új feladatot, vagy szerkessze a meglévő feladat beállításait.

A Kaspersky Endpoint Security távoli kezeléséhez a felsorolt típusok bármelyikéhez tartozó alábbi feladatokat használhatja:

- **Kulcs hozzáadása**. A Kaspersky Endpoint Security kulcsot – ideértve a további kulcsot is – ad meg alkalmazás aktiválásához.
- **Alkalmazásösszetevők módosítása**. A Kaspersky Endpoint Security a feladat beállításaiban megadott összetevőlista alapján összetevőket telepít vagy távolít el az ügyfélszámítógépeken.
- **Leltár**. A Kaspersky Endpoint Security adatokat fogad a számítógépeken tárolt összes alkalmazás végrehajtható fájljairól.

  Bekapcsolhatja a DLL modulok és szkriptfájlok leltárját. Ilyenkor a Kaspersky Security Center adatokat fogad azon a számítógépen betöltött DLL modulokról, amelyen a Kaspersky Endpoint Security telepítve van, valamint a szkripteket tartalmazó fájlokról.

  A DLL modulok és szkriptfájlok leltárjának bekapcsolásával a leltározási feladat időtartama és az adatbázis mérete jelentősen megnő.

  Ha az Alkalmazásfelügyelő összetevő nincs telepítve egy olyan számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, akkor a számítógépen futó leltározási feladat hibával tér vissza.

- **Frissítés**. A Kaspersky Endpoint Security adatbázisokat és az alkalmazásmodulokat a megadott frissítési beállításoknak megfelelően frissíti.
- **Utolsó frissítés visszagörgetése**. A Kaspersky Endpoint Security visszagörgeti az adatbázisok és modulok legutóbbi frissítését.

- **Vírusvizsgálat**. A Kaspersky Endpoint Security megvizsgálja a számítógép feladatbeállításokban megadott területein a vírusok és egyéb fenyegetések jelenlétét.
- **Integritás ellenőrzés**. A Kaspersky Endpoint Security adatokat fogad az ügyfélszámítógépen telepített alkalmazásmodulok készletéről, és megvizsgálja minden modul digitális aláírását.
- **Hitelesítési ügynök fiókok kezelése**. A feladat elvégzése során a Kaspersky Endpoint Security Hitelesítési ügynök-fiókok eltávolítására, hozzáadására és módosítására szolgáló parancsokat állít elő.

A következő műveleteket végezheti el a feladatokkal:

- Feladatok elindítása, leállítása, felfüggesztése és újraindítása.
- Új feladatok létrehozása.
- A feladatbeállítások szerkesztése.

A Kaspersky Endpoint Security feladatok beállításainak hozzáférési jogosultságai (olvasás, írás, végrehajtás) minden olyan felhasználóhoz meg van adva a Kaspersky Endpoint Security funkcionális területeihez való hozzáférés beállításain keresztül, aki hozzáfér a Kaspersky Security Center Adminisztrációs kiszolgálóhoz. A Kaspersky Endpoint Security funkcionális területeihez való hozzáférés beállításához lépjen a Kaspersky Security Center Adminisztrációs kiszolgáló tulajdonságok ablakában a **Biztonság** részhez.

A feladatkezelési mód beállítása

A Kaspersky Endpoint Security helyi felületén lévő feladatokkal való munkavégzés módjának beállítása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél be szeretné állítani a Kaspersky Endpoint Security helyi felületén lévő feladatokkal való munkavégzés módját.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.
6. A **Speciális beállítások** részben válassza ki az **Alkalmazás beállítások** alrészt.
7. Az **Működési mód** részben:
   - Ha engedélyezni szeretné, hogy a felhasználók a helyi feladatokkal a Kaspersky Endpoint Security felületén és parancssorában dolgozhassanak, jelölje be a **Helyi feladatok használatának engedélyezése** jelölőnégyzetet.

Ha a jelölőnégyzet nincs bejelölve, a helyi feladatok funkciói leállnak. Ebben a módban a helyi feladatok nem futnak az ütemezésnek megfelelően. A helyi feladatok nem indíthatók el és nem szerkeszthetők a Kaspersky Endpoint Security helyi felületén, illetve a parancssorban végzett munka során sem.

- Ha engedélyezni szeretné, hogy a felhasználók megtekinthessék a csoportos feladatok listáját, jelölje be a **Csoportfeladatok megjelenítésének engedélyezése** jelölőnégyzetet.
- Ha engedélyezni szeretné, hogy a felhasználók módosíthassák a csoportos feladatok beállításait, jelölje be a **Csoportfeladatok kezelésének engedélyezése** jelölőnégyzetet.

8. A módosítások mentéséhez kattintson az **OK** gombra.
9. Alkalmazza a rendszabályt.

   A Kaspersky Security Center-rendszabály alkalmazásának részleteit lásd a *Kaspersky Security Center Rendszergazdai útmutatóban*.

Helyi feladat létrehozása

Helyi feladat létrehozása:

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 ügyfélszámítógép tartozik.
3. Válassza ki a munkaterületen az **Eszközök** lapot.
4. Válassza ki azt a számítógépet, amelyen helyi feladatot szeretne létrehozni.
5. Végezze el az alábbiak egyikét:
   - Az ügyfélszámítógép helyi menüjében válassza ki az **Összes feladat** Feladat létrehozása elemet.
   - Az ügyfélszámítógép helyi menüjében válassza ki a **Tulajdonságok** elemet, majd a megnyíló **Tulajdonságok: <Számítógép neve>** ablakban kattintson a **Feladatok** lapon lévő **Hozzáadás** gombra.
   - A **Művelet végrehajtása** legördülő listán válassza ki a **Feladat létrehozása** lehetőséget.

   Elindul a Feladatvarázsló.
6. Kövesse a Feladatvarázsló utasításait.

Csoportos feladat létrehozása

Csoportos feladat létrehozása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Végezze el az alábbiak egyikét:

- Válassza ki az Adminisztrációs Konzol **Kezelt eszközök** mappáját csoportos feladatnak a Kaspersky Security Center által kezelt összes számítógép részére történő létrehozására.
- Válassza ki az Adminisztrációs Konzol **Kezelt eszközök** mappájában annak az adminisztrációs csoportnak a nevét viselő mappát, amelyhez az adott ügyfélszámítógépek tartoznak.

3. Válassza ki a munkaterületen a **Feladatok** lapot.
4. Kattintson a **Feladat létrehozása** gombra.

   Elindul a Feladatvarázsló.
5. Kövesse a Feladatvarázsló utasításait.

Feladat létrehozása kiválasztott eszközök számára

Feladatokat az alábbiak szerint hozhat létre kiválasztott eszközök számára:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki az Adminisztrációs Konzol fájában a **Feladatok** mappát.
3. Kattintson a **Feladat létrehozása** gombra.

   Elindul a Feladatvarázsló.
4. Kövesse a Feladatvarázsló utasításait.
5. A varázsló **Válassza ki azokat az eszközöket, amelyekhez a feladatot hozzárendeli** ablakában kattintson a **Feladat hozzárendelése kiválasztott eszközökhöz** gombra.
6. A varázsló következő ablakában kattintson a **Kijelölés** gombra.

   Megnyílik az **Eszköz kiválasztása** ablak.
7. Válassza ki a szükséges eszközöket.
8. Az **Eszköz kiválasztása** ablakban kattintson az **OK** gombra.
9. Kövesse a Feladatvarázsló utasításait.

Feladat elindítása, leállítása, felfüggesztése és folytatása

Ha a Kaspersky Endpoint Security alkalmazás fut egy adott ügyfélszámítógépen, akkor a Kaspersky Security Center révén a számítógépen futó feladatokat elindíthatja, leállíthatja, felfüggesztheti és újraindíthatja. A Kaspersky Endpoint Security felfüggesztése esetén a futó feladatok felfüggesztésre kerülnek, és a Kaspersky Security Center révén nem lehet többé feladatot elindítani, leállítani, felfüggeszteni és újraindítani.

Helyi feladat elindítása, leállítása, felfüggesztése és újraindítása:

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 ügyfélszámítógép tartozik.

3. Válassza ki a munkaterületen az **Eszközök** lapot.

4. Válassza ki azt a számítógépet, amelyen helyi feladatot szeretne elindítani, leállítani, szüneteltetni vagy újraindítani.

5. Az ügyfélszámítógép helyi menüjének megjelenítéséhez kattintson a jobb egérgombbal, és válassza a **Tulajdonságok** parancsot.

   Megnyílik az ügyfélszámítógép tulajdonságainak ablaka.

6. Válassza ki a **Feladatok** részt.

   A helyi feladatok listája az ablak jobb oldalán jelenik meg.

7. Válassza ki azt a helyi feladatot amelyet elindítani, leállítani, szüneteltetni vagy újraindítani szeretne.

8. A következő módszerek egyikével végezheti el a feladaton a szükséges műveletet:

   - A helyi feladat helyi menüjének megnyitásához kattintson a jobb egérgombbal, és válassza a **Futás** / **Leállítás** / **Szüneteltetés** / **Újraindítás** elemet.
   - Helyi feladat elindításához vagy leállításához kattintson a helyi feladatok listájának jobb oldalán lévő / gombra.
   - Végezze el az alábbiakat:

     a. Kattintson a helyi feladatok listája alatti **Tulajdonságok** gombra, vagy válassza ki a feladat helyi menüjében a **Tulajdonságok** elemet.

     Megnyílik a **Tulajdonságok: <Feladat neve>** ablak.

     b. Kattintson az **Általános** lapon a **Futás** / **Leállítás** / **Szünet** / **Újraindítás** gombra.

Csoportos feladat elindítása, leállítása, szüneteltetése és újraindítása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.

2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél csoportos feladatot szeretne elindítani, leállítani, szüneteltetni vagy újraindítani.

3. Válassza ki a munkaterületen a **Feladatok** lapot.

   A csoportos feladatok az ablak jobb oldalán jelennek meg.

4. Válassza ki azt a csoportos feladatot amelyet elindítani, leállítani, szüneteltetni vagy újraindítani szeretne.

5. A következő módszerek egyikével végezheti el a feladaton a szükséges műveletet:

   - A csoportos feladat helyi menüjében válassza a **Futás** / **Leállítás** / **Szüneteltetés** / **Újraindítás** elemet.
   - Csoportos feladat elindításához, illetve leállításához kattintson a / gombra az ablak jobb oldali részében.
   - Végezze el az alábbiakat:

a. Kattintson az Adminisztrációs Konzol munkaterületének jobb oldali részén a **Feladatbeállítások** hivatkozásra, vagy válassza ki a feladat helyi menüjében a **Tulajdonságok** elemet.

Megnyílik a **Tulajdonságok: <Feladat neve>** ablak.

b. Kattintson az **Általános** lapon a **Futás** / **Leállítás** / **Szünet** / **Újraindítás** gombra.

Feladat elindítása, leállítása, szüneteltetése és újraindítása kiválasztott számítógépeken:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol fájának **Feladatok** mappájában válassza ki azt a feladatot a kiválasztott számítógépeknél, amelyet szeretne elindítani, leállítani, szüneteltetni vagy újraindítani.
3. Végezze el az alábbiak egyikét:
   - A feladat helyi menüjében válassza a **Futás** / **Leállítás** / **Szünet** / **Újraindítás** elemet.
   - A feladat adott számítógépeken történő elindításához, illetve leállításához kattintson a / gombra az ablak jobb oldali részében.
   - Végezze el az alábbiakat:
     a. Kattintson az Adminisztrációs Konzol munkaterületének jobb oldali részén a **Feladatbeállítások** hivatkozásra, vagy válassza ki a feladat helyi menüjében a **Tulajdonságok** elemet.

     Megnyílik a **Tulajdonságok: <Feladat neve>** ablak.

     b. Kattintson az **Általános** lapon a **Futás** / **Leállítás** / **Szünet** / **Újraindítás** gombra.

A feladatbeállítások szerkesztése

A helyi feladatok beállításainak szerkesztése:

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 ügyfélszámítógép tartozik.
3. Válassza ki a munkaterületen az **Eszközök** lapot.
4. Válassza ki azt a számítógépet, amelyen meg szeretné adni az alkalmazás beállításait.
5. Az ügyfélszámítógép helyi menüjének megjelenítéséhez kattintson a jobb egérgombbal, és válassza a **Tulajdonságok** parancsot.

   Megnyílik az ügyfélszámítógép tulajdonságainak ablaka.
6. Válassza ki a **Feladatok** részt.

   A helyi feladatok listája az ablak jobb oldalán jelenik meg.
7. Válassza ki a helyi feladatok listáján a szükséges helyi feladatot.
8. Kattintson a **Tulajdonságok** gombra.

   Megnyílik a **Tulajdonságok: <Helyi feladatok neve>** ablak.

9. Válassza ki a **Tulajdonságok:<Helyi feladat neve>** ablakban a **Beállítások** részt.
10. Szerkessze a helyi feladat beállításait.
11. A módosítások mentéséhez kattintson a **Tulajdonságok: <Helyi feladat neve>** ablakban az **OK** gombra.
12. A módosítások mentéséhez kattintson a **Tulajdonságok: <Számítógép neve>** ablakban az **OK** gombra.

A csoportos feladatok beállításainak szerkesztése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Nyissa meg a **Kezelt eszközök** mappában annak a megfelelő adminisztrációs csoportnak a nevét viselő mappát.
3. Válassza ki a munkaterületen a **Feladatok** lapot.

   A csoportos feladatok az Adminisztrációs Konzol munkaterületén jelennek meg.
4. Válassza ki a szükséges csoportos feladatot.
5. A csoportfeladat helyi menüjének megjelenítéséhez kattintson a jobb egérgombbal, és válassza a **Tulajdonságok** lehetőséget.

   Megnyílik a **Tulajdonságok: <Csoportfeladat neve>** ablak.
6. Válassza ki a **Tulajdonságok:<Csoportfeladat neve>** ablakban a **Beállítások** részt.
7. Szerkessze a csoportos feladat beállításait.
8. A módosítások mentéséhez kattintson a **Tulajdonságok: <Csoportfeladat neve>** ablakban az **OK** gombra.

A kiválasztott számítógépekre vonatkozó feladatok beállításainak szerkesztése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolt.
2. Az Adminisztrációs Konzol fájának **Feladatok** mappájában válassza ki a kiválasztott számítógépekre vonatkozó azon feladatot, amelynek beállításait szerkeszteni szeretné.
3. A kiválasztott számítógépekre vonatkozó feladatok helyi menüjének megjelenítéséhez kattintson a jobb egérgombbal, és válassza a **Tulajdonságok** parancsot.

   Megnyílik a **Tulajdonságok**: **<A kiválasztott számítógépekre vonatkozó feladat neve>** ablak.
4. Válassza ki a **Tulajdonságok: <Kiválasztott számítógépekre vonatkozó feladat neve>** ablakban a **Beállítások** részt.
5. Szerkessze a kiválasztott számítógépekre vonatkozó feladatot.
6. A módosítások mentéséhez kattintson a **Tulajdonságok: <Kiválasztott számítógépekre vonatkozó feladat neve>** ablakban az **OK** gombra.

A feladatok tulajdonságainak ablakában a **Beállítások** rész kivételével az összes rész azonos a Kaspersky Security Centerben használtakkal. Részletes ismertetésük a Kaspersky Security Center Súgóban található. A **Beállítások** részben a Kaspersky Endpoint Security for Windows egyedi beállításai találhatók. Tartalma a kiválasztott feladattól vagy feladattípustól függ.

A rendszabályok kezelése

Ez a rész ismerteti a rendszabályok létrehozásának és beállításának menetét a Kaspersky Endpoint Security alkalmazásban. A Kaspersky Security Center Kaspersky Security Center rendszabályokon keresztül történő kezelésére vonatkozó további információ a *Kaspersky Security Center Rendszergazdai útmutatóban* található.

A rendszabályok

Rendszabályok segítségével ugyanazokat a Kaspersky Endpoint Security beállításokat alkalmazhatja egy adminisztrációs csoport összes ügyfélszámítógépére.

A Kaspersky Endpoint Security segítségével helyileg módosíthatja az adminisztrációs csoportba tartozó egyedi ügyfélszámítógépek rendszabályai által megadott beállítások értékeit. Csak azokat a beállításokat módosíthatja helyileg, amelyek módosítását a rendszabály nem tiltja.

Azt, hogy az ügyfélszámítógépen lehet-e az alkalmazásbeállításokat módosítani, a „lakat" állapota szabja meg a rendszabály tulajdonságaiban ezekben a beállításokban:

- A zárt „lakat" () az alábbit jelenti:
    - A Kaspersky Security Center blokkolja a lakat által jelzett beállítások módosításait a Kaspersky Endpoint Security felületéről az ügyfélszámítógépeken. A Kaspersky Endpoint Security az összes ügyfélszámítógépen ugyanazokat a beállítási értékeket használja: azokat, amelyek az irányelv tulajdonságaiban meg vannak adva.
    - A Kaspersky Security Center blokkolja a lakat által jelzett beállítások módosításait azoknál a beágyazott adminisztrációs csoportoknál és beosztott Adminisztrációs kiszolgálóknál, amelyeknél engedélyezve van a **Szülőirányelv-beállítások öröklése** funkció. A felső szintű irányelv tulajdonságaiban megadott beállítások értékei kerülnek felhasználásra.
- A nyitott „lakat" () az alábbit jelenti:
    - A Kaspersky Security Center engedélyezi a lakat által jelzett beállítások módosításait a Kaspersky Endpoint Security felületéről az ügyfélszámítógépeken. A Kaspersky Endpoint Security az egyes ügyfélszámítógépeken a helyi beállítási értékeknek megfelelően működik, ha az összetevő be van kapcsolva.
    - A Kaspersky Security Center engedélyezi a lakat által jelzett beállítások módosításait azoknál a beágyazott adminisztrációs csoportoknál és beosztott Adminisztrációs kiszolgálóknál, amelyeknél engedélyezve van a **Szülőirányelv-beállítások öröklése** funkció. A beállítások értékei nem függnek attól, hogy mi van megadva a felső szintű irányelv tulajdonságaiban.

A rendszabály első alkalommal történő alkalmazását követően a helyi alkalmazásbeállítások a rendszabály beállításainak megfelelően megváltoznak.

A rendszabályok beállításainak hozzáférési jogosultságai (olvasás, írás, végrehajtás) minden olyan felhasználóhoz meg van adva, aki hozzáfér a Kaspersky Security Center Adminisztrációs kiszolgálóhoz, és külön-külön a Kaspersky Endpoint Security egyes funkcionális hatóköreinél. A rendszabályok beállításaihoz való hozzáférés beállításához lépjen a Kaspersky Security Center Adminisztrációs kiszolgáló tulajdonságok ablakában a **Biztonság** részhez.

A Kaspersky Endpoint Security alábbi funkcionális hatóköreit lehet kiválasztani:

- Alapvető fenyegetések elleni védelem. A funkcionális hatókörhöz a Fájl védelem, Levelezés védelem, Web védelem, Hálózati védelem, Tűzfal és Vizsgálati feladatok összetevők tartoznak.
- Alkalmazásfelügyelő. A funkcionális hatókörhöz az Alkalmazásfelügyelő összetevő tartozik.
- Eszközfelügyelő. A funkcionális hatókörhöz az Eszközfelügyelő összetevő tartozik.

- Titkosítás. A funkcionális hatókörhöz a Teljes lemeztitkosítás és a Fájl szintű titkosítás összetevők tartoznak.
- Megbízható zóna. A funkcionális hatókörhöz a Megbízható zóna tartozik.
- Webfelügyelő. A funkcionális hatókörhöz a Webfelügyelő összetevő tartozik.
- Fejlett fenyegetések elleni védelem. A funkcionális hatókörhöz a KSN beállítások, valamint a Viselkedéselemzés, Biztonsági rések kihasználásának megelőzése, Behatolásmegelőző rendszer és Kármentesítő motor összetevők tartoznak.
- Alapvető funkciók. Ehhez a funkcionális hatókörhöz a más funkcionális hatókörök által meg nem adott általános alkalmazásbeállítások tartoznak, köztük a következők: licencelés, leltározási feladatok, alkalmazás adatbázisának és moduljainak frissítési feladatai, önvédelem, speciális alkalmazásbeállítások, jelentések és tárhelyek, jelszóvédelem és az alkalmazás felületének beállításai.

A következő műveleteket végezheti el a rendszabályokkal:

- Rendszabály létrehozása.
- A rendszabályok beállításainak szerkesztése.

  Ha az a felhasználói fiók, amellyel az Adminisztrációs kiszolgálóhoz hozzáfér, nem jogosult bizonyos funkcionális hatókörök beállításainak szerkesztésére, akkor az érintett beállítások nem szerkeszthetők.

- Rendszabály törlése.
- Rendszabály állapotának megváltoztatása.

A Kaspersky Endpoint Security alkalmazással való interakcióhoz nem kapcsolódó rendszabályok használatára vonatkozó információk a Kaspersky Security Center Súgóban találhatók.

Rendszabály létrehozása

Rendszabály létrehozása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Végezze el az alábbiak egyikét:
   - Válassza ki az Adminisztrációs Konzol **Kezelt eszközök** mappáját rendszabálynak a Kaspersky Security Center által kezelt összes számítógép részére történő létrehozására.
   - Válassza ki 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. Végezze el az alábbiak egyikét:
   - Kattintson a **Rendszabály létrehozása** gombra.
   - Kattintson a jobb egérgombbal a helyi menü megnyitásához, majd válassza a **Létrehozás** Rendszabály lehetőséget.

Elindul a Rendszabályvarázsló.

5. Kövesse a Rendszabályvarázsló utasításait.

A rendszabályok beállításainak szerkesztése

A rendszabályok beállításainak szerkesztése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol fájának **Kezelt eszközök** mappájában nyissa meg annak az adminisztrációs csoportnak a nevét viselő mappát, amelynél a rendszabály beállításait szeretne szerkeszteni.
3. A munkaterületen válassza ki a **Rendszabályok** lapot.
4. Válassza ki a szükséges rendszabályt.
5. Nyissa meg a **Tulajdonságok: <Rendszabály neve>** ablakot az alábbi módszerek egyikével:
   - A rendszabály helyi menüjében válassza ki a **Tulajdonságok** elemet.
   - Kattintson a **Rendszabály beállítása** hivatkozásra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

   A Kaspersky Endpoint Security 10 for Windows rendszabályok beállításaihoz az összetevők beállításai és az alkalmazásbeállítások tartoznak. A **Vírusvédelem** és a **Végpontfelügyelő** részek a **Tulajdonságok: <Rendszabály neve>** ablakban a védelmi és felügyeleti összetevők beállításait jelenítik meg, az **Adattitkosítás** részben a fájlok és mappák titkosítási beállításai láthatók, a **Speciális beállítások** részben pedig az alkalmazásbeállítások.

   Az adattitkosítási beállítások és a felügyeleti összetevőbeállítások rendszabály beállításaiban való engedélyezéséhez be kell jelölni a megfelelő jelölőnégyzeteket a Kaspersky Security Center **Felület beállításai** ablakában.
6. Szerkessze a rendszabályok beállításait.
7. A módosítások mentéséhez kattintson a **Tulajdonságok: <Rendszabály neve>** ablakban az **OK** gombra.

A Kaspersky Security Center rendszabályban megjeleníteni kívánt beállítások kiválasztása

A Kaspersky Security Center rendszabályban megjeleníteni kívánt beállítások kiválasztása:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Válassza ki az Adminisztrációs Konzol fájában lévő **Adminisztrációs kiszolgáló – <Számítógép neve>** csomópont helyi menüjében a Megtekintés → **Felület beállításai** elemet.

   Megnyílik a **Felület beállításai** ablak.
3. Jelölje be a **Felület beállításai** ablakban a jelölőnégyzeteket azokkal a beállításokkal szemben, amelyeket a Kaspersky Security Center rendszabálylétrehozási beállításaiban és a rendszabály tulajdonságaiban meg

szeretne jeleníteni:

- Jelölje be a **Végpontfelügyelő összetevők megjelenítése** jelölőnégyzetet, ha meg szeretné jeleníteni a felügyeleti összetevőbeállításokat a Kaspersky Security Center Új rendszabály varázslójának ablakában és a rendszabály tulajdonságaiban.

- Jelölje be a **Titkosítás és adatvédelem megjelenítése** jelölőnégyzetet, ha meg szeretné jeleníteni az adattitkosítási beállításokat a Kaspersky Security Center Új rendszabály varázslójának ablakában és a rendszabály tulajdonságaiban.

4. Kattintson az **OK** gombra.

Felhasználói üzenetek küldése a Kaspersky Security Center kiszolgáló részére

Az alábbi esetekben válhat szükségessé, hogy a felhasználók üzenetet küldjenek a helyi hálózati rendszergazda részére:

- Az Eszközfelügyelő blokkolta a hozzáférést az eszközhöz.

  A blokkolt eszközhöz való hozzáférést kérő üzenet sablonja a Kaspersky Endpoint Security felületén az Eszközfelügyelő részben található.

- Az Alkalmazásindítás-felügyelő blokkolta egy alkalmazás indítását.

  A blokkolt alkalmazás indításának engedélyezését kérő üzenet sablonja a Kaspersky Endpoint Security felületén az Alkalmazásindítás-felügyelő részben található.

- A Webes víruskereső 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 rendszabály azon a számítógépen, amelyen a Kaspersky Endpoint Security telepítve van, és hogy van-e kapcsolat a Kaspersky Security Center Adminisztrációs kiszolgálóval. Az alábbi forgatókönyvek lehetségesek:

- Ha nem fut Kaspersky Security Center rendszabály azon a számítógépen, amelyen a Kaspersky Security Center 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 rendszabály azon a számítógépen, amelyen a Kaspersky Security Center telepítve van, akkor szokásos üzenet kerül a Kaspersky Security Center Adminisztrációs kiszolgálóra.

  Ebben az esetben a felhasználói üzeneteket a Kaspersky Security Center eseménytárhelyen lehet megtekinteni. Az üzenet mezőibe a Kaspersky Security Center rendszabályban megadott sablonból származó mezőértékek kerülnek.

- Ha Kaspersky Security Center házon kívüli rendszabály 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 Adminisztrációs 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 rendszabályban megadott sablonból származó mezőértékek kerülnek.

A Kaspersky Security Center eseménytárban lévő felhasználói üzenetek megtekintése

Az Alkalmazásindítás-felügyelő, az Eszközfelügyelő és a Webfelügyelő összetevők lehetővé teszik, hogy azon számítógépek felhasználói, amelyeken telepítve van a Kaspersky Endpoint Security, üzeneteket küldjenek a rendszergazdának.

A felhasználók kétféleképpen küldhetnek üzeneteket a rendszergazdának:

- A Kaspersky Security Center eseménytárban lévő esemény formájában.

  A felhasználó eseménye akkor kerül a Kaspersky Security Center eseménytárba, ha a felhasználó számítógépén telepített Kaspersky Endpoint Security alkalmazás aktív rendszabály alapján működik.

- E-mail üzenet formájában.

  A felhasználói információk küldése e-mailben történik, ha a felhasználó számítógépén telepített Kaspersky Endpoint Security alkalmazás nem futtat rendszabályt, illetve irodán kívüli rendszabályt futtat.

A Kaspersky Security Center eseménytárában lévő felhasználói üzenet megtekintése:

1. Nyissa meg a Kaspersky Security Center Adminisztrációs Konzolját.
2. Az Adminisztrációs Konzol **Adminisztrációs kiszolgáló** 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 **Események kiválasztása** legördülő listán a **Felhasználói kérések** lehetőséget.
4. Válassza ki a rendszergazdának elküldeni kívánt üzenetet.
5. Az **Esemény beállításai** ablakot az alábbi módszerek egyikével nyissa meg:

   - Kattintson a jobb egérgombbal az eseményre. Válassza ki a **Tulajdonságok** elemet a megnyíló helyi menüben.
   - Kattintson az **Esemény tulajdonságainak megnyitása** gombra az Adminisztrációs Konzol munkaterületének jobb oldali részén.

Részvétel a Kaspersky Security Networkben

Ez a szakasz tájékoztatást nyújt a Kaspersky Security Network való részvétellel kapcsolatban, és ismerteti használatának be-, illetve kikapcsolását.

Részvétel a 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 hamis riasztások valószínűsége pedig csökken.

Az infrastruktúra helyétől függően létezik Globális KSN szolgáltatás (ahol az infrastruktúrát a Kaspersky kiszolgálói tartalmazzák) és Privát KSN szolgáltatás.

A licenc megváltoztatását követően nyújtsa be az új kulcs adatait a szolgáltatónak, hogy használhassa a Privát KSN-t. Ennek hiányában a Privát KSN-nel való adatcsere nem lehetséges.

A KSN-ben részt vevő felhasználóknak köszönhetően a Kaspersky azonnal képes naprakész információkat kapni a fenyegetések típusairól és forrásairól, megoldásokat fejleszteni semlegesítésükre, és minimálisra csökkenteni az alkalmazás-összetevők által megjelenített téves riasztások számát.

Kiterjesztett KSN módban az alkalmazás automatikusan elküldi az eredő működési statisztikákat a KSN-nek. Az alkalmazás további vizsgálat céljából elküldhet a Kaspersky részére bizonyos fájlokat (vagy azok részeit) is, melyeket kihasználva a bűnözők kárt tehetnek a számítógépben vagy az adatokban.

A KSN használata közben létrehozott statisztikai információk, ezen információk Kaspersky felé történő küldésének, valamint az ilyen információk tárolásának és megsemmisítésének részleteiért, kérjük, lásd a Kaspersky Security Netword nyilatkozatát és a Kaspersky weboldalt. 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 az alkalmazás olyan antivírus adatbázisait adja ki, amelyek átmenetileg kikapcsolják vagy részlegesen korlátozzák a Kaspersky Security Network részére küldött kéréseket. Ebben az esetben a KSN-kapcsolat állapota *Engedélyezve korlátozásokkal* lesz.

A Kaspersky Security Center Adminisztrációs 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 a feldolgozott adatokat gyorsítótárba helyezi, ezzel csökkentve a külső hálózati kapcsolat terhelését és felgyorsítva a felhasználó számítógépe által kért információk fogadását.

A KSN Proxy szolgáltatás további részleteiért, kérjük *lásd a Kaspersky Security Center Súgó útmutatót*.

A KSN Proxyszolgáltatás beállításait a *Kaspersky Security Center* rendszabály tulajdonságaiban lehet megadni.

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 Kaspersky Security Network való részvétel be- és kikapcsolása

A Kaspersky Security Network használatának engedélyezése és letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Speciális beállítások** részben válassza ki a **KSN beállítások** alrészt.

   A Kaspersky Security Network beállításai az ablak jobb oldalán jelennek meg.
3. Végezze el az alábbiak egyikét:

   - Ha szeretné engedélyezni a Kaspersky Security Network használatát, jelölje be az **Elfogadom a KSN nyilatkozatot és a részvételi feltételeket** jelölőnégyzetet.
   - Ha le szeretné tiltani a Kaspersky Security Network használatát, törölje az **Elfogadom a KSN nyilatkozatot és a részvételi feltételeket** jelölőnégyzetet.
4. A módosítások mentéséhez kattintson a **Mentés** gombra.

A Kaspersky Security Network szolgáltatással fennálló kapcsolat ellenőrzése

A Kaspersky Security Network fennálló kapcsolat ellenőrzése:

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak felső részén kattintson a **Kaspersky Security Network** gombra.

   Megnyílik a **Kaspersky Security Network** ablak.

   A **Kaspersky Security Network** ablak bal oldalán megjelenik a Kaspersky Security Network való kapcsolat a kerek **KSN** gomb formájában:

   - Ha a Kaspersky Endpoint Security nem kapcsolódik a Kaspersky Security Network, a **KSN** gomb szürke. A **KSN** gomb alatti állapot szövege: *Letiltva*.
   - Ha a Kaspersky Endpoint Security kapcsolódik a Kaspersky Security Network, és a KSN kiszolgálói elérhetőek, a **KSN** gomb zöld. A **KSN** gomb alatt alábbi információk jelennek meg: *Engedélyezve* állapot, használatban lévő KSN típusa – **Privát KSN** vagy **Globális KSN**, valamint a KSN kiszolgálóival való legutóbbi szinkronizálás dátuma és időpontja. Az ablak jobb oldali részén a fájlok hírnevére, a webes erőforrásokra és a szoftverekre vonatkozó statisztika látható.

A Kaspersky Endpoint Security statisztikai adatokat gyűjt a KSN használatáról, amikor megnyitja a **Kaspersky Security Network** ablakot. A statisztika nem frissül valós időben.

- Ha a Kaspersky Endpoint Security kapcsolódik a Kaspersky Security Network, de a KSN kiszolgálói nem érhetőek el, a **KSN** gomb piros. A **KSN** gomb alatti állapot szövege: *Engedélyezve*.

  Ha a KSN kiszolgálókkal való legutóbbi szinkronizálás 15 percnél régebben történt vagy állapota *Ismeretlen*, akkor a KSN kiszolgálók nem érhetőek el. Ilyenkor javasoljuk, hogy lépjen kapcsolatba a Terméktámogatással vagy a szolgáltatóval.

  A Kaspersky Security Network kiszolgálóival létrehozott kapcsolat a következő okok miatt maradhat el:

  - A számítógép nem csatlakozik az internethez.
  - Az alkalmazás nincs aktiválva vagy a licenc lejárt.
  - Kulcsra vonatkozó problémák észlelhetők (például a kulcs feketelistán szerepel).

Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével

A KSN szolgáltatás lehetővé teszi a Kaspersky reputációs adatbázisaiban található alkalmazásokra vonatkozó információk lekérdezését. Ez lehetővé teszi az alkalmazásindítási rendszabályok vállalati szintű rugalmas kezelését, megelőzve a reklámprogramok és egyéb, olyan programok elindítását, amelyekkel a bűnözők kárt tesznek a számítógépben vagy a személyes adatokban.

Fájlok hírnevének ellenőrzése a Kaspersky Security Network segítségével:

1. Kattintson a jobb egérgombbal azon fájl helyi menüjének megnyitásához, amelynek reputációját ellenőrizni szeretné.
2. Válassza ki a **Hírnév ellenőrzése a KSN-ben** lehetőséget.

   Ez a lehetőség akkor használható, ha elfogadta a Kaspersky Security Network nyilatkozatának feltételeit.

   Ezzel megnyílik a **<Fájlnév> - Hírnév a KSN-ben** ablak. A **<Fájlnév> - Hírnév a KSN-ben** ablakban az alábbi információk jelennek meg az ellenőrzés alatt álló fájlról:

   - **Elérési út**. A fájl mentésének elérési útja a lemezen.
   - **Verzió**. Az alkalmazás verziója (ez az adat csak végrehajtható fájloknál jelenik meg).
   - **Digitális aláírás**. A digitális aláírás megléte a fájlban.
   - **Aláírva**. A tanúsítvány digitális aláírással való ellátásának dátuma.
   - **Létrehozva**. A fájl létrehozásának dátuma.
   - **Módosítva**. A fájl legutóbbi módosításának dátuma.

- **Méret**. A fájl által elfoglalt lemezterület.
- Információ arról, hogy hány felhasználó bízik meg a fájlban, illetve hány blokkolja.

Kibővített védelem a Kaspersky Security Network révén

A Kaspersky egy további védelmi réteget kínál a felhasználók számára a Kaspersky Security Network révén. Ez a védelmi módszer arra szolgál, hogy leküzdje a fennmaradó fenyegetéseket és a nulladik napi támadásokat. A beépített felhőtechnológiák és a Kaspersky víruselemzőinek szakértelme jóvoltából a Kaspersky Endpoint Security párját ritkító választás a legkifinomultabb hálózati fenyegetések elleni védekezés terén.

A Kaspersky Endpoint Security kibővített védelméről részletesen olvashat a Kaspersky webhelyén.

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 oldala egy, az internetes áruházra mutató hivatkozást is tartalmaz. Itt megvásárolhatja vagy megújíthatja az alkalmazást.

A Kaspersky Endpoint Security oldal a Tudásbázisban

A *Tudásbázis* a Műszaki támogatás weboldal egy 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 Műszaki támogatás híreit is tartalmazhatják.

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 közösségünkben aktuális témákról olvashat, megjegyzéseket fűzhet a beszélgetésekhez és új témákat hozhat létre.

Kapcsolatfelvétel a Terméktámogatással

Ez a rész ismerteti a terméktámogatás igénybevételének módjait, és az igénybevétel feltételeit.

Terméktámogatás igénylése

Ha nem talál megoldást a problémájára az alkalmazás dokumentációjában vagy az alkalmazással kapcsolatos információforrásokban, javasoljuk, hogy lépjen kapcsolatba a Terméktámogatással. A terméktámogatási szolgáltatás szakemberei választ adnak minden, az alkalmazás telepítésére és használatára vonatkozó kérdésre.

Mielőtt igénybe venné a terméktámogatási szolgáltatást, olvassa el a terméktámogatási szabályokat.

A terméktámogatással az alábbi módokon veheti fel a kapcsolatot:

- Terméktámogatás hívása telefonon
- Kérelem küldése a Kaspersky Terméktámogatás részére a Kaspersky CompanyAccount portálon keresztül.

Terméktámogatás telefonon

A világ legtöbb régiójából felhívhatja a Terméktámogatás képviselőit. A terméktámogatás régiójában történő igénybevételéről és a Terméktámogatással való kapcsolatfelvételről további információkat találhat a Kaspersky Terméktámogatási webhelyen.

Mielőtt igénybe venné a terméktámogatási szolgáltatást, olvassa el a terméktámogatási szabályokat.

Terméktámogatás a Kaspersky CompanyAccounton keresztül

A Kaspersky CompanyAccount a Kaspersky alkalmazásait használó vállalatoknak szánt portál. A Kaspersky CompanyAccount portálnak az a célja, hogy elektronikus kérelmek révén megkönnyítse a felhasználók és a Kaspersky szakértői közti interakciót. A Kaspersky CompanyAccount portálon követheti az elektronikus kérelmek állapotát, és tárolhatja a kérelmek előzményeit.

A szervezet összes alkalmazottját regisztrálhatja a Kaspersky CompanyAccount portálon egyetlen fiókban. Ez az egyetlen fiók lehetőséget nyújt a regisztrált alkalmazottak által a Kaspersky részére benyújtott elektronikus kérelmek központi kezelésére, valamint az alkalmazottak jogosultságainak kezelésére a Kaspersky CompanyAccount portálon keresztül.

A Kaspersky CompanyAccount portál az alábbi nyelveken áll rendelkezésre:

- angol
- spanyol
- olasz

- német
- lengyel
- portugál
- orosz
- francia
- japán

A Kaspersky CompanyAccount portálról további információt a Terméktámogatás webhelyén találhat.

Információgyűjtés a terméktámogatáshoz

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, utasításaikat betartva szabad elvégezni. Ha az alkalmazásbeállításokat a Rendszergazdai útmutatóban nem ismertetett, illetve a Terméktámogatás szakembere által nem utasított módon felügyelet nélkül módosítja, akkor az operációs rendszer lelassulhat, illetve lefagyhat, csökkenhet a számítógép védelme, és sérülhet a feldolgozott adatok rendelkezésre állása és épsége.

Alkalmazás-nyomkövetési fájl létrehozása

Az *Alkalmazás-nyomkövetés* az alkalmazás által végrehajtott műveletek és alkalmazás működése során bekövetkezett eseményekről szóló üzenetek részletes nyilvántartása.

Az alkalmazás-nyomkövetési fájl létrehozásához:

1. Kattintson a fő alkalmazásablakban a **Támogatás** gombra.

   Megnyílik a **Támogatás** ablak.

2. A **Támogatás** ablakban kattintson a **Rendszer-nyomkövetés** gombra.

   Megnyílik az **Információ a Terméktámogatás részére** ablak.

3. A nyomkövetési folyamat megkezdéséhez válassza ki valamelyik elemet a **Alkalmazás-nyomkövetések** legördülő listán:

   - **engedélyezve**

     Válassza ki ezt a nyomkövetés engedélyezéséhez.

   - **forgatással**.

     Válassza ki ezt az elemet a nyomkövetés engedélyezéséhez, továbbá a nyomkövetési fájlok maximális számának és az egyes nyomkövetési fájlok maximális méretének korlátozásához. A maximális számú és maximális méretű követési fájl kiírása esetén a legrégebbi nyomkövetési fájl törlődik, hogy az újat ki lehessen írni.

     Ha ez az elem van kiválasztva, megadhatja az alábbi mezők értékét:

     - **Fájlok maximális száma a forgatásnál**

       Ebben a mezőben lehet megadni a kiírt nyomkövetési fájlok maximális számát.

     - **Az egyes fájlok maximális mérete**

       Ebben a mezőben lehet megadni a kiírt nyomkövetési fájlok maximális méretét.

4. 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.

5. Indítsa újra a Kaspersky Endpoint Security alkalmazást.

6. A nyomkövetési folyamat leállításához lépjen vissza az **Információ a Terméktámogatás részére** ablakba, és válassza ki a **Letiltott** elemet a **Alkalmazás-nyomkövetések** legördülő listán.

Továbbá létrehozhat nyomkövetési fájlokat, ha telepíti az alkalmazást a parancssorból, például a setup.ini fájl használatával.

Nyomkövetési fájlok tartalma és tárolása

A felhasználó személyesen felelős a számítógépén tárolt adatok biztonságáért, különösen az adatokhoz való hozzáférés megfigyeléséért és korlátozásáért, amíg el nem lesz küldve a Kaspersky számára.

A nyomkövetési fájlok a számítógépen vannak tárolva az alkalmazás használata során, az alkalmazás eltávolításakor pedig véglegesen törlődnek.

A nyomkövetési fájlok tárolási mappája: ProgramData\Kaspersky Lab.

A nyomkövetési fájlok nevének formátuma a következő: `KES<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

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 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 felhasználónév és jelszó, ha azok átvitele nyíltan történt. Ezek az adatok az internetes forgalom vizsgálata során nyomkövető fájlokba kerülhetnek. A forgalom csak a trafmon2.ppl-ből kerül nyomkövető fájlokba.
- A felhasználónév és jelszó, ha azok HTTP-fejlécekben megtalálhatók.
- A Microsoft Windows fiók neve, ha az egy fájlnévben szerepel.
- Az Ön e-mail címe vagy fiókja nevét és jelszavát tartalmazó webcím, ha azok az észlelt objektum nevében találhatók.
- Az Ön által felkeresett webhelyek és átirányítások ezekről a webhelyekről. Ezek az adatok kerülnek nyomkövetési fájlokba, ha az alkalmazás webhelyeket vizsgál.

- Proxykiszolgáló címe, számítógépnév, port, IP-cím, valamint a proxykiszolgálóra való bejelentkezéshez szükséges felhasználónév. Ezek az adatok kerülnek nyomkövetési fájlokba, ha az alkalmazás proxykiszolgálót használ.
- Távoli IP-címek, melyekkel a számítógép kapcsolatokat létesített.
- Üzenet tárgya, azonosító, feladó neve és a feladó weblapjának címe közösségi hálózaton. Ezek az adatok kerülnek nyomkövetési fájlokba, ha a Webfelügyelő összetevő engedélyezve van.

A HST.log, BL.log, Dumpwriter.log, WD.log és AVPCon.dll.log nyomkövetési fájlok tartalma

A HST.log nyomkövetési fájl az általános adatokon felül információkat tartalmaz egy adatbázis- és alkalmazásmodul-frissítési feladatot végrehajtásával kapcsolatban.

A BL nyomkövetési fájl az általános adatokon felül információkat tartalmaz az alkalmazás működése közben bekövetkező eseményekkel, valamint az alkalmazáshibák hibakereséséhez szükséges adatokkal kapcsolatban. Ez a fájl akkor jön létre, ha az alkalmazást az avp.exe –bl paraméterrel indítják el.

A Dumpwriter.log nyomkövetési fájl az általános adatokon felül szervizinformációkat tartalmaz, melyek az alkalmazás memóriakiíratásának írásakor bekövetkező hibák hibaelhárításához szükségesek.

A WD.log nyomkövetési fájl az általános adatokon felül információkat tartalmaz az avpsus szolgáltatás működése közben bekövetkező eseményekkel, köztük az alkalmazásmodulok frissítési eseményeivel kapcsolatban.

Az AVPCon.dll.log nyomkövetési fájl az általános adatokon felül információkat tartalmaz a Kaspersky Security Center csatlakozási modul működése közben bekövetkező eseményekkel kapcsolatban.

Az AMSI Védelmi szolgáltató nyomkövetési fájljainak a 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 shellex.dll.log nyomkövetési fájl információkat tartalmaz a vizsgálati feladat elvégzéséről és az alkalmazás hibakereséséhez szükséges adatokról, továbbá az általános információkról.

Az alkalmazás-webbővítmények nyomkövetési fájljainak tartalma

A nyomkövetési fájlok azon a számítógépen találhatók, ahol a Kaspersky Security Center 11 Web Console üzembe van helyezve, a Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 11\logs mappában. A Web Console a telepítése után megkezdi az adatok írását, az eltávolítása után pedig törli a nyomkövetési fájlokat.

A Kaspersky Endpoint Security nyomkövetési fájljainak neve a következő: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`.

Az alkalmazás-webbővítmények nyomkövetési fájljai az általános adatokon felül az alábbi információkat tartalmazzák:

- A KLAdmin felhasználói jelszót a Kaspersky Endpoint Security felület feloldásához (Jelszavas védelem).
- Átmeneti jelszót a Kaspersky Endpoint Security felület feloldásához (Jelszavas védelem).
- Felhasználónevet és jelszót az SMTP levelező kiszolgálókhoz. (E-mail értesítések).
- Felhasználónév és jelszó az internetes proxykiszolgálóhoz (Proxykiszolgáló).
- Felhasználónév és jelszó az *Alkalmazásösszetevők módosítása* feladathoz.
- A fiókbejelentkezési adatokat és az útvonalakat, amik meg vannak adva a Kaspersky Endpoint Security feladatokban és az irányelvek tulajdonságaiban.

A Hitelesítési ügynök nyomkövetési fájl tartalma

A Hitelesítési ügynök nyomkövetési fájl az általános adatokon felül információkat tartalmaz a Hitelesítési ügynök működésével és a felhasználó által a Hitelesítési ügynökkel elvégzett műveletekkel kapcsolatban.

Kiíratási és nyomkövetési fájlok Kaspersky részére történő küldésének be- és kikapcsolása

Kiíratási és nyomkövetési fájlok Kaspersky részére történő küldésének be- és kikapcsolása:

1. Nyissa meg az alkalmazásbeállítások ablakot.
2. Az ablak bal oldalán válassza ki a **Speciális beállítások** részt.

   A speciális alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. Az **Működési mód** részben kattintson a **Beállítások** gombra.

   Megnyílik az **Működési mód** ablak.
4. Jelölje be az **Működési mód** ablakban a **Kiíratás engedélyezése** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás kiíratási fájlokat írjon.
5. Végezze el az alábbiak egyikét:

   - Jelölje be a **Kiíratási és nyomkövetési fájlok küldése a Kaspersky** jelölőnégyzetet, ha azt szeretné, hogy az alkalmazás az **A Terméktámogatásnak szóló információk feltöltése a kiszolgálóra** ablakban kérdezzen rá a kiíratási és nyomkövetési fájlok alkalmazáshibák okainak elemzése céljából a Kaspersky részére történő elküldésére az alkalmazás legközelebbi elindításakor.
   - Ha ezt nem szeretné, törölje a **Kiíratási és nyomkövetési fájlok küldése a Kaspersky** jelölőnégyzetet.
6. Kattintson az **OK** gombra az **Működési mód** ablakban.
7. A módosítások mentéséhez kattintson a **Mentés** gombra a fő alkalmazásablakban.

Fájlok feltöltése a Terméktámogatás kiszolgálójára

Az operációs rendszerről, nyomkövetési fájlokról és kiíratási fájlokról szóló információkat tartalmazó fájlokat a Kaspersky Terméktámogatási szakértőinek kell elküldeni.

Fájlok elküldése a Terméktámogatás kiszolgálójára:

1. Minden működési hibát követően indítsa újra a Kaspersky Endpoint Security alkalmazást.

   Ekkor megnyílik **Az előző alkalmazásindítás sikertelen volt** ablak.

   > **Az előző alkalmazásindítás sikertelen volt** ablak a Kaspersky Endpoint Security minden indításakor megnyílik (a számítógép újraindítását követően is), amíg a kiíratási és nyomkövetési fájlokat el nem küldi a Terméktámogatás részére, illetve amíg a **Nincs küldés** gombra nem kattint..

2. Nyissa meg **Az előző alkalmazásindítás sikertelen volt** ablakban az előállított fájlok listáját **ide** kattintva.

3. Jelölje be a Terméktámogatás részére elküldeni kívánt fájlok melletti jelölőnégyzeteket.

4. Kattintson a **Kivonatszöveg megjelenítése** gombra.

   Megnyílik az **Adatszolgáltatási nyilatkozat** ablak.

5. Olvassa el az Adatszolgáltatási nyilatkozat szövegét, majd kattintson a **Bezárás** gombra.

6. elölje be **Az előző alkalmazásindítás sikertelen volt** ablakban az **Elfogadom az Adatszolgáltatási nyilatkozatot** jelölőnégyzetet.

7. Kattintson a **Küldés** gombra.

   Ezzel megnyílik a **Kérésszám** ablak.

8. Adja meg a **Kérésszám** ablakban azt a számot, amely a kéréshez hozzárendelésre került, amikor a Terméktámogatással kapcsolatba lépett a Kaspersky CompanyAccount portálon keresztül.

9. Kattintson az **OK** gombra.

A kiválasztott adatfájlokat a rendszer összecsomagolja, és elküldi a Terméktámogatás kiszolgálójára.

Kiíratási és nyomkövetési fájlok védelmének be- és kikapcsolása

A kiíratási és nyomkövetési fájlok az operációs rendszerre vonatkozó információkat, valamint a felhasználó bizalmas adatait tartalmazzák. 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. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a bal oldalon lévő **Speciális beállítások** részt.

   Az alkalmazásbeállítások az ablak jobb oldalán jelennek meg.
3. Az **Működési mód** részben kattintson a **Beállítások** gombra.

   Megnyílik az **Működési mód** ablak.
4. Végezze el az alábbiak egyikét:

   - Jelölje be a **Kiíratási és nyomkövetési fájlok védelmének engedélyezése** jelölőnégyzetet, ha be szeretné kapcsolni a védelmet.
   - Törölje a **Kiíratási és nyomkövetési fájlok védelmének engedélyezése** jelölőnégyzetet, ha ki szeretné kapcsolni a védelmet.
5. Kattintson az **OK** gombra az **Működési mód** ablakban.
6. A módosítások mentéséhez kattintson a **Mentés** gombra a fő alkalmazásablakban.

A védelem bekapcsolt állapotában írt kiíratási és nyomkövetési fájlok védelme a funkció kikapcsolását követően is fennmarad.

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.

Adathalászat

Ez egy olyan internetes visszaélés, amely során bizalmas információk, leggyakrabban pénzügyi adatok megszerzése céljából küldenek e-mail üzenetet.

Adminisztrációs csoport

Olyan eszközök készlete, amelyek közös funkciókon osztoznak, és a Kaspersky alkalmazásainak ugyanaz a készlete van rajtuk telepítve. Az eszközök azért vannak csoportosítva, hogy kényelmesen, egyetlen egységként lehessen kezelni őket. A csoport további csoportokat is tartalmazhat. A csoporton belül minden telepített alkalmazás számára csoportrendszabályokat és csoportfeladatokat lehet előállítani.

Adminisztrációs kiszolgáló

A Kaspersky Security Center egyik összetevője, amely központilag tárolja a vállalati hálózaton telepített összes Kaspersky alkalmazás adatait. Használható az alkalmazások kezelésére is.

Aktív kulcs

Az a kulcs, amelyet az alkalmazás jelenleg használ.

Aláírás-elemzés

Egy olyan fenyegetéseket észlelő technológia, amely a Kaspersky Endpoint Security adatbázisát használja fel, mely az ismert fenyegetések leírásait és törlésük módszereit tartalmazza. Az aláírás-elemzésen alapuló védelem a legalacsonyabb elfogadható szintű biztonságot nyújtja. A Kaspersky szakértőinek ajánlásának megfelelően ez a módszer mindig be van kapcsolva.

Alkalmazás beállítások

Az összes feladattípusra jellemző alkalmazásbeállítások, amelyek az alkalmazás egészének működését szabályozzák, például a teljesítményre, a jelentésekre vagy a karanténra vonatkozó beállítások tekintetében.

Alkalmazásmodulok

Az alkalmazás telepítőfájljában található fájlok, amelyek az alkalmazás alapfunkcióit valósítják meg. Az alkalmazás által végrehajtott összes feladattípusnak (valós idejű védelem, kézzel indított keresés, frissítés) egy-egy különálló végrehajtható modul felel meg. A számítógép teljes vizsgálatának a fő alkalmazásablakból való elindításakor a felhasználó az adott feladatmodult kezdeményezi.

Antivírus adatbázisok

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.

Archívum

Egy vagy több, egyetlen tömörített fájlba csomagolt fájl. Az adatok be- és kicsomagolásához egy speciális, archiváló nevű alkalmazás szükséges.

Biztonsági mentés

A fájlok vírusmentesítését vagy törlését megelőzően létrehozott biztonsági másolatok tárolására szolgáló speciális tárolóhely.

Biztonsági rés kiaknázása

A rendszerben vagy szoftverekben megtalálható valamilyen fajtájú sebezhetőséget kihasználó programkód. A biztonsági rések kiaknázásait gyakran használják rosszindulatú programok telepítésére a felhasználó tudta nélkül.

Címek feketelistája

Azon e-mail-címek listája, amelyekről a kapott üzeneteket a Kaspersky alkalmazásnak tartalomtól függetlenül blokkolnia kell.

Fájlmaszk

Helyettesítő karakterekkel megadott fájlnév és kiterjesztés.

A fájlmaszkok bármilyen, a fájlnevekben megengedett karaktert tartalmazhatnak, köztük helyettesítő karaktereket:

- ***** – Nulla vagy több karaktert lecserél.

- **?** – Egy darab bármilyen karaktert helyettesít.

Fontos megjegyezni, hogy a fájlnév és a kiterjesztés között mindig egy pont áll.

Fájlok áthelyezése a Karanténba

A valószínűleg fertőzött fájlok egyik feldolgozási módszere a fájlhoz való hozzáférés blokkolásával és az eredeti helyről a Karantén mappába való áthelyezésével, ahol a fájl titkosított formában – és ezáltal a fertőzés veszélyét kizáró módon – tárolódik.

Feladat

A Kaspersky alkalmazás által feladatként végrehajtott funkciók, például: Valós idejű fájlvédelem, Teljes vizsgálat, Adatbázisfrissítés.

Feladatbeállítások

Az egyes feladattípusokra jellemző alkalmazásbeállítások.

Fertőzhető fájl

Olyan fájl, amelyet szerkezetéből vagy formátumából adódóan a behatolók a rosszindulatú kódok tárolására és terjesztésére szolgáló „tárolóként" használhatnak fel. Ezek rendszerint végrehajtható fájlok, és kiterjesztésük például .com, .exe és .dll lehet. A rosszindulatú kódok aktiválódásának kockázata az ilyen fájloknál meglehetősen magas.

Fertőzött fájl

Rosszindulatú programokat tartalmazó fájl (a fájl vizsgálata során ismert rosszindulatú programok kódja észlelhető). A Kaspersky nem javasolja az ilyen fájlok használatát, mert azok megfertőzhetik a számítógépet.

Frissítés

A Kaspersky frissítéskiszolgálóiról származó új fájlok (adatbázisok vagy alkalmazásmodulok) hozzáadása vagy korábbi fájlok helyetti beillesztése.

Hálózati szolgáltatás

Olyan paraméterkészlet, amely hálózati tevékenységet határoz meg. A hálózati tevékenységhez a Tűzfal működését szabályozó hálózati szabályt lehet létrehozni.

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.

Hálózati Ügynök Csatoló

Az alkalmazást a Hálózati Ügynökkel összekapcsoló funkcionalitás. A Hálózati Ügynök lehetővé teszi az alkalmazás távoli kezelését a Kaspersky Security Centeren keresztül.

Heurisztikus elemzés

Ez a technológia a Kaspersky alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelése érdekében került kifejlesztésre. Észleli az olyan fájlokat, amelyek ismeretlen vírussal, vagy egy ismert vírus új változatával lehetnek megfertőzve.

Hibajavítás

Az alkalmazás kisebb kiegészítése, amely az alkalmazás működése során felfedezett hibákat javítja ki, vagy frissítéseket telepít.

Hitelesítési ügynök

A hitelesítési folyamat elvégzésére szolgáló felület, mellyel hozzá lehet férni a titkosított merevlemezekhez, és be lehet tölteni az operációs rendszert a rendszermerevlemez 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.

Karantén

A Kaspersky Endpoint Security a valószínűleg fertőzött fájlokat ebbe a mappába helyezi. A karanténba helyezett fájlok titkosított formában vannak tárolva.

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.

Kiegészítő kulcs

Az a kulcs, amely tanúsítja az alkalmazás használatára vonatkozó jogot, de jelenleg nincs használatban.

Licenctanúsítvány

Olyan dokumentum, amelyet a Kaspersky a felhasználónak a kulcsfájllal, illetve aktiváló kóddal együtt ad át. A felhasználó részére adott licencről tartalmaz információkat.

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.

Tanúsítvány

Olyan elektronikus dokumentum, amely a privát kulcsot és a kulcs tulajdonosával és hatókörével kapcsolatos információkat tartalmazza, továbbá megerősíti, hogy a nyilvános kulcs a tulajdonoshoz tartozik. A tanúsítványt az azt kiállító tanúsítványközpontnak alá kell írnia.

Tanúsítvány alanya

A tanúsítványhoz kapcsolódó privát kulcs tulajdonosa. Ez lehet felhasználó, alkalmazás, valamely virtuális objektum, számítógép vagy szolgáltatás.

Tanúsítvány kibocsátója

A tanúsítványt kiállító tanúsítványközpont.

Tanúsítvány ujjnyoma

A tanúsítványkulcs azonosítására szolgáló információ. Az ujjnyom úgy készül, hogy a rendszer kriptográfiai hash funkciót alkalmaz a kulcs értékére.

Téves riasztás

Akkor következik be téves riasztás, ha a Kaspersky alkalmazása egy nem fertőzött objektumot fertőzöttnek tekint, mivel az aláírása hasonló egy víruséhoz.

Trusted Platform Module (TPM)

Egy biztonsághoz kapcsolódó alapvető funkciók nyújtására (például titkosítási kulcsok tárolására) szolgáló mikrocsip. A Trusted Platform Module általában a számítógép alaplapján helyezkedik el, és a rendszer többi összetevőjével a hardverbuszon keresztül lép kapcsolatba.

Valószínűleg fertőzött fájl

Egy ismert vírus módosított kódját vagy egy vírus kódjára hasonlító, de a Kaspersky által még nem ismert kódot tartalmazó fájl. A valószínűleg fertőzött fájlok észlelése a Heurisztikus elemző segítségével történik.

Védelem hatóköre

Futás közben a vírusvédelem által folyamatosan vizsgált objektumok. A különböző összetevők védelmi hatóköreinek más-más tulajdonságai vannak.

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 forrás címének szöveges ábrázolása adott szabályok alapján (például a HTTP bejelentkezési név, jelszó és csatlakozási port webes forrás címének szöveges ábrázolásából való kizárásával, továbbá a webes forrás címének nagybetűsről kisbetűssé alakításával) megváltozik.

A vírusvédelem vonatkozásában a webes források 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.

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 nevek felett azok tulajdonosai rendelkeznek.

Az Adobe, az Acrobat és a Shockwave az Adobe Systems Incorporated védjegyei vagy bejegyzett védjegyei az Amerikai Egyesült Államokban és / vagy más országokban.

A Mac és a FireWire az Apple Inc. Egyesült Államokban és más országokban bejegyzett védjegyei.

Az AutoCAD az Autodesk, Inc. és / vagy leányvállalatai és / vagy társvállalatai védjegye vagy bejegyzett védjegye az Egyesült Államokban és máshol.

A Bluetooth kifejezés és emblémája a Bluetooth SIG, Inc. tulajdona.

A Borland a Borland Software Corporation védjegye vagy bejegyzett védjegye az Egyesült Államokban és máshol.

A Citrix és a Citrix Provisioning Services a Citrix Systems, Inc. és / vagy leányvállalatai védjegyei, mely az Egyesült Államok és egyéb országok szabadalmi hivatalában be vannak jegyezve.

A dBase a dataBased Intelligence, Inc. védjegye.

Az EMC és a SecurID az EMC Corporation védjegyei, illetve az EMC Corporation Egyesült Államokban és máshol bejegyzett védjegyei.

Az ICQ az ICQ LLC védjegye és / vagy szolgáltatási védjegye.

Az Intel és a Pentium az Intel Corporation bejegyzett védjegye az Egyesült Államokban és más országokban.

A Logitech a Logitech Company bejegyzett védjegye vagy védjegye az Egyesült Államokban és máshol.

A Mail.ru a Mail.Ru. LLC bejegyzett védjegye.

A Microsoft, a Windows, az Internet Explorer, az Access, az Excel, a PowerPoint, az Outlook, az Outlook Express, a Windows Server, a Visual Basic, a Visual FoxPro, a BitLocker, a LifeCam Cinema, a PowerShell és a Surface a Microsoft Corporation Egyesült Államokban és más országokban bejegyzett védjegyei.

A Mozilla és a Thunderbird a Mozilla Foundation védjegyei.

A Novell a Novell Inc. Egyesült Államokban és egyéb országokban bejegyzett védjegye.

A Java és a JavaScript az Oracle Corporation és / vagy leányvállalatai bejegyzett védjegyei.

A SafeNet a SafeNet, Inc. bejegyzett védjegye.

A UNIX bejegyzett védjegy az Egyesült Államokban és máshol, és használata az X/Open Company Limited licence alapján történik.